Black Book

Edition 10

Advanced MPLS

http://www.ixiacom.com/blackbook

June 2014

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 tenth edition of the black books includes twenty two 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

Volume 19 – 802.11ac Wi-Fi Benchmarking

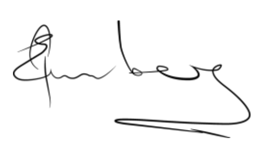
Volume 20 – SDN/OpenFlow

Volume 21 – Network Convergence Testing

Volume 22 – Testing Contact Centers

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.



Errol Ginsberg, Acting CEO

Advanced MPLS

Test Methodologies

This advanced MPLS testing booklet provides several examples with detailed steps showing how to utilize Ixia IxNetwork emulation software and applications to achieve functional and performance test objectives for key MPLS protocols.

Introduction to MPLS and MPLS-based Applications

The multiprotocol label switching (MPLS) technology was initially designed for core networks with the intention of switching instead of routing packets across the core. With the help of signaling protocols such as LDP or RSVP-TE, packets entering the network at the provider edge (PE) are classified in order to assign proper labels. Once labels are assigned, packets that have similar properties, such as a particular prefix length or TOS value, are directed towards the same Label Switch Path (LSP). It had never been possible with traditional routing protocols - in fact, every packet was examined and routed hop-by-hop in a completely connectionless datagram-delivery fashion.

Essentially, MPLS allows packets of certain characteristics to follow a pre-determined path, with negotiated QoS guarantees. This strategy makes it possible to provide QoS or SLA guarantees on a traditionally best-efforts based IP network in a way that was previously only achievable through connection-oriented technologies such as Frame Relay and ATM. With MPLS, it's possible to deploy Ethernet everywhere, including in access, metro and core networks. In fact, MPLS has become the de-facto technology for a converged network that is capable of delivering triple-play services.

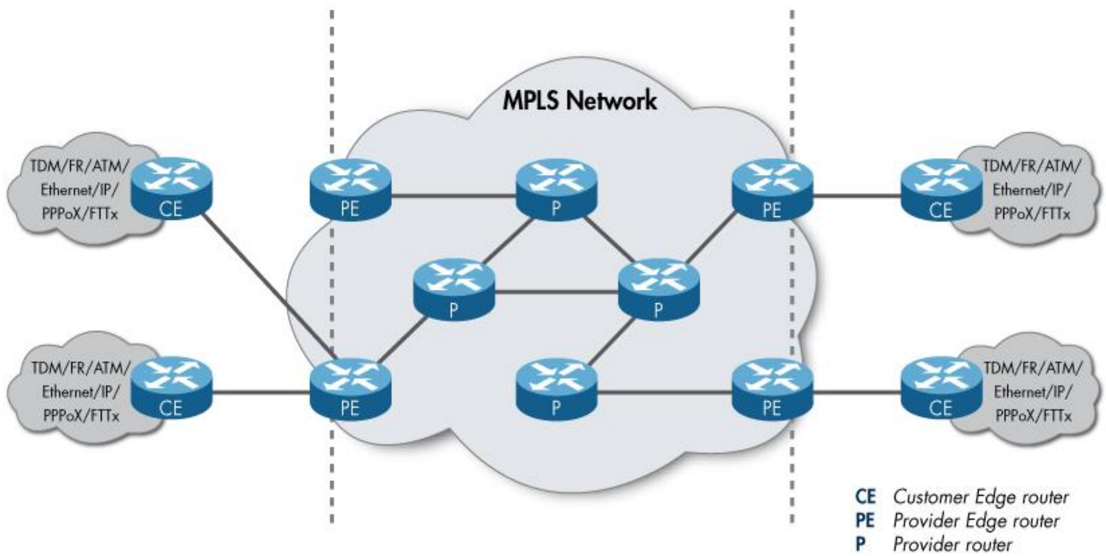


Figure 1. MPLS plays key roles in a converged triple-play network

The primary applications for MPLS include VPN and traffic engineering. There are various VPN flavors. They are generally referred to as L2VPN and L3VPN. L2VPNs were created to provide point-to-point (P2P) connection across an MPLS core in much the same way as an IP connection was established across an ATM core network, as defined in RFC1483. This P2P connection simulates a pseudo-wire that connect two isolated VPN sites (hence the term, pseudo-wire emulation). Connections are built from a layer 2 standpoints, and thus may support multiple dissimilar technologies, including PPP, HDLC, FR and ATM, in addition to the standard Ethernet and VLAN.

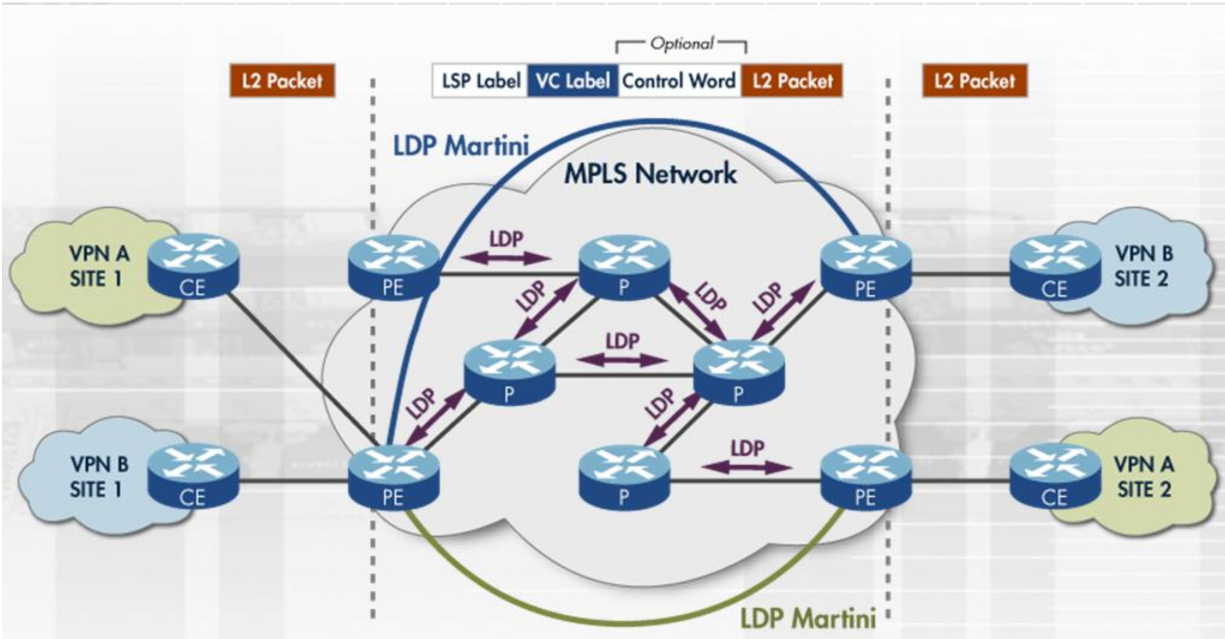


Figure 2. Emulated L2 pseudo-wire connection over an MPLS Network

One of the variants of L2VPN is known as virtual private LAN service (VPLS). This type of VPN binds multiple L2VPN pseudo-wires (Ethernet and VLAN only) to form a virtual Ethernet switch. Ethernet connectivity had traditionally been limited to the LAN area, but VPN application technology has made it possible to expand the concept and bridge the Ethernet across the metro and core network. To improve the scalability of the VPLS, a hierarchical VPLS (HVPLS) was proposed and has gained tremendous success over the past few years.

L3VPN is based on RFC 2547bis. L3VPN works quite differently from L2VPN and is one of the first MPLS applications that has enjoyed successful deployment in large scale service provider networks. Since these VPNS are layer 3-based, packets are routed through the MPLS core with the help of MPLS LSPs. Customer VPN sites form routing peers with the service provider PE routers and expose routing information to the service provider. Before packets are delivered over the MPLS tunnel (or LSP), L3VPN information is pre-pended along with an additional label that uniquely identifies the VPN sites. The provider PE router generates and stores a separate routing table for each VPN (known as a virtual routing forwarding instance -VRF). Typical L3VPN applications include a wholesale service provider who supplies connections for two or more retail service providers, or a large enterprise customer needing connectivity among sites in geographically separated locations.

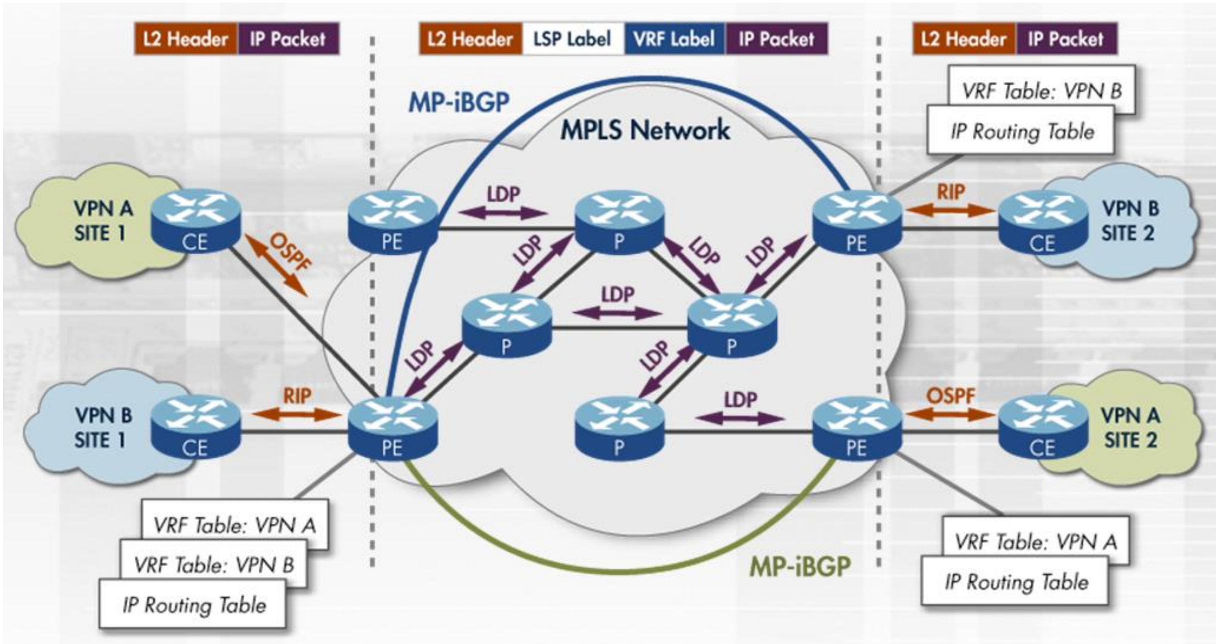


Figure 3. Emulated L3 virtual routing and forwarding (VRF) instances across an MPLS network

Another key MPLS application is the multicast VPN (mVPN). This overlay model delivers multicast traffic over exactly the same MPLS infrastructure built for unicast traffic (i.e., L3VPN). To keep the infrastructure intact, multicast traffic is delivered over GRE tunnels between PE routers. To maintain a multicast distribution tree (MDT), PIM-SM/SSM is deployed in the core to maintain both the default MDT for all interested receivers and the data MDT for only selected receivers.

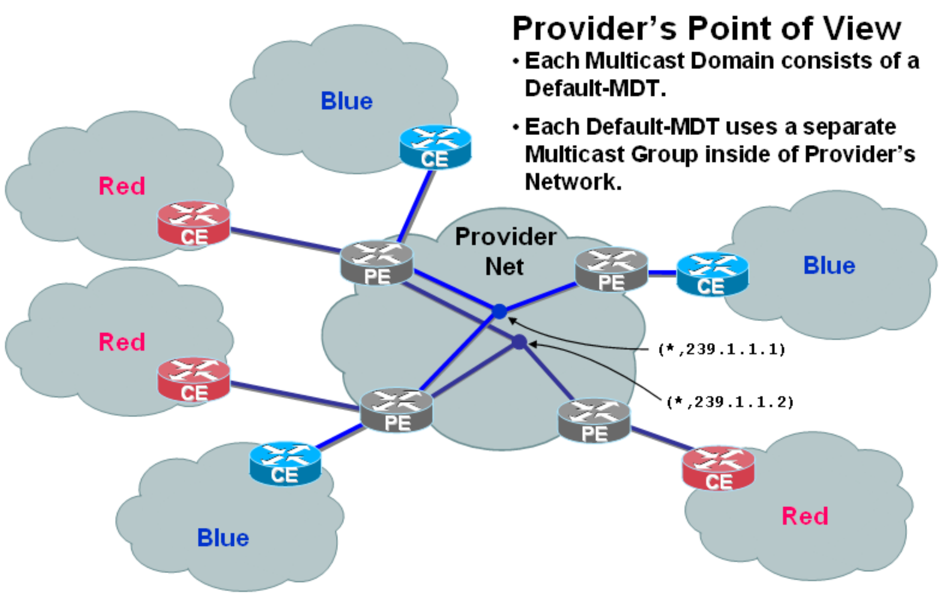


Figure 4. Multicast VPN – delivery of multicast traffic over MPLS infrastructure

The traffic engineering portion of MPLS technology was crucial in making it possible for Ethernet to extend beyond the LAN. A dedicated LSP with a particular QoS (requirement e.g. bandwidth) can be negotiated and signaled through the MPLS core using the RSVP-TE protocol. RSVP-TE P2P has existed for a few years and one of its most popular applications is fast reroute (FRR), which supports both link and node protection – allowing traffic restoration in sub 50ms in the case of a system failure. Quite recently, point to multi-point (P2MP) has become a hot MPLS application, offering better infrastructure utilization in delivering multicast or broadcast traffic.

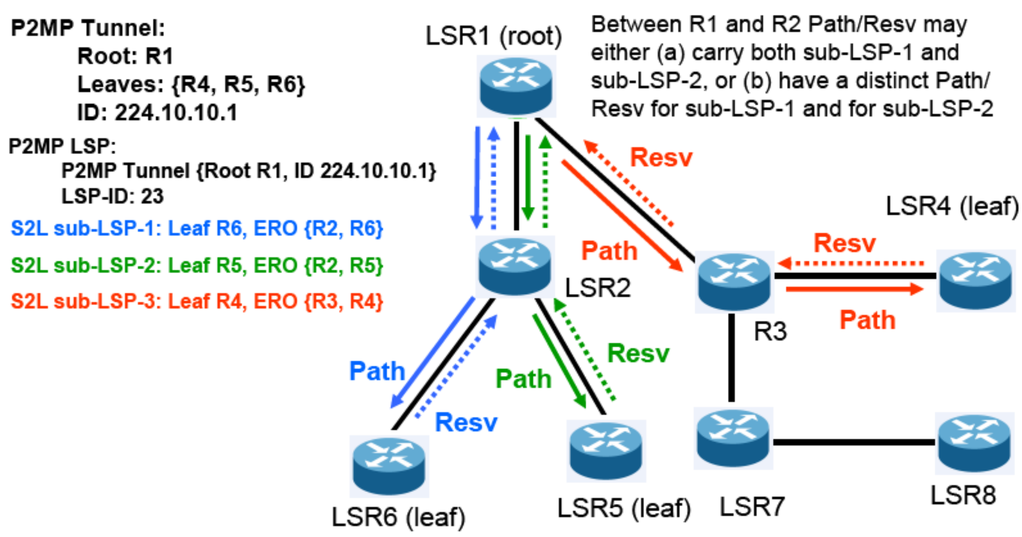


Figure 5. RSVP-TE based P2MP Tree for Better Utilization of Infrastructure Bandwidth

MPLS and MPLS based applications are complex, which is why, comprehensive Operation, Administration, and Management (OAM) tools are developed to help maintain and troubleshoot MPLS networks. MPLS OAM is a set of debugging and diagnostic tool that includes LSP Ping/Traceroute, LSP BFD, PW VCCV Ping and VCCV BFD. The combination of BFD and Ping/Traceroute is perfect to maintain a large-scale MPLS network.

With advanced development in MPLS technologies, and more and more MPLS VPN applications being deployed, it is usual for MPLS VPN to venture cross Autonomous Systems or administrative regions to offer end-to-end MPLS services. MPLS VPN Option A, B, and C defined various ways of inter-connect VPNS across AS or regions. Seamless MPLS is another way to say that end-to-end MPLS services encompass edge nodes, aggregation devices, and core transport. Finally, to make MPLS more scalable when the number of P and PE routers becomes huge, a tiered approach, namely, Hierarchical L3VPN, is required not only to scale, but also to provide service resilience against failure of key devices.

Advanced MPLS Test Methodologies

Test methodologies that should be applied to a given device under test (DUT) generally include tests for conformance, functionality, interoperability, performance and scalability. Conformance testing validates basic functionality in both positive and negative cases. It is an important tool that verifies whether a DUT complies with protocol standards. Functional and interoperability tests are more focused on specific DUT features in more realistic conditions. While conformance testing provides assurance of protocol conformity to standards or RFCs, the test topology is limited and not very realistic. Functional and interoperability tests, on the other hand, allow expansion of the test coverage to more realistic configuration.

Performance and scalability tests assume that a DUT is performing correctly in a realistic environment in various test scenarios, including invalid and inopportune events. These tests attempt to address the question of how well the DUT will work with increasing traffic load under different scenarios. There are many performance metrics that should be collected and scalability scenarios that should be evaluated before the device is deployed in the field, where it must support revenue generating traffic.

This *Advanced MPLS Testing* booklet selects a few key MPLS protocols and applications and offers concrete examples and step-by-step instructions showing how to utilize Ixia's IxNetwork emulation software to achieve functional and performance objectives. The technologies covered here include:

- RSVP-TE P2P full mesh scalability and performance Test
- RSVP-TE P2MP functional, scalability, and performance test
- L2 VPN PWE scalability and performance test
- L2 VPLS scalability, performance, and Impairment testing
- L3 VPN scalability and performance test
- MPLS OAM
    - Troubleshooting LDP or RSVP-TE LSPs with LSP Ping/Traceroute and LSP BFD
    - Maintain and support a live BGP VPLS network using VCCV Ping and VCCV BFD
- L3VPN Inter-AS Option B test
- L3VPN Inter-AS Option C test
- Seamless MPLS with scalability test
- H-L3VPN functional and scalability test
- mVPN scalability and Data MDT switchover performance test.

The test cases listed here are examples to get you started – they are by no means exhaustive, and we encourage you to expand them for your test needs.

Test Case: RSVP-TE P2P Full Mesh Scalability and Performance Test

Introduction to the RSVP-TE P2P Signaling Protocol

RSVP-TE, along with LDP, forms the basic signaling protocol of an MPLS network. Known for its traffic engineering (TE) capability, it is typically used in the core network between core provider (P) or core provider edge (PE) routers. RSVP-TE is a resource-intensive protocol that maintains a soft state for every tunnel that it creates. The soft state is periodically refreshed via refresh message. The state of each tunnel is closely monitored by the RSVP-TE state machine so that if changes occur in a network, corrective actions may be promptly taken in order to accommodate TE requirements.

Basic RSVP-TE state machine messages, including error handling, are: HELLO, PATH, RESV, PATH-ERR, RESV-ERR, PATH-TEAR and RESV-TEAR.

Advanced features that utilize the RSVP-TE state machine include: refresh reduction and reliable delivery, message bundling, graceful restart, fast reroute, and re-optimization. All of these features are critical components of an RSVP-TE implementation in a core network that is traffic-engineering capable.

Relevant Standards

- Resource reSerVation Protocol (RSVP) – RFC 2205
- Integrated service framework's QoS control services – RFC 2210
- RSVP Refresh Overhead Reduction Extensions – RFC2961
- Extensions to RSVP for LSP Tunnels – RFC 3209
- Fast reroute – draft-ietf-mpls-rsvp-lspfastreroute-02.txt
- RSVP-TE Graceful Restart – RFC 3473

Overview

RSVP-TE is one of the most important protocols in a core MPLS network. It is extremely important that RSVP-TE scalability and performance be tested to ensure that it not only satisfies the today's network demand, but also that of the foreseeable future. An RSVP-TE full mesh topology offers the most stressful setup that can be used to benchmark scale and performance limits.

Objective

This scenario is designed to test a few core P routers to see whether they can establish and sustain large number of RSVP-TE tunnels in a full mesh situation. Line rate traffic may be generated and verified for long duration testing. Network flapping may be added to periodically introduce disturbances into the network. It is vital that the system be observed while under test in order to determine if it can recover and re-converge quickly and reliably under network failures.

Setup

In this example four Ixia test ports are used to emulate anywhere from 100 to 400 core P routers connected via a few real core routers under test (the DUT); see Figure 6. Each test port emulates an equal number of core P routers that both initiate and terminate RSVP-TE tunnels to all of the other core P routers emulated by the other three test ports. You may increase the number of emulated P routers to match your real-world network requirements.

Due to the complexity of RSVP-TE topologies, the IxNetwork RSVP-TE protocol wizard is used to configure a port pair at a time. For a setup that includes 4 ports, there are 6 port pairs and thus you need to run the wizard 6 times. There are tips and tricks that avoid duplicated configuration, as each node is shared by multiple port pairs. For example, you may configure port pair 1-2 and port pair 3-4 first to set the OSPF-TE configuration for the emulated topology used by all test ports. In the subsequent configuration of port pair 1-3, port pair 1-4, port pair 2-3 and port pair 2-4, there is no need to modify the OSPF-TE configuration. A common trick is to use ISIS as the IGP for these port pairs, and use the Append function at the end of the configuration wizard to append the RSVP-TE configuration to the existing configuration while keeping the OSPF-TE configuration unchanged. After all port pairs are done, simply deselect ISIS from the protocol management.

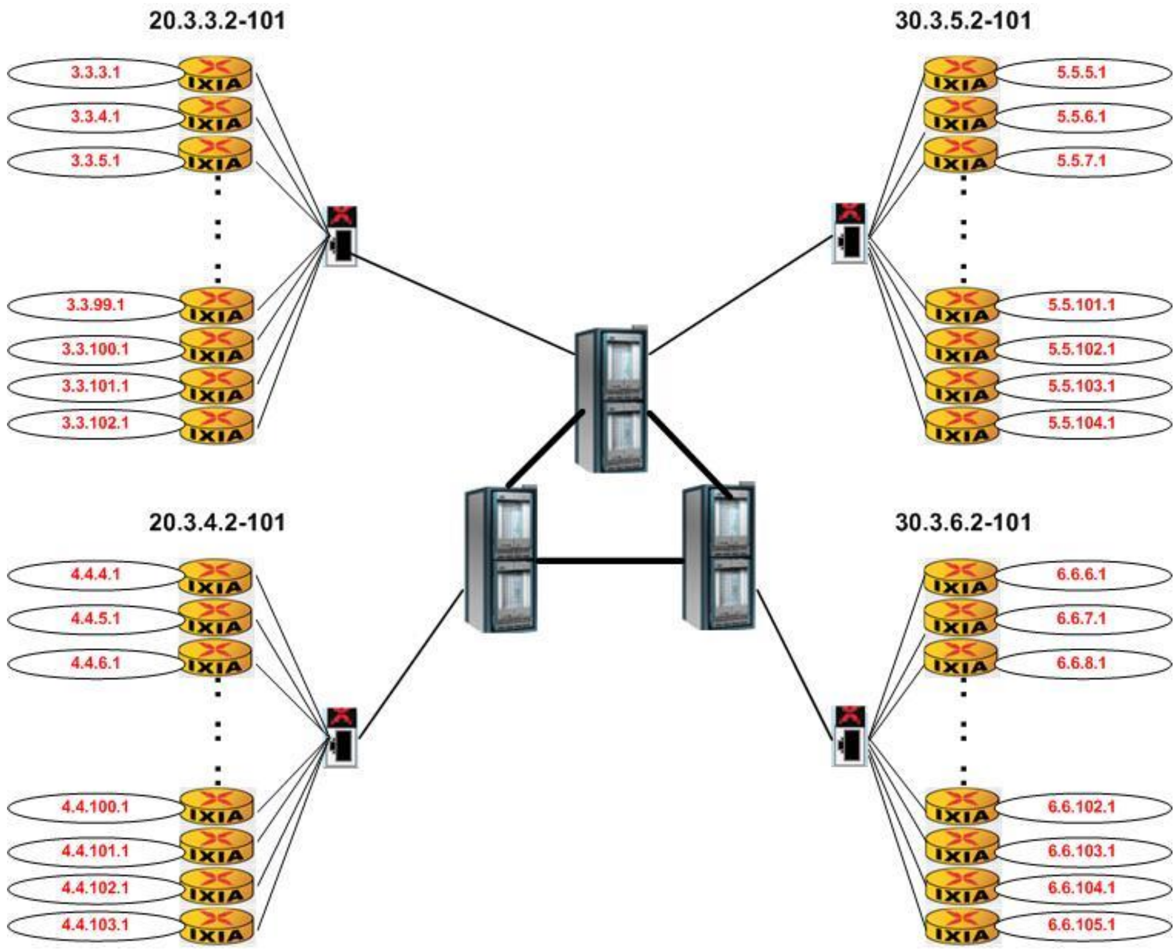


Figure 6. RSVP-TE P2P Scalability and Performance Test Setup

Step-by-Step Instructions

1. Launch the **RSVP-TE Wizard** and configure port pair 1-2, and then port pair 3-4 in a similar manner. On Screen #1 of 8, make sure you select **P2P**, **Bi-Directional**, and **SUT=Transit** as indicated below.

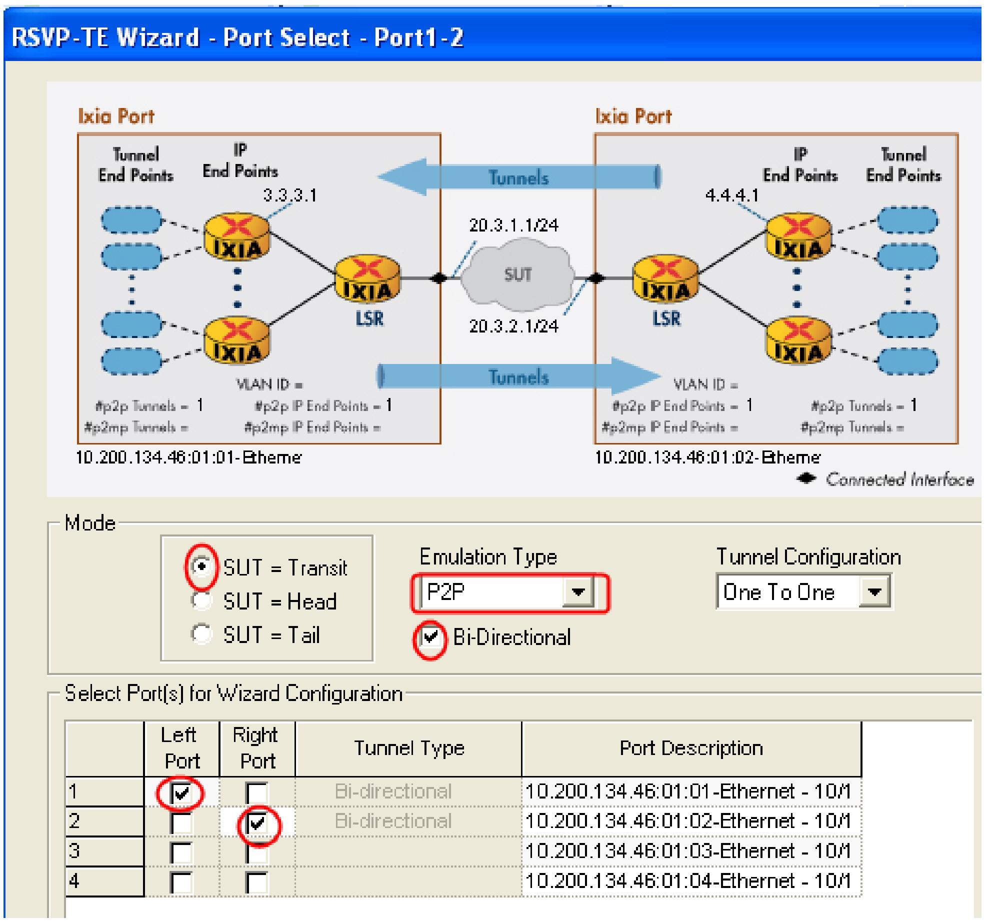


Figure 7. RSVP-TE wizard screen #1 of 8

2. On Screen #2 of 8, select **OSPF** as the **IGP**. Even though it's shown as OSPF, the wizard is actually using opaque LSAs to create the needed OSPF-TE topology. Enter the **Number of Neighbors** (i.e., the number of P routers) that you want each Ixia test port to emulate. Input the **SUT IP Address** for the **Left Port** and **Right Port** according to your actual setup. Use **Enable VLAN** and configure VLANs to separate each P router as needed.

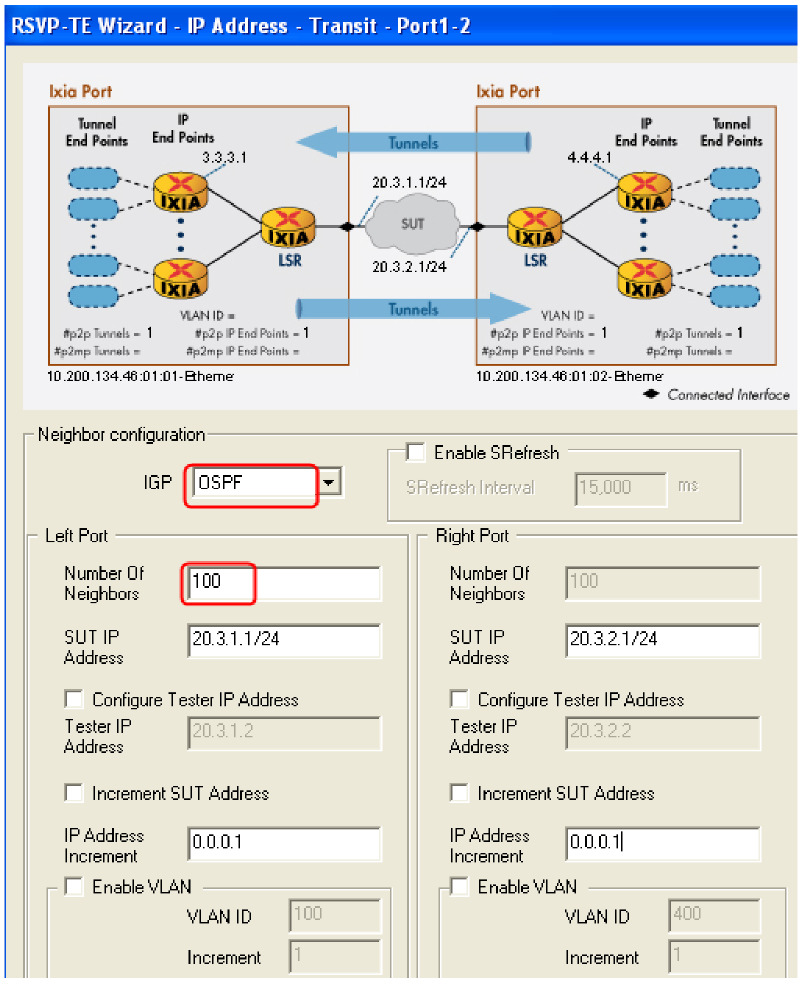


Figure 8. RSVP-TE Wizard Screen #2 of 8

3. On Screen #3 of 8, enter *1* as the **Number of IP End Points** to indicate that there will be a single Label Edge Router (LER) behind each Label Switching Router (LSR). Enter the loopback address (the **Head** and **Tail Endpoint IP Address**es) according to the actual setup. Leave the **Tunnel** and **LSP Instance** sections at their default values.

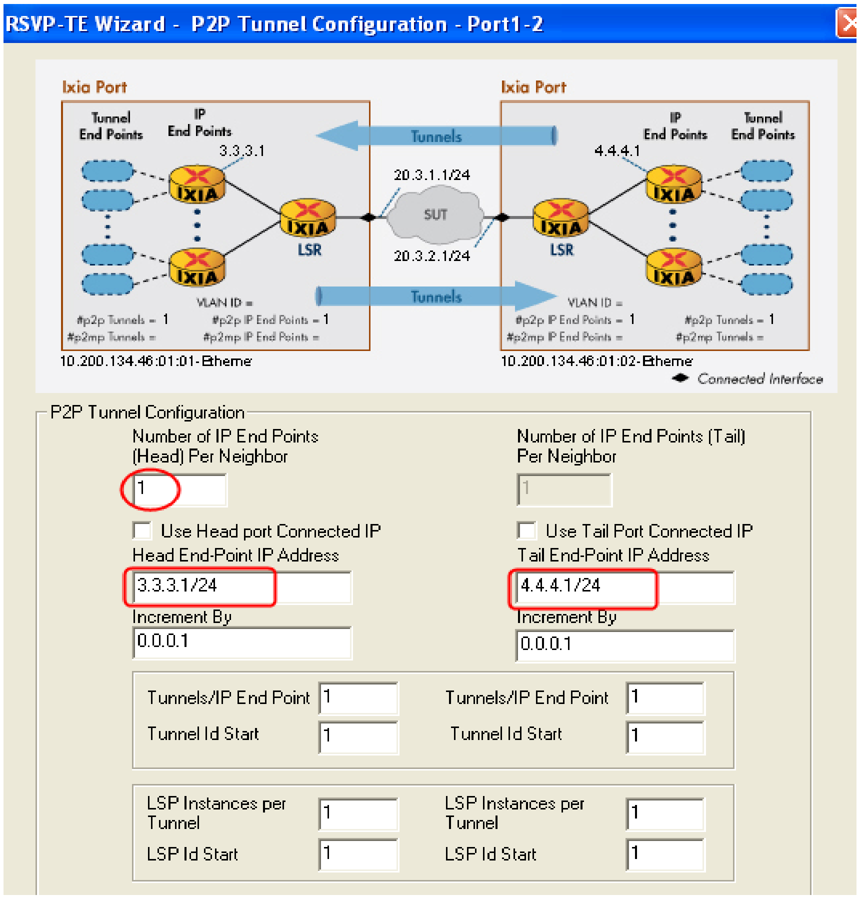


Figure 9. RSVP-TE Wizard Screen #3 of 8

4. Skip Screens #4-7 of 8 of the wizard to keep the default values, or change the parameters to match your actual setup (for example, change the **TSpec** parameters to match your setup – the defaults are zero). On Screen #8 of 8, enter a meaningful name for the configuration, for example *Port1-2*, and select **Generate and Overwrite Existing Configuration.**

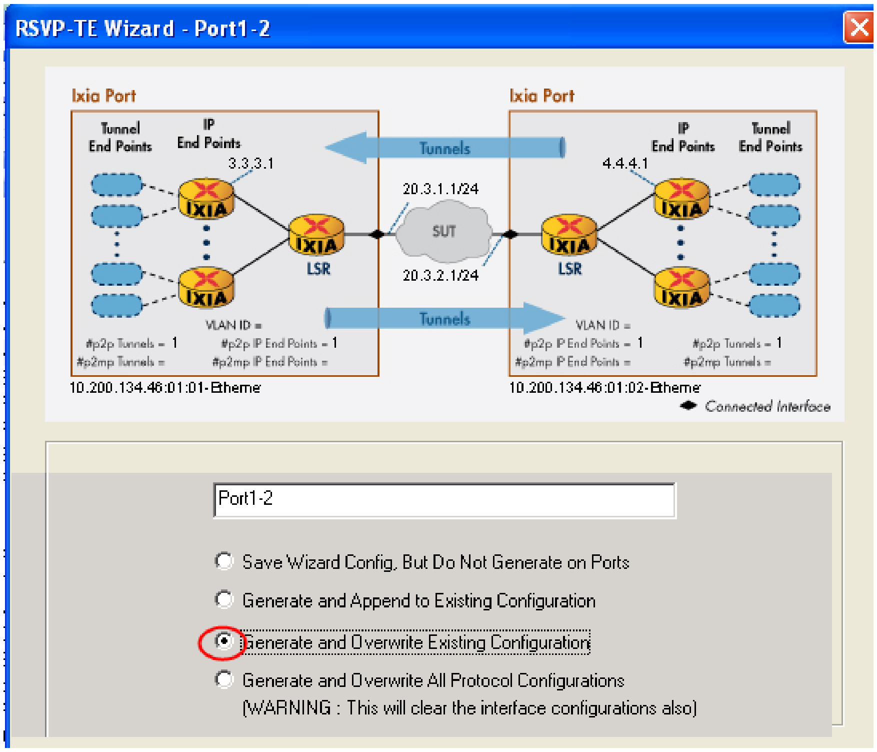


Figure 10. RSVP-TE wizard screen #8 of 8

5. In a similar way, generate the configuration for ports 3 and 4. The only items that change are the **SUT IP Address** for the **Left Port** and **Right Port** and the LER loopback addresses (the **Head** and **Tail Endpoint IP Address**). Make sure to select **OSPF** as **IGP** and choose **Generate and Overwrite Existing Configuration** at the end of the configuration.

6. From this step forward, you should select **ISIS** for the **IGP** and select **Generate and Append to Existing Configuration** at the end of the wizard. Selecting ISIS will avoid duplicating the OSPF-TE configuration performed in steps 1-5. We will deselect **ISIS** after the remainder of the configuration is complete. Selecting **Generate and Append** will keep the existing port configuration unchanged and append new configuration. Figure 11 and Figure 12 illustrate the configuration of port pair 1-3. Proceed in the same way to configure port pair 1-4, port pair 2-3 and port pair 2-4. Note that the sequence in which you configure the port pairs has an impact on the way traffic is built in the traffic wizard. See step 10 for more details.

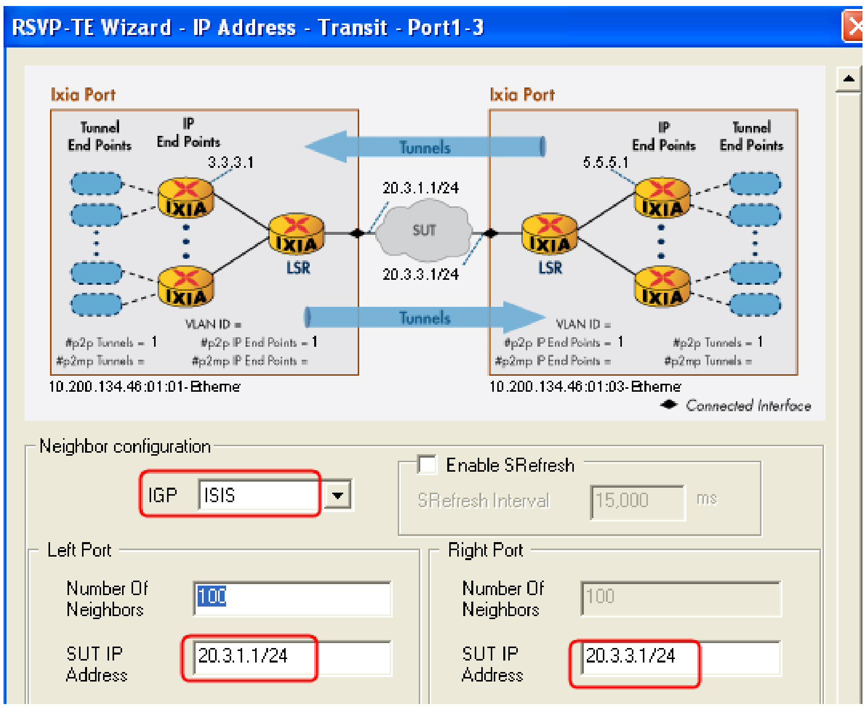


Figure 11. RSVP-TE wizard screen #2 of 8

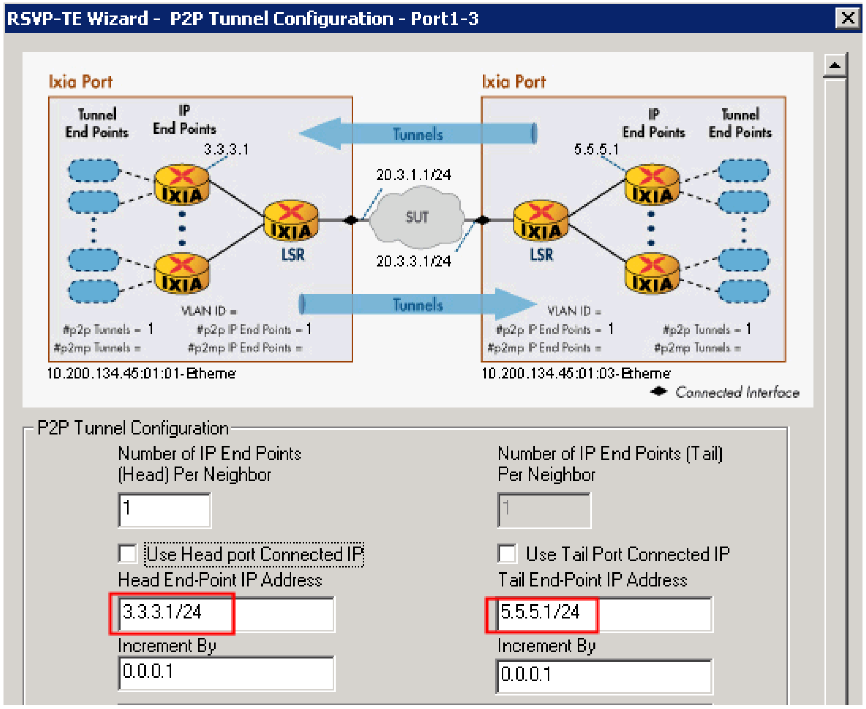


Figure 12. RSVP-TE wizard screen #3 of 8

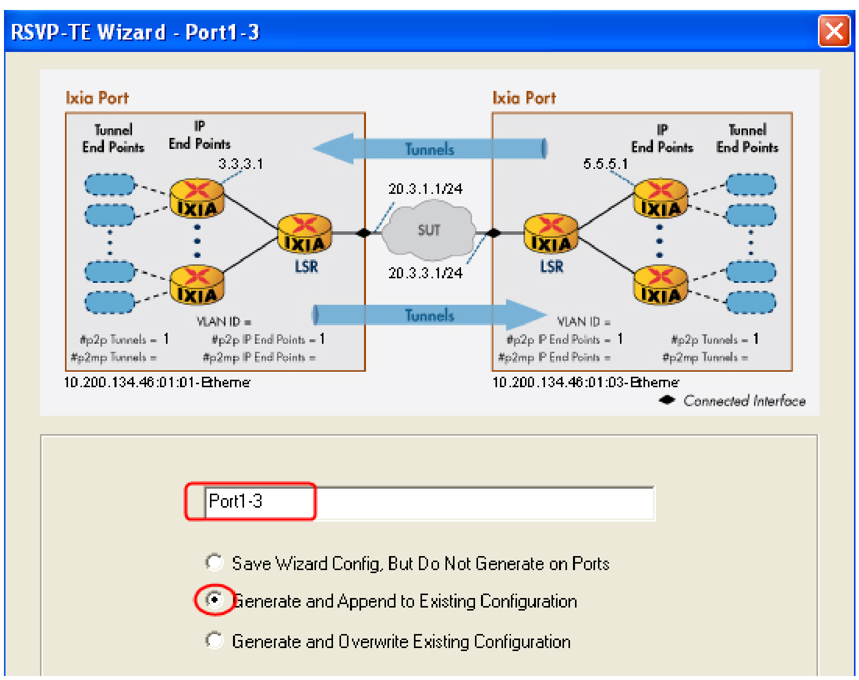


Figure 13. RSVP-TE wizard screen #8 of 8

7. After the final pair is done, deselect **ISIS** configuration from the generated topology. ISIS is used to avoid overwrite of an existing OSPF configuration.

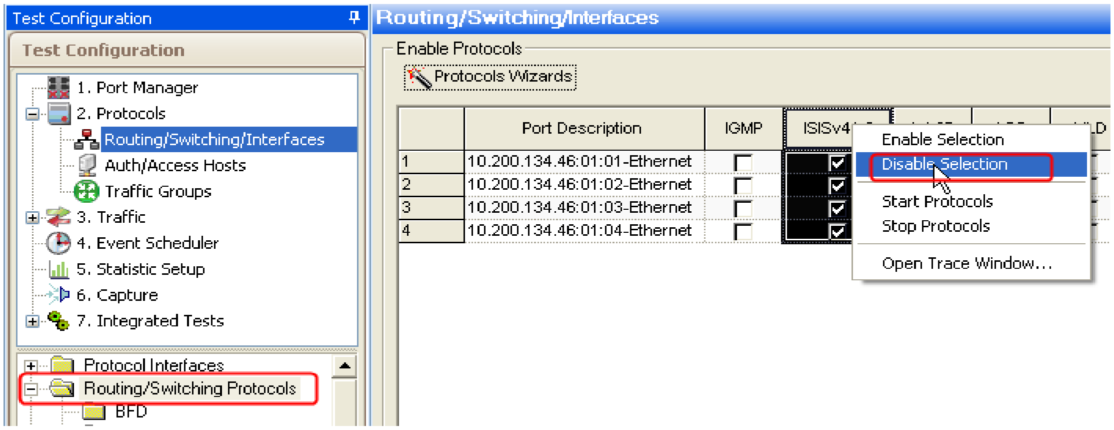


Figure 14. Deselect redundant configuration

8. Select the **Tunnel Head Ranges** tab. In the **LSP ID Start** column, right-click each entry and select **Increment,** so that each tunnel request is treated as individual request. By default, the values are all set to1 by the configuration wizard.

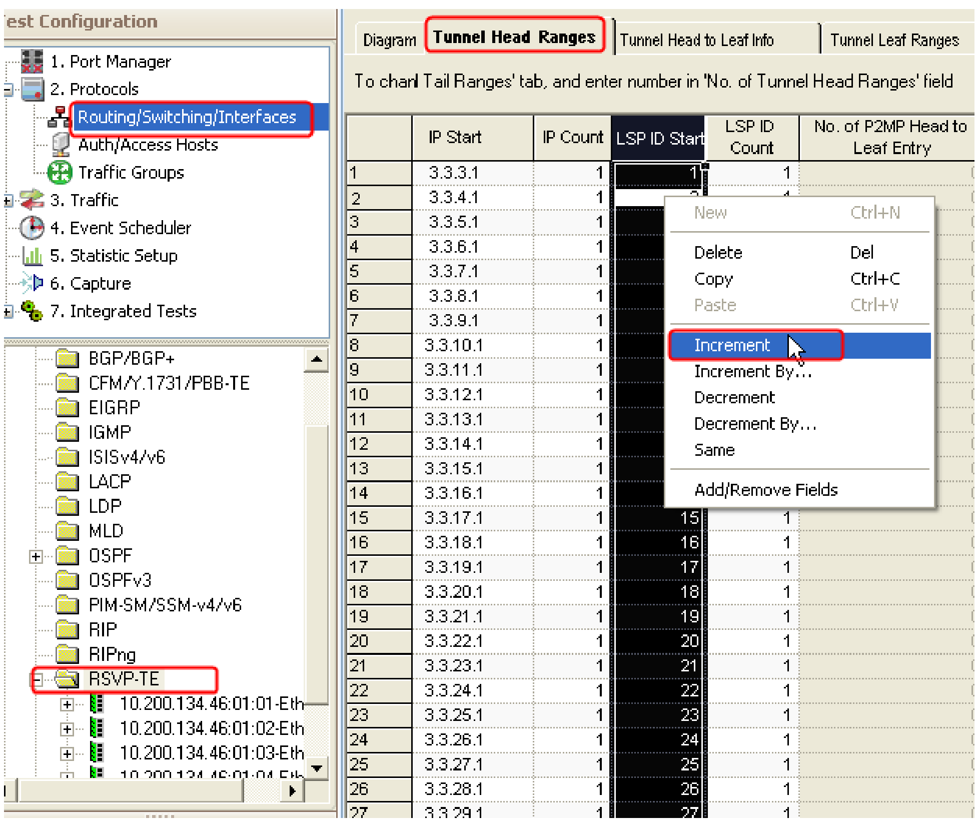
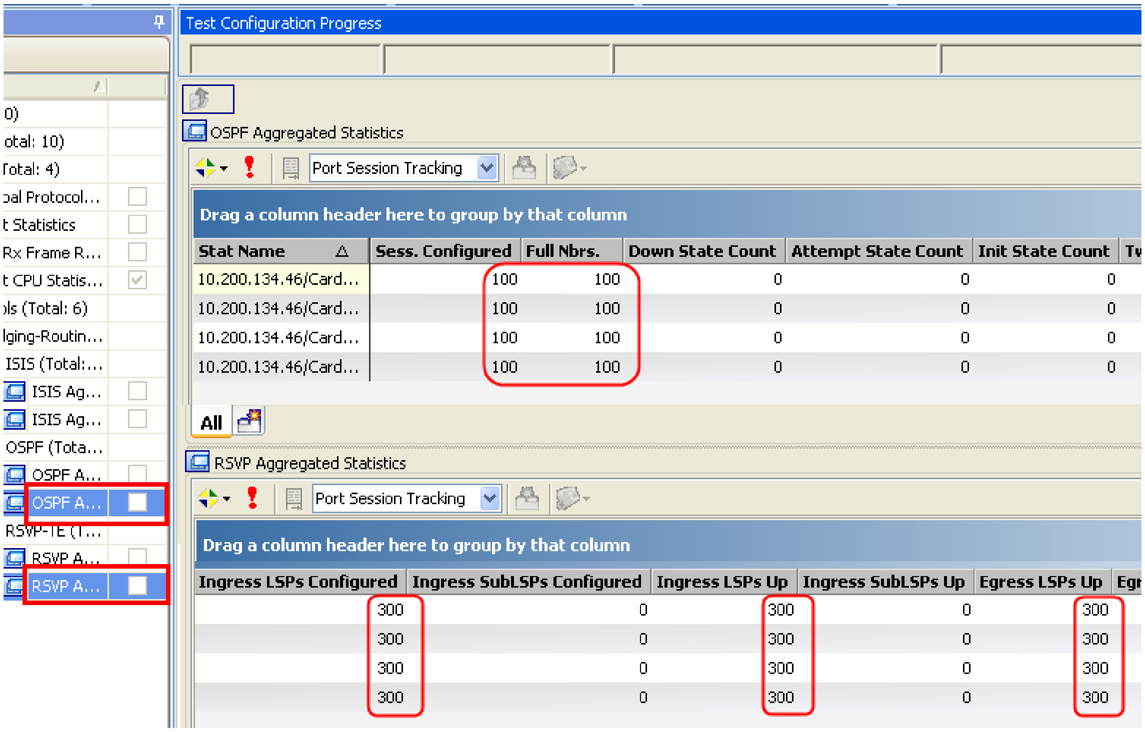


Figure 15. Global change of LSP ID

9. Right click on **Routing/Switching Protocol** and select **Start Protocols** to run all protocols and ensure that both OSPF and RSVP-TE are up.

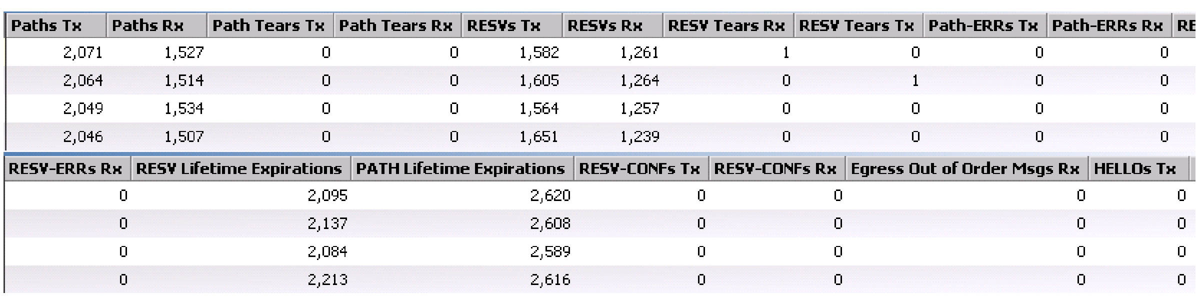


Stat Name	Sess. Configured	Full Nbrs.	Down State Count	Attempt State Count	Init State Count
10.200.134.46/Card...	100	100	0	0	0
10.200.134.46/Card...	100	100	0	0	0
10.200.134.46/Card...	100	100	0	0	0
10.200.134.46/Card...	100	100	0	0	0

Ingress LSPs Configured	Ingress SubLSPs Configured	Ingress LSPs Up	Ingress SubLSPs Up	Egress LSPs Up
300	0	300	0	300
300	0	300	0	300
300	0	300	0	300
300	0	300	0	300

Figure 16. Run-time protocol statistics

10. In addition to general session statistics, IxNetwork provides comprehensive RSVP-TE state machine statistics. Control plane statistics can be used to determine the source of problems in most cases.



Paths Tx	Paths Rx	Path Tears Tx	Path Tears Rx	RESVs Tx	RESVs Rx	RESV Tears Rx	RESV Tears Tx	Path-ERRs Tx	Path-ERRs Rx
2,071	1,527	0	0	1,582	1,261	1	0	0	0
2,064	1,514	0	0	1,605	1,264	0	1	0	0
2,049	1,534	0	0	1,564	1,257	0	0	0	0
2,046	1,507	0	0	1,651	1,239	0	0	0	0

RESV-ERRs Rx	RESV Lifetime Expirations	PATH Lifetime Expirations	RESV-CONFs Tx	RESV-CONFs Rx	Egress Out of Order Msgs Rx	HELLOs Tx
0	2,095	2,620	0	0	0	0
0	2,137	2,608	0	0	0	0
0	2,084	2,589	0	0	0	0
0	2,213	2,616	0	0	0	0

Figure 17. RSVP-TE protocol engine statistics

11. Additionally, IxAnalyzer provides bidirectional capture of control plane information flow and may be used to troubleshoot functional issues.

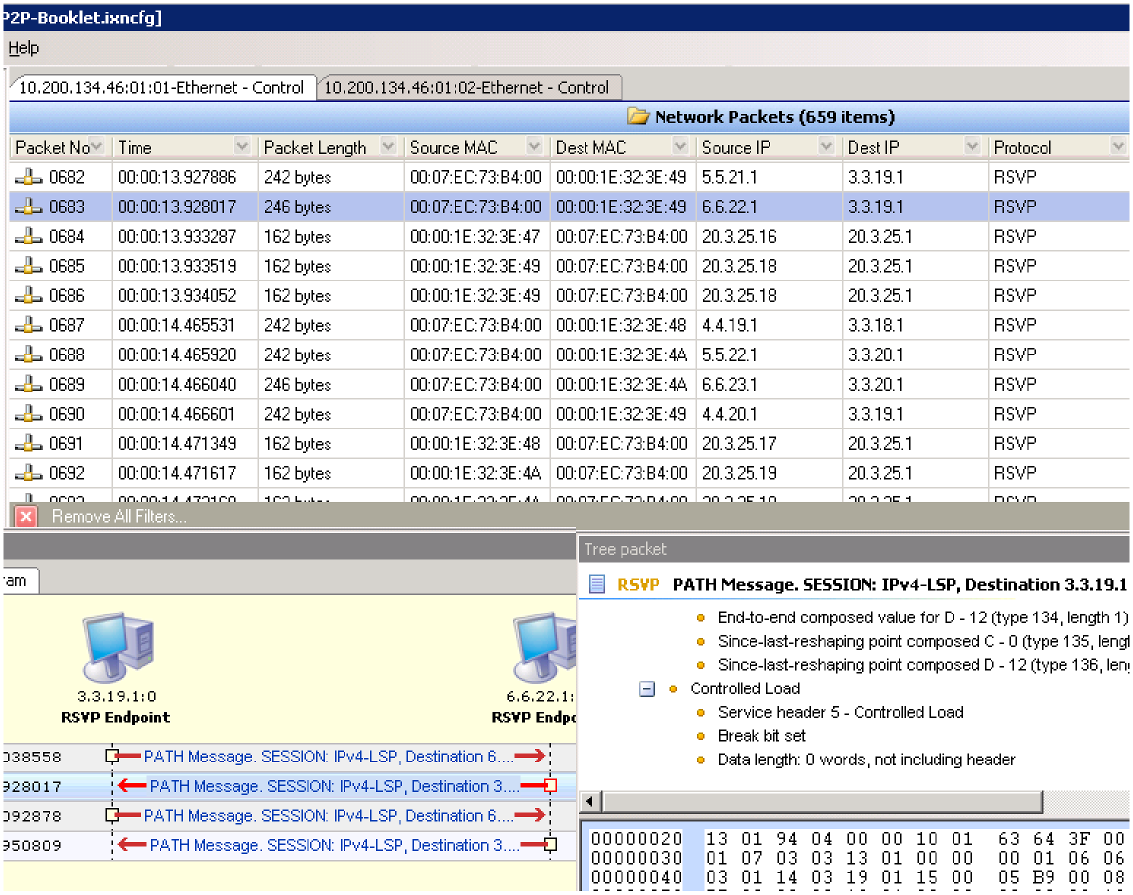


Figure 18. IxAnalyzer for bi-directional protocol capture

12. Once all RSVP-TE sessions are up, you must build bidirectional traffic over the MPLS LSPs. Since tunnel endpoints will appear in the traffic wizard on a first-come-first-serve basis, it's important to understand the sequence in which the tunnel chunks will appear in the traffic wizard. Figure 19 depicts the expected sequencing. Assuming that tunnels are built in the order shown in the figure, then tunnel endpoints will appear in the traffic wizard in sequence according to the numbers shown. When selecting a traffic pair, it's important to pick up the right ranges – otherwise, the wizard won't be able to find the correct MPLS labels, resulting in the failure of the traffic building process.

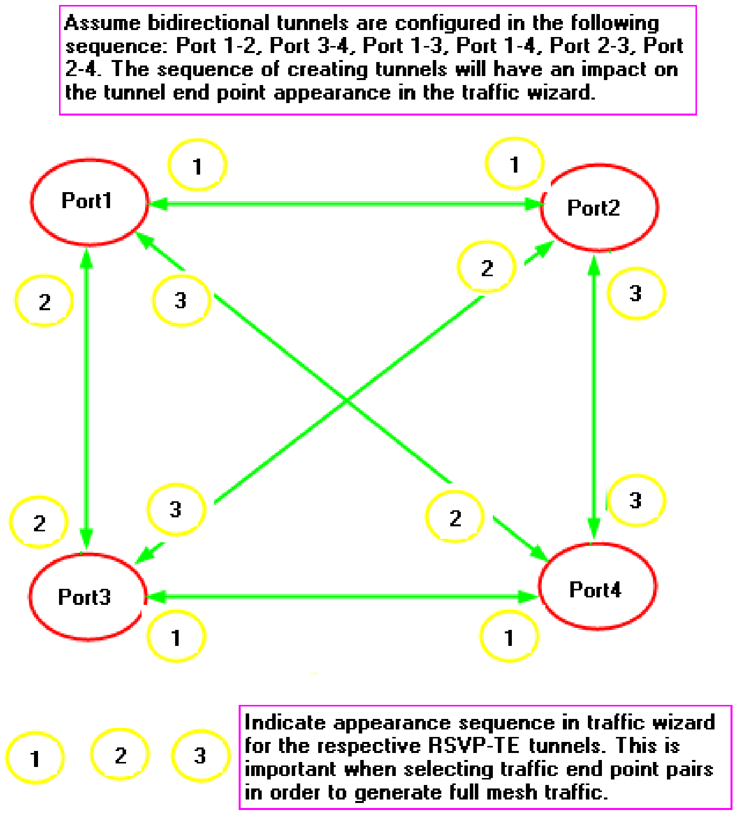


Figure 19. Traffic Endpoints Sequence in Traffic Wizard

Take port pair 1-4 as an example. According to the sequence diagram above, the P1 traffic endpoints for this bidirectional stream appear as the third chunk in the list, while the P4 traffic endpoints for the stream appear as the second chunk.

Even though there are multiple ways to build full-mesh traffic, we recommend that you build one port pair at a time in order to select the right traffic endpoints, as indicated below:

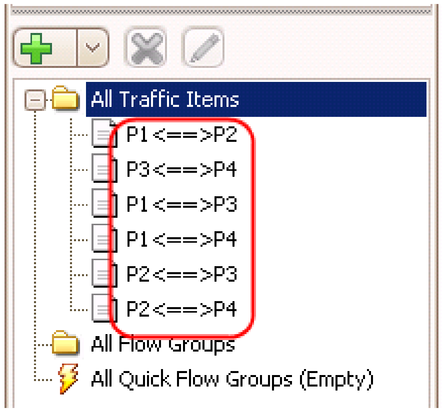


Figure 20. Suggested traffic items for a full-mesh setup

13. To configure this bidirectional stream, select **One-One** for **Src/Dst Mesh**, **One-One** for **Route Mesh**, and **MPLS** as the **Encapsulation Type**. Then, for P1→ P4 traffic, expand the RSVP-TE neighbor list for P1. In **Source Endpoints**, find the third chunk of 100 endpoints and then right-click and select **Enable Selection Groups → RSVP Head Ranges**. Similarly, expand the neighbor pairs on P4 from the **Destination Endpoints** list. Locate the second chunk of 100 endpoints and right-click to choose **Enable Selection Groups → RSVP Tail Ranges**. Click **+** to add traffic streams for the P1→P4 direction. Similarly, add another stream for the reverse P4→P1 direction under the same traffic item. Note that the **Source Endpoints** will be the second chunk of 100 endpoints from the P4 source list. **Destination Endpoints** will be the third chunk of 100 endpoints from the P1 destination list.

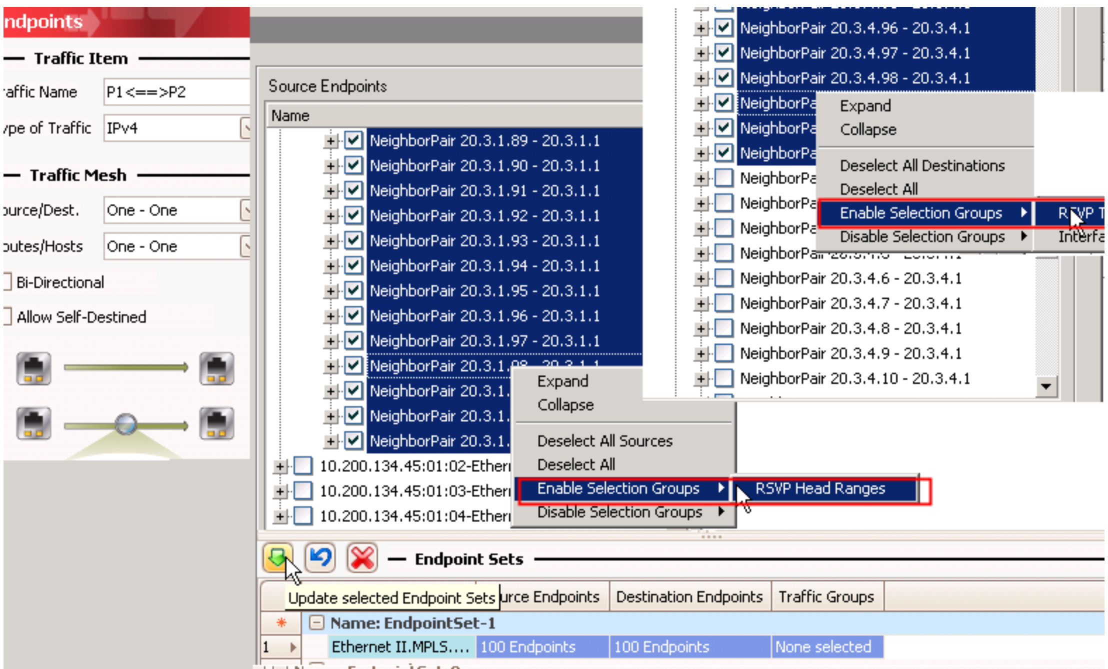


Figure 21. Traffic Wizard to Build Traffic Items

14. Perform the same steps for all other port pairs. Carefully locate the proper chunk of endpoints for each port as shown in Figure 19.

You may track the flows based on MPLS labels for each traffic item created. Click **Apply** to push the flow definition to the Ixia ports and create full flow-based statistics. Make sure traffic is flowing without loss before you add flapping, as described in next step.

15. Design a flap schedule to introduce periodic failures that allow you to observe whether or not the DUT can recover and re-converge. Failures may be introduced on any of the RSVP-TE sessions on any port. Figure 22 shows an example of flapping on all RSVP-TE sessions on port 1.

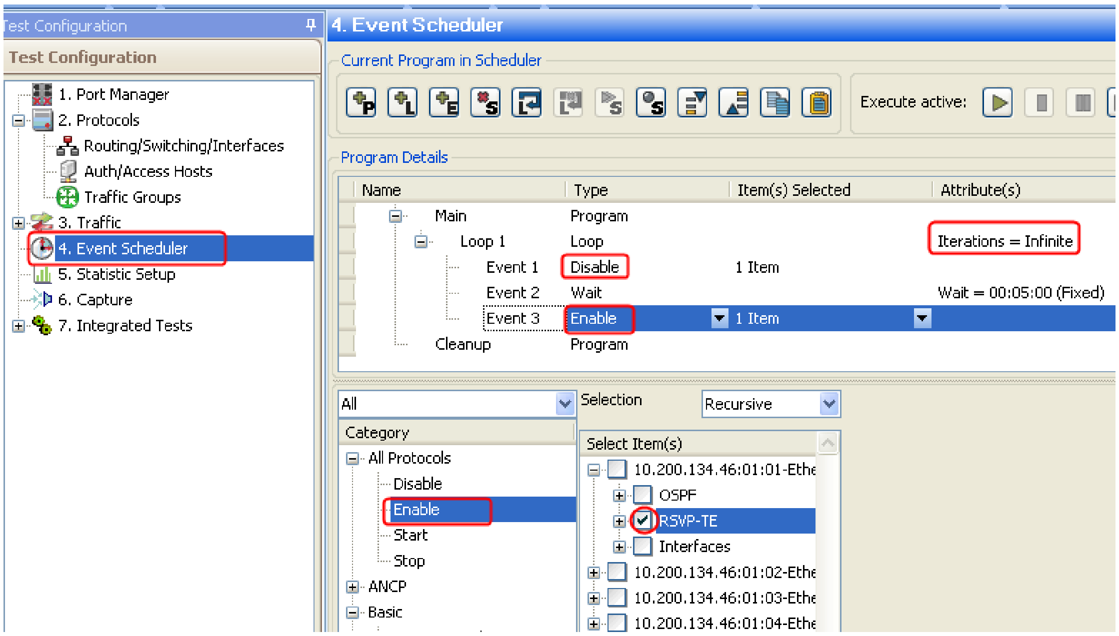


Figure 22. Event Scheduler to Introduce Flap

Test Variables

Any of the following variables may be scaled up in the test to further determine the scalability and performance of the DUT/SUT:

1. Number of test ports
2. Number of LSR/P routers per test port
3. Number of LER/PE routers per LSR/P router
4. Number of tunnels per LER/PE endpoint pair
5. Number of ports/sessions under flap
6. Flap duration

Result Analysis

It's important to ensure that the basics work before proceeding with scalability, performance or flap testing. This means that all of the OSPF and RSVP-TE sessions must be up.

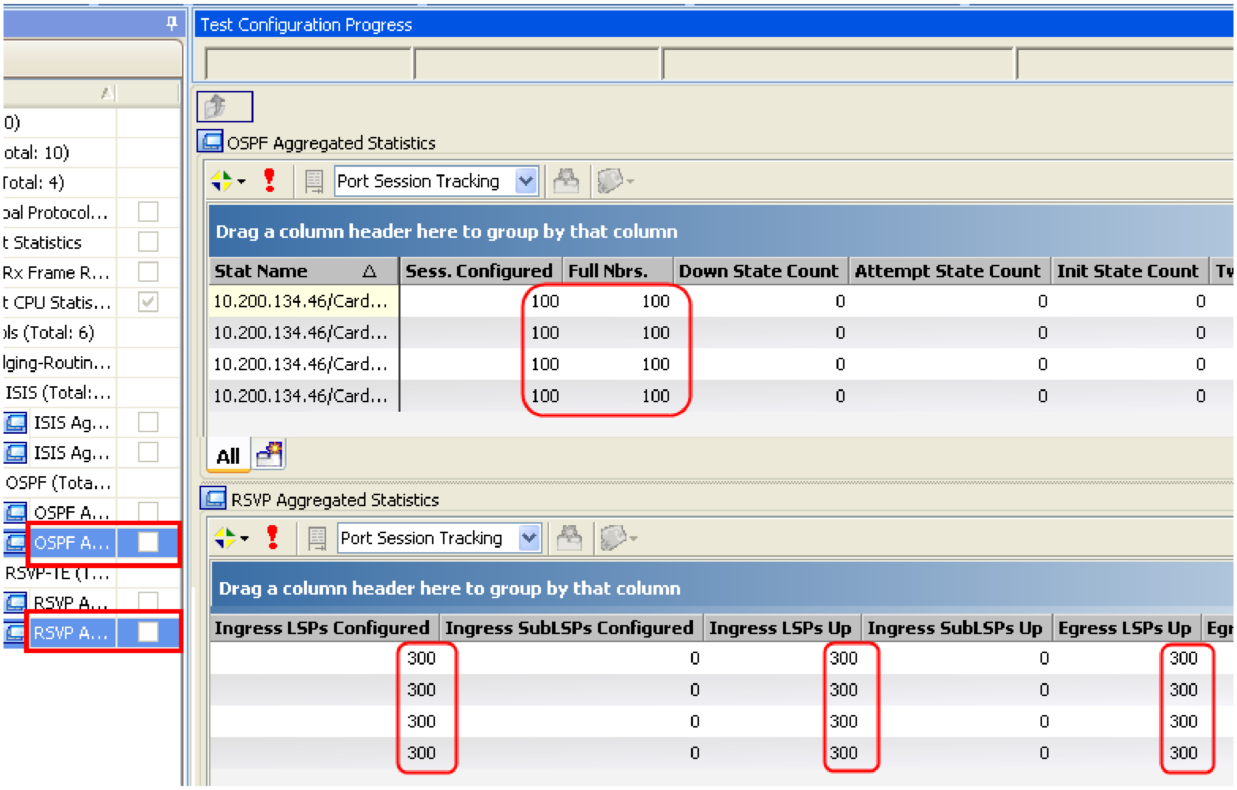


Figure 23. Overall protocol statistics

In case some RSVP-TE sessions are not up, you may use **Port Learned Info** to determine which sessions are up or down and whether or not a session has been assigned the correct MPLS labels.

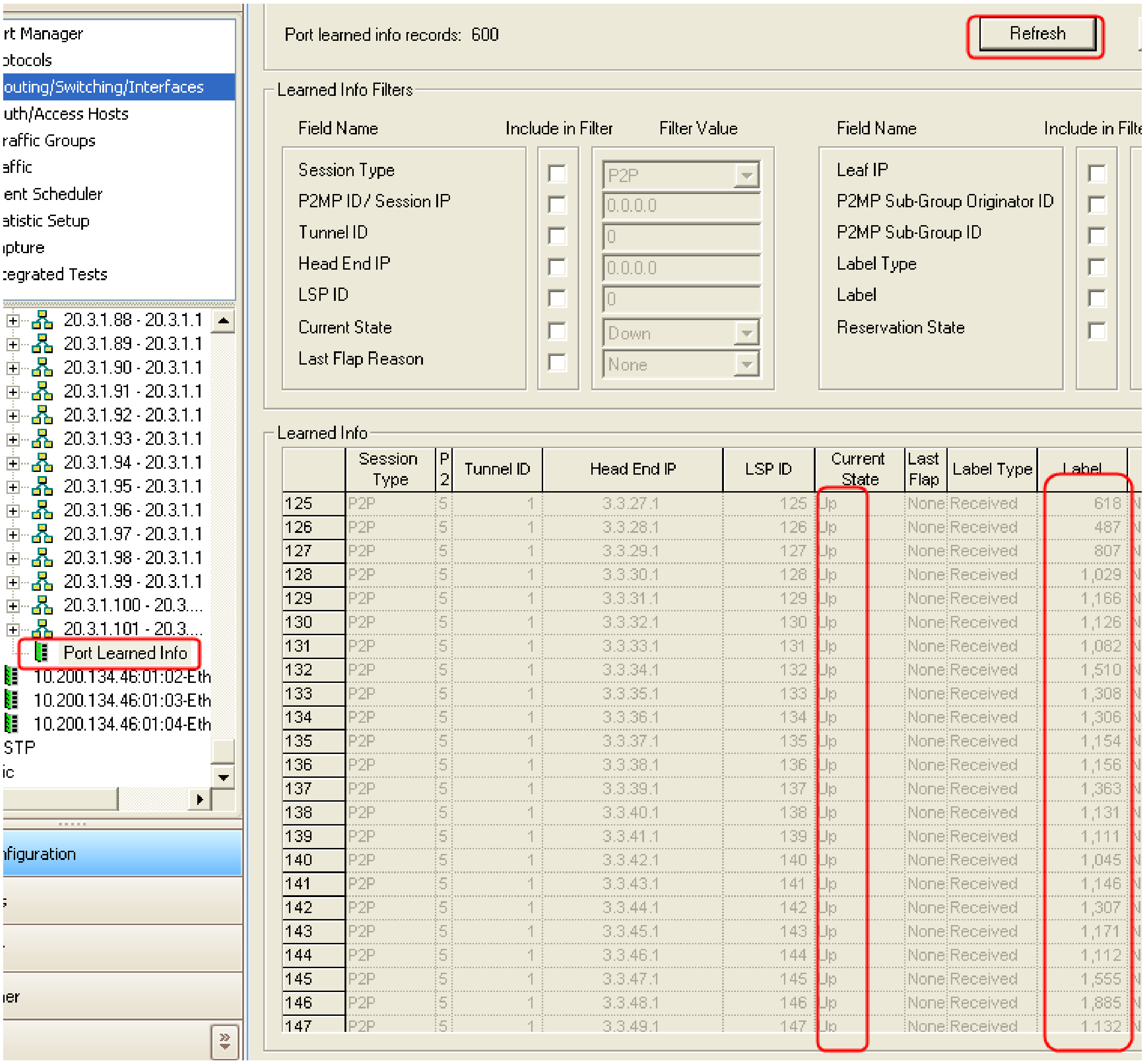


Figure 24. Port learned info used for troubleshooting

End-to-end traffic should be verified before introducing flapping to ensure that the DUT can handle the configuration for both the control and data planes.

Stream	Flow	PGID	Tx Frames	Rx Frames	Frames Delta	Tx Frame Rate	Rx Frame Rate
P1<==>P4 (000002-...	MPLSLabel-2037	001000	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1836	001001	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1377	001002	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1825	001003	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1581	001004	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1329	001005	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1696	001006	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1512	001007	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1769	001008	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1837	001009	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-2032	001010	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1398	001011	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1697	001012	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1335	001013	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1912	001014	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1400	001015	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1284	001016	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1299	001017	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1914	001018	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1328	001019	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-2028	001020	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1513	001021	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1483	001022	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1713	001023	69,499	69,499	0	472.941	473.941
P1<==>P4 (000002-...	MPLSLabel-1948	001024	69,499	69,499	0	472.942	473.942
P1<==>P4 (000002-...	MPLSLabel-1809	001025	69,499	69,499	0	472.943	473.943
P1<==>P4 (000002-...	MPLSLabel-1669	001026	69,499	69,499	0	472.944	473.944
P1<==>P4 (000002-...	MPLSLabel-1468	001027	69,499	69,499	0	472.945	473.945

Figure 25. Per-Flow Traffic Statistics

Troubleshooting and diagnostics

Problem	Description
Can't Ping from DUT	Check the **Protocol Interface** window and look for red exclamation marks (**!**). If any are found, there is likely an IP address/gateway mismatch.
Sessions won't come up or come up partially	• Go to **Port Learned Info** to discover which sessions are up and which ones are not. Use **Filter** if it is necessary to pinpoint the exact LSP in question. • Enable **Store Down LSP** under **Neighbor Pairs** to allow **Learned Info** to store dead LSP information indefinitely. From the **Test Configuration** window, turn on **Control Plane Capture**, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.
After stop/start protocols or link down/up Traffic 100% loss	Check the **Warnings** columns in the **Traffic** view and make sure there are no streams that say VPN label not found. The DUT may have sent new label info. If so, regenerate traffic by right-clicking the traffic item. Then **Apply** traffic.

Problem	Description
Traffic not passing on all flows	Double check the endpoints sequence in the traffic wizard to ensure that they are correct. Step 12 gives detailed info regarding the expected sequence.
Event scheduler doesn't seem to work	The event scheduler is designed for control plane flapping. Due to current limitations, the traffic plane doesn't have the dynamic label binding capability. Each time the control plane flaps, it's likely that labels for existing LSPs have changed. You must either manually regenerate the streams, or configure the DUT so that it assigns fixed labels to LSPs.

Conclusions

RSVP-TE is the building block of a traffic engineering capable MPLS network. Ixia's IxNetwork provides comprehensive, yet flexible RSVP-TE emulation to allow DUT stress testing in order to determine performance limits. Using just a few ports, IxNetwork can emulate hundreds of core P routers and build a complete full mesh topology to test a DUT's scalability and performance under stressful scenarios.

DUT Configuration Excerpt

```
! global command to enable mpls te
mpls traffic-eng tunnels
Interface Loopback0
   ip address 6.6.6.6 255.255.255.255
interface GigabitEthernet2/1
  description connection to IXIA port1
  ip address 192.168.3.1 255.255.255.0
  no ip directed-broadcast
  full-duplex
  mpls traffic-eng tunnels
! the following claims the interface (link) has reservable bw of 100,000 kbps (100Mbps)
  ip rsvp bandwidth 100000 100000
….
! make sure IGP is enabled with te
router ospf 10
 mpsl traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 are 0
 network 6.6.6.6 0.0.0.0 are 0
```

Test Case: RSVP-TE P2MP Functional and Scalability Test

This section addresses testing of the RSVP-TE P2MP protocol, one of the newest MPLS developments, from both functional and scalability perspectives. This section includes a complete review of the protocol followed by an introduction to applications that use the P2MP protocol. Test methodologies are also described, with functional and scalability test examples.

Introduction to RSVP-TE P2MP

RSVP-TE (P2P) and LDP are the two basic signaling protocols used by MPLS and MPLS-based applications, such as L2VPN PWE, VPLS, L3VPN, and 6VPE. Their primary function is to provide a signaling mechanism and protocol state machine to establish and maintain end-to-end MPLS LSPs across the network. The LSPs (i.e., tunnels) are by nature unidirectional, point-to-point, and hop-by-hop as bounded by labels agreed upon by adjacent LSRs. The difference between LDP and RSVP-TE is that LDP is resource-unaware (or best effort) while RSVP-TE is resource-aware and usually requires the underlying IGP (such as OSPF and ISIS) to be TE capable. Since they are point-to-point in nature, these two protocols are also known as P2P MPLS signaling protocols.

The RSVP-TE P2MP signaling protocol is the same as RSVP-TE P2P, except that it is used for establishing and maintaining point-to-multipoint MPLS LSPs in an MPLS network. As may be expected, the signaling messages and protocol state machine are more complex in the P2MP protocol. New definitions and terminologies are necessary in order to describe exactly how it works. RSVP-TE P2MP is specified in RFC 4875.

RSVP-TE P2MP Components

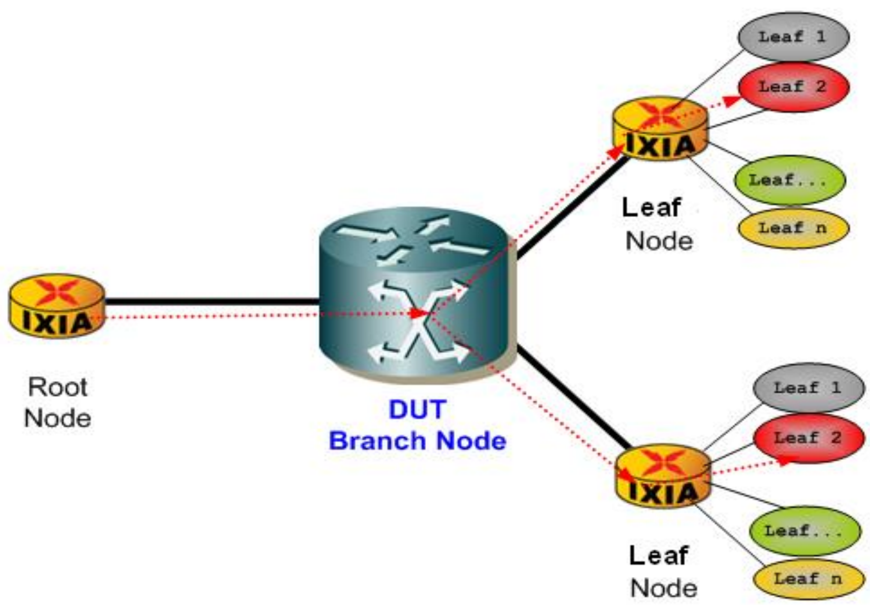


Figure 26. RSVP-TE P2MP Components

Root Node – The ingress router that initiates the P2MP tunnel, known simply as **Head** in the IxNetwork GUI. Tunnel request message PATH is sent from the root node to leaf Nodes.

Branch Node – The intermediate router that is responsible for branching the tunnel into multiple leaf nodes. The PATH message from the root node will be processed and fan out to multiple S2L PATH messages if needed.

Leaf Node – The egress router that terminates one of the P2MP branches. The PATH message will be terminated and a RESV message with label assignment will be looped back to the root Node. When the branch node delivers the final RESV message back to the root node, a P2MP tunnel is established.

Theory of Operation

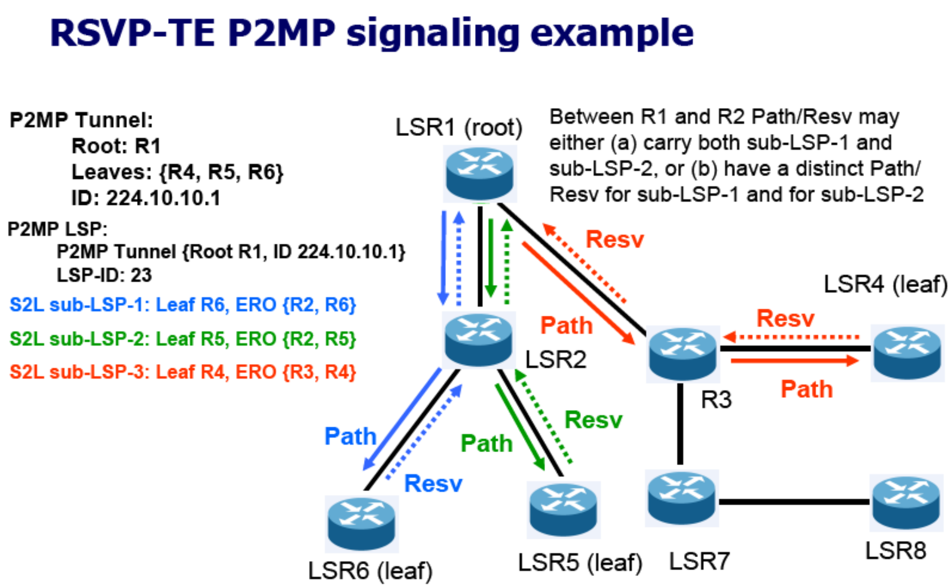


Figure 27. RSVP-TE P2MP Theory of Operation

The root (LSR1) is responsible for send PATH messages to reach each leaf node in the network. The PATH message contains the P2MP Tunnel, P2MP LSP and S2L sub-LSPs. In this example, the root is also a branch node so it will send at least two separate PATH messages (optionally three) – one contains the P2MP tunnel, P2MP LSP and the red S2L sub-LSP, while the other contains the same P2MP tunnel, P2MP LSP and a different S2L sub-LSPs (blue and green). LSR1 and LSR2 may exchange a single PATH message that contains both S2L sub-LSPs or send two separate PATH messages, each containing a single S2L sub-LSP. LSR2 is another branch node that repeats the same process as LSR1 (root).

When LSR4, 5, and 6 receive the S2L PATH message, if they all have the resources available for the requested tunnel, then they will each respond by sending a RESV message upstream with a label assignment. The branch nodes LSR2 and 3 will act on the received RESV from their leaves and will send a single RESV upstream for all downstream leaves. After the root LSR1 (also a branch node) receives both RESVs from downstream branch nodes, it considers a new P2MP tunnel to be in place.

Which Applications Need P2MP?

NG Multicast VPN – mVPN

mVPN was an instant success when it was introduced. The reason is simple: customers who want L3VPN service also want to run both unicast and multicast on the same port, over exactly the same infrastructure. L3VPN was designed for unicast traffic only. A special design was needed to satisfy mVPN requirements.

The core network requires PIM-SM in order to build a multicast delivery tree among the PE routers (called the default MDT). For scalability reasons, GRE tunnels are used to encapsulate multicast control and data plane packets over the default MDT. There is at least one default MDT for every VPN/VRF served in the core. Customer multicast control plane and data plane packets are not seen by the core, facilitating scalability. As the number of VPNs increases, however, so will the default MDTs in the core. The concept of data MDT was introduced to deal efficiently with chatty customers who have a large amount of multicast traffic destined for only a few receivers. The ingress router (PE) detects the bandwidth usage of incoming multicast traffic and when a threshold is crossed, builds a separated MDT within the core, so only those who are interested may join and receive the traffic. This prevents large amounts of multicast traffic from being unnecessarily multiplied in the core and consuming precious bandwidth.

This was all before P2MP was invented. As discussed, mVPN based on GRE tunnels is an overlay architecture that builds a virtual layer on top of the same network used by MPLS L3VPNs. This works, but in a cumbersome way. First of all, multicast traffic has nothing to do with MPLS LSPs – they use GRE in native IP format. Therefore, they lose all of the advantages associated with MPLS label switching and traffic engineering. Secondly, running PIM-SM in the core with ever increasing default and data MDTs is a management nightmare. Recall that part of the L3VPN design philosophy was to allow the core running to only run necessary protocols (such as OSPF/ISIS, LDP/RSVP-TE) and to keep resource-intensive protocols such as BGP completely out of the core. Using PIM-SIM for multicast in the core is analogous to using BGP in the core for. This method, using GRE tunneling to deliver both unicast and multicast traffic over the same infrastructure, works but it's only a band-aid solution.

P2MP tunnels solve the problem completely and elegantly. PIM-SIM is no longer required in the core; a modified version of MPLS LSP – P2MP LSP is used instead. Multicast traffic is built between the ingress router (multicast source) and all the leaf nodes that have receivers behind them, and is treated in exactly the same manner as the unicast traffic. Specifically, multicast traffic uses MPLS label switched in the core instead of being routed by the core as with the GRE tunnel case.

VPLS

VPLS (virtual private LAN service) was designed as a flat switching architecture such that frames with unknown destination MAC addresses are treated as broadcast packets – sending them to all remote PE routers that belong to the same VPLS instance. Understanding that there are usually many multicast and broadcast traffic sources in a switched network, a VPLS network based on blind flooding could easily collapse if unknown frames were not handled intelligently.

In Figure 28, incoming traffic with an unknown destination address is received by PE1 at 10 Mbps and must be broadcast to all remote PEs (PE2/PE3/PE4). Since LSPs from PE1->PE2 usually have a different label than LSPs from PE1 to PE3/PE4, each frame will likely must be multiplied three times to go over three separate tunnels in order to reach PE2, PE3, and PE4. This creates an instant utilization surge on the links between PE1 and its immediate next-hop P1 router. The same situation will occur on the P1 to P2 link to a lesser degree because PE2 branches out from P1.

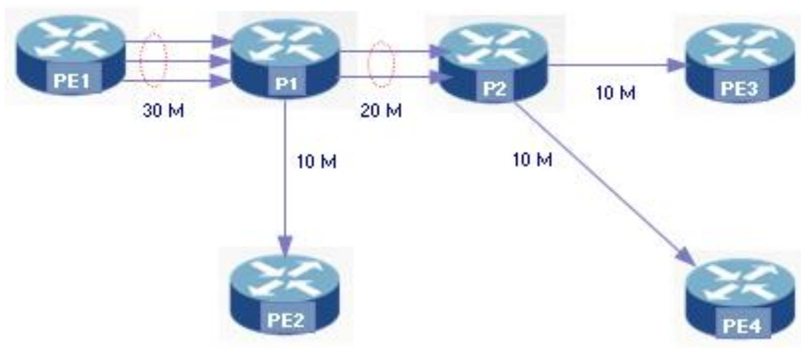


Figure 28. VPLS unknown packets without P2MP

On the other hand, if a dedicated point-to-multipoint (P2MP) LSP is created between PE1 and PE2/PE3/PE4, as depicted in the diagram below, to carry all unknown unicast, broadcast, and multicast traffic for each VPLS instance in the network, the efficiency of the network increases dramatically. In this case, there is no need to flood traffic to all intermediate nodes until it reaches the branch nodes. Figure 29 below shows that if the same network topology is employed with P2MP LSP, no bandwidth surge will occur on all of the connecting links between the root node and the branching nodes.

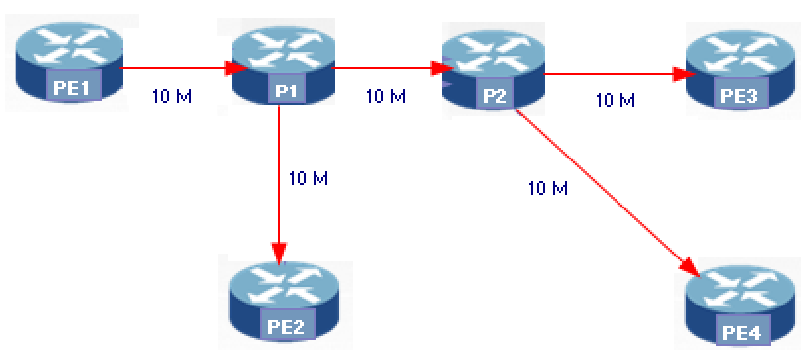


Figure 29. VPLS Unknown Packets with P2MP

Relevant Standards

Resource reSerVation Protocol (RSVP) – RFC 2205

Integrated service framework's QoS control services – RFC 2210

RSVP Refresh Overhead Reduction Extensions – RFC2961

Extensions to RSVP for LSP Tunnels – RFC 3209

Fast reroute – draft-ietf-mpls-rsvp-lspfastreroute-02.txt

RSVP-TE Graceful Restart – RFC 3473

Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) – RFC 4875

Test Case: P2MP Functional Test

Overview

P2MP testing is complex, not only because it has more protocol messages and far more objects than P2P, but also because of the overall test topology and the role that the DUT plays in an end-to-end test setup.

As discussed earlier, a DUT may be a root, branch or leaf or any combination in a P2MP test topology. IxNetwork must be configured. For example, you must configure Ixia's emulation as root to test a DUT acting as a branch or leaf. Or you must set Ixia emulation to leaf in order to test a DUT acting as a Root.

Objective

In this setup, Ixia's left port emulates 3 root nodes, each initiating a separate P2MP tunnel (tree). Ixia's right port emulates 3 distinct RSVP-TE neighbors (LSRs) separated by 3 VLANs. In this case, the DUT branches over sub-interfaces. Similar test procedures would apply in a scenario in which the DUT branches over physical interfaces. Additionally, the Ixia right port emulates a different set of leaf nodes. To vary the scenario, we will select the number of leaf nodes to be 3, 2, and 3, respectively for the three neighbors or VLANs. The setup may be easily expanded.

Setup

Figure 30 shows a common test topology where the DUT is a branch node while IxNetwork emulates both root and leaf nodes to form an end-to-end test topology.

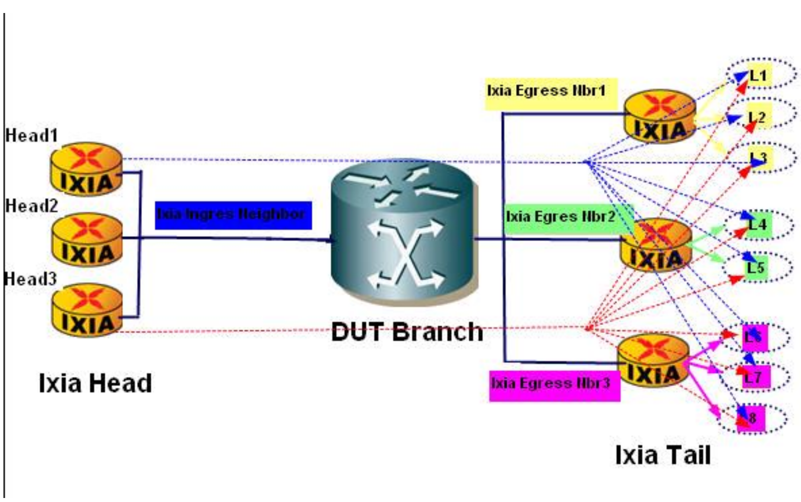


Figure 30. P2MP functional test topology

Step-by-Step Instructions

1. Launch the RSVP-TE protocol wizard and select **SUT = Transit**, set **Emulation Type** to **P2MP**, and **Tunnel Configuration** to **Fully Meshed**.

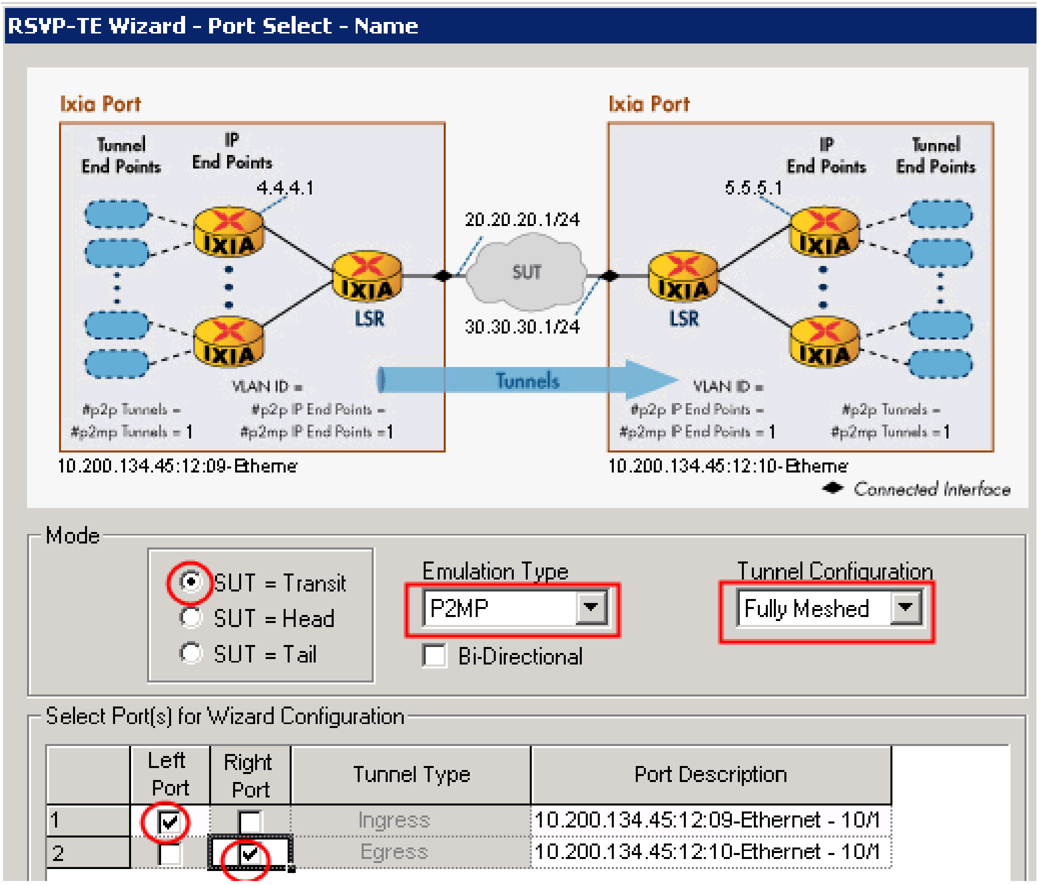


Figure 31. P2MP wizard screen #1 of 9

2. Set the **Number of Neighbors** to be *1* and *3* respectively for the **Left Port** (root) and the **Right Port** (leaf). Click **Enable VLAN** for the leaf port to provide sub-interfaces for the three leaf nodes. Configure the **VLAN ID** and step size as appropriate.

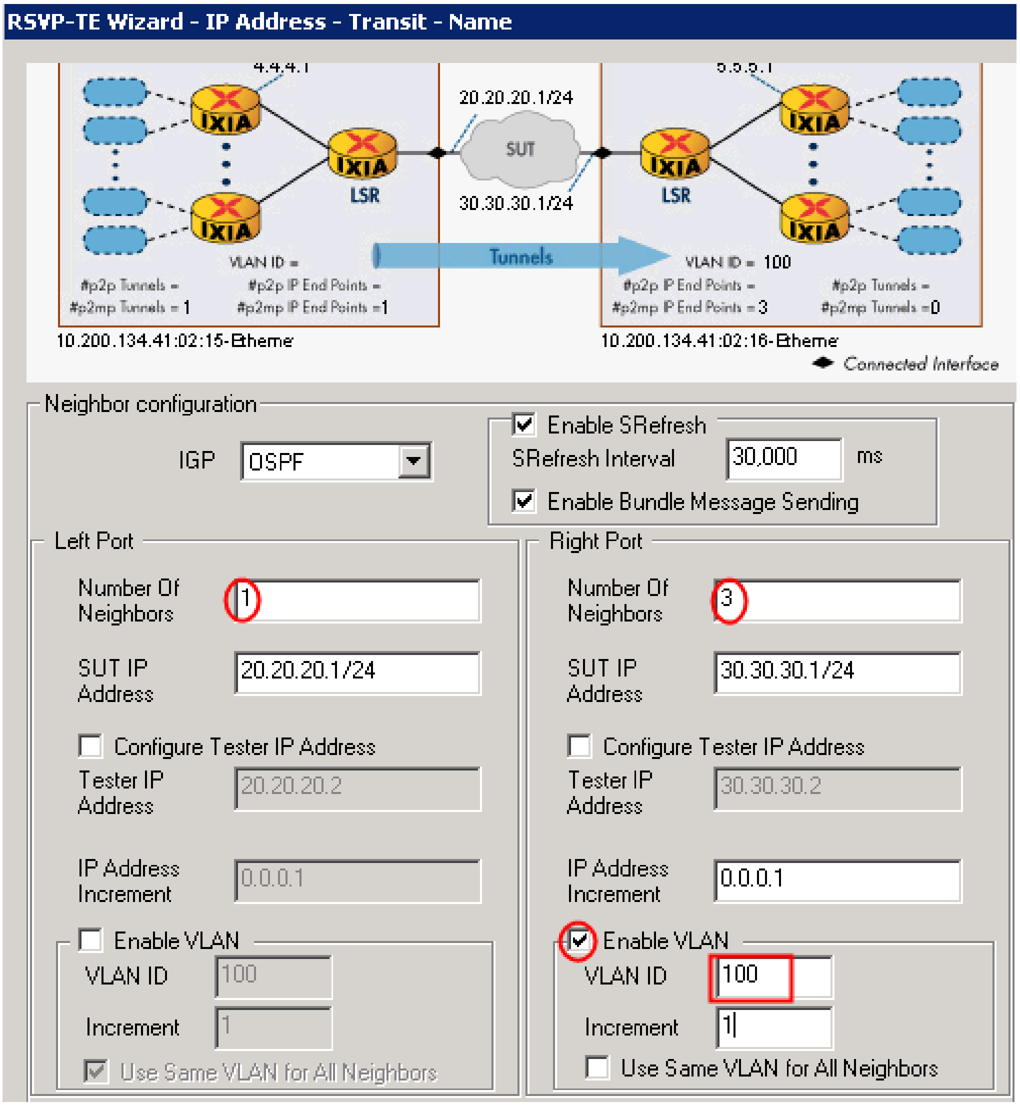


Figure 32. P2MP Wizard Screen #2 of 9

3. Set **Number of IP Endpoints** for both neighbors (**Head** and **Tail**) to *3*. This creates three root nodes and three leaf nodes for each of the three egress (tail) neighbors. The wizard assumes symmetric configuration, so that in later steps we can manually tweak the number of leaf nodes for the second neighbor. Select **Per Sender** as the **Number of P2MP IDs**. Input the start **P2MP ID** and toggle on the **Inter Sender P2MP ID Increment**. These parameters simply mean that each sender will initiate a separate P2MP tunnel with a unique P2MP ID. Enter the appropriate **Tunnel ID Start** and **LSP ID Start**.

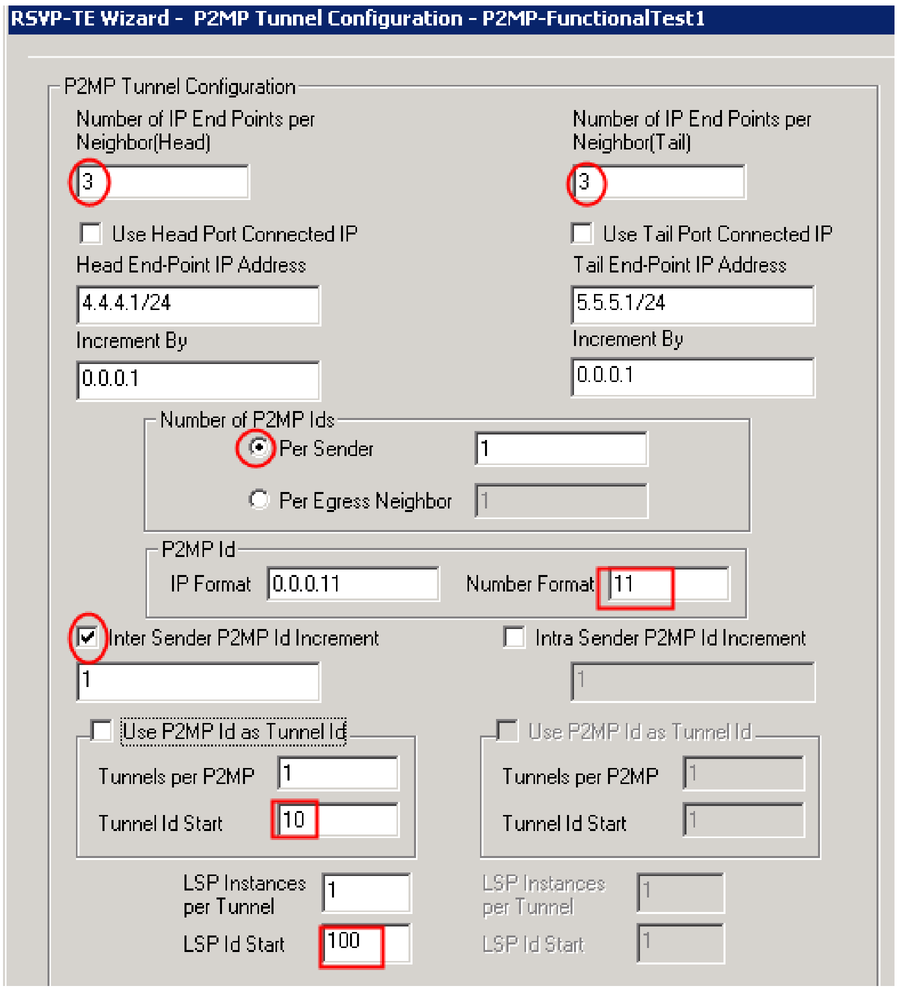


Figure 33. P2MP wizard screen #3 of 9

4. On the next screen, either keep the default values or change them as appropriate. This screen sets up the traffic endpoints for the traffic wizard. The traffic wizard will use these as Src and Dest IP addresses for packets to be transmitted, and it also has mapping logic to ensure that each address is associated with the right P2MP label so that traffic is sent over the correct P2MP tunnel.

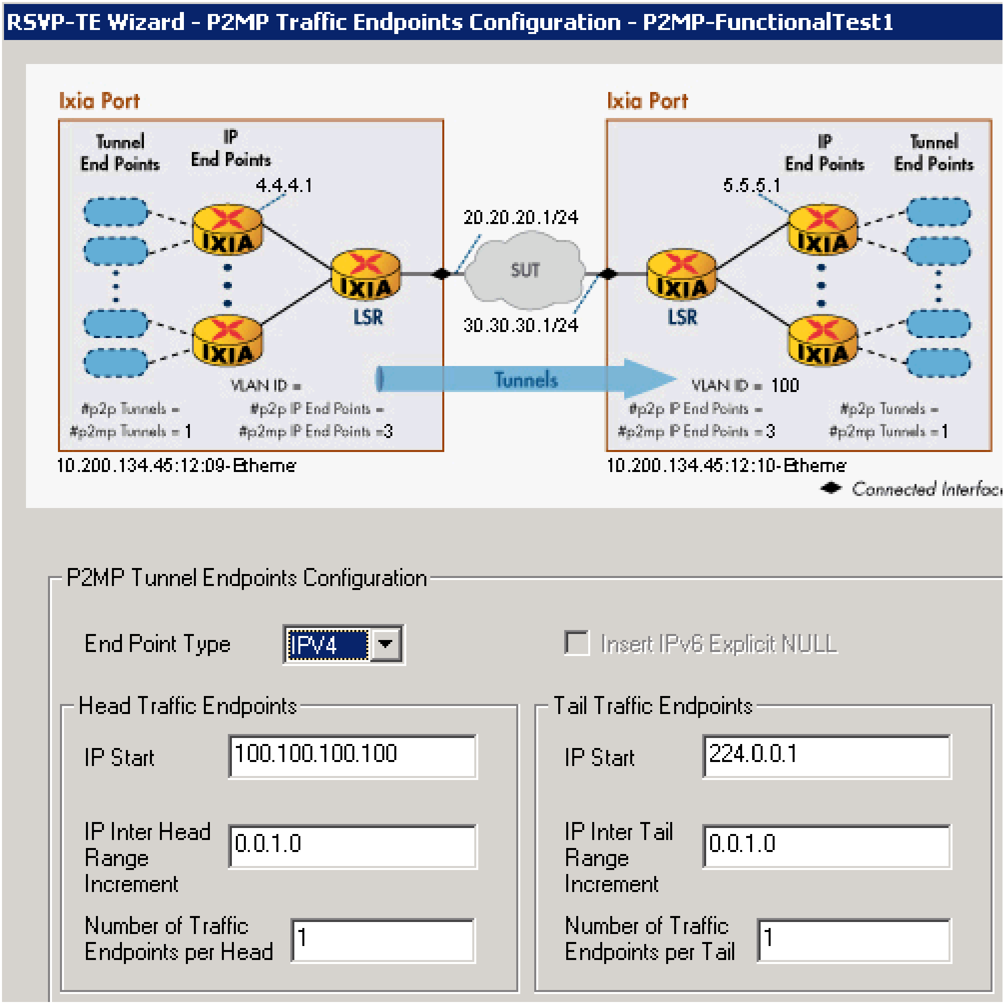


Figure 34. P2MP wizard screen #4 of 9

5. Skip screens 5,6 and 7 (or change them as needed) and proceed to screen 8. Input meaningful values so that the P2MP tunnel is sent with appropriate bandwidth requirements. Note that the units are bytes per second for rates, and bytes for all other fields.

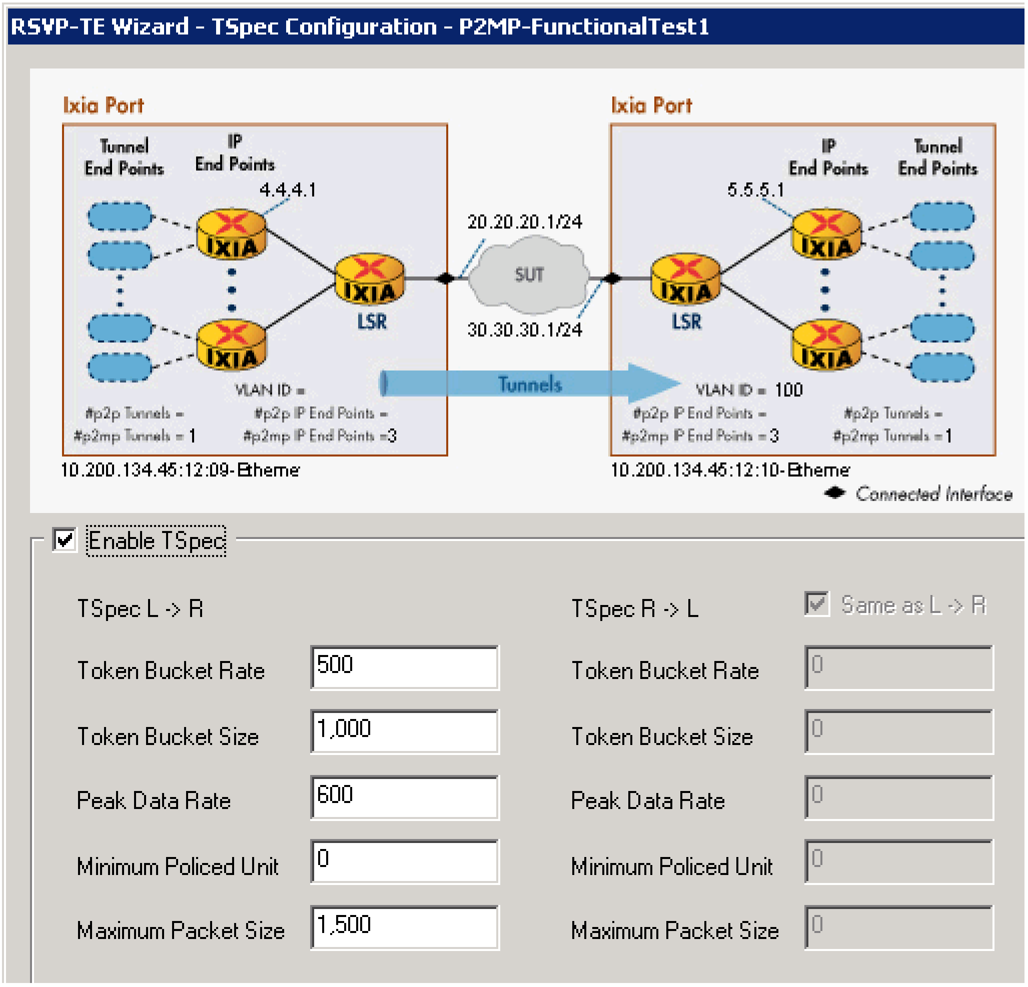


Figure 35. P2MP Wizard Screen #8 of 9

6. In the last screen of the wizard, give this configuration an appropriate name and then select **Generate and Overwrite Existing Configuration**.

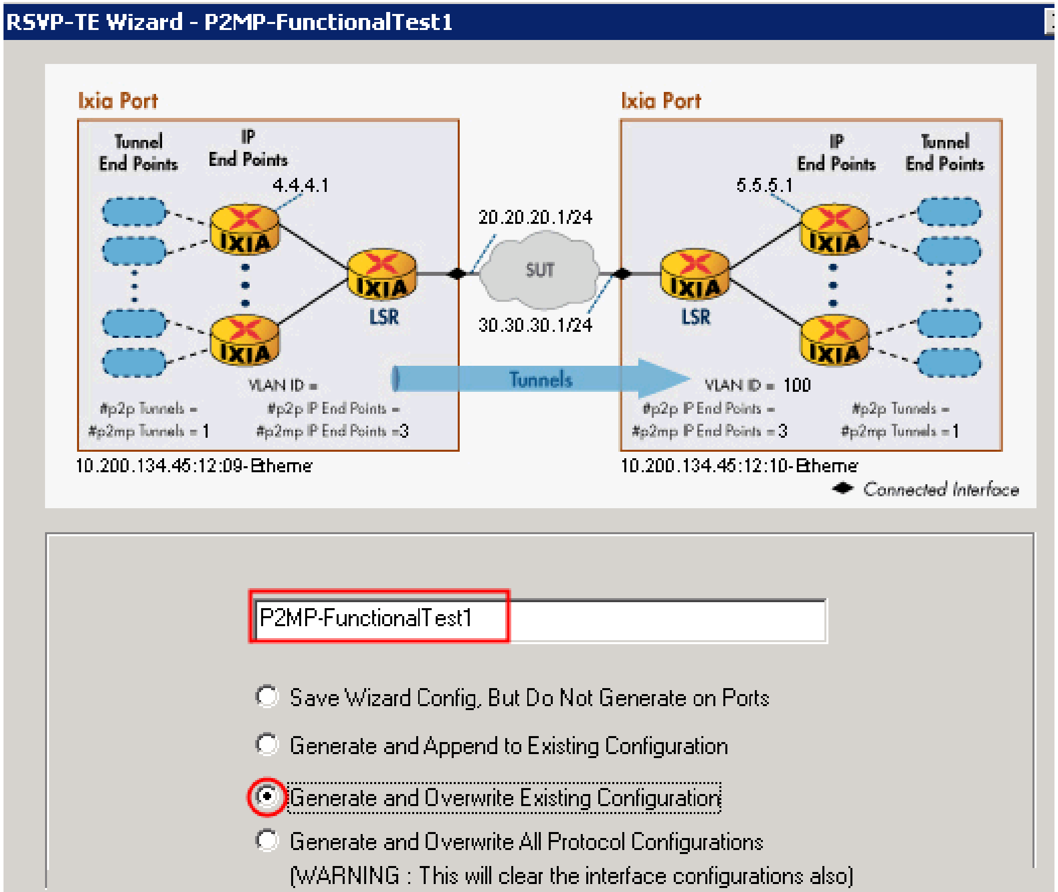


Figure 36. P2MP Wizard Screen #9 of 9

7. After the configuration is generated, you may inspect the IP addresses that were generated. Select the **Connected Interfaces** tab (Figure 37) – these correspond to the LSRs that connect directly to the DUT. **Unconnected Interfaces** (Figure 38) correspond to the leaf nodes behind the connected LSRs. Ixia emulates a branching node in front of the leaf nodes for high scalability.

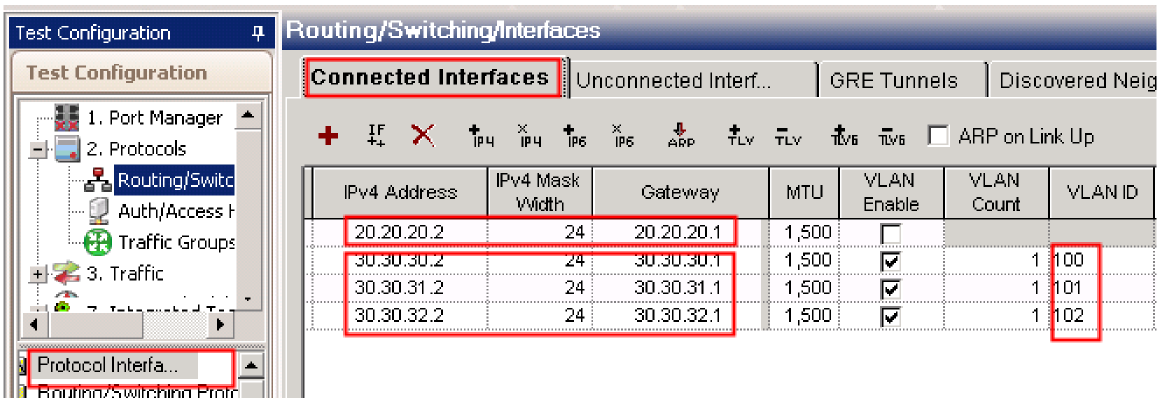


Figure 37. Connected interfaces

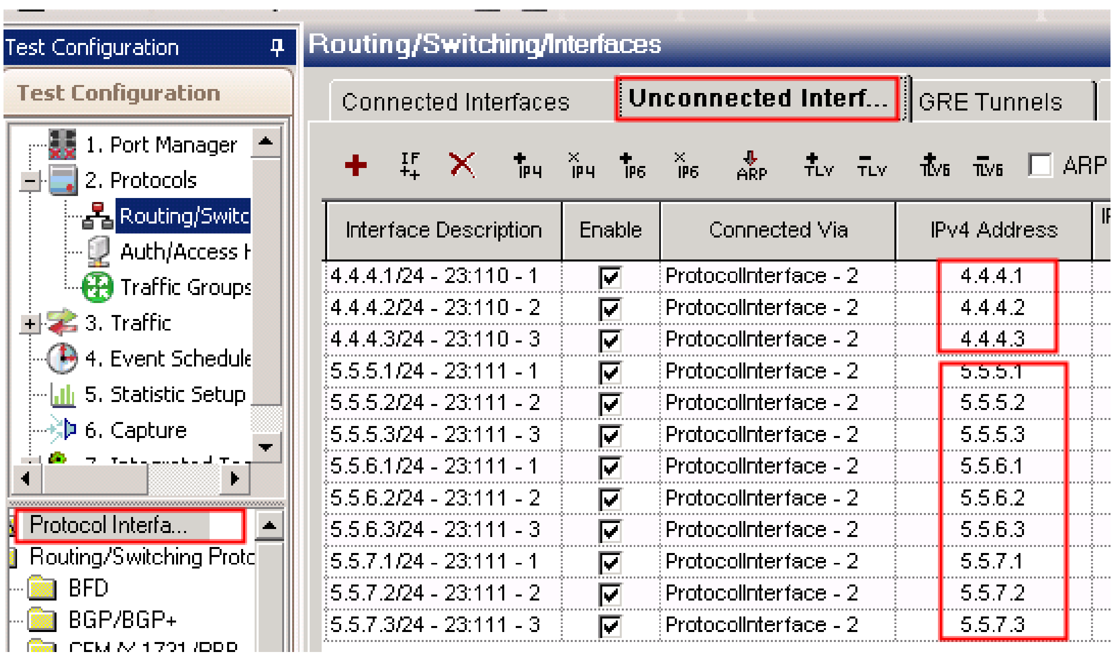
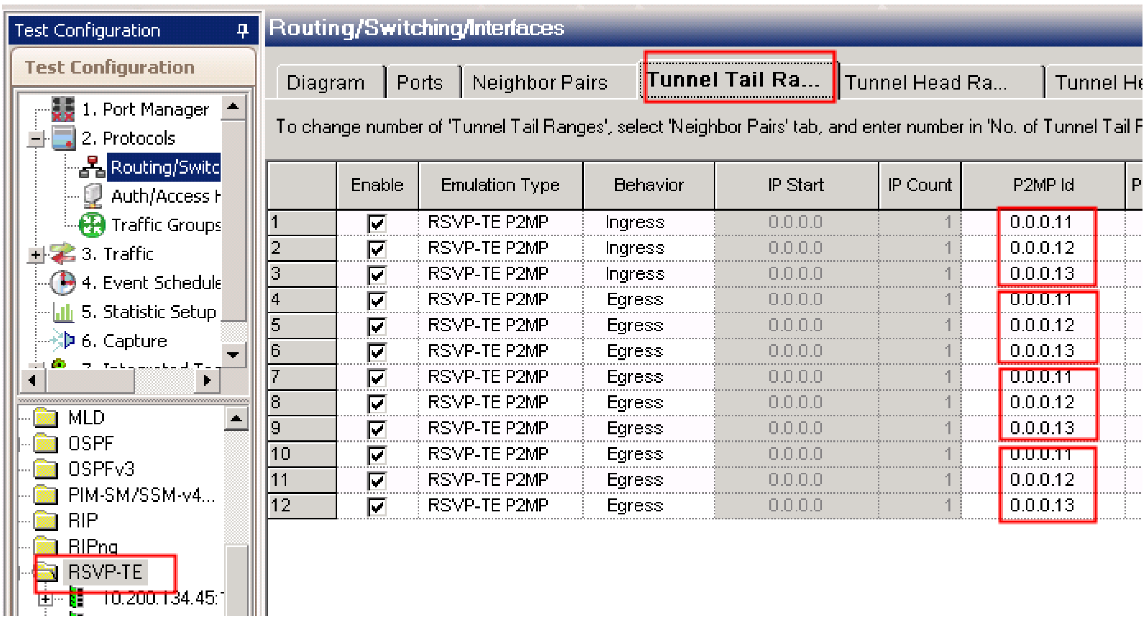


Figure 38. Unconnected interfaces

8. Select the **Tunnel Tail Ranges** tab and examine the number of **P2MP IDs** created to ensure that they have the right quantity of unique numbers. Each unique number corresponds to a separate P2MP tree.



	Enable	Emulation Type	Behavior	IP Start	IP Count	P2MP Id
1	☑	RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.11
2	☑	RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.12
3	☑	RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.13
4	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.11
5	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.12
6	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.13
7	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.11
8	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.12
9	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.13
10	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.11
11	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.12
12	☑	RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.13

Figure 39. Tunnel Tail Ranges

9. In order to manually adjust the number of leaf nodes in the second neighbor, select the **Tunnel Leaf Ranges** tab and manually change the **IP Count** for the second neighbor (this corresponds to IP 5.5.6.1 in Figure 40) from *3* to *2*.

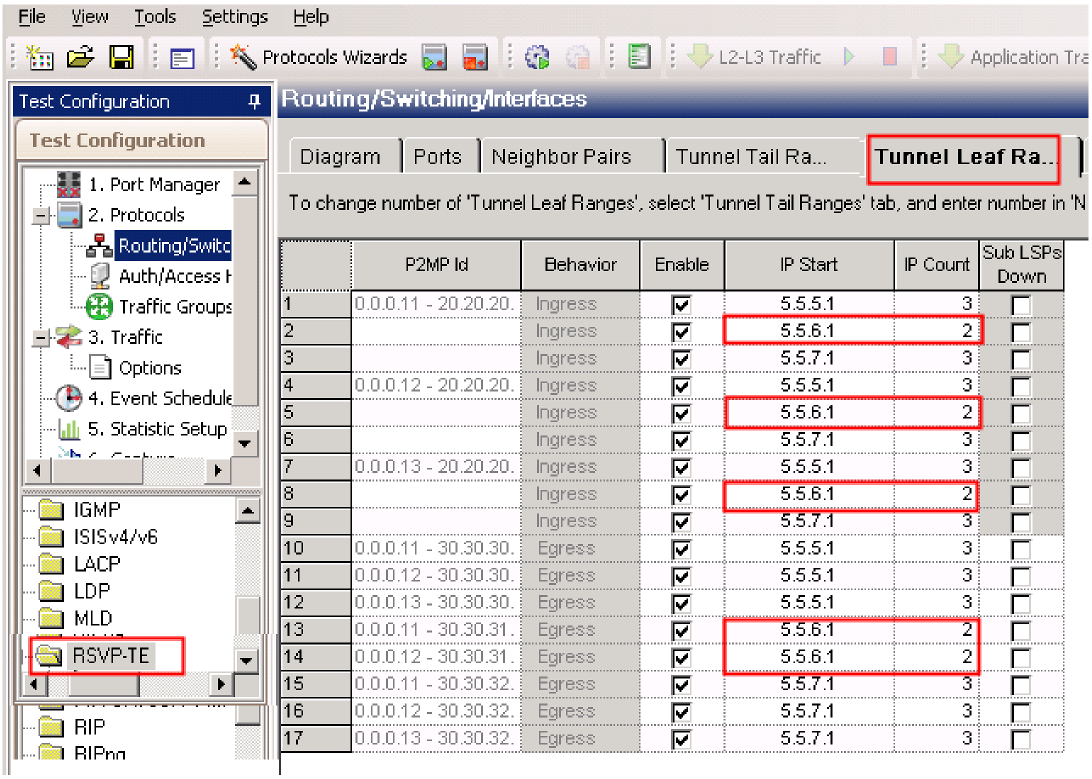


Figure 40. Tunnel Leaf Ranges

10. One tip to aid troubleshooting is to configure each of the neighbors to use a different start label value so that if something doesn't work, you can easily identify which neighbor is not working based on the label value.

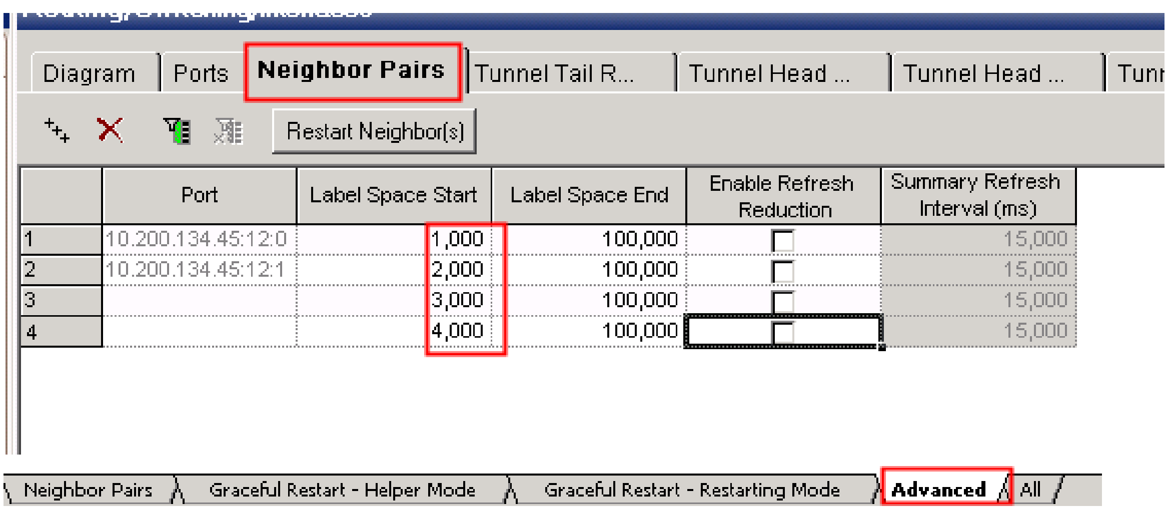


Figure 41. Neighbor Pairs to Change Label Start Value

11. Once you're certain that the generated configuration exactly matches what the test calls for, you may go ahead and start all protocols by clicking on the **Start All Protocols** button near the top of the window. This will start not only RSVP-TE as well as the dependency protocol OSPF-TE.

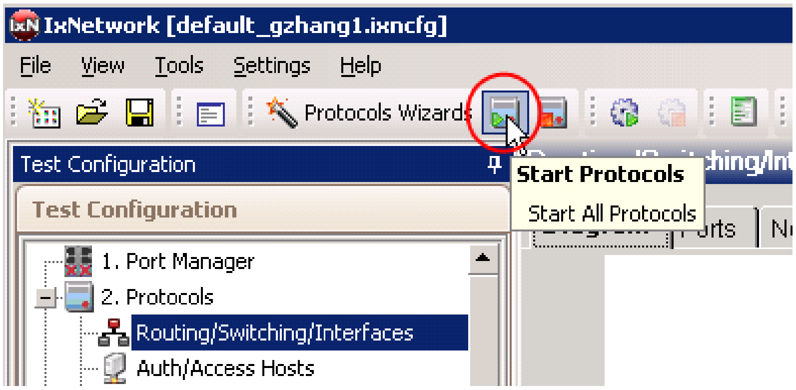


Figure 42. Start All Protocols

12. The quickest way to verify that all P2MP LSPs and sub-LSPs are up is by going to the RSVP-TE protocol statistics display as shown below. There should be 3 P2MP LSPs (or tunnels) since there are 3 senders. There are 24 sub-LSPs because there are 3 LSPs, each trying to reach 8 leaf nodes distributed across 3 VLANs. You can tell that the DUT worked exactly as expected in Figure 43.

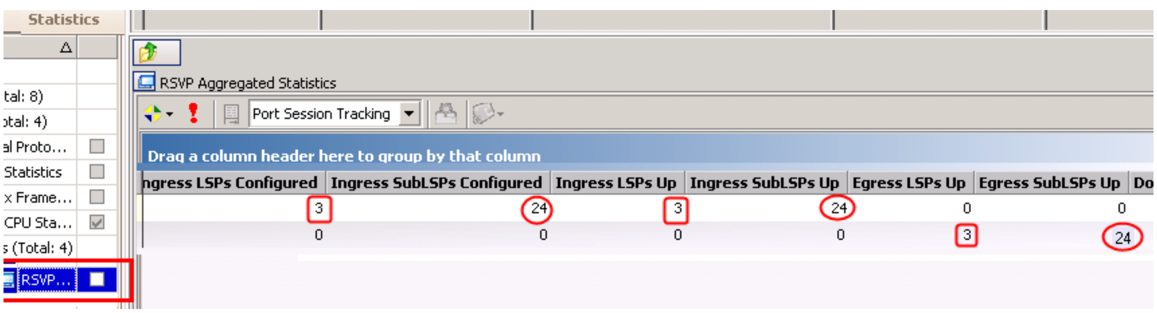


Figure 43. Overall Protocol Statistics

13. In addition to the high-level view of the total numbers of **LSPs Up** shown above, IxNetwork provides comprehensive RSVP-TE state machine statistics, as shown in Figure 44. In most cases, the statistics themselves may tell you what is wrong when some of the LSPs are not up.

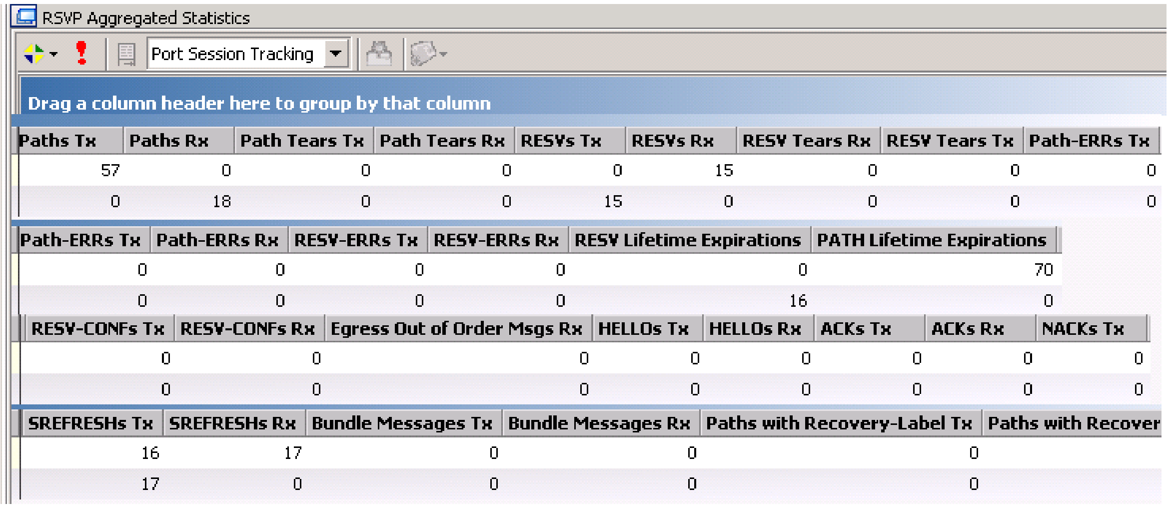


Figure 44. Comprehensive protocol engine statistics

14. In addition, Analyzer provides bidirectional capture of control plane packets and may be used to troubleshoot setup issues easily.

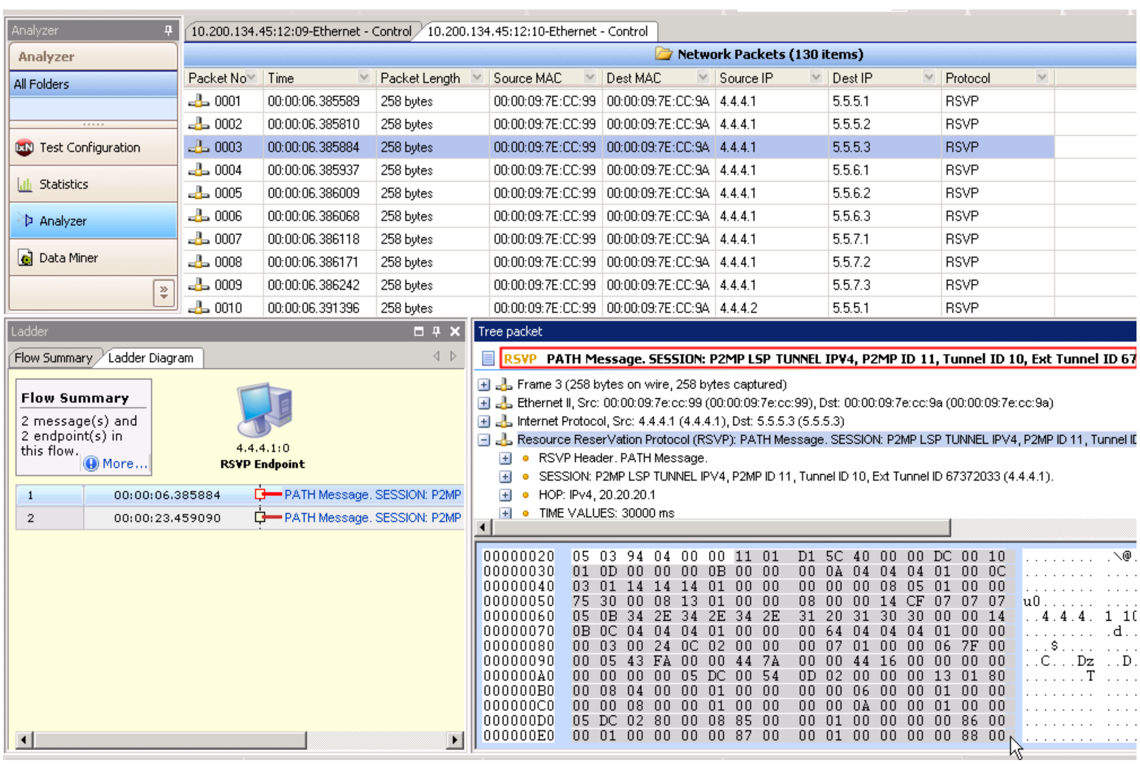


Figure 45. IxAnalyzer for Bi-directional protocol capture and decode

15. To get a complete view of the status of all LSPs, you may go to the **Port Learned Info** to list all LSPs and sub-LSPs and their status for that physical port, as well as detailed configuration parameters associated with the LSP.

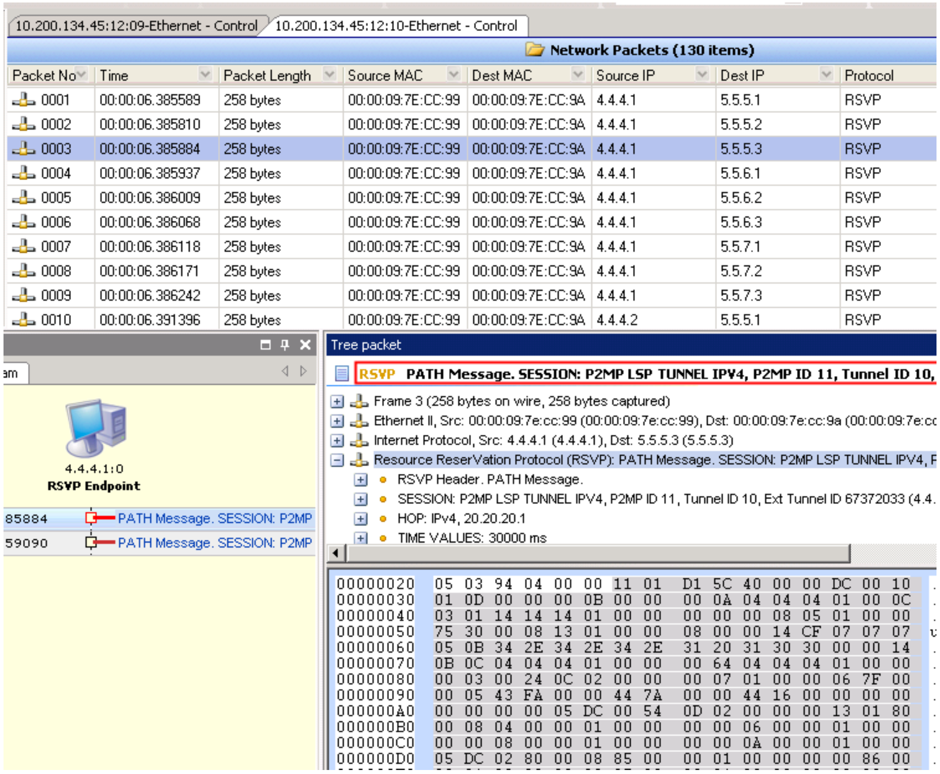


Figure 46. Port Learned info to aid troubleshooting

16. There are situations in which the sub-LSPs were initially up but gradually go down. In order to save memory, IxNetwork will by default discard these sub-LSPs. If you want to keep the dead LSPs visible in the **Port Learned Info**, enable the feature called **Store Down LSP** under the **Neighbor Pairs** tab before you start the protocol.

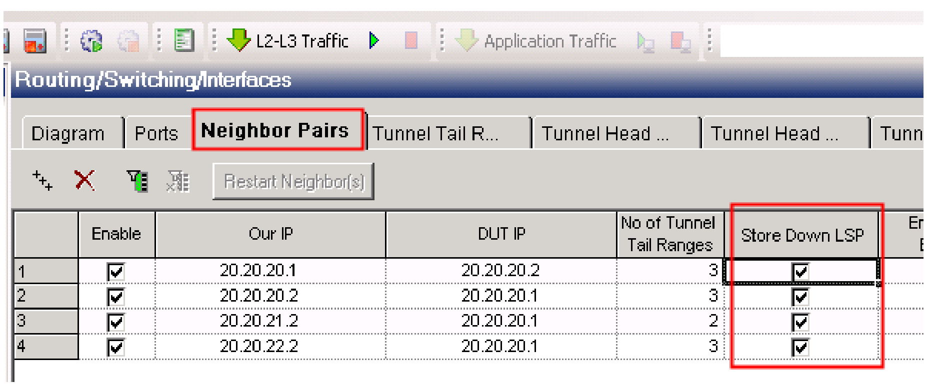


Figure 47. Enable/disable store down LSP

17. Launch the advanced traffic wizard. Set **Source/Dest Mesh** to **Many-Many** and **Route Mesh** to **Fully Meshed**. The **Merge Destination Range** option should be checked. This is to ensure correct measurement for multicast traffic. In the **Source** list, expand the **All Ports** list and select **RSVP Head Ranges**. In the **Destination** list, expand the **All Ports** list and select **RSVP Tail Ranges**. Click the add endpoint sets icon.

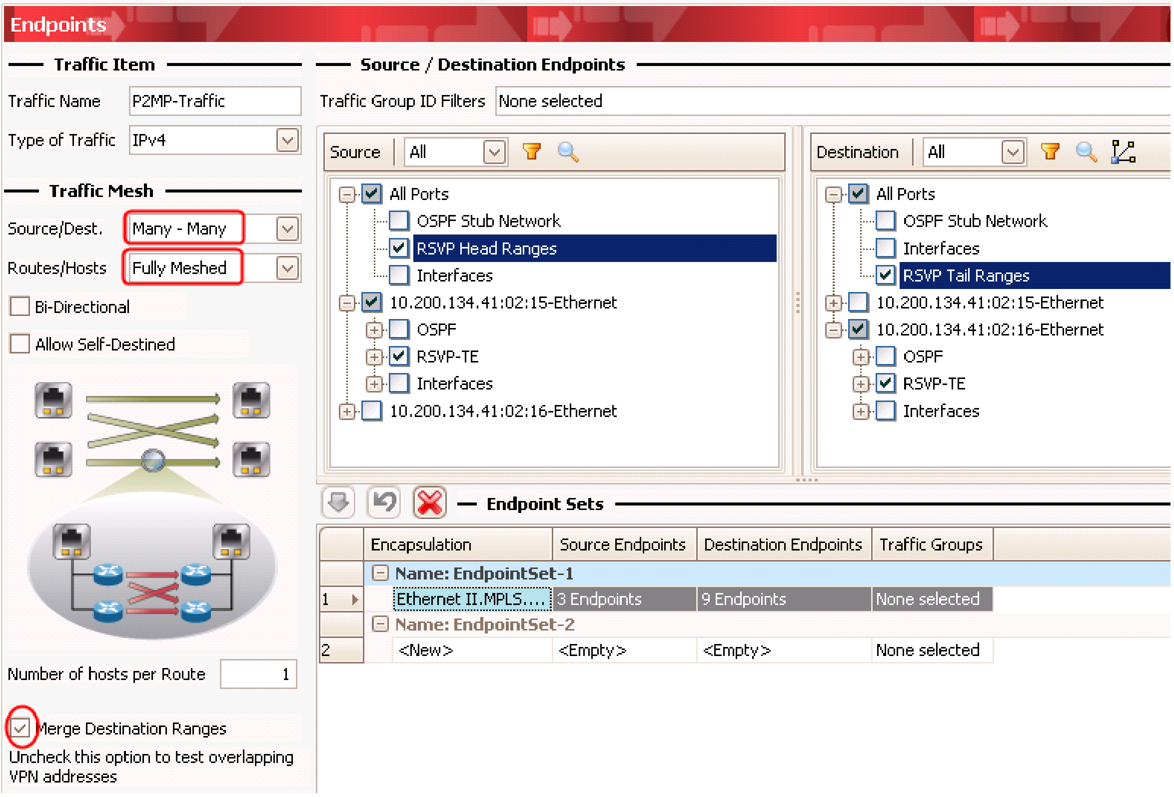


Figure 48. Advanced traffic wizard used to construct P2MP traffic items

18. Skip the next few wizard pages and go to **Flow Tracking**. Select **MPLS: Label Value** and **IPv4: Destination Address**. This will track per-flow stats for the selected fields.

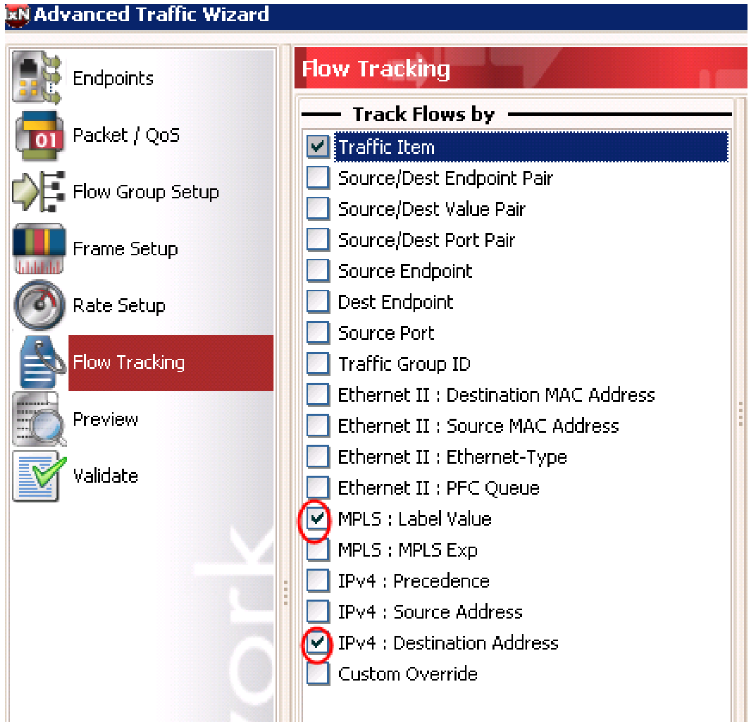


Figure 49. Flow Tracking for P2MP Traffic

19. If there are any traffic generation errors, resolve them before proceeding. Once error-free traffic is created, you may push the traffic definition to the Ixia hardware by clicking **L2-L3 Traffic**. Then start traffic by clicking the green triangle symbol.

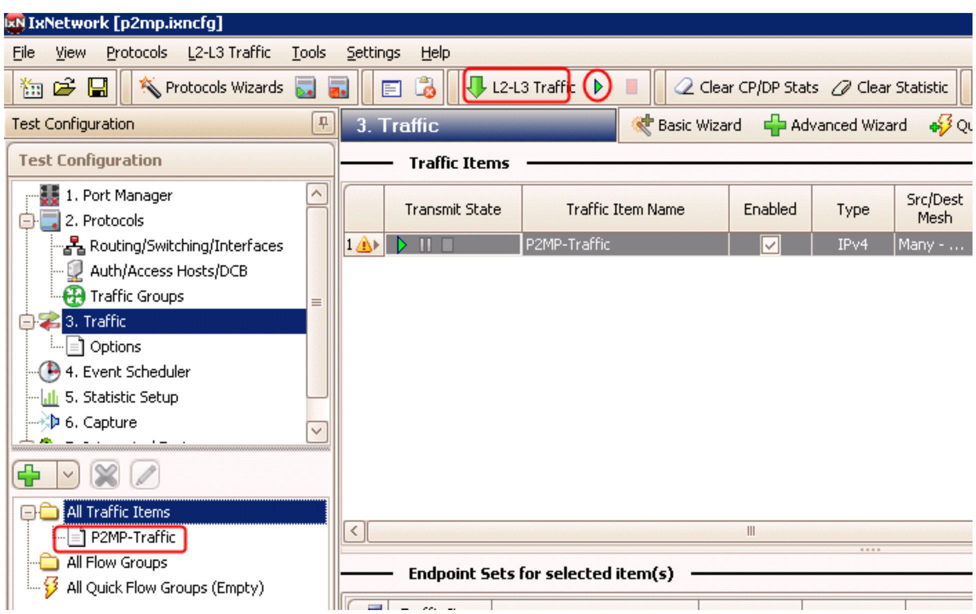


Figure 50. Push traffic streams to hardware and start traffic

20. View per-flow statistics by going to the **Statistics** tab on the main window and clicking on **Traffic Item Statistics**. This will provide an overview of traffic for all RSVP-TE neighbors. In case of loss, right-clicking on the traffic items statistics allows you to select a drill down level view for any tracking items previously selected. The drill down view provides important troubleshooting details and allows quick isolation of troubled LSP.

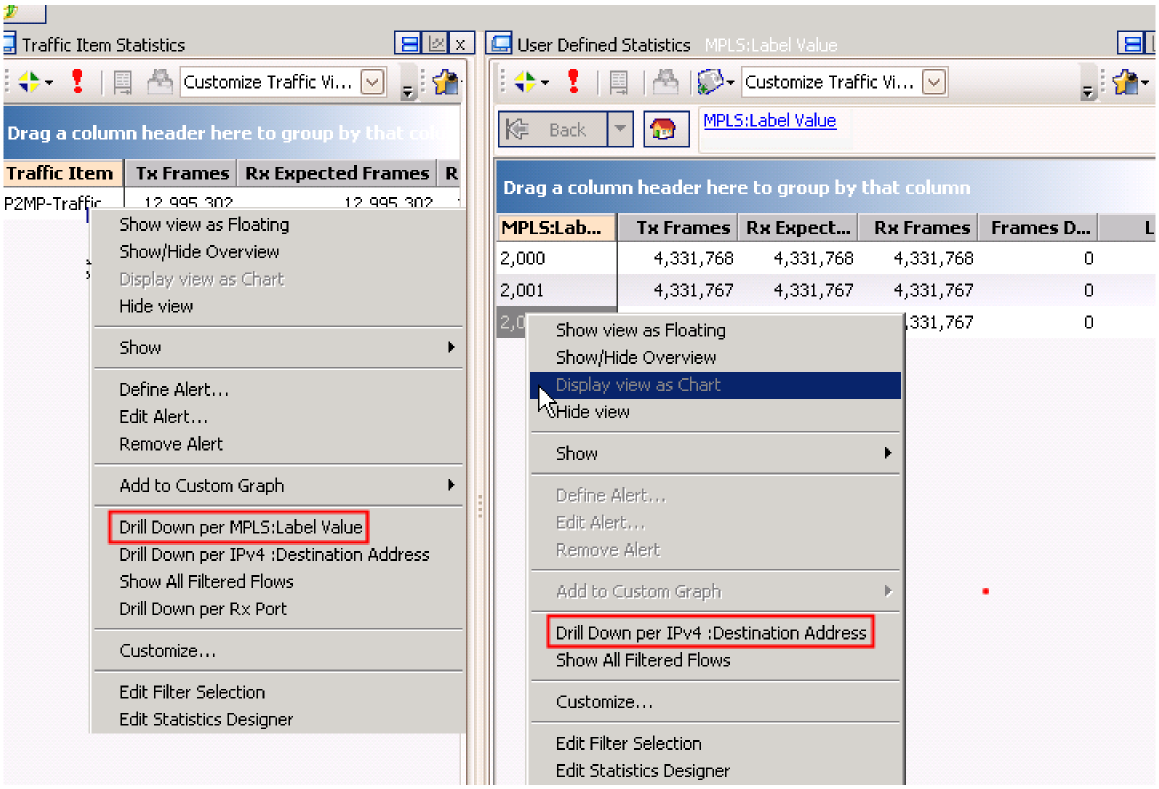


Figure 51. Multi-level Drill Down Per Flow Statistics

Test Variables

For functional test, the key is to cover all the basic functions of the DUT. The test may be easily expanded to test the following list of key features. IxNetwork P2MP emulation software may be used to cover all of these test variables.

- Add more test ports to test DUT branching capability on a physical port
- Test DUT branching on both physical ports and VLAN sub-interfaces
- Test DUTs acting as a root or leaf
- Test DUT's ability to handle EROs and SEROs
- Test DUT's ability to handle refresh and message bundling
- Test DUT's ability to perform fast reroute and measure convergence time

Results Analysis

If the test is set up correctly, the control plane statistics will show a matching amount of **Ingress LSPs Configured** and **Ingress LSP Up** at the root port and **Egress LSP Up** at leaf ports. This indicates that P2MP tunnels are all up from both the ingress and egress points of view. Moreover, the **Ingress SubLSPs Configured** and **Ingress SubLSPs Up** at the root port should match the **Egress SubLSPs Up** at the leaf port. This indicates that all sub-LSPs are up and all tunnels from root have reached all intended leaf nodes.

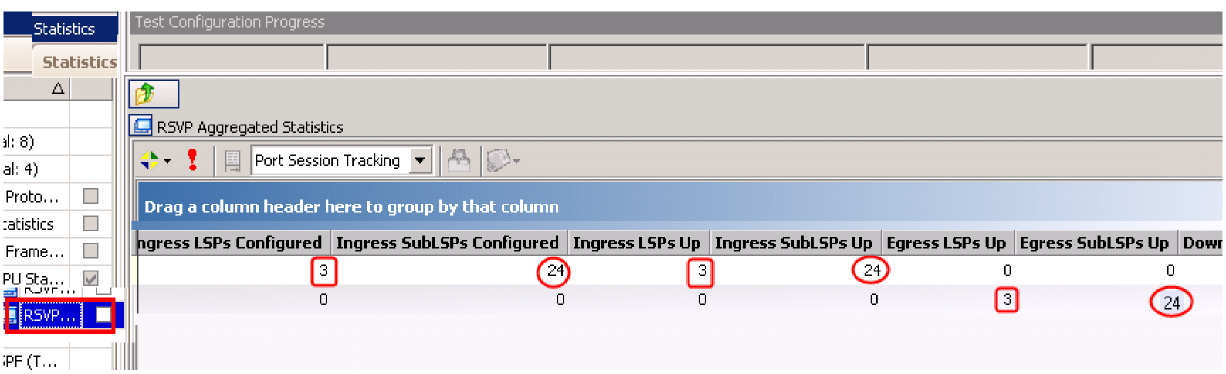


Figure 52. Control plane statistics

In case of full or partial failure, **Port Learned Info** may be used to provide a comprehensive summary of LSPs and sub-LSPs. It's very easy to spot bad LSPs from this page. If there are a large number of LSPs, filters are available to identify and isolate the specific LSPs of interest. Don't forget LSPs that have been dead for a long time are automatically removed from memory. If you want to keep them in memory, you should enable **Store Down LSP** under **Neighbor Pair** in the main protocol GUI before you start protocols (see Step 16).

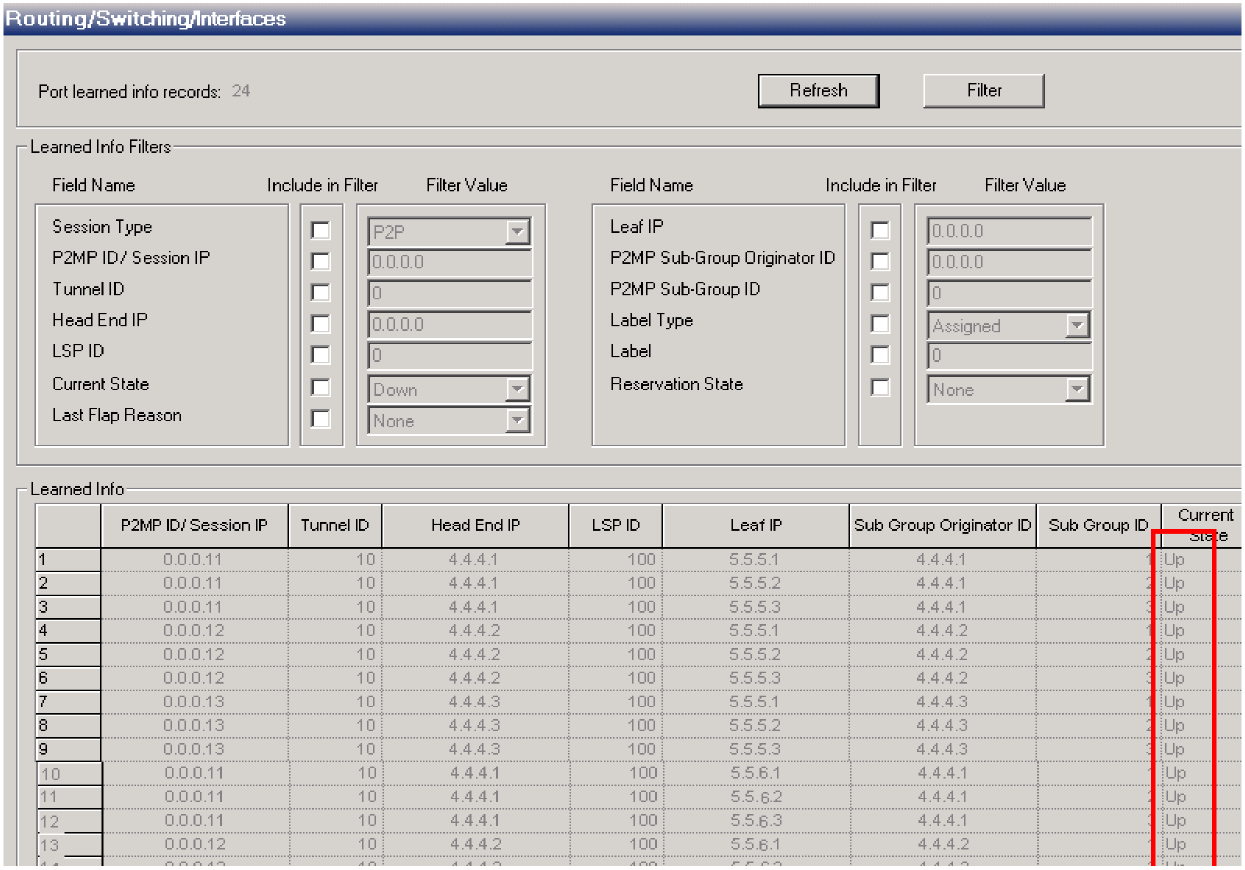


Figure 53. Port learned info for troubleshooting and single page view of all Sub-LSPs

From the data plane perspective, all flows should pass traffic without frame loss. In the case of frame loss, you can drill down on the MPLS label to see which labels are experiencing losses. You can also open the packet editor on the traffic wizard using the flow group property and examine the list of labels placed in the packets. In case of doubt, go to **Port Learned Info** to find exactly which label was assigned to the sub-LSP by the DUT and by cross checking these values, problems may be easily identified.

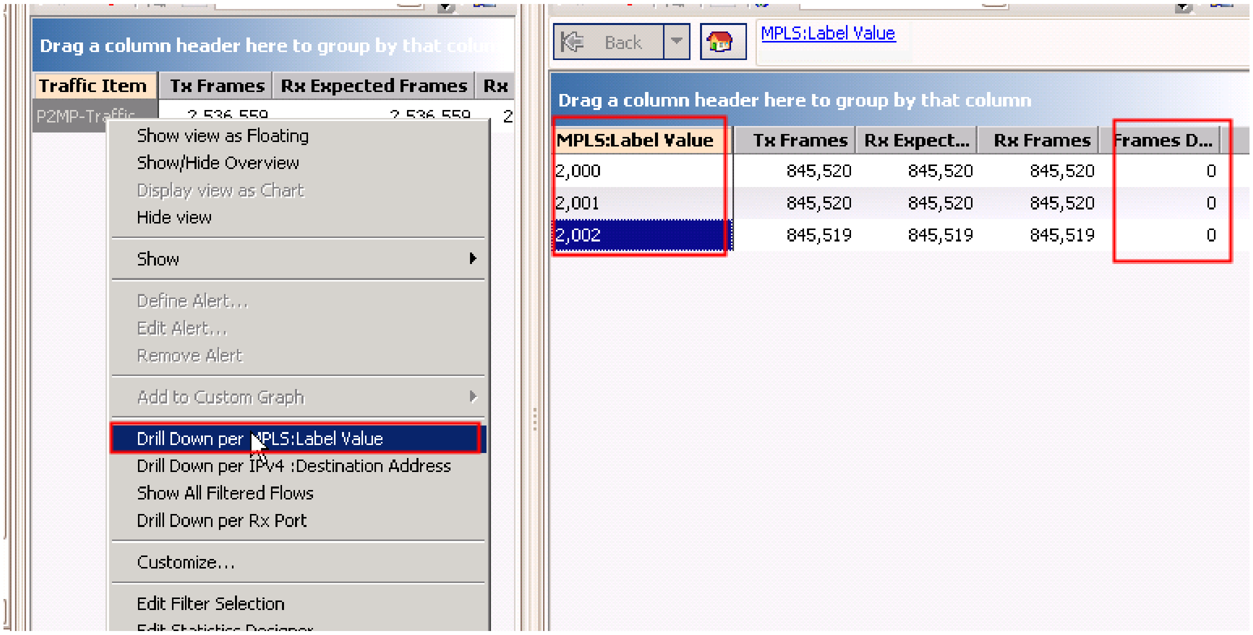


Figure 54. Drill Down Per flow statistics

Troubleshooting and Diagnostics

Problem	Description
Can't Ping from DUT	Check the **Protocol Interface** window and look for red exclamation marks (**!**). If any are found, there is likely an IP address/gateway mismatch.
LSPs won't come up or partially up	• Go to **Port Learned Info** to discover which sub-LSPs are up and which ones are not. Use **Filter** if needed to pinpoint to the exact LSP in question. • Enable **Store Down LSP** under **Neighbor Pairs** to allow the **Learned Info** to store dead LSPs indefinitely. • From the **Test Configuration** window, turn on **Control Plane Capture**, then start Analyzer for a real-time sniffer decode between the Ixia Port and the DUT port.
After stop/start protocols or link down/up Traffic 100% loss	Check the **Warnings** columns in the **Traffic** view and make sure there are no streams that say *VPN label not found*. The DUT may have sent new label info. If so, regenerate traffic by right-clicking the traffic item. Then **Apply** traffic.
Traffic statistics are not correct	Make sure the needed traffic options are enabled as described in step 17 and 19.
Not all sub-LSPs are up and it's hard to tell which ones are not	One tip is to assign different label spaces for different neighbors (as described in step 10). Based on the label value it may be easily spotted which neighbors contain bad sub-LSPs. The wizard, by default, will generate the same label start value for all neighbors.

Conclusions

RSVP-TE P2MP emulation software in IxNetwork is a feature rich and comprehensive testing tool. It covers all major protocol features typically implemented by a DUT. The protocol wizard is easy to use and very flexible, not only for functional tests but also for scalability test. IxNetwork includes many built-in troubleshooting utilities which allow you to quickly identify and isolate problems. The traffic wizard allows you to send traffic with specified endpoints over the correct P2MP tunnel. Statistic displays provides an instant indication of whether or not there are any problems from either the control or data plane.

Test Case: P2MP Scalability Test

Overview

P2MP scalability testing is a bit more challenging than feature testing. There are a number of ways to scale up a test; each of them will test DUT scalability, measuring multiple limits. Figure 55 illustrates different dimensions in which a test may be scaled up, labeled **D1** through **D4**.

- **D1**: By simply increasing the number of emulated leaf nodes per neighbor, you may discover the maximum number of leaf nodes supported by a DUT, and the maximum number of sub-LSPs that may be sustained by a DUT.
- **D2**: By increasing the number of neighbors or the number of sub-interfaces, you may find the maximum number of VLANs a DUT can branch either on a single physical interface or as a whole. This usually is determined by a DUT's ability to replicate labels on a per-interface or per-system level, which is a key measurement of system performance.
- **D3**: By increasing the number of root nodes (head end of the tunnel), you may determine the maximum number of P2MP tunnels (or trees) that a DUT can sustain with unique head end info and P2MP IDs.
- **D4**: Even with the same set of root and leaf nodes, you may also increase the number of tunnels (as identified by unique tunnel ID) or the number of tunnel instances (as identified by unique LSP ID). Both may be used to discover the tunnel, LSP and sub-LSP capacity of a given DUT.

In real-world scenarios, it usually takes a combination of all of the above to truly identify system limits.

Objective

The test objective is to discover whether or not the DUT can establish and maintain:

- Ten P2MP trees with five distinct root nodes to reach the same set of 20 leaf nodes
- The 20 leaf nodes are separated by five distinct VLANs
- Each of the 10 P2MP trees contains 20 unique P2MP tunnels
- Each of the 200 P2MP tunnels contains 5 unique LSP instances

This test is designed to reveal whether the DUT can handle the following capacity requirements: 10 P2MP Trees, 200 P2MP Tunnels, 1000 P2MP LSP Instances and 20,000 P2MP sub-LSPs.

Setup

Two Ixia test ports are used to emulate root and leaf nodes that surround the DUT with the specified number of nodes.

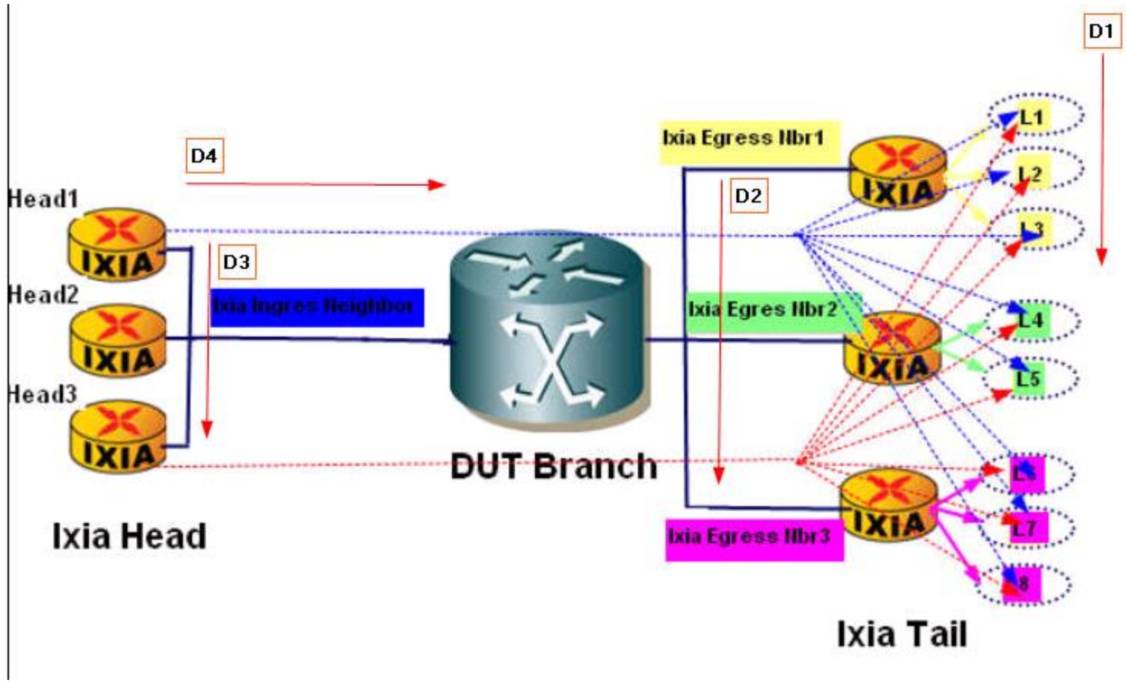


Figure 55. P2MP test setup allows many dimensions for scalability test

Step-by-Step Instructions

1. Launch the RSVP-TE Wizard and select SUT = Transit, set Emulation Type = P2MP, and Tunnel Configuration = Fully Meshed.

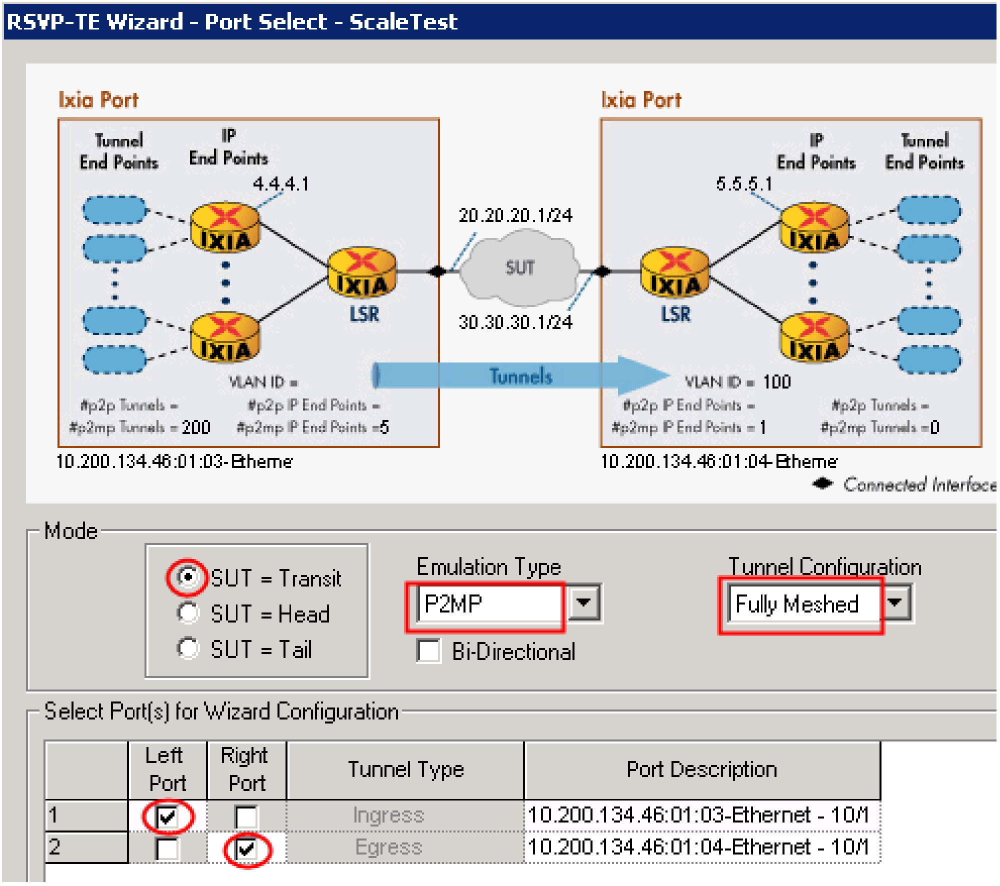


Figure 56. P2MP wizard screen #1 of 9

2. We strongly recommended that you enable both SRefresh and Bundle Message Sending for scalability test. Enter 1 and 5 as the number of neighbors for the root port and leaf port respectively. As an aide, a yellow box with a letter has been placed alongside the parameter value to indicate which dimension the parameter is for (refer to the dimension explanation of D1, D2, D3 and D4 above). Make sure Enable VLAN is checked and enter an appropriate VID and step size.

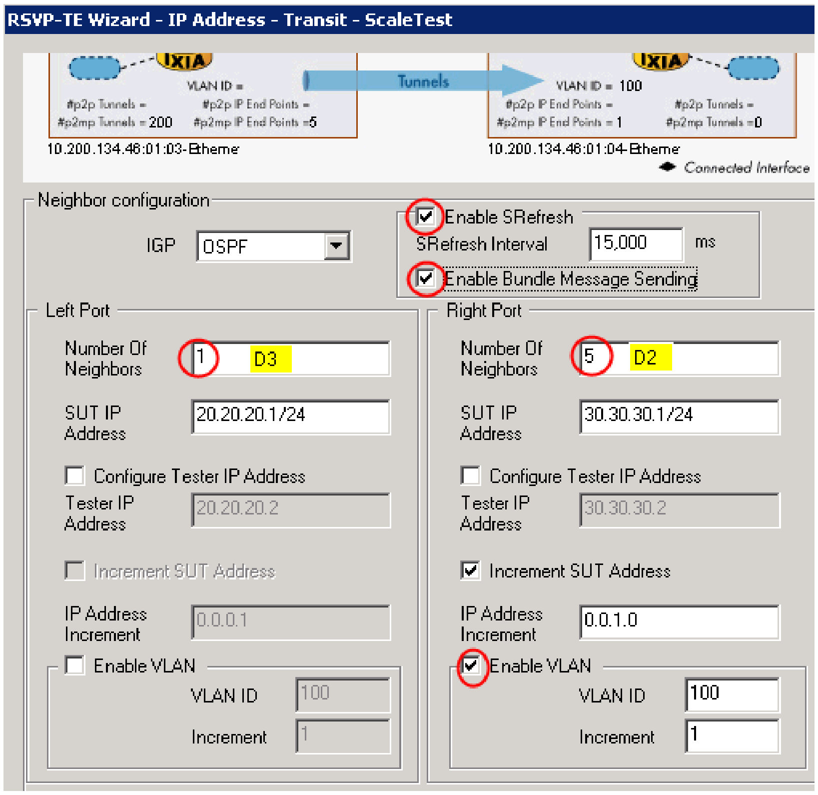


Figure 57. P2MP wizard screen #2 of 9

3. Set the **Number of IP Endpoints per Neighbor (Head)** to *5* to simulate 5 unique root nodes. Set the **Number of IP Endpoints per Neighbor (Tail)** to *4* for each of the 5 egress neighbors to simulate a total of 20 leaf nodes. Under **Number of P2MP IDs**, enable **Per Sender** and enter *2*. This will generate 10 unique P2MP IDs to simulate a total of 10 P2MP trees. Note that in order to make sure each tree is using different IDs, it's necessary to enable both **Inter-** and **Intra–Sender P2MP ID Increment**. Enter *20* as the number of **Tunnels per P2MP** to create a total of 10*20=200 P2MP tunnels. Also enter *5* in **LSP Instances per Tunnel**. This will create a total of 200*5=1000 P2MP LSP Instances. Enter the appropriate values for **Tunnel ID Start** and **LSP ID Start**.

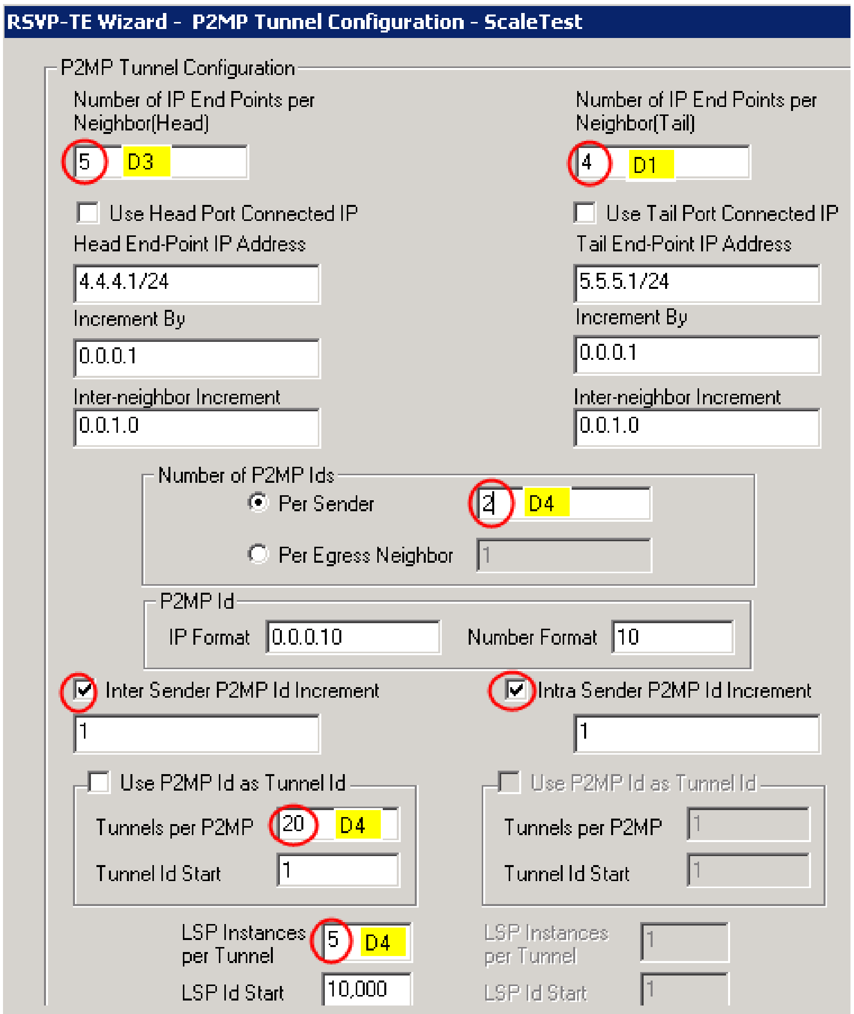


Figure 58. P2MP wizard screen #3 of 8

4. Skip the rest of the wizard screens or make changes on them as needed and scroll through to the last page of the wizard. If needed, you may refer to the functional test for explanations of the screens and parameters. Give an appropriate name and select **Generate and Overwrite Existing Configuration.**

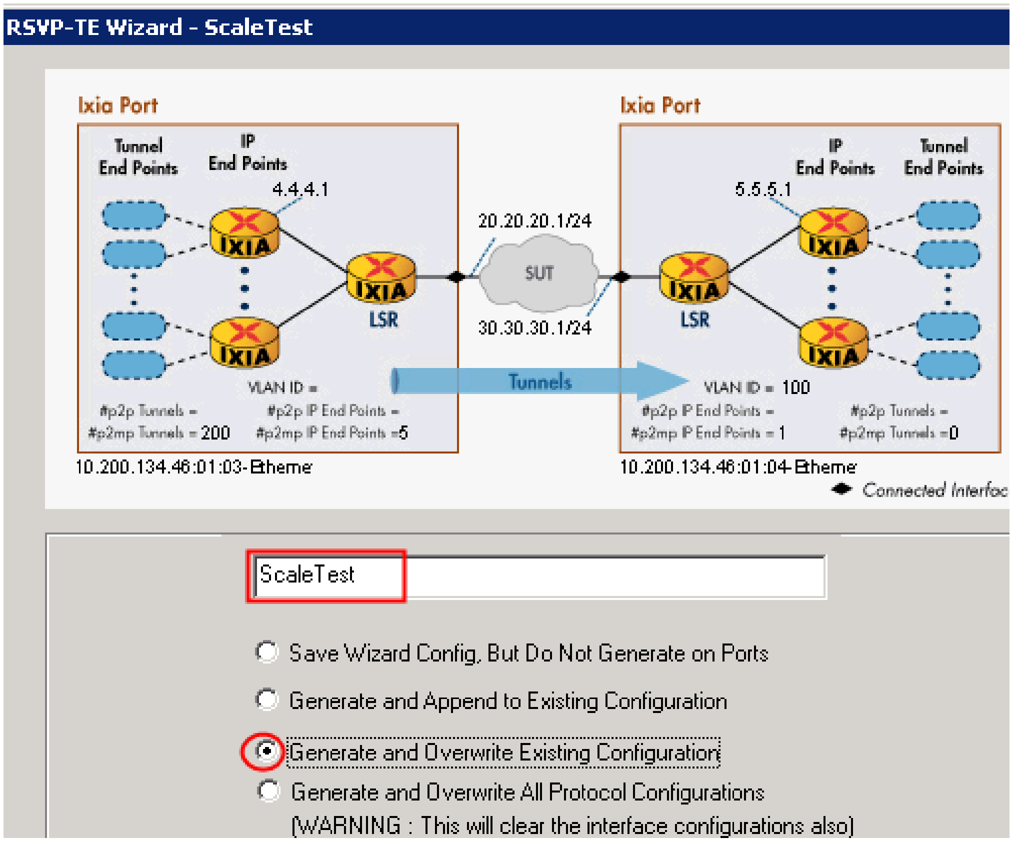
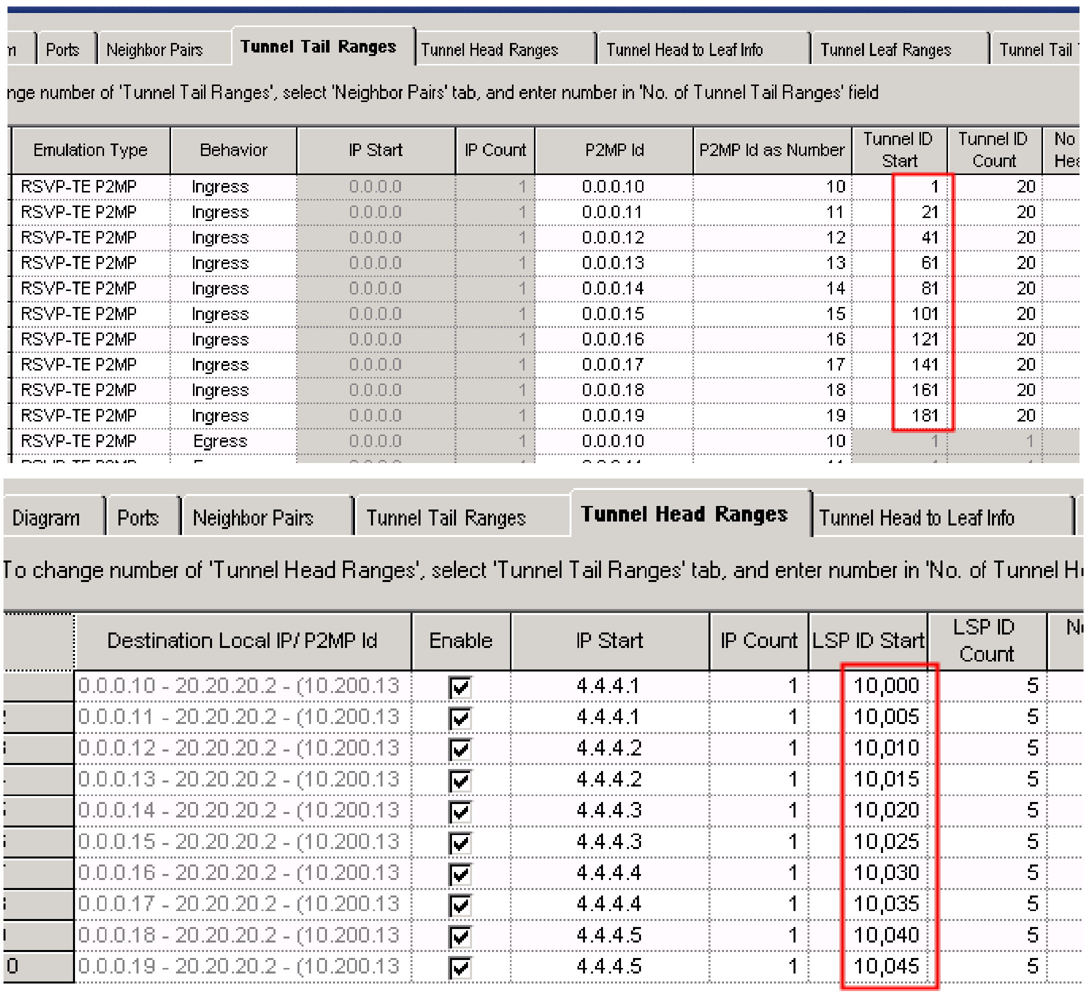


Figure 59. P2MP wizard screen #9 of 9

5. Visually examine the configuration generated by the protocol wizard and make adjustments as required by the DUT. For example, by default the wizard will use the same tunnel ID (1-20) for all tunnels belonging to different P2MP trees. This is fine. If you want each tunnel to use a unique tunnel ID to aid troubleshooting when something doesn't work, however, you may optionally click on the **Tunnel ID Start** column and right-click for **Increment by** and then enter a value of *20*. This will force all tunnels to use different tunnel IDs. In a similar way, you may make the same changes on the LSP IDs as shown below.


n | Ports | Neighbor Pairs | Tunnel Tail Ranges | Tunnel Head Ranges | Tunnel Head to Leaf Info | Tunnel Leaf Ranges | Tunnel Tail

nge number of 'Tunnel Tail Ranges', select 'Neighbor Pairs' tab, and enter number in 'No. of Tunnel Tail Ranges' field

Emulation Type	Behavior	IP Start	IP Count	P2MP Id	P2MP Id as Number	Tunnel ID Start	Tunnel ID Count	No Hea
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.10	10	1	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.11	11	21	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.12	12	41	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.13	13	61	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.14	14	81	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.15	15	101	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.16	16	121	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.17	17	141	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.18	18	161	20	
RSVP-TE P2MP	Ingress	0.0.0.0	1	0.0.0.19	19	181	20	
RSVP-TE P2MP	Egress	0.0.0.0	1	0.0.0.10	10	1	1	

Diagram | Ports | Neighbor Pairs | Tunnel Tail Ranges | Tunnel Head Ranges | Tunnel Head to Leaf Info

To change number of 'Tunnel Head Ranges', select 'Tunnel Tail Ranges' tab, and enter number in 'No. of Tunnel H

	Destination Local IP/ P2MP Id	Enable	IP Start	IP Count	LSP ID Start	LSP ID Count	N
	0.0.0.10 - 20.20.20.2 - (10.200.13	☑	4.4.4.1	1	10,000	5	
	0.0.0.11 - 20.20.20.2 - (10.200.13	☑	4.4.4.1	1	10,005	5	
	0.0.0.12 - 20.20.20.2 - (10.200.13	☑	4.4.4.2	1	10,010	5	
	0.0.0.13 - 20.20.20.2 - (10.200.13	☑	4.4.4.2	1	10,015	5	
	0.0.0.14 - 20.20.20.2 - (10.200.13	☑	4.4.4.3	1	10,020	5	
	0.0.0.15 - 20.20.20.2 - (10.200.13	☑	4.4.4.3	1	10,025	5	
	0.0.0.16 - 20.20.20.2 - (10.200.13	☑	4.4.4.4	1	10,030	5	
	0.0.0.17 - 20.20.20.2 - (10.200.13	☑	4.4.4.4	1	10,035	5	
	0.0.0.18 - 20.20.20.2 - (10.200.13	☑	4.4.4.5	1	10,040	5	
0	0.0.0.19 - 20.20.20.2 - (10.200.13	☑	4.4.4.5	1	10,045	5	

Figure 60. Change P2MP tunnel ID and LSP ID to ensure uniqueness

6. One tip to aid troubleshooting is to configure each of the neighbors to use a different start label value so that if something doesn't work, you may easily identify which neighbor is not working based on label value.

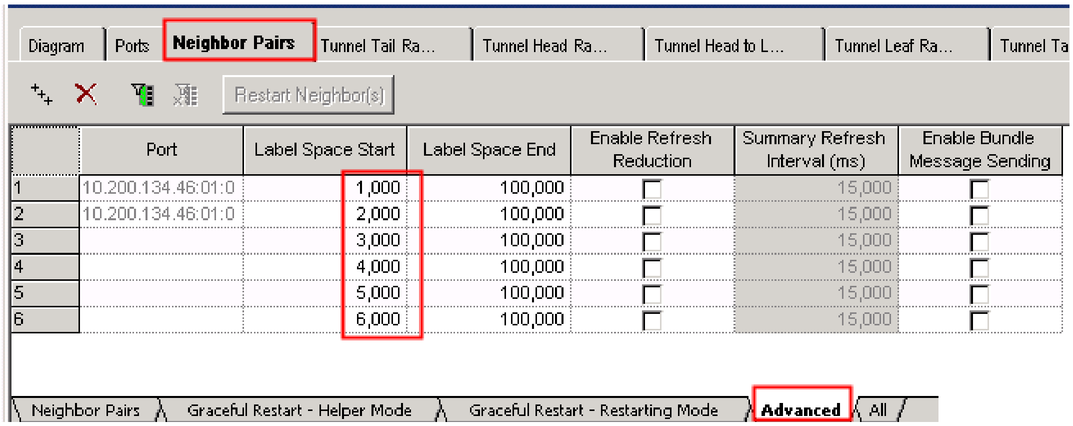


Figure 61. Change label start value

7. After the manual adjustment is complete, you may click **Run All Protocols**. Select the **Statistics** tab and pick **RSVP Aggregated Statistics** from the list. If everything works as expected, you should see a total of 20,000 sub-LSPs and 1,000 LSPs as shown below.

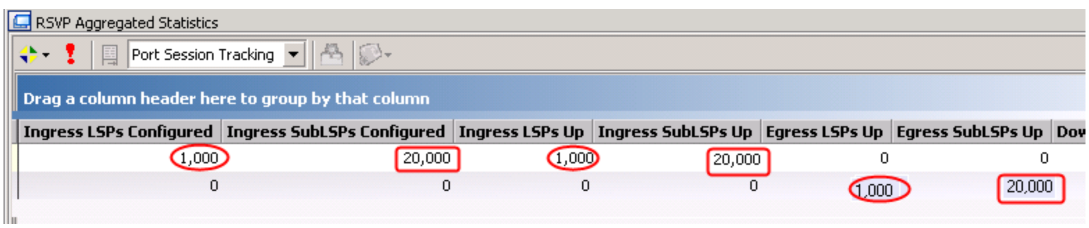
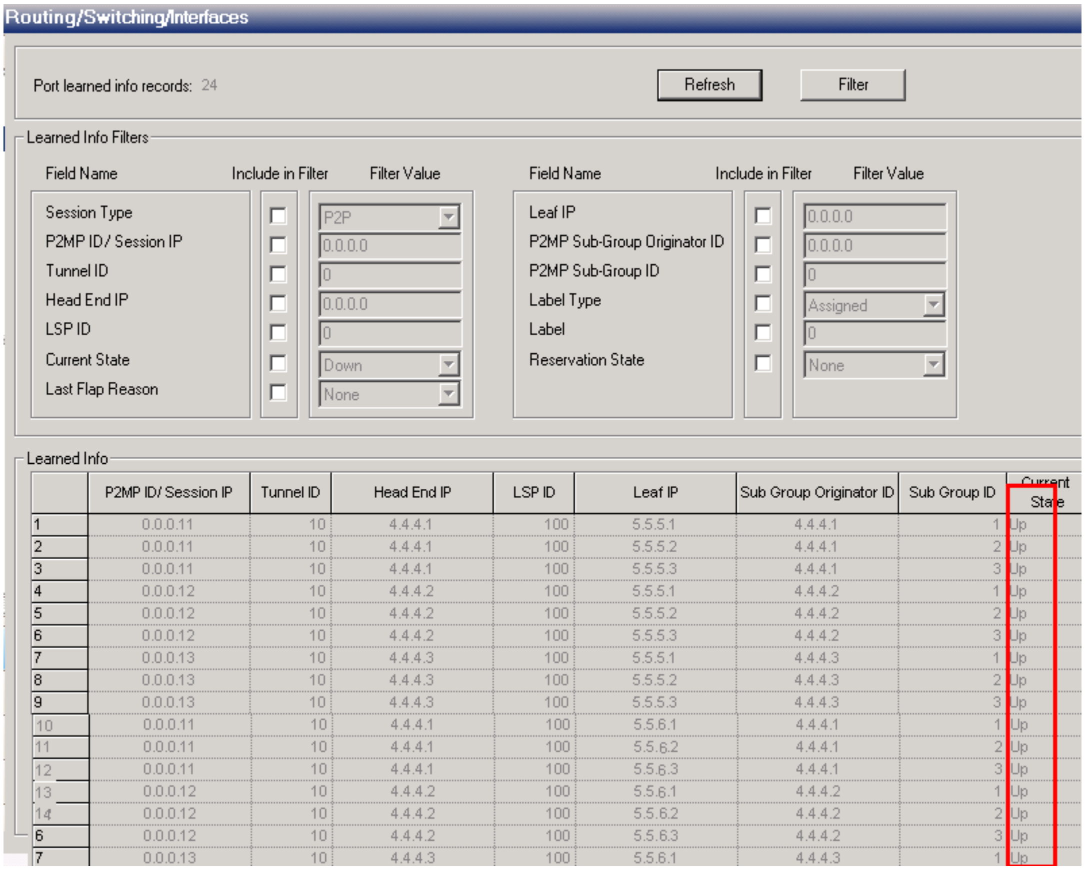


Figure 62. Overall protocol statistics

8. In case only some of the LSP/sub-LSPs are up, you may go to **Port Learned Info** to display all learned LSPs with all the information associated with each LSP.



	P2MP ID/ Session IP	Tunnel ID	Head End IP	LSP ID	Leaf IP	Sub Group Originator ID	Sub Group ID	Current State
1	0.0.0.11	10	4.4.4.1	100	5.5.5.1	4.4.4.1	1	Up
2	0.0.0.11	10	4.4.4.1	100	5.5.5.2	4.4.4.1	2	Up
3	0.0.0.11	10	4.4.4.1	100	5.5.5.3	4.4.4.1	3	Up
4	0.0.0.12	10	4.4.4.2	100	5.5.5.1	4.4.4.2	1	Up
5	0.0.0.12	10	4.4.4.2	100	5.5.5.2	4.4.4.2	2	Up
6	0.0.0.12	10	4.4.4.2	100	5.5.5.3	4.4.4.2	3	Up
7	0.0.0.13	10	4.4.4.3	100	5.5.5.1	4.4.4.3	1	Up
8	0.0.0.13	10	4.4.4.3	100	5.5.5.2	4.4.4.3	2	Up
9	0.0.0.13	10	4.4.4.3	100	5.5.5.3	4.4.4.3	3	Up
10	0.0.0.11	10	4.4.4.1	100	5.5.6.1	4.4.4.1	1	Up
11	0.0.0.11	10	4.4.4.1	100	5.5.6.2	4.4.4.1	2	Up
12	0.0.0.11	10	4.4.4.1	100	5.5.6.3	4.4.4.1	3	Up
13	0.0.0.12	10	4.4.4.2	100	5.5.6.1	4.4.4.2	1	Up
14	0.0.0.12	10	4.4.4.2	100	5.5.6.2	4.4.4.2	2	Up
6	0.0.0.12	10	4.4.4.2	100	5.5.6.3	4.4.4.2	3	Up
7	0.0.0.13	10	4.4.4.3	100	5.5.6.1	4.4.4.3	1	Up

Figure 63. Port learned info display all sub-LSPs in one page

9. Launch the advanced traffic wizard. Set Source/Dest Mesh to Many-Many and Route Mesh to Fully Meshed. The Merge Destination Range option should be checked. This is to ensure correct measurement for multicast traffic. In the Source list, expand the All Ports list and select RSVP Head Ranges. In the Destination list, expand the All Ports list and select RSVP Tail Ranges. Click the add endpoint sets icon.

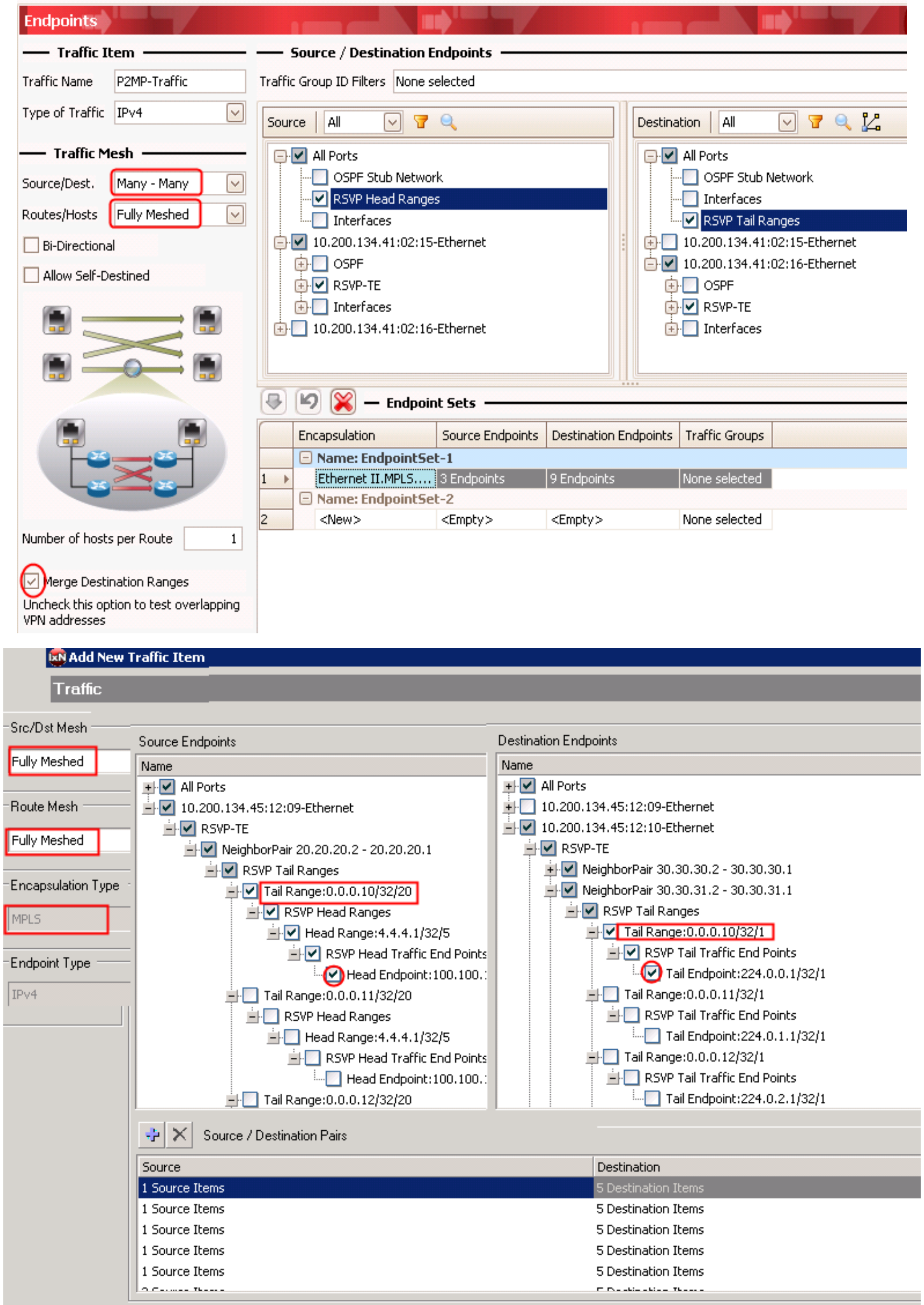


Figure 64. Advanced traffic wizard to set P2MP traffic items

10. Skip the next few wizard pages and go to **Flow Tracking**. Select **MPLS: Label Value** and **IPv4: Destination Address**. This will track per-flow stats for the selected fields.

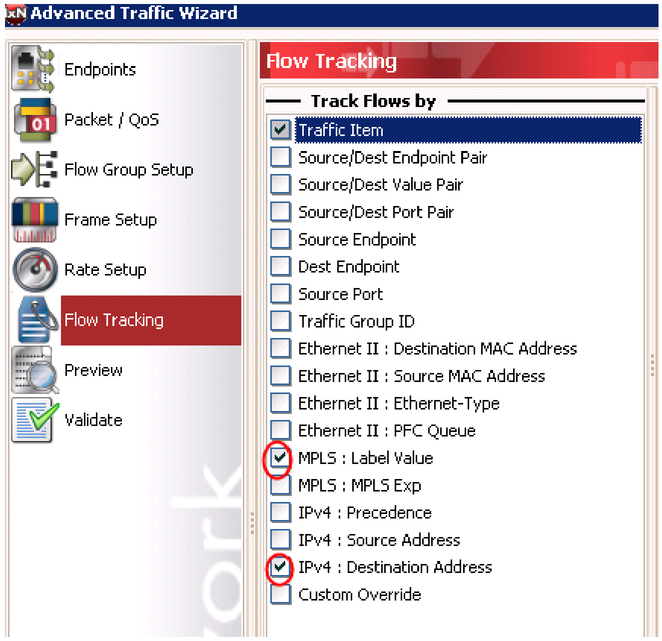


Figure 65. Flow tracking for P2MP traffic

11. Resolve any errors before proceeding. After error-free traffic is created, you may push the traffic definition to the Ixia hardware by clicking **L2-L3 Traffic**. Then start the traffic by clicking on the green triangle symbol.

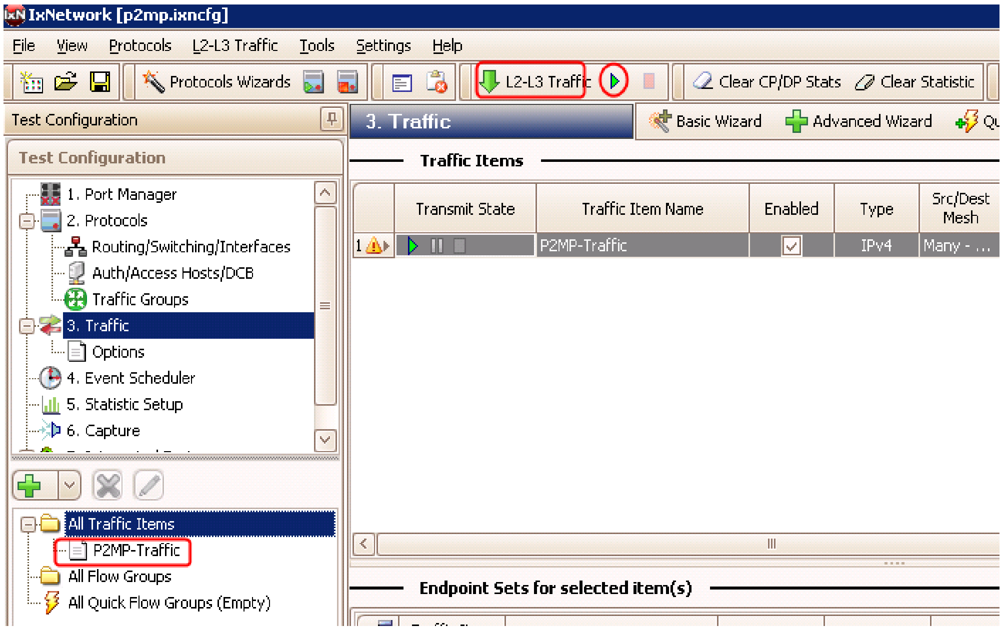


Figure 66. Push traffic streams to hardware

12. View per-flow statistics by going to the **Statistics** tab on the main window and clicking on **Traffic Item Statistics**. This will provide an overview of traffic for all RSVP-TE neighbors. In case of loss, right-clicking on the traffic items statistics allows you to select a drill down level view for any tracking items previously selected. The drill down view provides important troubleshooting details and allows quick isolation of troubled LSP.

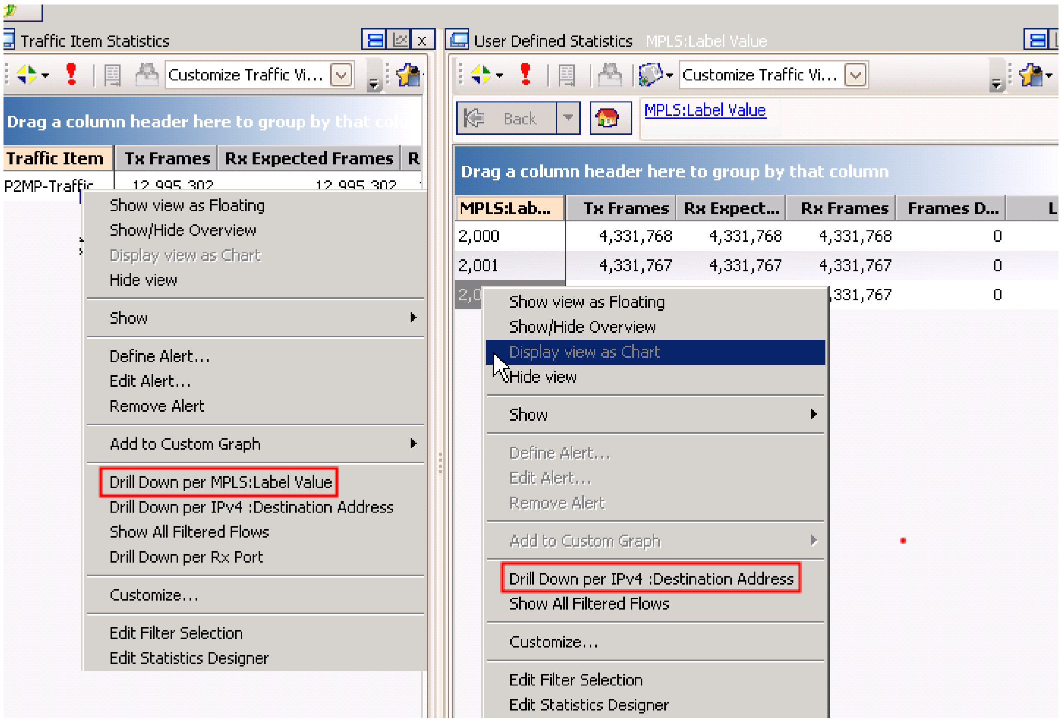


Figure 67. Multi-level drill down Per-Flow Statistics

Test Variables

As explained earlier, there are many possible dimensions for testing DUT scalability and performance limits. The following are some possible scenarios that are similar to the test described. IxNetwork's P2MP emulation software may be used to cover all the test variables.

- Use distinct root nodes and limit the number of tunnels per tree and LSPs per tunnel to find the maximum number of P2MP trees that the DUT can support, each with a reasonable number of leaf nodes.

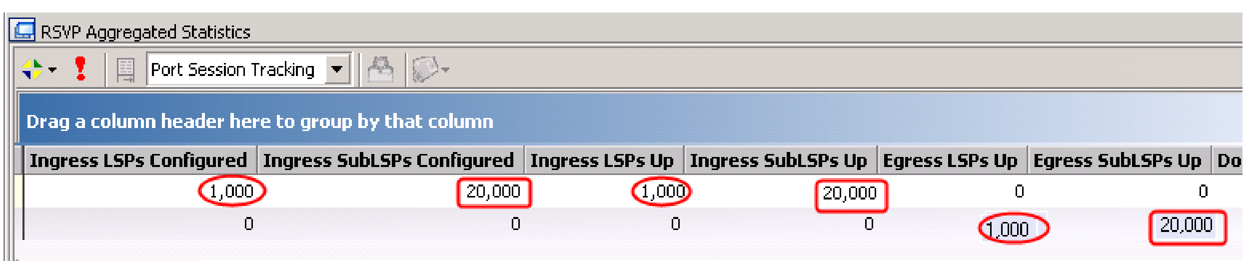
- Limit the number of root nodes, the number of tunnels per tree, and the number of LSPs per tunnel. Increase the number of leaf nodes per neighbor. This tests the maximum number of sub-LSPs whose state can be maintained by a DUT.

- Increase the number of egress neighbors while limiting the numbers on all other dimensions to discover the maximum number of sub-interfaces whose state can be maintained by a DUT while it is performing traffic replication up to line rate;

- Test scalability with mixed modes: running both P2P and P2MP on the same topology, and discover if the DUT can handle the specified number of tunnels for both P2P and P2MP simultaneously.

Results Analysis

If set up correctly, the control plane statistics will show the expected numbers for **Ingress LSPs Configured** and **Ingress LSPs Up** at the root port and **Egress LSPs Up** at the leaf port. This indicates that the P2MP tunnels are all up from both ingress and egress points of view. Moreover, the **Ingress SubLSPs Configured** and **Ingress SubLSPs Up** at the root port should match the **Egress SubLSPs Up** at the leaf port. This indicates that all sub-LSPs are up and all tunnels from the root have reached all intended leaf nodes.



Ingress LSPs Configured	Ingress SubLSPs Configured	Ingress LSPs Up	Ingress SubLSPs Up	Egress LSPs Up	Egress SubLSPs Up	Do
1,000	20,000	1,000	20,000	0	0	
0	0	0	0	1,000	20,000	

Figure 68. Overall protocol statistics

Additionally, **Port Learned Info** gives a comprehensive summary of LSPs and sub-LSPs. It's very easy to spot bad LSPs using this page. If you have a large number of LSPs, filters are available to identify and isolate the specific LSPs. Don't forget that LSPs that have been dead for a long time are automatically removed from memory. If you want to keep them in memory, you must enable **Store Down LSP** under **Neighbor Pair** in the main protocol GUI.

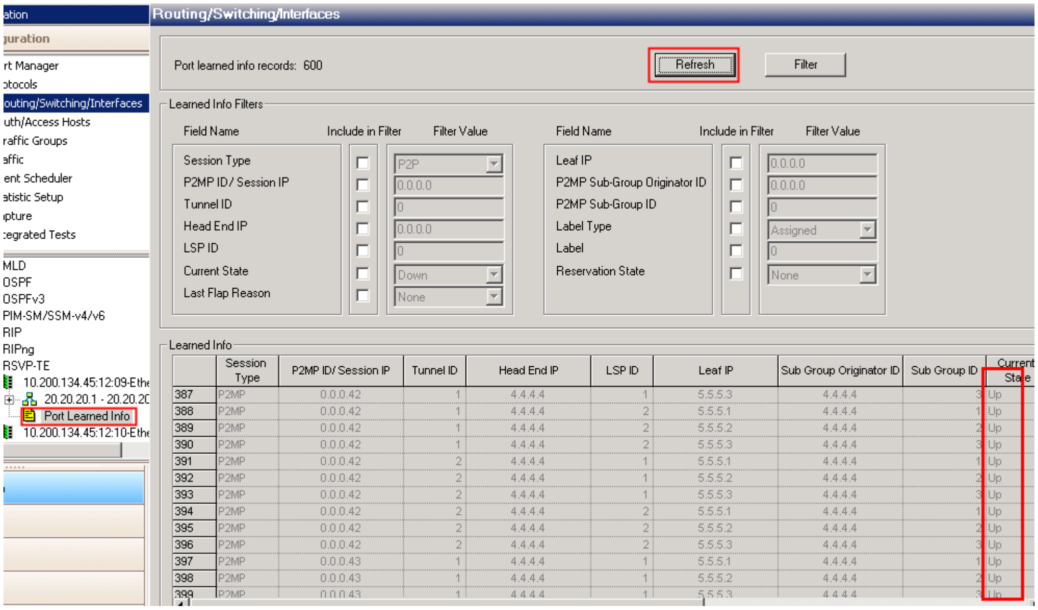


Figure 69. Port learned info

From a data plane perspective, all flows should pass traffic with no frame loss. In the case of frame loss, you should visually inspect the labels built by the traffic wizard. Open the packet editor in the traffic wizard and examine the list of labels placed in the packets. In case of doubt, go to **Port Learned Info** to find exactly which label was assigned to the sub-LSP. By cross checking these values, problems may be easily identified.

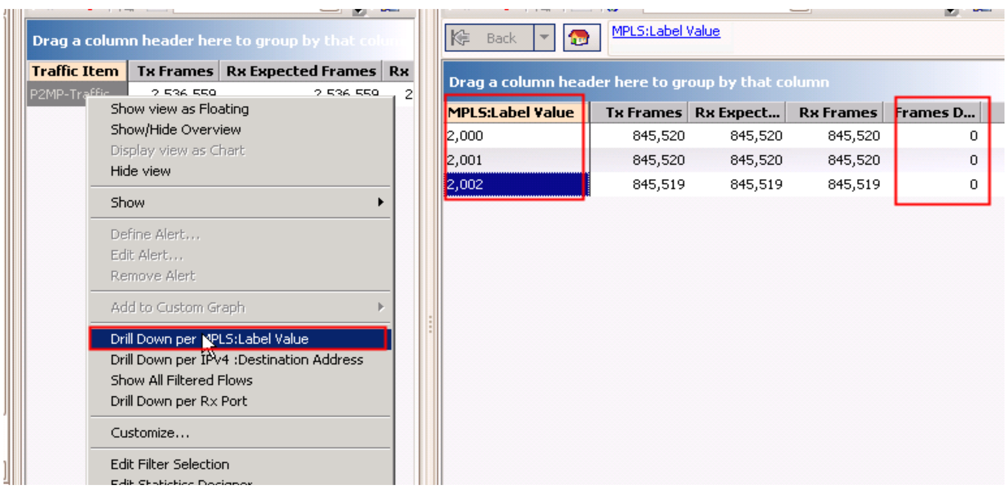


Figure 70. Drill down Per-flow statistics

Troubleshooting and Diagnostics

Problem	Description
Can't Ping from DUT	Check the **Protocol Interface** window and look for red exclamation marks (**!**). If any are found, there is likely an IP address/gateway mismatch.
LSPs won't come up or partially up	• Go to **Port Learned Info** to discover which sub-LSPs are up and which ones are not. Use **Filter** if needed to pinpoint to the exact LSP in question. • Enable **Store Down LSP** under **Neighbor Pairs** to allow the **Learned Info** to store dead LSPs indefinitely. • From the **Test Configuration** window, turn on **Control Plane Capture**, then start Analyzer for a real-time sniffer decode between the Ixia Port and the DUT port.
After stop/start protocols or link down/up Traffic 100% loss	Check the **Warnings** columns in the **Traffic** view and make sure there are no streams that say *VPN label not found*. The DUT may have sent new label info. If so, regenerate traffic by right-clicking the traffic item. Then **Apply** traffic.
Traffic statistics are not correct	Make sure the needed traffic options are enabled as described in step 17 and 19.
Not all sub-LSPs are up and it's hard to tell which ones are not	One tip is to assign different label spaces for different neighbors (as described in step 10). Based on the label value it may be easily spotted which neighbors contain bad sub-LSPs. The wizard, by default, will generate the same label start value for all neighbors.

Conclusions

IxNetwork's RSVP-TE P2MP emulation software is a feature-rich and comprehensive tool to test a DUT's multi-dimensional scalability. The built-in wizard allows easy setup of various parameters to match your specific requirements.

DUT Configuration Example

Below is an excerpt of a DUT configuration when the DUT is acting as a root node. The objective is to test DUT scalability in performing head end branching over sub-interfaces.

```
interface Tunnel11
 ip unnumbered Loopback11
 ip pim passive
 tunnel mode mpls traffic-eng point-to-multipoint
 tunnel destination list mpls traffic-eng name HE_SCALE
 tunnel mpls traffic-eng priority 0 0

interface Loopback11
 ip address 9.9.9.9 255.255.255.255

interface TenGigabitEthernet6/4.1
 encapsulation dot1Q 1500
 ip address 100.100.100.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface TenGigabitEthernet6/4.2
 encapsulation dot1Q 1501
 ip address 100.100.101.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface TenGigabitEthernet6/4.3
 encapsulation dot1Q 1502
 ip address 100.100.102.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface TenGigabitEthernet6/4.4
 encapsulation dot1Q 1503
 ip address 100.100.103.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface TenGigabitEthernet6/4.5
 encapsulation dot1Q 1504
 ip address 100.100.104.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
……
interface TenGigabitEthernet6/5
 ip address 192.192.192.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
```

```
router ospf 111
 log-adjacency-changes
 network 9.9.9.9 0.0.0.0 area 111
 network 100.100.100.0 0.0.0.255 area 111
 network 100.100.101.0 0.0.0.255 area 111
 network 100.100.102.0 0.0.0.255 area 111
 network 100.100.103.0 0.0.0.255 area 111
 network 100.100.104.0 0.0.0.255 area 111
 mpls traffic-eng router-id Loopback11
 mpls traffic-eng area 111
```

Layer 3 MPLS VPN Testing

Layer3 MPLS VPNs are IP services offered by Service Providers. This service offers point-to-multipoint Ethernet IP connectivity over a provider managed IP/MPLS network.

All customer sites that belong to a VPN (aka an enterprise customer) will appear to be on the same IP Local Area Network (LAN), regardless of their locations. The Service Provide cloud will act as a single IP router to all sites of the customers VPN, nullifying the customers need to build his own routed core network. An L3 MPLS VPN-capable network consists of three types of devices:

- Customer Edge (CE) Routers – The CE is a router (not a switch) located at the customer's premises. It connects to a PE router. Unlike L2 VPN –VPLS services that use the PE as a switch, each L3 MPLS VPN CE router runs one of various IPv4 routing protocols to exchange IP routes between the customer and the provider PE Router, including RIP, OSPF, ISIS, E-BGP, or EIGRP.
- Provider Edge (PE) Routers - The PE is where the intelligence of the customers VPN originates and terminates. The PE routers maintain separate routing tables for each customer (VPN), and route the IP traffic over the Service Provider (SP) network using MPLS and BGP, through Provider (P) routers, to other Service Provider PE routers. The PE routers run an IGP protocol (like OSPF or ISIS) to the Service Provider Core, an MPLS Protocol (either LDP or RSVP-TE), as well as an I-BGP connection to the other PE to exchange VPN information.
- P Router - The P interconnects the PEs and runs the Provider MPLS core network. It does not participate in the VPN functionality. It simply switches the VPN traffic using MPLS labels. The P routers run an IGP protocol (like OSPF or ISIS) to other Ps and PEs within the Service Provider network, along with LDP or RSVP-TE for MPLS signaling.

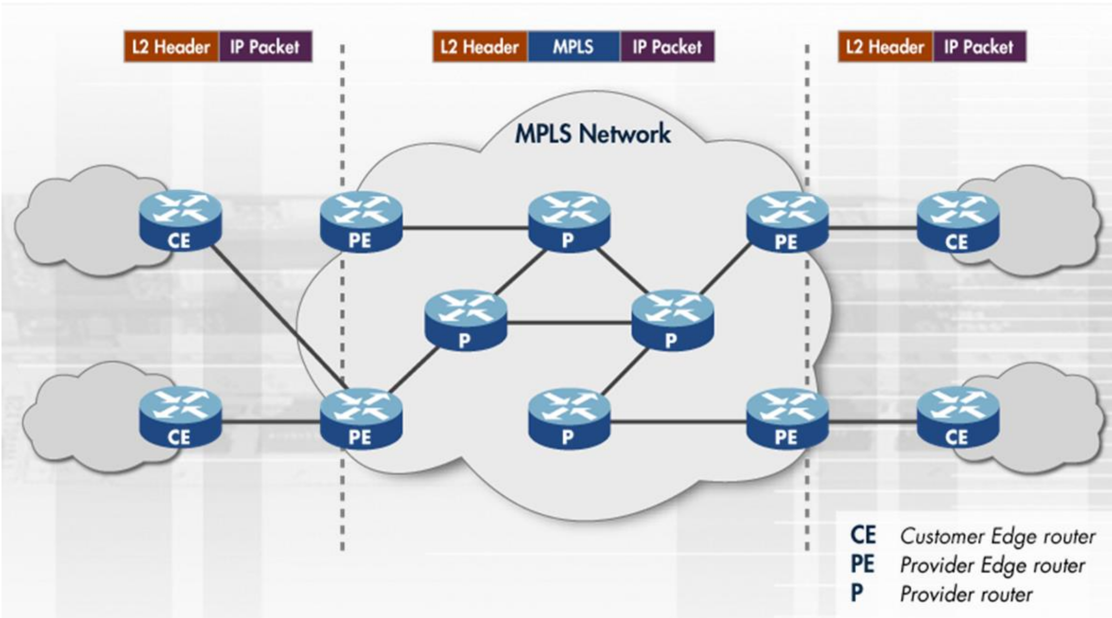


Figure 71. Typical layer 3 MPLS VPN network

Testing of an L3 VPN network is mostly concerned with the PE routers.

The PE routers use and Ipv4 or IPv6 routing protocol to peer with CE routers. Each PE router maintains separate forwarding tables for each CE that belongs to a unique VPN. These routing tables are called VPN routing and forwarding tables (VRFs). The tables must be maintained by the PE router without route leakage. In addition, the CE routers are sometimes maintained by the customer, and run a variety of protocols (such as EBGP, RIP, ISIS, OSPF, or EIGRP). The uncertainty of routing table sizes, route flapping, unique protocols, and router security threats require a plethora of functional and performance tests for the PE.

On the Service Provider side of the PE router, (Internal) BGP is used to peer with all PE routers in the network (or they peer with a Route Reflector) and exchange VPN route information. In addition, the PE router runs an MPLS protocol (RSVP or LDP) with its neighboring P/PE routers to complete the MPLS backbone.

In addition to this, L3 MPLS VPNs require that BGP and MPLS work together, with BGP VPN MPLS labels stacked on an underlying MPLS backbone.

All of these aspects of the PE router require initial testing at the functional level, but more importantly at the performance level, including:

- Scaling CEs over VLANs using various protocols, various numbers of routes, and route flapping.
- Scaling PEs in the provider network. All IBGP neighbors must peer with each other, and many VPN/VRF routing tables are exchanged. Flapping is another key test case.

- Scaling Ps in the core of the provider network so as to switch massive amount of MPLS and, in some case, non-MPLS packets. These Ps are also sometimes called upon to be the IGBP route reflectors.
- Data plane performance at the maximum CE, PE, or P scale. Testing should not only include throughput, but also verify that route leakage does not occur.

Further performance test cases using Ixia's IxNetwork can be verified with the following step-by-step test case, along with the **Test Variables** section.

Relevant Standards

- BGP emulation messages encoded and decoded as per draft_ietf_idr_bgp4-17, A Border Gateway Protocol (BGP-4) (supersedes IETF RFC 1771)
- BGP route reflections encoded and decoded as per to IETF RFC 2976, BGP Route Reflection - an Alternative to Full Mesh IBGP (supersedes IETF RFC 1996)
- BGP communities encoded and decoded as per IETF RFC 1997, BGP Communities Attribute
- BGP confederations encoded and decoded as per IETF RFC 3065, Autonomous System Confederations for BGP
- BGP-4 RFC 1771
- Multi-protocol extensions for BGP-4 as per RFC 2283
- Capabilities advertisement with BGP-4 as per RFC 3392
- Multi-protocol extensions for BGP-4 as per RFC 2858
- Carrying label information in BGP-4 as per RFC 3107
- BGP/MPLS IP VPNs as per draft-ietf-l3vpn-rfc2547bis-01.txt
- Extended communities attribute as per draft-ietf-idrbgp-ext-communities-02.txt
- Multi-protocol extensions for BGP-4 as per draft-ietfidr-rfc2858bis-05.txt
- AS-wide unique BGP identifier for BGP-4 as per draft-ietf-idr-bgp-identifier-00.txt
- Connecting IPv6 islands across IPv4 MPLS clouds with BGP (GPE) as per draft-ooms-v6ops-bgp-tunnel-02.txt

Test Case: Layer 3 MPLS VPN Scalability and Performance Test

Overview

Since layer3 MPLS VPNs are becoming widely available and are growing in deployment, router vendors and service providers should carefully consider a number of scalability issues relating to the technology.

Service provider PE routers must allow partitioning of their resources between unique customer VPNs, and at the same time partition their Internet routing resources. The PE router in an L3 MPLS VPN network must:

- Maintain separate, unique routing tables for each customer or VPN.
- Run MPLS, IBGP, and an IGP into the core of the SP network, usually connecting to faster P/PE routers on high-speed links.
- Peer with all other IBGP PE neighbors and exchange VPN/VRF route info with them or peer with route reflectors.
- Make forwarding decisions at microsecond speeds while bi-directionally adding/popping MPLS and BGP VRF labels.
- Keep enterprise customers VPN traffic and Internet traffic separate from each other.

Because of this, the focus of tests is largely oriented on the PE, since all the unique customer/VPN intelligence is implemented within the PE routers. Layer 3 MPLS VPN technology takes advantage of the emerging MPLS technology for tunneling data packets from different VPNs over the same service provider network. BGP is extensively used for VPN exchange and for the distribution of VPN reachability information. The combination of MPLS and BGP working together make up this exciting technology.

The best methodology for performance testing a PE is to create a scalable baseline test, and then modify it in different ways to test PE control plane and data plane performance. This testing will verify the PEs ability prior to being deployed in a real-world, revenue-generating SP network.

Objective

The objective of this test is to baseline the scalability of a single DUT acting as a PE router in a Layer 3 MPLS VPN network.

At the end of this test other test variables will be discussed that will provide many more performance test cases, using the topology shown in Figure 72 as the baseline.

Setup

As shown in Figure 72 below, the test consists of a DUT, acting as a PE router, and four Ixia test ports.

Two Ixia test ports will emulate a total of four customer edge (CE) routers. Each port supports one site of two unique VPNs per customers. Port 1's CE will run OSPF, while port 2's CEs will run E-BGP.

Two other Ixia ports will emulate the entire service provider network and eight additional CEs (four for each VPN/Customer)

In total, this test will emulate 12 CEs, 2 Ps, and 4 PEs for 2 VPNs per customers (each with 6 sites).

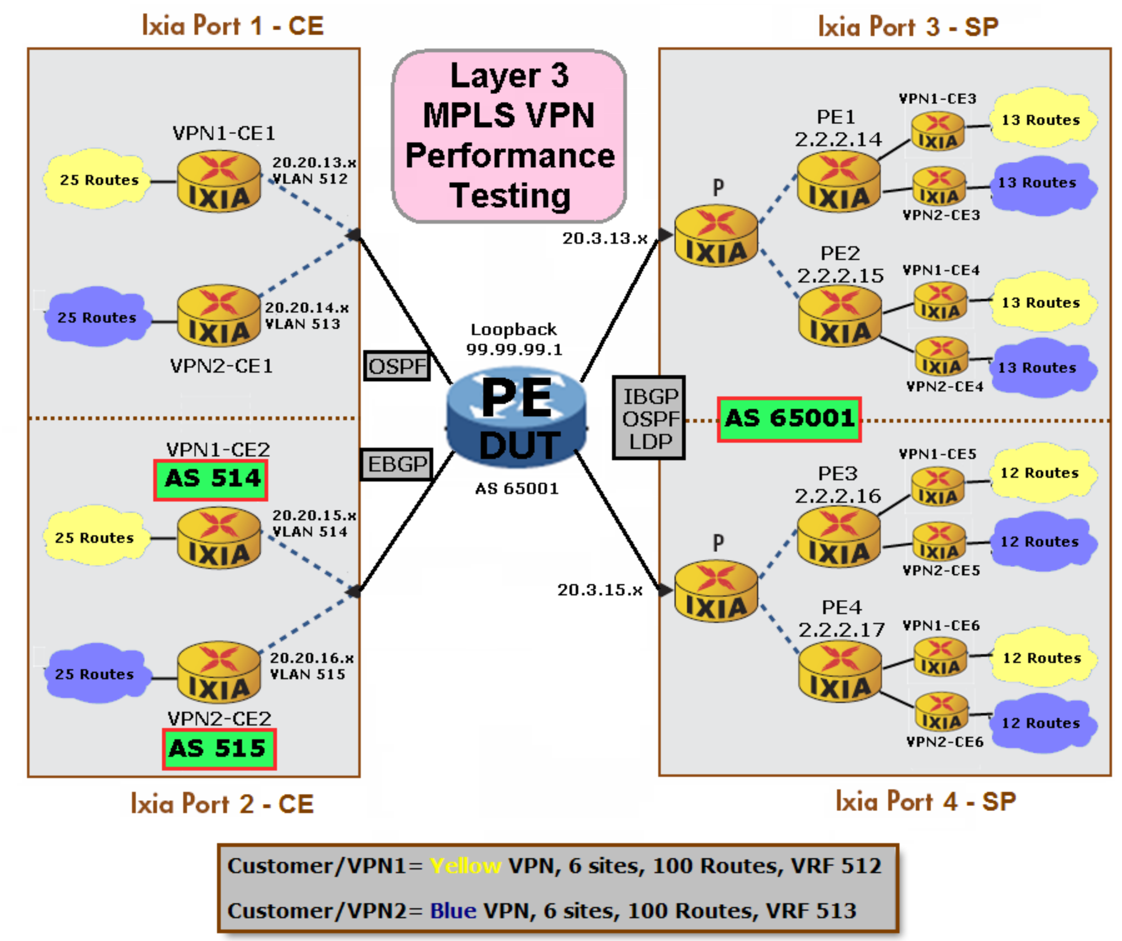


Figure 72. Ixia emulated layer 3 MPLS VPN network

Step-by-step Instructions

Follow the step-by-step instructions to create a layer 3 MPLS VPN performance test exactly as shown in Figure 72 above. In addition, you can use the steps below as a guide for building many other layer 3 MPLS VPN performance test scenarios.

1. Reserve four ports in IxNetwork.

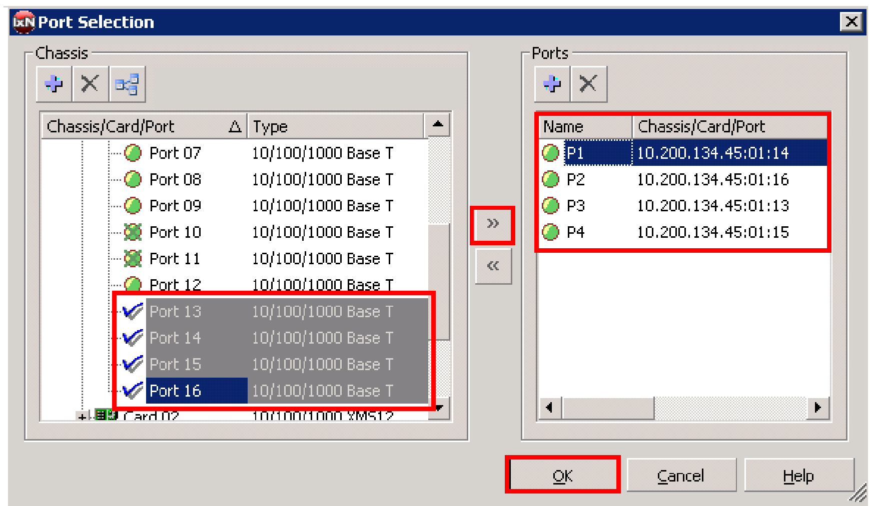


Figure 73. Port Reservation

2. Rename the ports for easier use throughout the IxNetwork application.

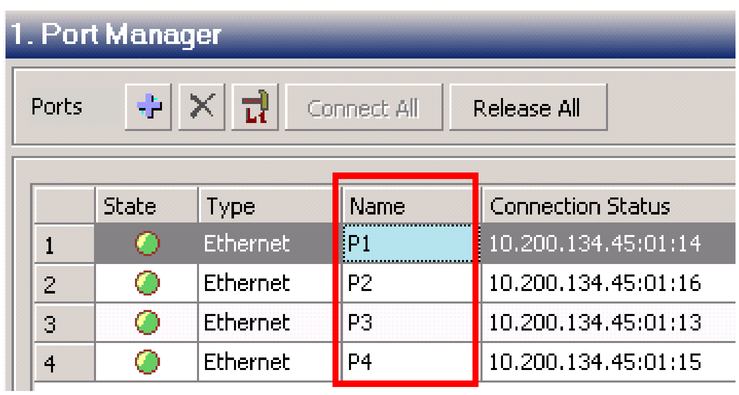


Figure 74. Port Naming

3. Click the **Protocol Wizards** button on the top toolbar in the IxNetwork application.

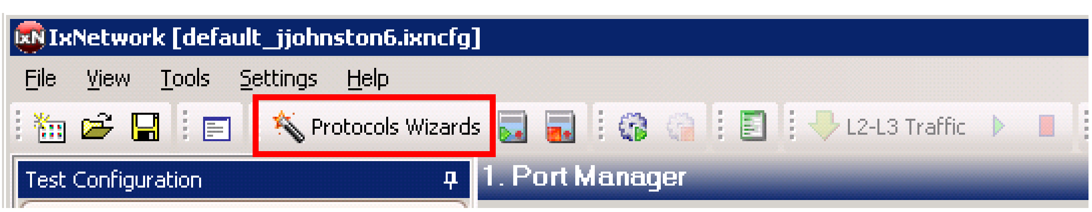


Figure 75. Protocol Wizards

4. Run the **L3 VPN/6VPE** protocol wizard.

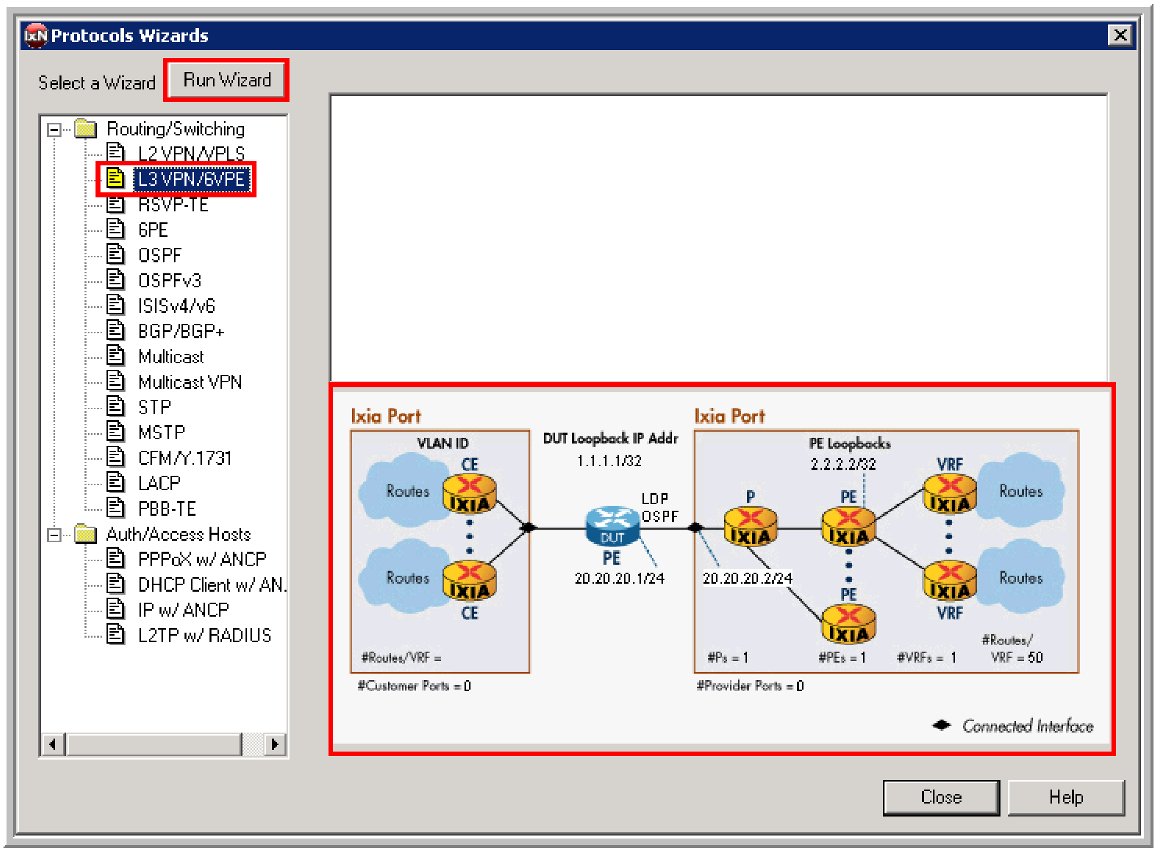


Figure 76. L3 VPN Wizard

Note: the wizard also supports 6VPE testing, which supports CEs running IPv6 routing protocols in addition to IPv4. The PEs have the ability to send the IPv6 routes over the SP network to other PEs.
Note: the picture represents a typical test case for testing a PE router in an L3 VPN network.

5. Configure **P1** and **P2** to emulate the CE (left) side of the topology, and **P3** and **P4** for the SP (right) side of the topology, then click **Next**.

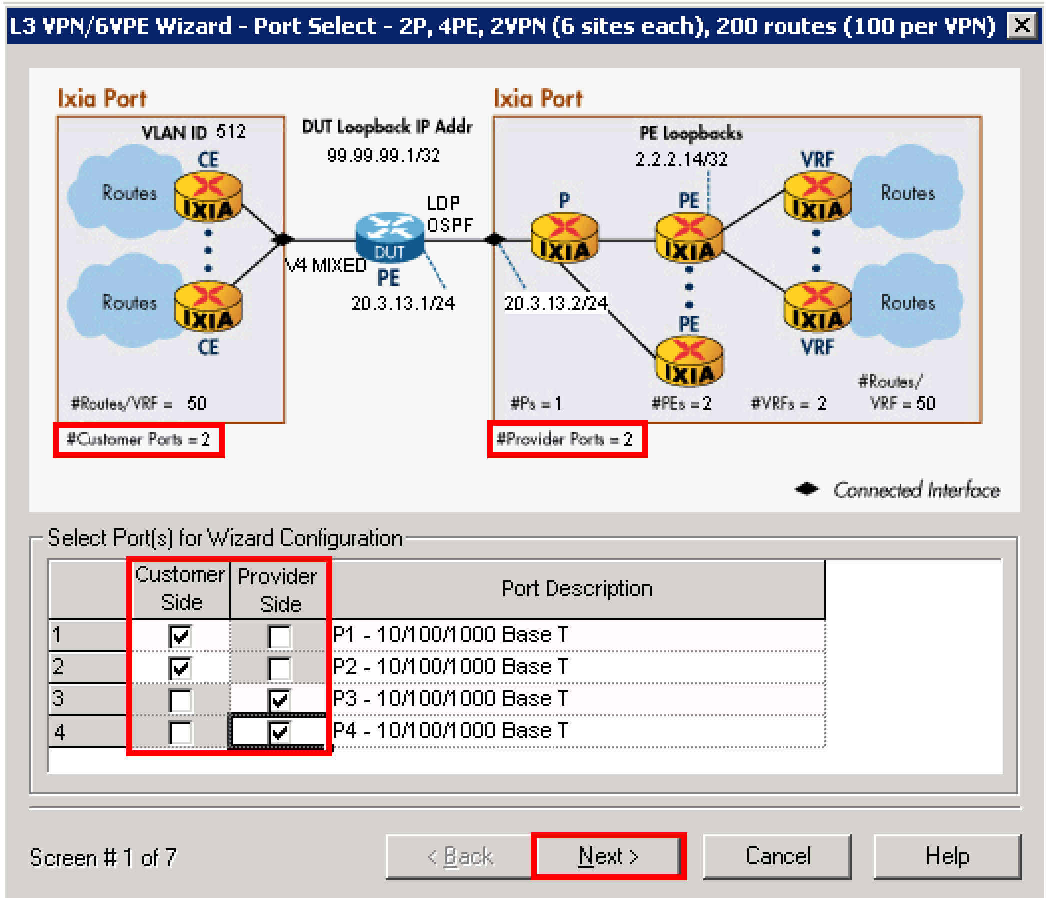


Figure 77. L3 VPN Wizard Screen1 of 7

Note: The picture at the top updates with number of customer-side ports as well as number of provider-side ports.

Performance test variable: Increase the number of customer and provider ports to test the DUT's (PE) ability to scale at a port level. In a real-world network, there are more customer ports than provider ports.

6. This window configures **P3** and **P4** with emulation of one or more P routers. These ports are configured to talk directly to the DUT (PE) router.
    a. Keep the default of *1* P router. This is a per-port setting.
    b. Configure the **IGP** and **MPLS** protocol running in the SP core.
        1. In this test use the defaults of **OSPF** and **LDP**, respectively.
    c. Configure the Ixia P router's IP address on **P3** and the **DUT IP** address
        2. In this test they are *20.3.13.2/24* and *20.3.13.1/24*, respectively.
        3. Note: **P4** will automatically be assigned 20.3.14.2 and 20.3.14.1.
    d. Click **Next**.

    Optionally:
    a. Disable (**uncheck**) P router emulation. In this case, the Ixia ports(s) would only emulate PE routers and would test the DUT in PE-to-PE scenario.

    Performance test variables:
    - Increase the number of emulated P Routers to test the DUT's ability to peer with many P routers, all running an IGP/MPLS protocol.
    - Check the **Enable VLAN** checkbox (not shown) to run these protocols over VLANs. Enter the first VLAN ID and choose an incrementing function.

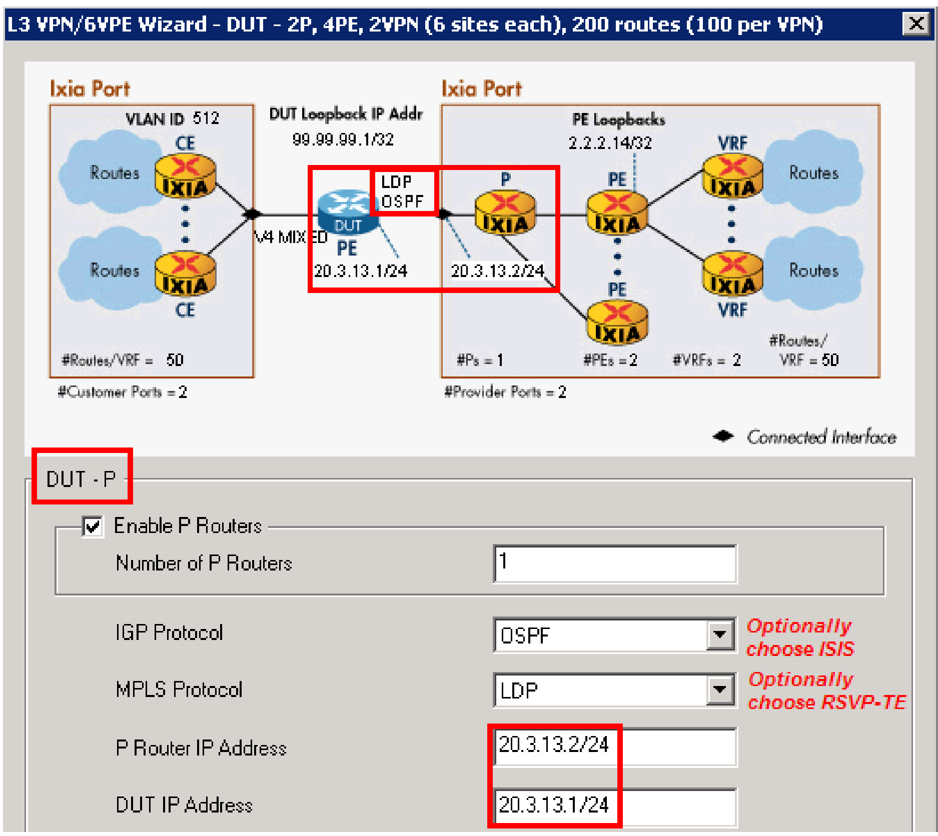


Figure 78. L3 VPN wizard screen 2 of 7

Note: The picture above updates with the configured protocols/IP addresses.

7. This window configures **P3** and **P4** with emulation of one or more **PE Routers** that work directly behind the emulated P router(s).
   a. Configure the number of PE routers per P Router. This is a per-port setting.
      i. In this test it is *2* PEs (per P)
   b. Configure the AS # of the DUT/SUT.
      ii. In this test it is *65001*.
   c. Configure **Emulated PE Loopback IP address** (and its incrementing function for the additional PEs
      iii. In this test it is *2.2.2.14* (the second, third and fourth PE will be automatically assigned 2.2.2.15, 2.2.2.16, and 2.2.2.17, respectively).
   d. Configure **DUT Loopback IP Address**
      iv. In this test it is *99.99.99.1.*
   e. Click **Next**.

   Performance test variable: Increase the number of PE routers per P router. This will test the DUT's ability to peer with many PE routers that potentially use many VPN/VRFs.

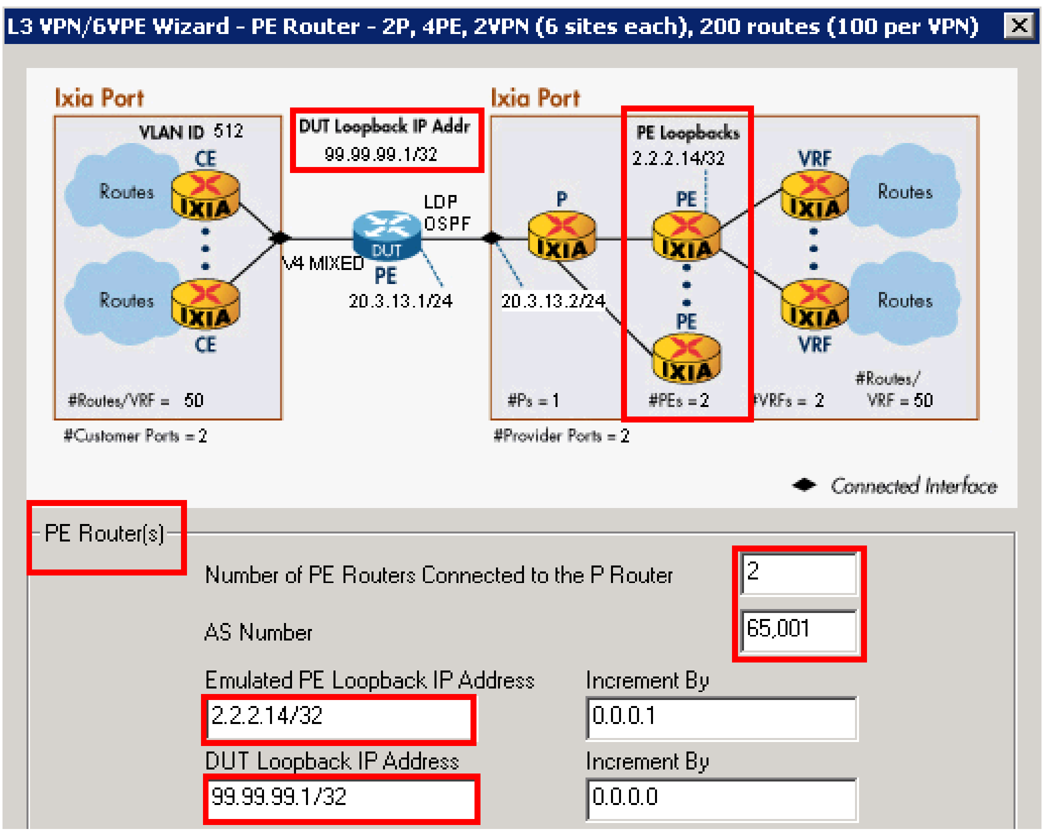


Figure 79. L3 VPN wizard screen 3 of 7 (Part 1)

Performance test variable: Enable the use and quantity of **Route Reflectors**, and their loopback addresses. This will offload the number of IBGP peers that the DUT must peer with and test the route reflectors ability to properly re-distribute the VPN/VRF routes to all PE peers in the same AS.

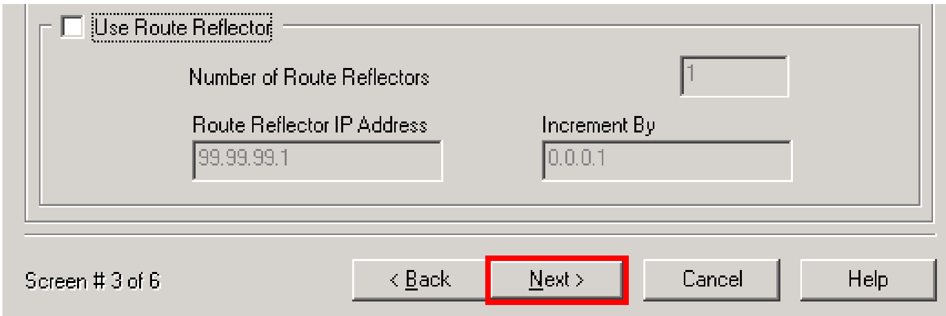


Figure 80. L3 VPN wizard screen 3 of 7 (Part 2)

Note: All test equipment manufacturers cannot emulate a route reflector. A second DUT must be used to be the router reflector.

8. This window configures **P3** and **P4** with emulation of VPNs/VRFs on top of the just-configured PE Routers.
   a. Configure the **VPN Traffic ID Name Prefix**…For most L3 VPN test cases use *L3VPN.*
   b. Configure the **Route Target** for the first VPN/VRF. In most test cases this is a combination of the AS # and a unique identifier. The **Route Distinguisher** is set to the same value.
      In this test it is *65001:512*. The second VPN will use 65001:513
   c. Configure the number of **VPNs per PE**. This will partially determine the number of customers/VPNs that will be used in the test. This number will also determine the number of CE Routers in *Step 9*.
      In this test it is *2*.
   d. Configure the **Routes per VPN**.
      In this test it is *100* routes per VPN (200 routes across 2 VPNs)
   e. Configure the **First Route in the VPN**
      In this test it is *106.1.1.0/24.*

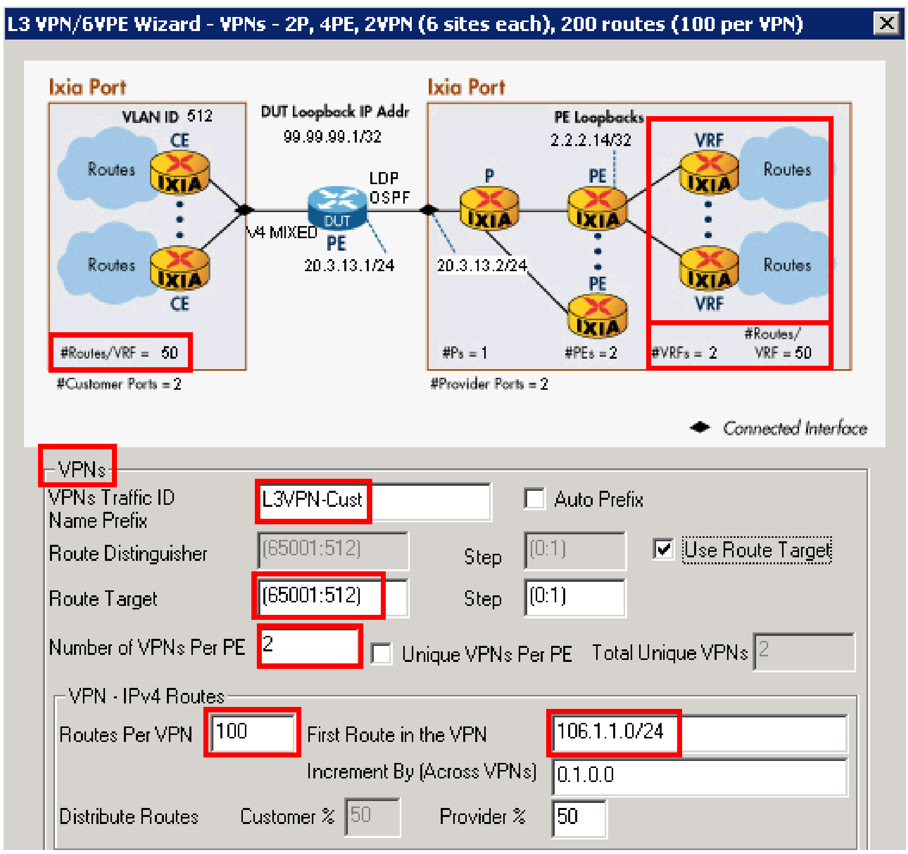


Figure 81. L3 VPN wizard screen 4 of 7

Performance test variables:

- Increase the number of VPNs per PE. This will test the DUT's ability to peer with more CE routers and also create more VRF entries.
- Increase the number of routes per VPN. This will test the DUT's ability to hold more VRF entries.

9. This window configures the parameters of **P1** and **P2** and its emulation of **Customer CE**s.
   a. Configure the **CE-PE Protocol**, or select **Mixed CE protocols**
      In this test case check the box for **Mixed CE Protocols.**
   b. Configure the CE **DUT IP address**.
      In this test the first IP address is *20.20.13.1***.** The second CE is 20.20.14.1, the third CE (on P2) is 20.20.15.1, and the fourth CE (on P2) is 20.20.16.1.
   c. **Enable VLAN**, **VLAN ID**. In most cases multiple CEs will be received by the same PE DUT port over VLANs.
      i. In this test it is 512.
      ii. Note: The second CE on P1 will use VLAN 513, and P2 will use 514 and 515
   d. Click **Next**.

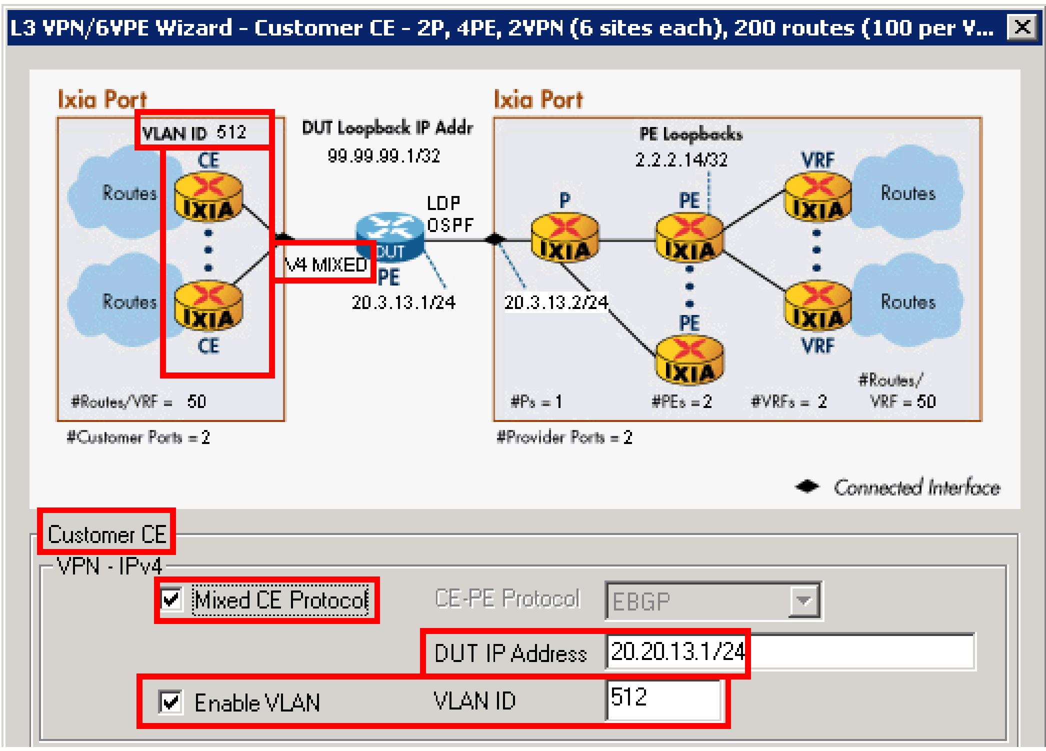


Figure 82. L3 VPN wizard screen 5 of 7

10. This window configures the **Mixed IGP Protocol Selection** for the CE ports **P1** and **P2.**
    a. Depending on the number of CEs, as specified in the previous window, choose the ratio of IGP protocols to use on **P1** and **P2.**
       In this case choose *2* **OSPF** and *2* **EBGP**. This will configure OSPF on the 2 CEs on P1 and EBGP on P2.
    b. Since EBGP was chosen as one of the protocols, choose the starting AS #
       In this test it is *514***.** The second CE on P2 will use AS# 515.
    c. Click **Next**.

Performance test variable: Use a mixture of as many IGP protocols as possible. This will test the DUT's ability to maintain protocol state across multiple CEs on the same port, and further data plane tests will verify there is no route leakage between VPNs/Customers.

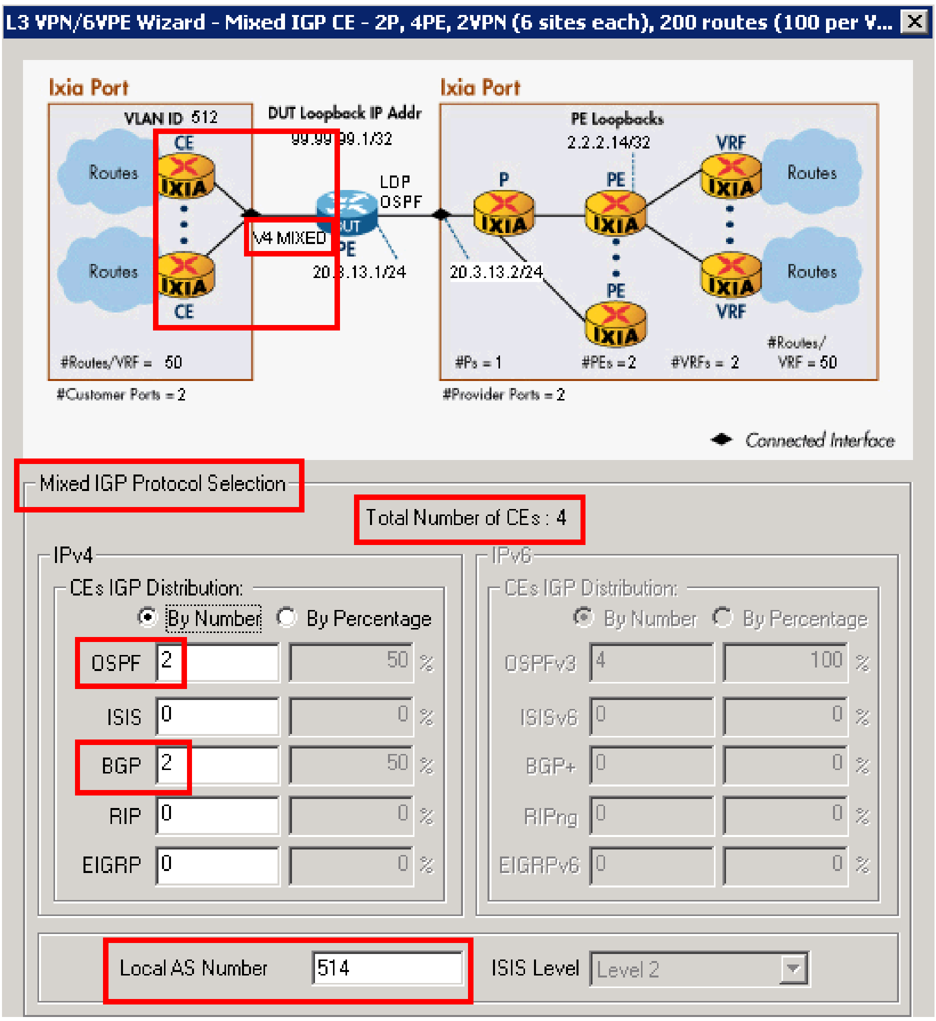


Figure 83. L3 VPN Wizard Screen 6 of 7

11. This window configures the name of the wizard run and the action to take with this run of the wizard.
    a. Use a descriptive **Name** for the wizard.
       In this test use *2P, 4PE, 2VPN (6 sites each), 200 routes (100 per VPN)*
    b. Specify what to do with the finished wizard configuration.
       In this test select **Generate and Overwrite All Protocol Configurations**. This will overwrite all previous configuration.
    c. Click **Finish**.

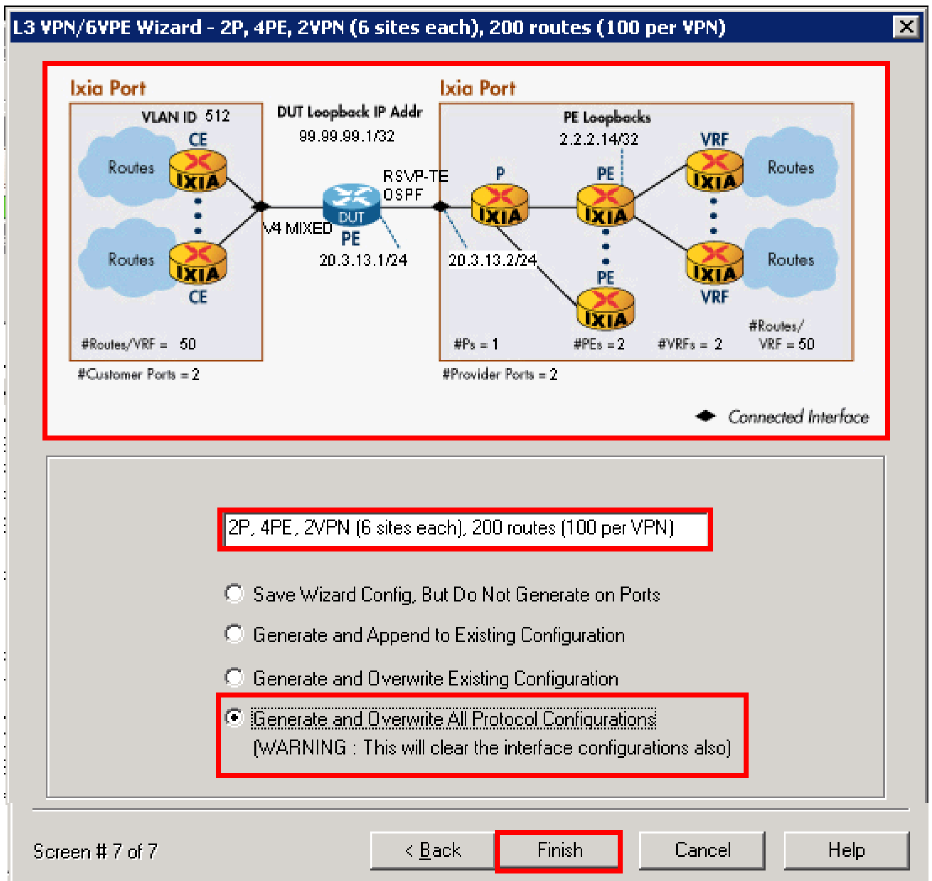


Figure 84. L3 VPN Wizard Screen 7 of 7

12. This window shows the saved wizard template.
    a. Select **Close** to finish the wizard configuration
    b. ***Optionally***, with saved wizard templates, you may:
        - Come back to the same wizard using the double-click to view and/or modify.
        - Save new or modified wizards with a new name, or overwrite an existing version.
        - Create a library of templates for use in different tests.
        - Highlight each template and preview the configuration in the topology below.

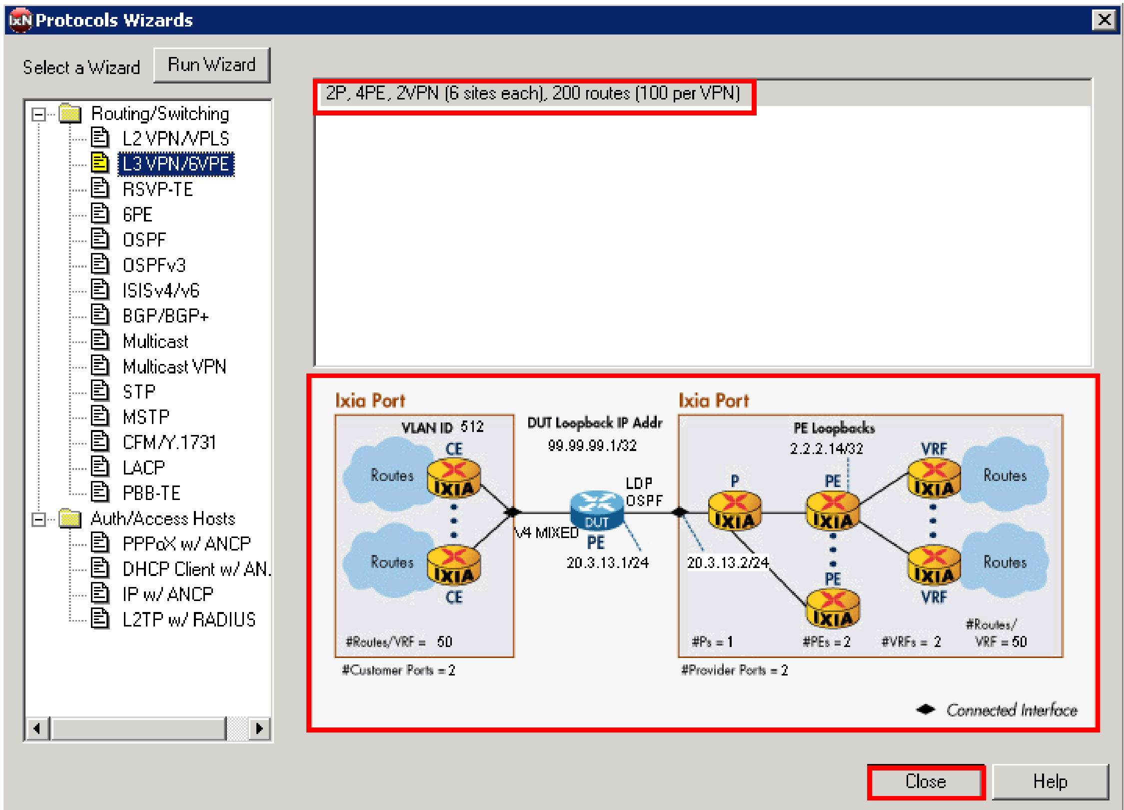


Figure 85. L3 VPN Wizard Saved Wizard Template

13. Once the wizard has completed, examine the contents of the IxNetwork configuration windows to see how the values were set. Verify IP connectivity between the DUT interfaces and the Ixia port interfaces. For example,
    a. Click on the **Routing/Switching/Interfaces** window on the top, and the **Protocol Interfaces** in the middle.
    b. Verify that the IP addressing/incrementing functions of the wizard properly created IP interfaces that connect to the DUT. If necessary, manually change them to match the DUT.
        i. In Figure 86 below the wizard incremented the IP addresses properly except the DUT IP address is for Ixia **P4** should be ***20.3.15.x***, so manually changing the Ixia port.
        ii. **Note:** The red **!** sign means ARP failed, which usually indicated a mismatch in Ixia Port/DUT IP addressing.

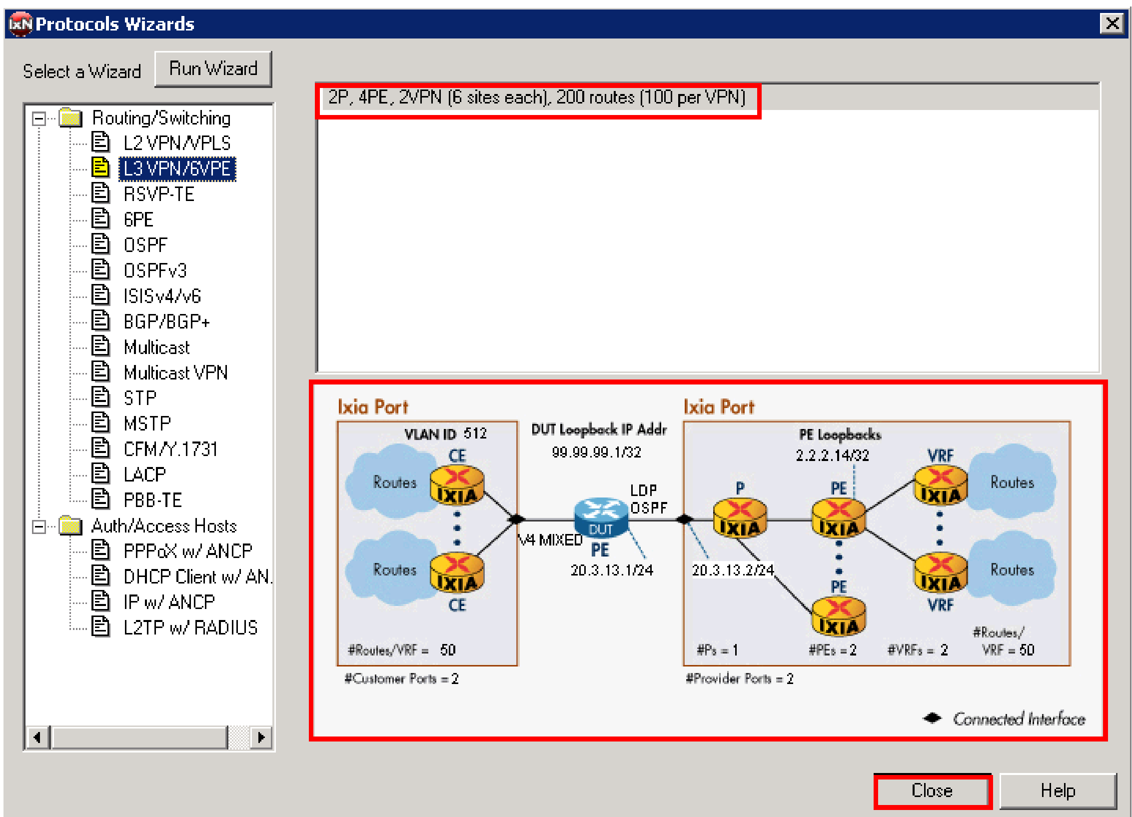


Figure 86. Protocol Interface Window

14. Check the protocol configuration. Make sure the settings will work with the DUT's configuration. For example;
    a. Click on **BGP/BGP+** in the middle window.
    b. Note the 2 E-BGP peers going to the emulated CEs.
    c. Note the 4 I-BGP peers going to the emulated PEs.
    d. If necessary, manually change the configuration in the protocol table/grid to your liking. Optionally highlight columns and right-mouse click to further customize with **Same** or **Fill Increment** options.

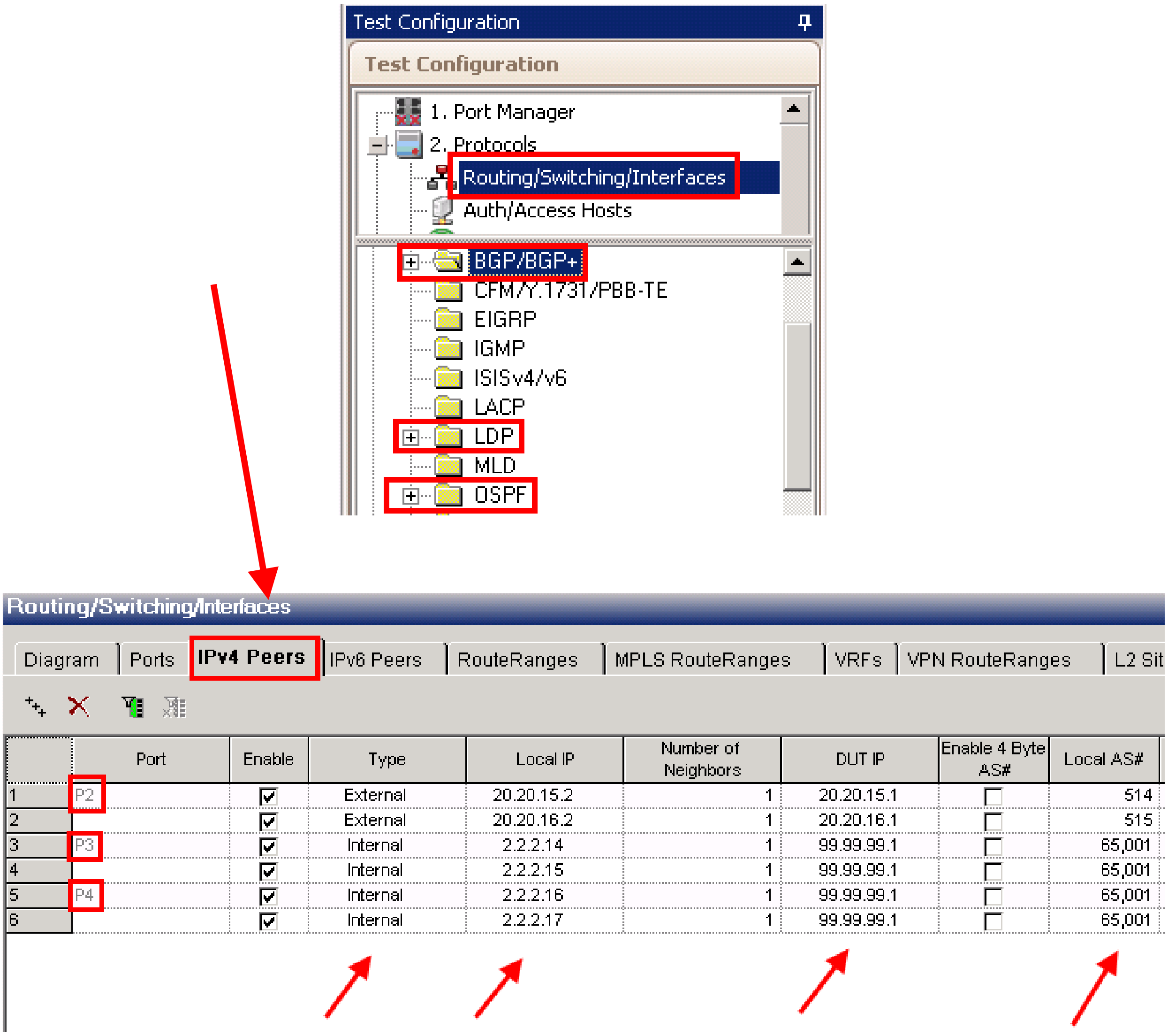


Figure 87. Protocol configuration window

Note: Additionally check the **OSPF** and **LDP** folders to verify the configuration that the wizard generated will work with the DUT configuration.

15. Click the **Statistics** window on the bottom left and click the **Start all Protocols** button on the toolbar.

16. Click on the **Global Protocol Statistics** option for a summary of all protocols running on each port.
    a. Check if all of the BGP, OSPF, and LDP sessions are up.
    b. Optionally, click on each of the protocol stats (BGP, LDP, OSPF) to view more statistics for each protocol (including up/down status as shown in Global Stats).

Troubleshooting tips: If the sessions are not up:

- Go back to the Test Configuration window and double check the protocol configuration against the DUT.
- From the Test Configuration window, turn on Control Plane Capture, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.

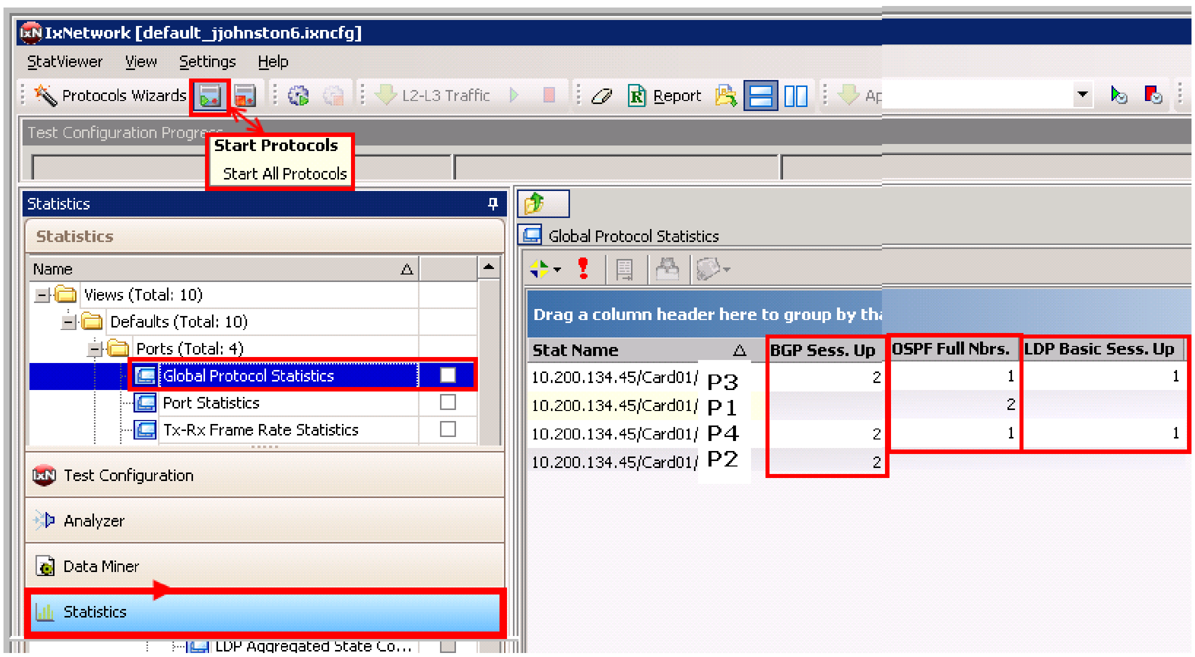


Figure 88. Global protocol statistics window

17. After the protocols have been started, use the Ixia **Learned Routes** option to verify that each Ixia peer is receiving the correct routes/labels for each peer.
    a. View the MPLS labels learned by the Ixia BGP peers on **P3**.
    Click on **Learned Routes** and then **Refresh** to see the labels learned by the Ixia peer. In this test case there should be **100** VPN routes.

    Optionally:

    b. View a more granular view of each VRFs labels (65001:512 and 65001:513) by clicking **Learned VPN Routes.**
    c. View the EBGP routes learned by the Ixia **P2** BGP peering sessions on P1.
    d. View the OSPF routes learned by the Ixia **P1 OSPF** peering sessions and make sure the BGP routes are being redistributed properly.
    e. View the LDP labels coming from the DUT(PE) to the Ixia P Routers (on **P3** and **P4**).

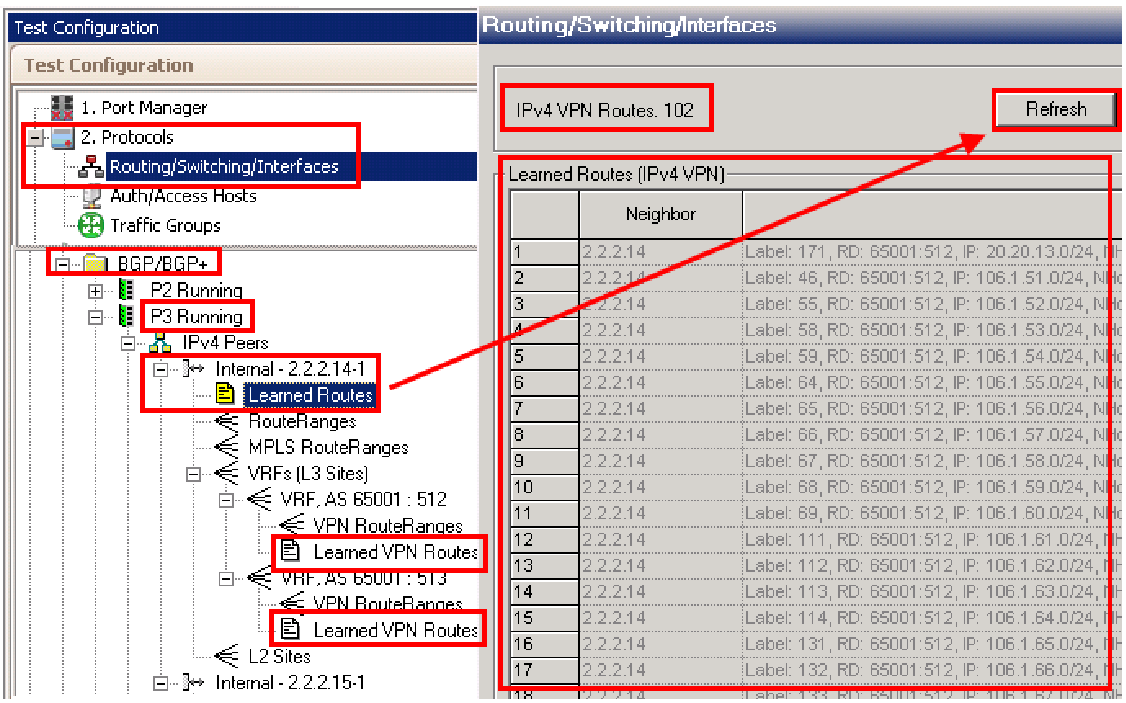


Figure 89. Protocol learned Info

18. After all of the sessions are up, you need to build bi-directional traffic from the CE to the PE, and from the PE to the CE.
    a. *Optionally***,** change the **Traffic Group Id Description** to the names shown below. This will help when running the traffic wizard.
        i. Traffic group 1 = L3VPN – Cust/VPN1 – Yellow.
        ii. Traffic group 2 = *L3VPN – Cust/VPN2 – Blue.*

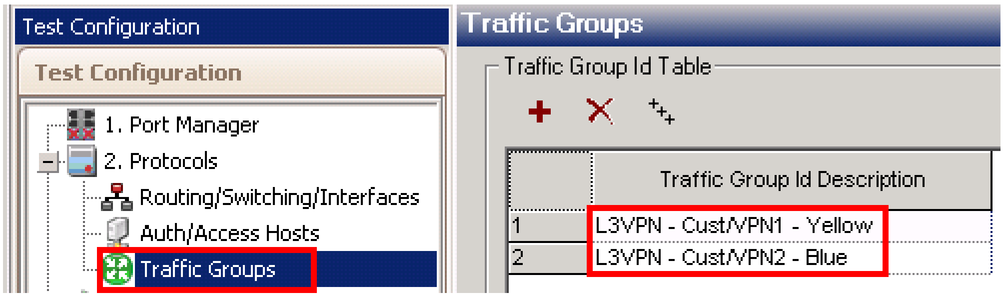


Figure 90. Traffic Group Window

19. Next, launch the **Advanced Traffic Wizard** by clicking on the **+** sign.

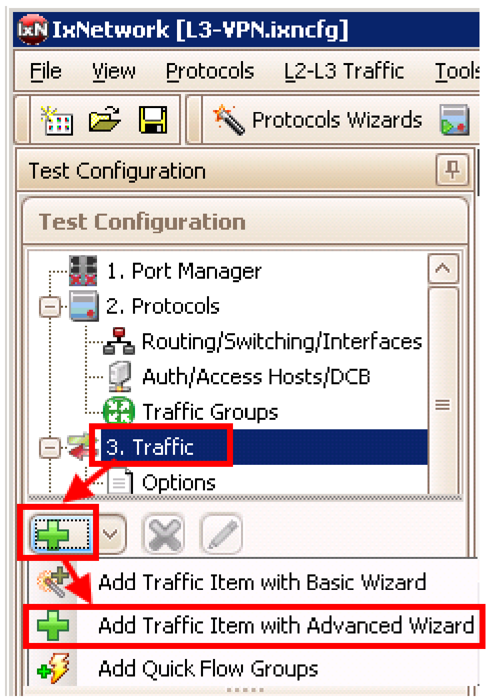


Figure 91. Create traffic

20. First configure the CE-PE traffic.
    a. Name the **Traffic Item** as **CE-PE**
    b. Set the **Traffic Type** to **IPv4**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select both the **L3VPN – Cust/VPN1 – Yellow** and **L3VPN – Cust/VPN2 – Blue** checkboxes and click **Apply Filter.**
        i. This will filter the Source and Destination trees to only display items that belong to these customer/VPNs. It is also possible to select only one Traffic Group ID at a time to see an exact view of all sources/destinations that belong to that customer's VPN.
        ii. Even though both Traffic Group ID filters were selected at the same time, IxNetwork is smart enough to only send traffic to/from sources and destinations that belong to the same VPN.
    e. Set the source **Encapsulation Type** to **non-MPLS**, and the destination to **L3VPN**. This will further filter the source/destination tree for CE-PE traffic.
    f. Enable the **Source - OSPF Route Ranges** and **BGP Route Ranges** checkbox. This is a global option to select all of the BGP routes for the source ports.
    g. Enable the **Destination** - **BGP VPN Route Ranges** checkbox .
    This is a global option to select ALL of the BGP VPN routes for the destination ports.
    h. Click the **down arrow** sign to add the four sources and eight destinations as a traffic **Endpoint Set**.
    i. Click **Next**

Note: It is possible to configure the PE-CE traffic at the same time by selecting the **Bi-Directional** checkbox within this window. However, by doing them in separate **Traffic Wizard** runs, the resources (flows) used will be saved, allowing better use of flow tracking as selected in the **Flow Tracking** page of this wizard.

Note: Make sure to uncheck the **Merge Destination Ranges** checkbox if the same routes are used on two or more VPNS in the test.

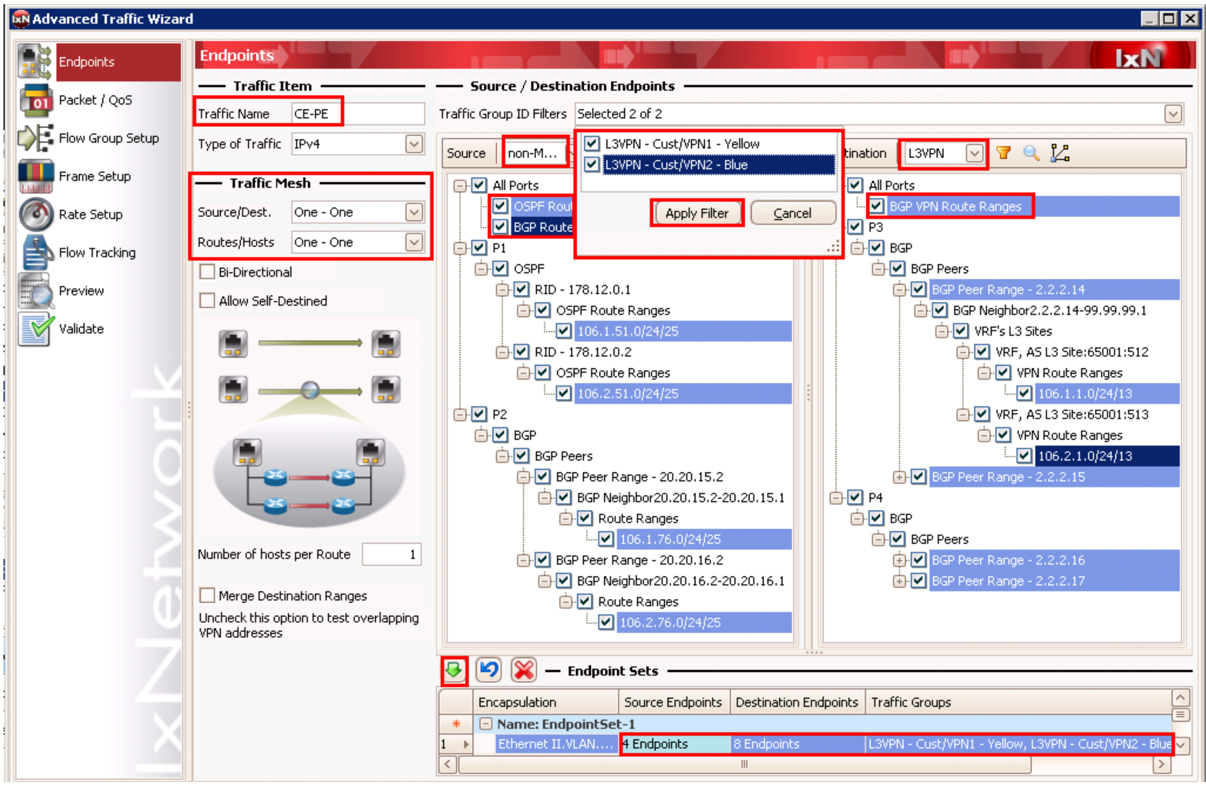


Figure 92. Advanced Traffic wizard screen 1

21. Optionally use the **Packet/QOS** window (not shown) to add a TCP or UDP header, or configure VLAN priority bits or IP QOS levels for each **Endpoint Set**.

22. Optionally, use the **Flow Group Setup** window (not shown) to separate the VLANs (i.e. VPNs) per port, or separate the QoS levels per port, into separate **Flow Groups**. Each **Flow Group** utilizes its own transmit engine and can have unique content, and its own rate and frame size.

23. Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration, such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing use of the wizard.

24. Select the **Flow Tracking** options for CE-PE traffic.
    a. In this test it is **Traffic Item, Source/Dest Value (IP) Pair,** and **VLAN-ID**. Selecting this option will create a track able flow for every combination of the selected items. Each flow will provide full statistics, including rate, loss, and latency.
    b. Click **Next.**

Note: These options are also be available as **Drill-down** views in the **Statistics** windows. In this case there is an aggregated **Traffic Item** statistic that shows all of the combined statistics for every flow within this **Traffic Wizard**. Using a right-mouse-click the **Traffic Item** and drill-down per **Src/Dst Value pair** and/or **VLAN-ID** can be used to view the detailed flow statistics within this traffic Item. This helps immensely in pinpointing trouble areas without investigating many flows.

Note: In large-scale tests, it may not be feasible to select multiple checkboxes. Use the **Resource Bar** at the bottom to see how many resources are used and available when you check each box. Also use the **Validate** window at the end of this wizard to understand the precise number of resources used.

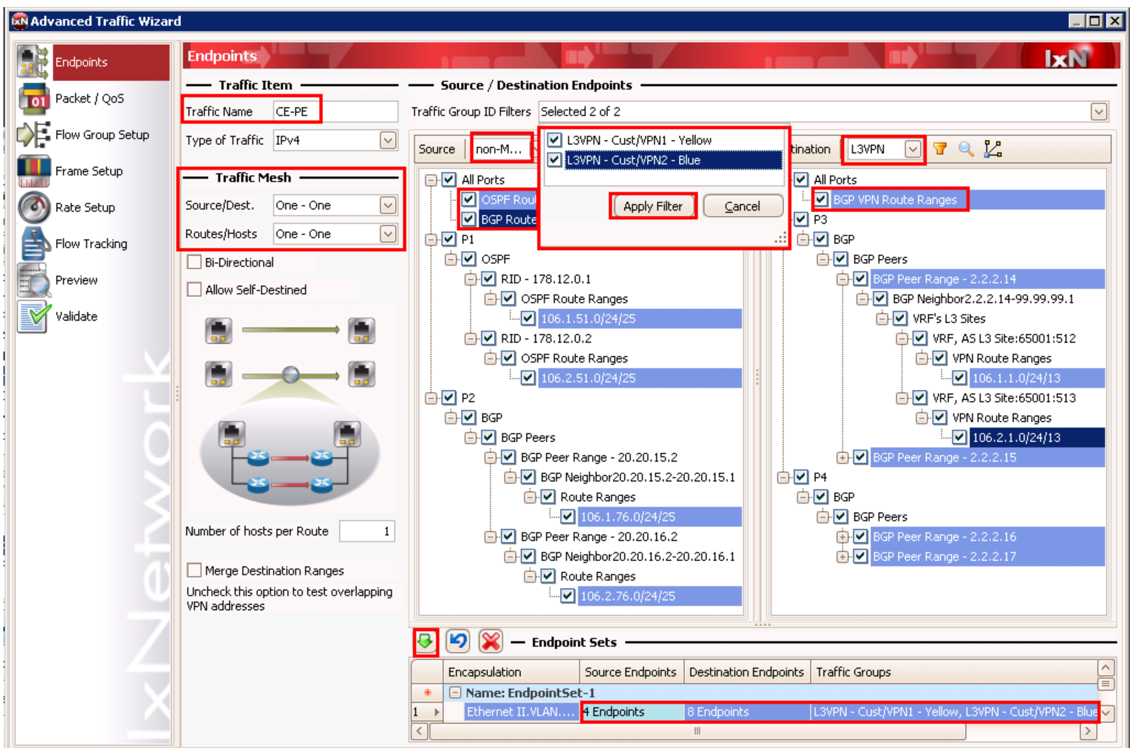


Figure 93. Advanced Traffic Wizard Screen 6

25. Optionally, on the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that will be transmitted from each Port/Flow Group.
    a. In this case, on P1, Flow Group 1, there are 100 unique packets/flows that will be sent. As shown in the setup topology, 25 routes from each of the 2 VPNs on P1 will send to the 25 routes on the same VPN on P3 and P4. Clicking on P2, Flow Group 2, will yield the same number of packets/flows to P3 and P4.

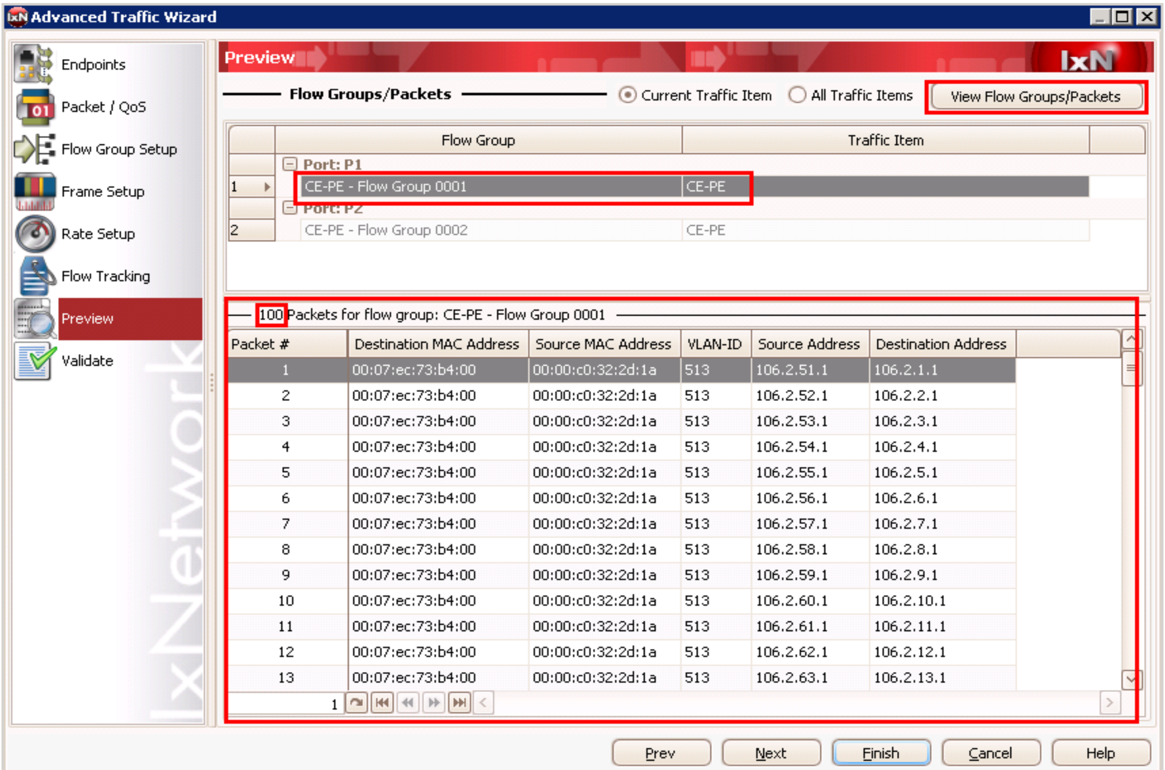


Figure 94. Advanced Traffic Wizard Screen 7

26. Optionally, on the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

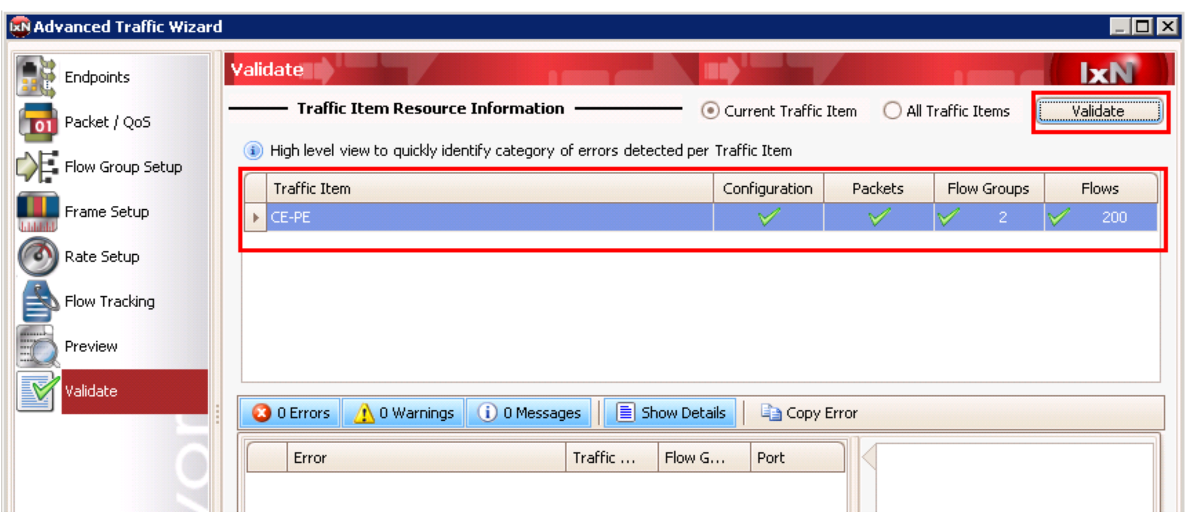


Figure 95. Advanced Traffic Wizard Screen 8

Troubleshooting Tip: If errors are generated after hitting finish, see the **Errors** window at the bottom of the screen. Follow the explanation/steps provided. In this type of test, it is likely that the test ports cannot create the traffic because the DUT has not sent all the information (usually MPLS labels) on the PE side. Check the protocols and view the **Learned** information on both the Ixia and DUT side. To finish again, simply right-click on the affected **Traffic Item** and choose **regenerate.**

Regenerate must also be used if the DUT sends new label information – for example, if a topology change or flapping occurs. The symptom that this has occurred is usually when certain flows experience 100% loss.

27. Now configure the PE-CE traffic. Run the **Traffic Wizard** again by hitting the **+** sign. The steps are practically the same as used for CE-PE, except "in the other direction". Here are the shortened steps (screenshot not shown).
    a. Name the **Traffic Item** as **PE-CE**
    b. Make sure the **Traffic Type** is **IPv4**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select both the **L3VPN – Cust/VPN1 – Yellow** and **L3VPN – Cust/VPN2 – Blue** checkbox and click **Apply Filter.**
    e. Set the source **Encapsulation Type** to **L3VPN,** and the destination to **non-MPLS**.
    f. Select the **Source - BGP VPN Route Ranges** checkbox.
    g. Select the **Destination - OSPF Route Ranges** and **BGP Route Ranges** checkbox .
    h. Click the **down arrow** sign to add the eight sources and four destinations as a traffic Endpoint Set.
    i. Click **Next.**
28. Optionally, use the **Packet/QOS** window (not shown) to add a TCP or UDP header, or configure MPLS EXP bits or IP QOS levels for each **Endpoint Set**.

29. Optionally, use the **Flow Group Setup** window (not shown) to separate the MPLS labels or QoS values per port into separate **Flow Groups**. Each **Flow Group** uses a separate transmit engine and can have unique content, and its own rate/frame size.

30. Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration, such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing the wizard.

31. Select the **Flow Tracking** options for PE-CE traffic (screenshot not shown).
    a. For this direction of traffic it is best to choose **Traffic Item, Traffic Group ID, MPLS Label (1),** and **Source/Dest Value (IP) Pair.**
    b. All possible combinations from all checkboxes will create a track able flow in the statistics (rate, loss, latency, etc.)

    Note: If necessary, also choose **MPLS Label,** but only if the DUT sends something other than label value '3' or '0' for the LDP (or RSVP) label.

32. Optionally, on the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that will be transmitted from each Port/Flow Group.
    a. In this case on P3, Flow Group 1, there are 100 unique packets/flows that will be transmitted. As shown in the **Setup** topology, 25 routes from each of the 2 VPNs on P3 will send to the 25 routes on the same VPN on P1 and P2. Clicking on P2, Flow Group 2, will yield the same number of packets/flows to P1, P2.

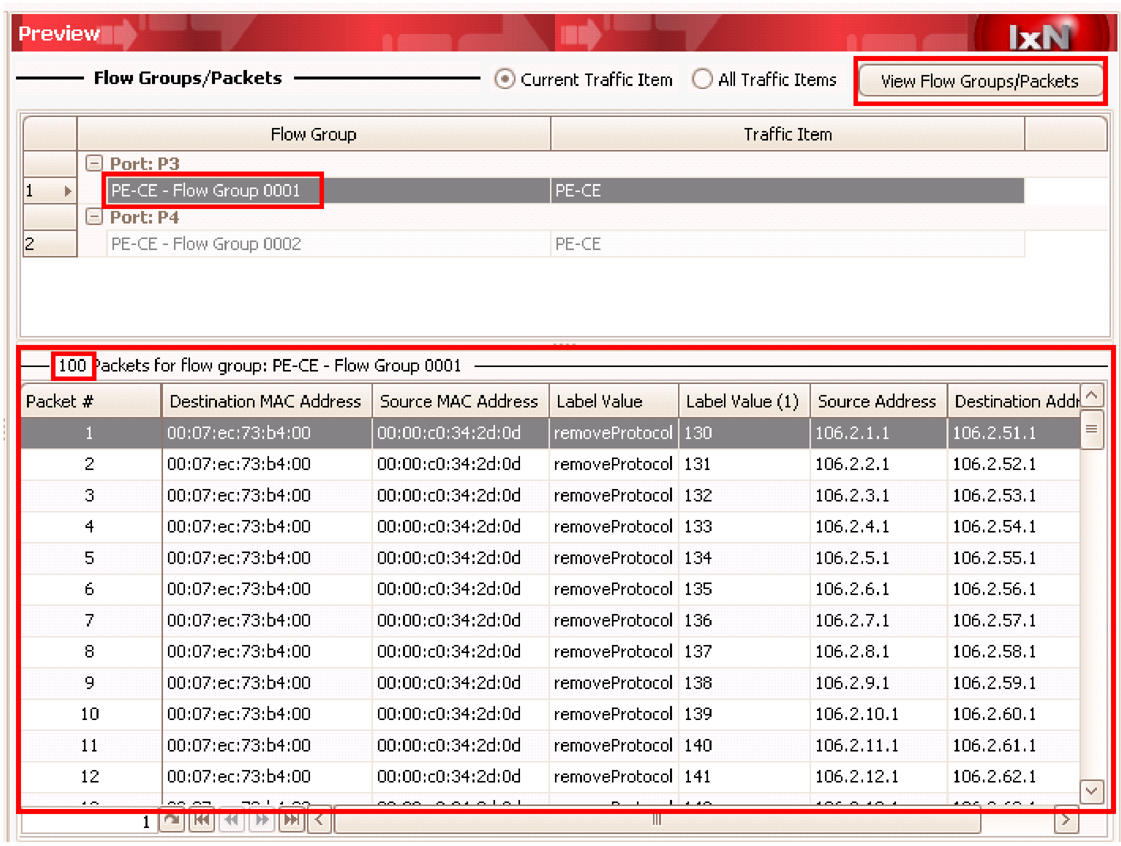


Figure 96. Advanced Traffic Wizard Screen 8

33. Optionally, on the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

34. Optionally, after finishing the **Traffic Wizard**, you will see the **Traffic** (grid) window. There are many operations that can be done here, including:
    - Adding new (tab) views
    - Adding new columns to existing views, including packet contents fields
    - Many grid operation, including multi-select, and copy down/increment.
    - Changing the rate/frame size on the fly without stopping traffic.
    - Double-clicking a flow group to configure its properties/packet contents.

    Performance test variables:
    - Manual performance testing of the data plane can be accomplished by increasing the frame size and data rate.
    - Automatic throughput tests can be accomplished using IxNetwork's integrated tests, as discussed in the *Test Variables* section below.

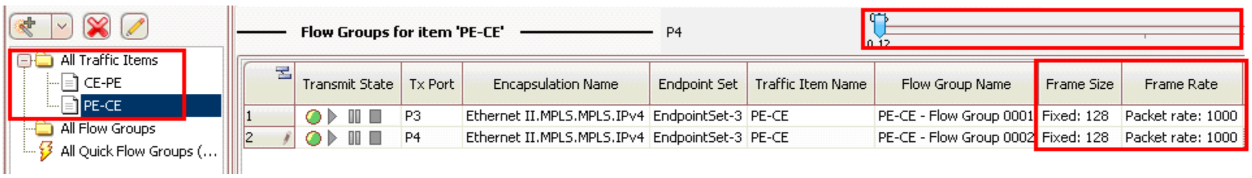
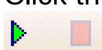


Figure 97. Post-Wizard Traffic Grid

35. **Apply,** and **Start** the traffic.
    a. Click the **Apply Traffic** button at the top of the screen. This will send the Traffic Item configuration down to the hardware.

    b. Click the **Start** (play) button

36. View the traffic statistics.
    a. Click on **Statistics** -> **Traffic Item Statistics**. This will show the aggregated view of all the traffic of each Traffic Item…from CE-PE, and PE-CE.

       Note: The Traffic Item aggregated view is very helpful in understanding the performance of the DUT at a high-level without having to investigate large volumes of results. If everything looks fine, then there is no need to drill-down further. However, if there is loss or high latency, drilling down within each traffic item to pinpoint the problem can become very useful.

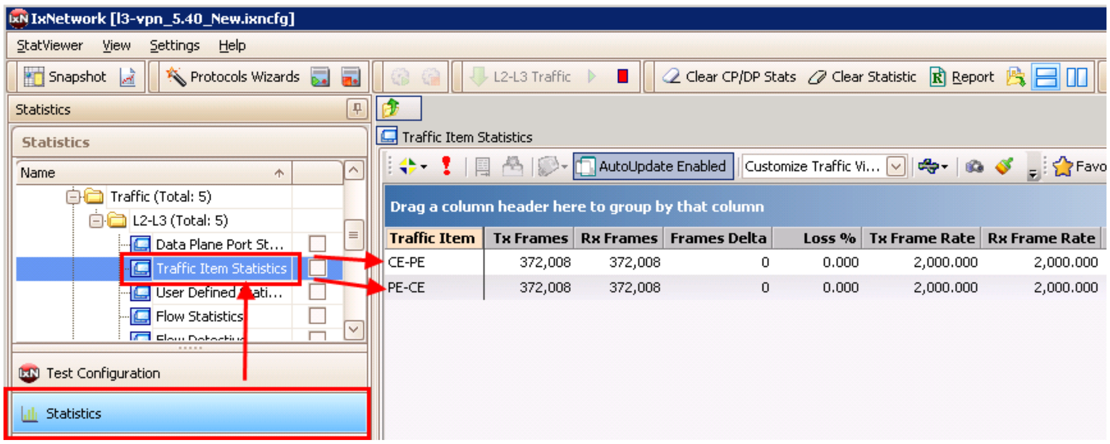


Figure 98. Statistics -> Traffic Item View

Performance test variable*:* Go back to the **Test Configuration** window and increase the rate (in real time) of one or more flow groups until loss occurs. Then use the following step to drill-down to find the problem.

    b. Now **Drill Down** on the CE-PE traffic by right-mouse clicking on the CE-PE Traffic Item and finding the **Flow Tracking** options as defined in the Traffic Wizard. In the example below click on **Drill Down per VLAN ID** to see all the VLAN stats inside the CE-PE Traffic Item. These are the per-VLAN detailed statistics that make up the aggregated CE-PE Traffic Item stat.

       Note: This is very helpful to see if, or which, particular VLAN (i.e. customer VPN) is having issues.

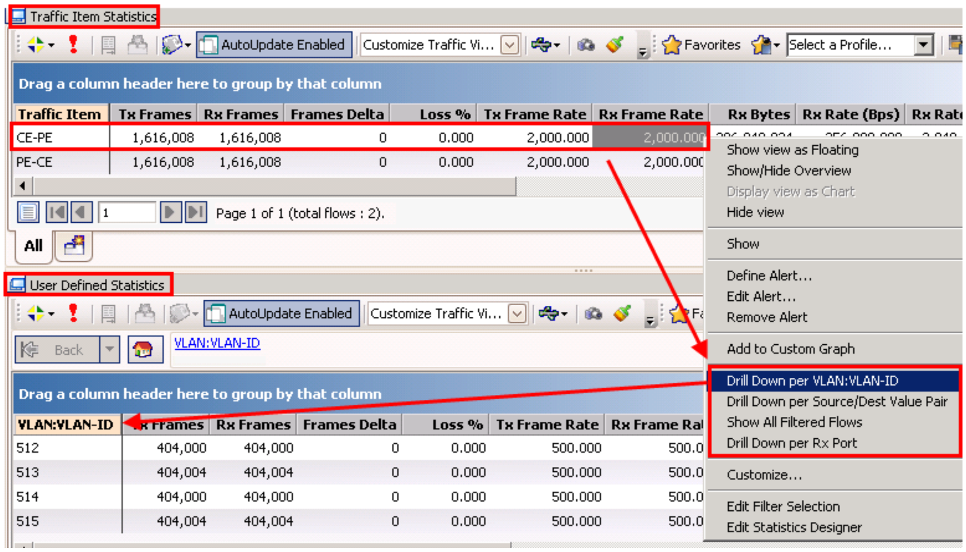


Figure 99. Statistics -> Drill down from Traffic Item to VLAN ID

c. Now **Drill Down** again on VLAN 512 (right-click -> **Drill Down per Src/Dst Value (IP) Pair).** You see all 50 IP flows within VLAN 512 from the CE-PE side

Note: This is very helpful to see if, or which, particular Src/Dst IP within the given VLAN (i.e. customer VPN) is having issues.

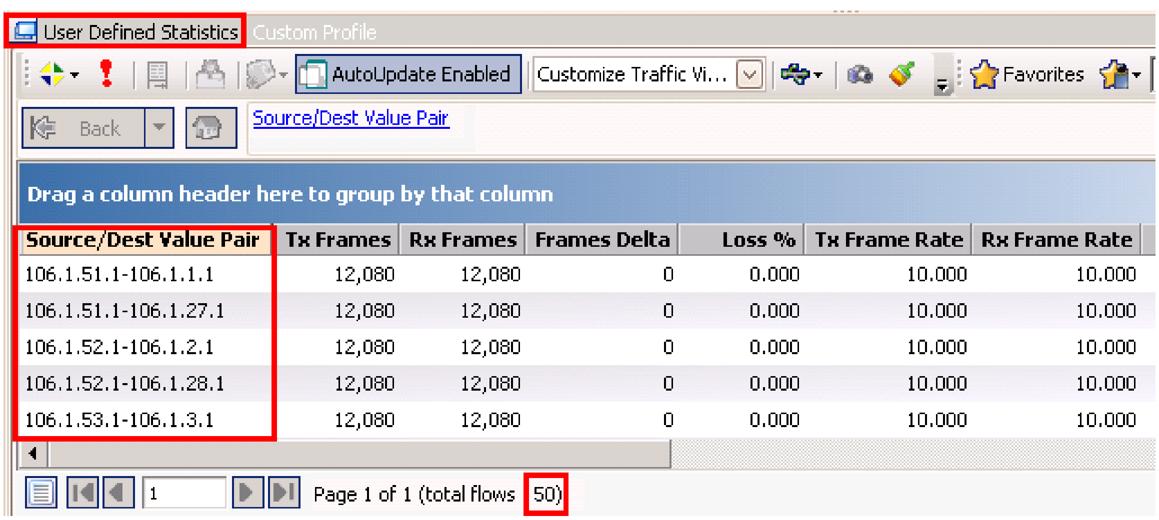


Figure 100. Statistics -> Drill down from VLAN ID to Src/Dst Value (IP) pair

d. Likewise, **Drill Down** on the PE-CE Traffic Item to the **Traffic Group ID.**

Note: This is very helpful to understand how the traffic on each VPN (Traffic Group ID) within the PE-CE traffic is performing. The **Traffic Group ID** can also be used in the CE-PE traffic item.

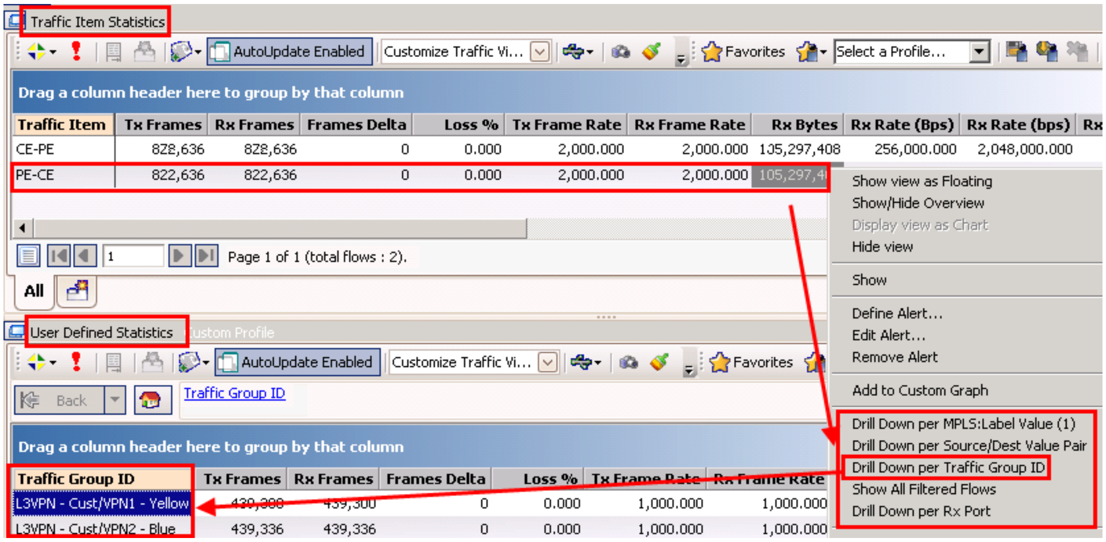


Figure 101. Statistics -> Drill down from Traffic Item to Traffic Group ID

e. Drill down *again* from each **Traffic Group ID** to **MPLS label.**

Note: It is very helpful to understand how the traffic on each MPLS label within the given VPN (Traffic Group ID) is performing.

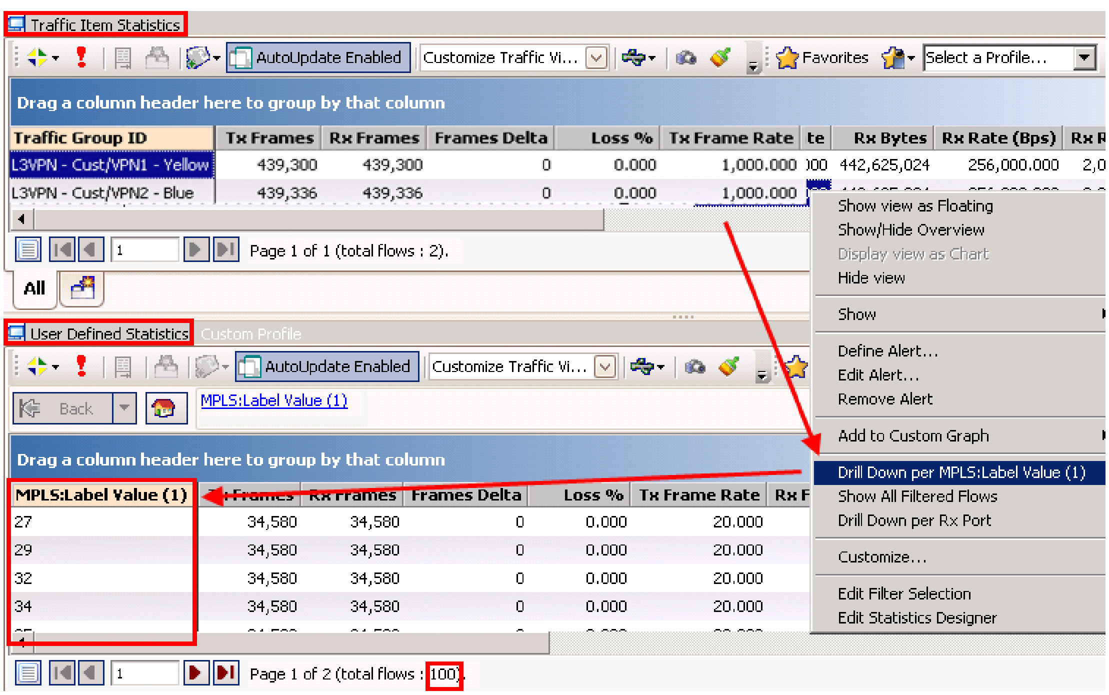


Figure 102. Statistics -> Drill down from Traffic Group ID to MPLS label

f. Optionally, drill down again from each **MPLS Label** to **Source/Dest Value (IP) Pair.**

Note: This is very helpful to understand how the traffic on the IP routes within each MPLS label is performing.

Note: **Drill-down per Rx Port** is included by default with every drill-down view. In this case, it will help determine which RX port on the CE side is receiving the suspect MPLS traffic from the PE side. It may help determine which VPN is the source of the problem without having to go to the label database and track the label through the network to the CE side.

Troubleshooting tip: In any of the above views, a small frame delta statistic does not necessarily mean that loss is present. Stopping traffic will fully synchronize the results. No test tool can measure Tx and Rx instantaneously, since the traffic must go through the DUT first. If the frame delta is continually increasing, however, there is likely loss.

Test Variables

Each of following items can be used as separate test cases to test a PE Router in an L3 VPN network. They all use the test case developed thus far as a baseline. By simply modifying a few parameters, you can create control plane scalability tests from 10x to 100x or higher to fully stress the DUTs capability as a PE router and understand its capacity to peer with CEs, Ps, and other PEs. Once control plane scalability is understood, data plane performance can be added and measured in terms of throughput, latency, and loss for every frame size or IMIX pattern available.

Control Plane Performance Variables

Performance Variable	Description
Increase CE Ports	**Step 5**: On a real world PE router, there will be many more CE ports than P or PE ports, and each CE ports will have many CEs/VLANs on them.
Increase PE Ports	**Step 5**: On a real-world PE router, there is typically a minimum of 2 provider ports (1 for backup), and it's possible some or many of these ports will be high speed (10G) and therefore high control plane scalability requirements.
Increase Emulated Ixia P Routers	**Step 6**: Increasing Ixia P Routers per port will stress the DUT's (PE) ability to peer/run MPLS and IGP protocols. If needed, use VLANs.
Use different IGP, or MPLS Protocols	**Step 6**: Try the other routing protocols, such as ISIS and RSVP-TE. These protocols may have higher or lower overhead on the DUT and performance may vary.
Increase Emulated Ixia PE Routers	**Step 7**: This is one area that can grow quite large in a SP network, both in terms of IBGP connections and VPN/VRF information

Performance Variable	Description
	exchanged. This will test the DUT's ability to store/maintain VPN/VRF information and not leak the information to incorrect VPNs.
Peer with Route Reflectors	**Step 7**: In boot-up or fail-over scenarios, route reflectors can sometimes flood the PE routers with a number of routes very quickly. Tests can verify the PE's ability to maintain tables and data traffic while being flooded by these RRs.
Increase VPNs/VRFs per PE	**Step 8**: This is another area that can easily produce massive amounts of VRF tables to be maintained by the DUT.
Increase Routes per VPN	**Step 8**: Increasing routes increases memory consumption. This should be tested to measure the max Routes per VPN**.**
Use "Unique VPNs per PE"	**Step 8**: By simple checking this box, it means that the number of VPNs times the number of PEs equates to the total number of VPNs in the test, and this number is tallied not only to the provider side, but also to the number of emulated CEs on the customer side.
Mix CE Routing Protocols	**Step 9**: Only Ixia offers offer all five of the "normal" protocols are run by CE routers, those being EBGP, OSPF, ISIS, RIP and EIGRP. Running a configurable mix/percentage of these protocols ensures the DUT can handle any SP network.

Data Plane Performance Variables

Performance Variable	Description
Increase Traffic Rate	**Steps 23/34**: Manually increase the rate at which traffic is sent. Verify that latency and loss levels per flow are at expectations**.**
Change Frame Size	**Steps 23/34**: Manually change the frame size of the traffic. Smaller frames typically cause more trouble for switches/routers, so tests run with 64-byte packets at a high frame rate will be expected by the SP network operators. Additionally, select one of the real-world IMIX patterns that Ixia provides**.**
Run Binary-search Throughput tests using Ixia's "Integrated Tests"	Go to IxNetwork Test Configuration Window and look for "7. Integrated Tests". These tests will automatically run "binary-search" Throughput tests using any/all frame sizes, and industry standard methodology to determine the maximum amount of Throughput (with no loss) the DUT can handle.

Results Analysis

The test constructed in this booklet proved that the DUT, acting as a PE router, could maintain and run a network consisting of two customer VPNs, each with six sites. Added to that was emulation of two P routers, and four PE routers. In addition, the DUT was able to forward 64-byte data traffic at a rate of 10% (of a 1Gb/s link) across the network with no loss and low latency.

However, even in a small-to-medium size service provider network there can be 10s or 100s of VPNs covering 100s of locations, across 10s or 100s of ports, spanning hundreds or thousands of miles.

Because of this, control plane scalability testing and data plane performance testing is critical to ensure that these networks, and therefore DUTs, can handle the load placed upon them in real-world scenarios. The next section discusses the various ways in which the test case can be further transformed into much more formidable scalability and performance tests.

As the control plane variables are increased to the DUT's maximums, special attention must be paid to the detailed protocol statistics, including up/down sessions, and protocol counters. As well, on the data plane side, each and every IP address should be checked for loss and latency as it flows through the DUT. Packet and route leakage is another critical check to make sure one VPN customers' traffic or forwarding table is not mixed with others. Lastly, long duration tests at maximum scale are required with and without real-world outage situations to ensure expected behavior in a volatile real-world network environment.

Troubleshooting and Diagnostics

Issue	Troubleshooting Solution
Can't Ping from DUT	**Step 13**: Check the Protocol Interface window and look for red exclamation marks (!). If found, there is likely an IP address or gateway mismatch**.**
Sessions won't come up	**Step 16**: Go back to the Test Configuration window and double check the protocol configuration against the DUT. From the Test Configuration window, turn on Control Plane Capture, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.
No "Learned" info	**Step 17**: There is likely a mismatch in the VPN/VRF configuration on the Ixia or the DUT. Check RD/RT, VRF#**.**
Traffic 100% Loss from PE-CE	**Steps 26/33**: Check the "warnings" columns in the Traffic View (and make sure there are no streams that say VPN label not found. The DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then Apply traffic**.**
After Stop/Start Protocols or Link Down/Up Traffic 100% Loss from PE-CE	**Steps 26/33**: Check the "warnings" columns in the **Traffic View** (and make sure there are no streams that say VPN label not found. The DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then Apply traffic**.**

Conclusions

This test verified that the DUT can perform at four ports of scale as a PE router in a layer 3 MPLS VPN network.

However, further scalability and performance are of paramount importance when testing a DUT acting as a PE router. Follow the **Test Variables** section above to test the PE at its maximum capacity before deploying into a real-world L3 MPLS VPN Network.

Layer 2 MPLS VPNs – PWE Testing

Pseudo-wire emulation (PWE) is a L2 VPN service offered by service Providers. PWE provides L2 point-to-point circuits over a provider managed IP/MPLS network.

Each pair of customer sites that need to communicate with each other and belong to the same VPN (i.e. enterprise customer) appears to be on the same dedicated circuit regardless of their locations – just as in a leased line. The customer's connection into the provider network can use various L2 encapsulations, providing legacy support into the provider MPLS (Ethernet) backbone. A PWE-capable network is composed of three types of devices:

- **Customer edge (CE) routers** – The CE is a router or switch located at the customer's premises. It connects to a PE router. Unlike L2 VPLS (virtual private LAN service) that can only interface to the PE over Ethernet, with PWE the interface between the CE and PE can use frame relay, ATM, HDLC, PPP, Ethernet, or other media with PWE.
- **Provider edge (PE) routers** – The PE is where the intelligence of the customer's VPN originates and terminates. All of the necessary virtual circuits (VCs) are set up to connect to all the other PEs within the provider MPLS network. Unlike L2 VPLS networks that require the PE to maintain a forwarding/MAC table for each customer's VPN across many sites, PWE is a point-to-point pipe between two sites, and therefore the PE does little work in maintaining CE tables and information. However, if there are many sites to a customer VPN, a full mesh of PWE VCs between sites may be required. The PE routers run an IGP protocol (such as OSPF or ISIS) to the service provider core as well as LDP Extended-Martini protocol to the other PEs to exchange VPN/VC information.
- **Provider (P) router** - A P router interconnects the PEs and runs the provider MPLS core network. It does not participate in the VPN functionality. It simply switches the VPN traffic using MPLS labels. The P routers run an IGP protocol (such as OSPF or ISIS) to other Ps and PEs within the service provider network, along with LDP or RSVP-TE for MPLS signaling.

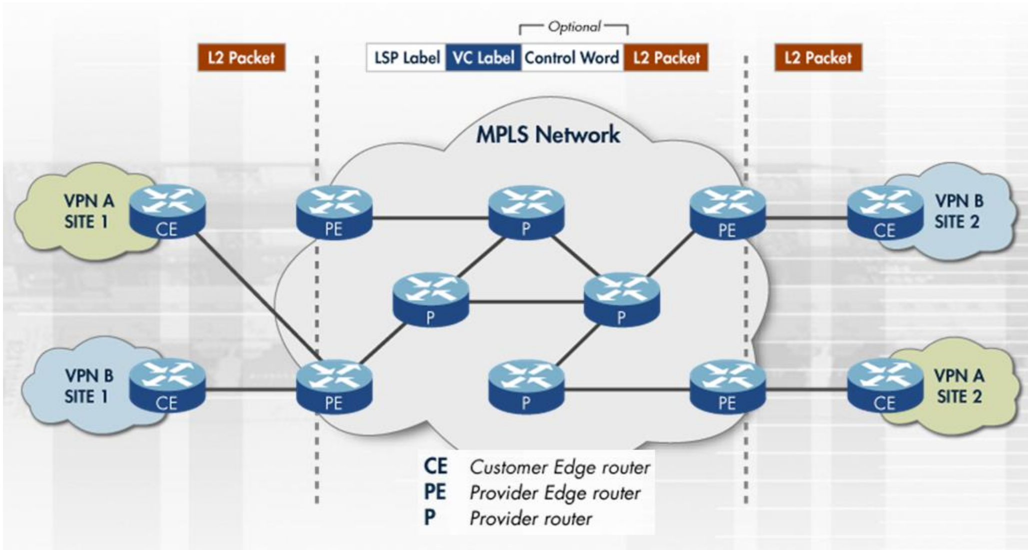


Figure 103. Typical L2 VPN – PWE network

Testing a L2 VPN – PWE-based network centers on the PE routers.

The PE routers need to maintain separate VCs for every point-to-point site within a given VPN. These VPN/VCs must be maintained by the PE router without leakage to other customer VPNs/VCs. The uncertainty of the number of CEs for a given customer/VPN, different types of L2 connections into the PE router (ATM, FR, etc.), CE flapping, and CE-based router security threats create the need for a plethora of functional and performance tests for the PE.

On the service provider side of the PE router, an IGP such as ISIS or OSPF must be chosen, as well as a core MPLS protocol – either LDP or RSVP-TE. Combinations of these protocols must be tested to ensure efficient operation in a service provider network.

The LDP Extended-Martini protocol is the brain of PWE networks and requires significant testing, including interaction with the existing IGP/MPLS protocols already running in the provider core.

All of these aspects of the PE router need initial testing at the functional level, but more importantly at the performance level, including:

- Scaling CEs (over VLANs) with a varied number of L2 interfaces.
- Scaling PEs in the provider network. All PE neighbors must peer with each other, causing many VPN/VC tables to be exchanged. Flapping is another key test case. It is also very important to test the scalability of the LDP Extended-Martini signaling protocols in terms of number of point-to-point VCs supported.
- Scaling Ps in the core of the provider network to switch the massive amount of MPLS and (in some case) non-MPLS packets.

- Data plane performance at the maximum CE, PE, or P scale. Testing should not only include throughput, but verify that MAC/VPN leakage is not present.

Further performance test cases using Ixia's IxNetwork can be verified with the following step-by-step test case, along with the *Test Variables* section further below.

Relevant Standards

- The PE Router LDP Specification – RFC 3036
- LDP Applicability – RFC 3037
- LDP State Machine – RFC 3215
- Transport of Layer 3 Frames Over MPLS – draft-martini-l2circuit-trans-mpls-09.txt
- Pseudo-wire emulations:
  - draft-martini-ethernet-encap-mpls-01.txt
  - draft-martini-ppp-hdlc-encap-mpls-00.txt
  - draft-ietf-pwe3-frame-relay-02.txt
  - draft-martini-atm-encap-mpls-01.txt
  - draft-malis-sonet-ces-mpls-05.txt

Test Case: Layer 2 MPLS VPN – PWE Scalability and Performance Test

Overview

Although L2 MPLS VPN – PWE networks are becoming widely available, router vendors and service providers should carefully consider a number of scalability issues.

Service provider PE routers need to allow for the partitioning of their resources between unique customer VPNs/VCs, and at the same time partition their Internet routing resources. The PE router in a L2 MPLS VPN - PWE network must:

- Create separate point-to-point VCs from any/all sites to any/all sites within a given VPN for each customer/VPN to ensure communications.
- Run MPLS and IGP protocols into the core of the service provider network, usually connecting to faster P/PE routers on high-speed links.
- Peer with all other PE neighbors and exchange VPN/VC info with them.
- Make forwarding decisions at microsecond speeds while bi-directionally adding/popping MPLS and VC labels.
- Keep enterprise customers' VPN traffic and Internet traffic separate from each other.

Because of this, the focus of the tests is mostly centered on the PE, as all the unique customer/VPN intelligence is implemented within the PE routers. L2 MPLS VPN – PWE technology takes advantage of the emerging MPLS technology for tunneling data packets from different VPNs over the same service provider network. LDP Extended-Martini is extensively used for VPN exchange and for the distribution of VPN reachability information. The combination of the core MPLS protocols and the LDP Extended-Martini working together make up this exciting technology.

The best methodology for performance testing of a PE is to create a scalable baseline test, and then modify it in different ways to test the control plane and data plane performance. This testing will verify the PE's ability prior to being deployed in a real-world, revenue generating, service provider network.

Objective

The objective of this test is to baseline the scalability of a single DUT acting as a PE router in a Layer2 VPN – PWE network.

At the end of this test, other test variables will be discussed that will provide many more performance test cases, using the topology discussed below as the baseline.

Setup

The test will consist of a DUT acting as a PE router, and four Ixia ports.

Two Ixia test ports will emulate four customer edge (CE) devices. Also within each port will be four CE routers, each belonging to a different customer/VPN.

The other two Ixia ports will emulate the entire service provider network as well as the other CE sites for each PWE circuit.

In total, this test will emulate two Ps, four PEs, and eight VPNs (each with two sites), as shown in the Figure 104 below.

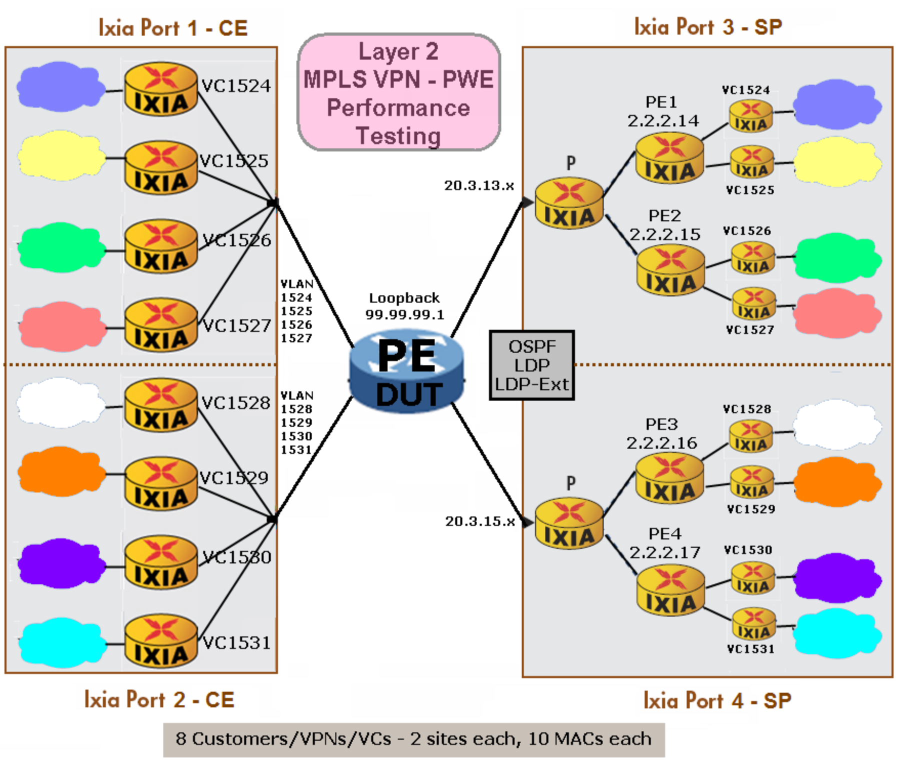


Figure 104. Ixia emulated L2 VPN - PWE network

Step-by-Step Instructions

Following these step-by-step instructions will produce a Layer2 VPN – PWE performance test as shown in Figure 105. Optionally, you may use the steps below as a guide to building other Layer2 VPN – PWE performance test scenarios.

1. Reserve four ports in IxNetwork.

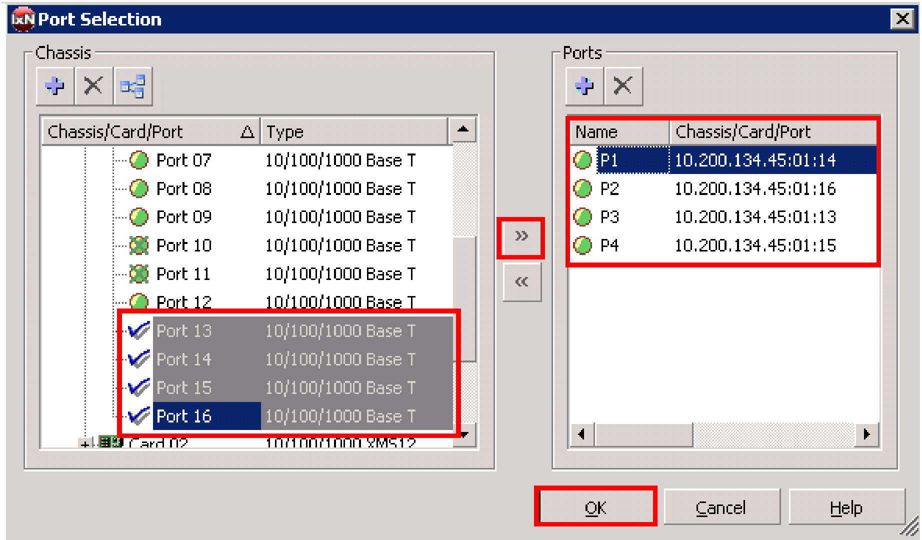


Figure 105. Port reservation

2. Rename the ports for easier use throughout the IxNetwork application.

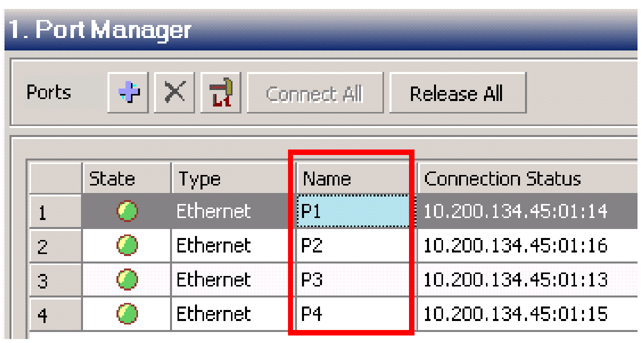


Figure 106. Port naming

3. Click the **Protocol Wizards** button on the top toolbar in the IxNetwork application.

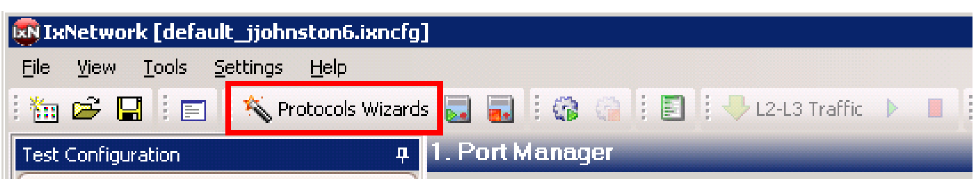


Figure 107. Protocol wizards

4. Run the **L2 VPN/VPLS** protocol wizard.

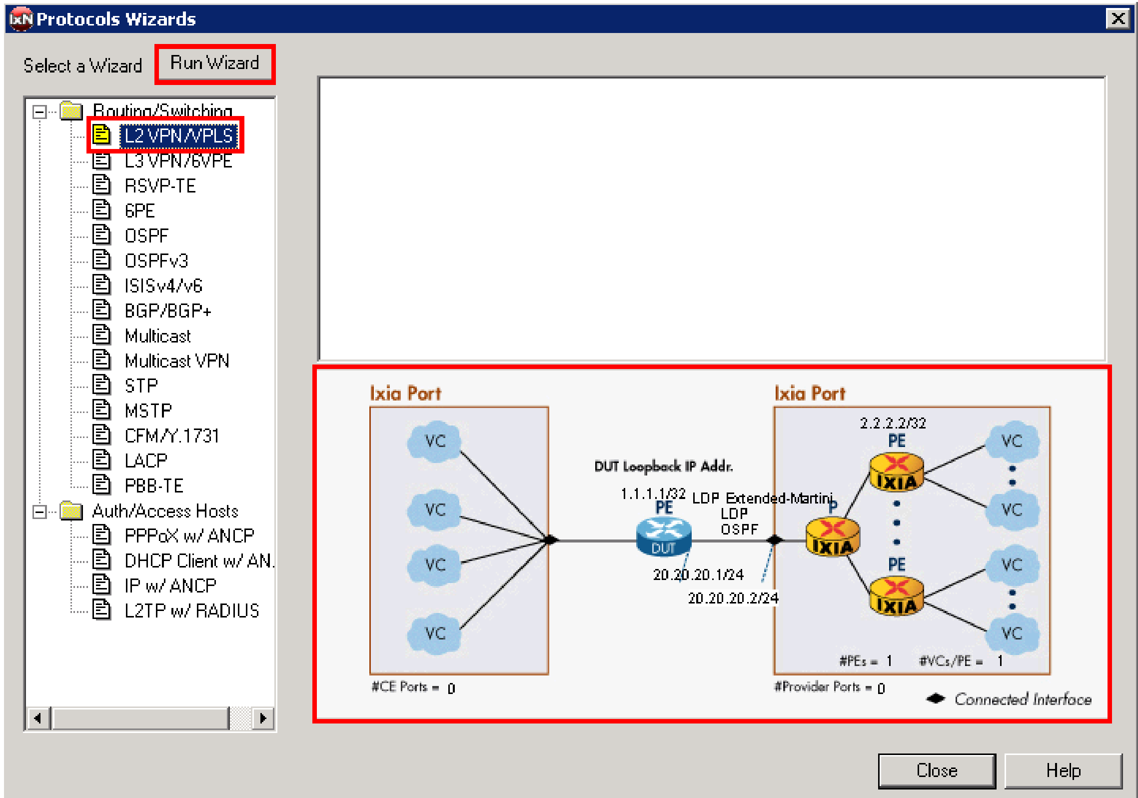


Figure 108. L2 VPN Wizard

Note: the wizard supports **both** L2 VPN – PWE as well as L2 VPN – VPLS. In brief, L2 VPN – PWE runs point-to-point virtual circuits across the MPLS core, and L2 VPN – VPLS supports the MPLS as an effective L2 switch for point-to-multipoint.

Note: the picture represents a typical test case for testing a PE router in an L2 VPN network.

5. Configure **P1** and **P2** to emulate the CE (left) side of the topology, and **P3** and **P4** for the SP (right) side of the topology, then click **Next**.

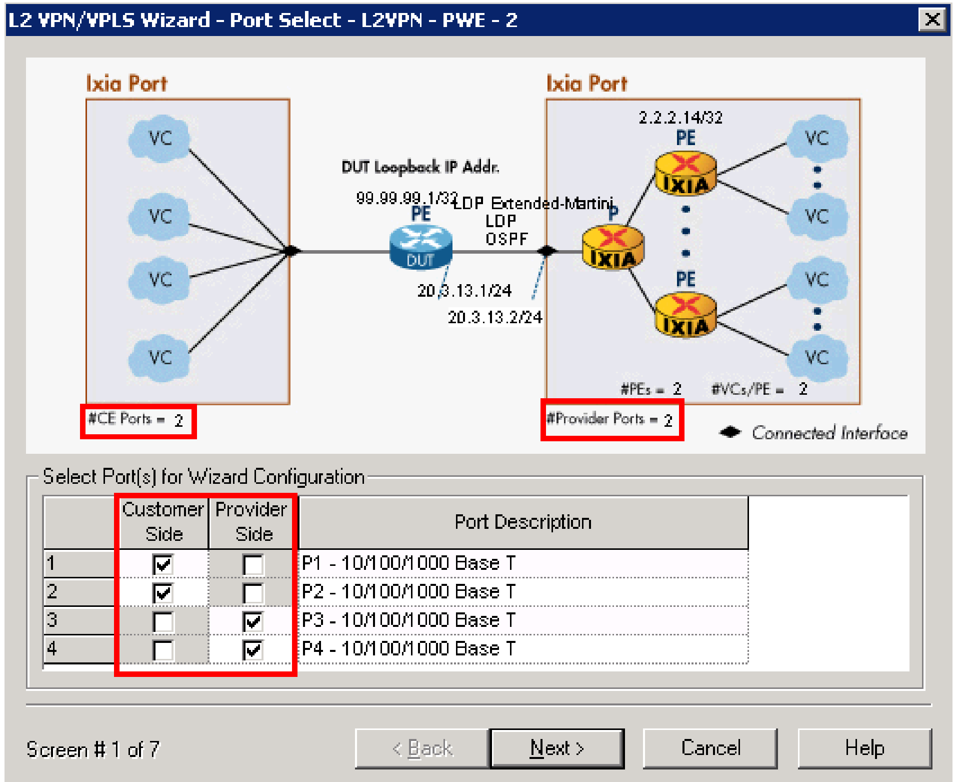


Figure 109. L2 VPN Wizard Screen1 of 6

Note: The picture in the top window will update with the number of customer-side ports as well as the number of provider-side ports.

Performance test variable*:* Increase the number of customer and provider ports to test the DUT's (PE's) ability to scale at a port level. In a real-world network, there are more customer ports than provider ports.

6. This window configures **P3** and **P4** with emulation of one or more P routers. These ports will be configured to talk directly to the DUT (PE) Router.
   a. Keep the default of **1** P Router. This is a per-port setting.
   b. Configure a starting subnet between the Ixia P router and the Ixia PE routers. Any subnet will work. In this case, use *11.1.1.0/24.*
   c. Configure the **IGP Protocol** and **MPLS Protocol** running in the SP core.
      - In this test use the defaults of **OSPF** and **LDP**, respectively.
   d. Configure the **L2 VPN Signaling Protocol** running in the SP core.
      - In this test use **LDP Extended-Martini**.
   e. Configure the Ixia **P Router IP Address** on **P3** and the **DUT IP Address**.
      - In this test they are *20.3.13.2/24* and *20.3.13.1/24*, respectively.
   f. Configure the **Increment per port** option to support the **P4** IP address
      - In this test it is *0.0.2.0.*
   g. Click **Next**.

Optionally:

a. Disable (uncheck) **Enable P routers**. The Ixia port(s) would then only emulate PE routers (i.e. no P router emulation), and would test the DUT in a PE-to-PE scenario.

Performance test variables:

- Increase **the number of emulated P Routers** to test the DUT's ability to peer with many P routers, all running an IGP/MPLS protocol.
- Check the **Enable VLAN** checkbox (not shown) to run these protocols over VLANs. Enter the first **VLAN ID** and choose an incrementing function.

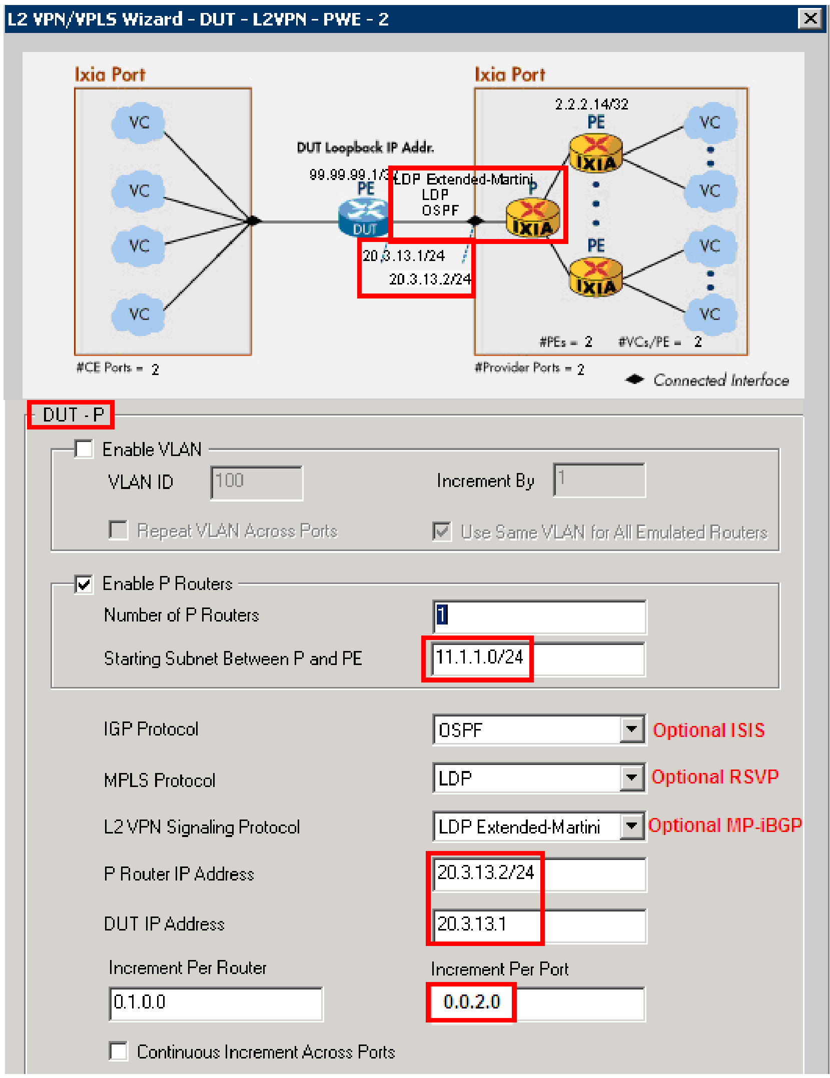


Figure 110. L2 VPN wizard screen 2 of 6

Note: The screen above updates with the configured protocols/IP addresses.

7. This window configures **P3** and **P4** with emulations of one or more **PE routers** that operate directly behind the emulated P router(s).
    a. Configure the **Number of PE Routers Connected to the P Router**. This is a per-port setting.
        In this test it is *2* PEs (per P)
    b. Configure **Emulated PE Loopback Address** and its incrementing function for the additional PEs.
        In this test it is *2.2.2.14* (the 2nd, 3rd, and 4th PE will be assigned **2.2.2.15, 2.2.2.16,** and **2.2.2.17,** respectively)
    c. Configure **DUT Loopback IP Address.**
        In this test it is *99.99.99.1*
    d. Click **Next**.

Performance test variable: Increase the number of PE routers per P router. This will test the DUT's ability to peer with many PE routers and potentially many VPNs/VCs.

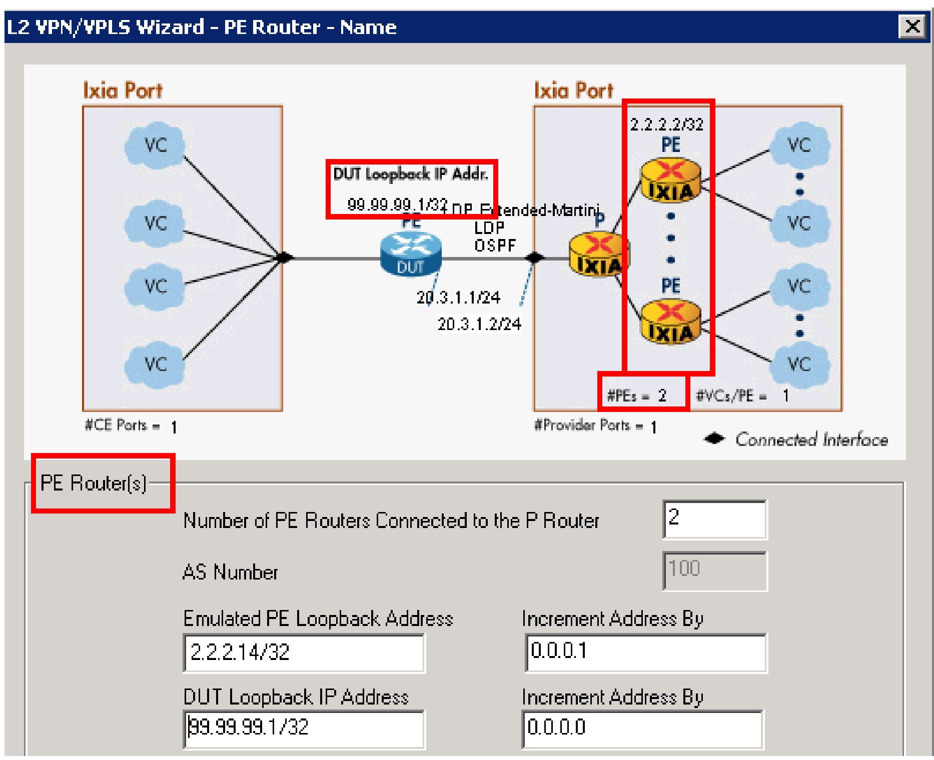


Figure 111. L2 VPN wizard screen 3 of 6

8. This window configures the number of L2 Interfaces (VCs) for all ports in the test; refer to Figure 112.
    a. Configure the **VPN Traffic ID Name Prefix**.
       For most L2 VPN test cases use *L2VPN*.
    b. Configure the **VC Pack Type**. The option **All VCs in one VC range** will combine all of the VCs from each PE into a single line (row) in the post-wizard LDP configuration tab called **L2 VC Ranges**. This helps summarize each PE's VCs, but is less granular than **One VC per VC Range** – which allows all post-wizard configuration options to be assigned per VC.
       In this test use **One VC per VC range**.
    c. Configure the **VC Interface Type**. This option specifies the type of L2 interface configured on the port.
       It is **VLAN** for P1 and P2 in this test .
    d. Configure the **Number of VC/VPN IDs per PE**. The number entered here will be multiplied by the number of PEs configured and the sum will represent the total number of VCs in the test.
       In this test it is *2* VCs per PE (= 8 VCs in the test)
    e. Configure the **First VC/VPN ID**. This is the VC number that will be used over the extended LDP session to talk to the DUT (PE).
       In this test it is *1524* (it is just a coincidence that in this test case it is the same as the VLAN ID, although this is a common practice).
    f. Click **Next**.

Optionally:
Check the **Enable VPLS** box to run point-to-multipoint VPLS using LDP Extended-Martini signaling. In this test topology scenario, the VPNs on the PE side would be repeated across PEs, meaning that each of the 6 PEs would have the same 2 VPNS connected to it, creating two 7-site VPNs.

Performance test variables:
- Increase the **Number of VC/VPN IDs per PE**. This will test the DUT's maximum capacity for number of VCs.
- Test with different **VC Interface Types** (**ATM, FR, Ethernet**, and so on).

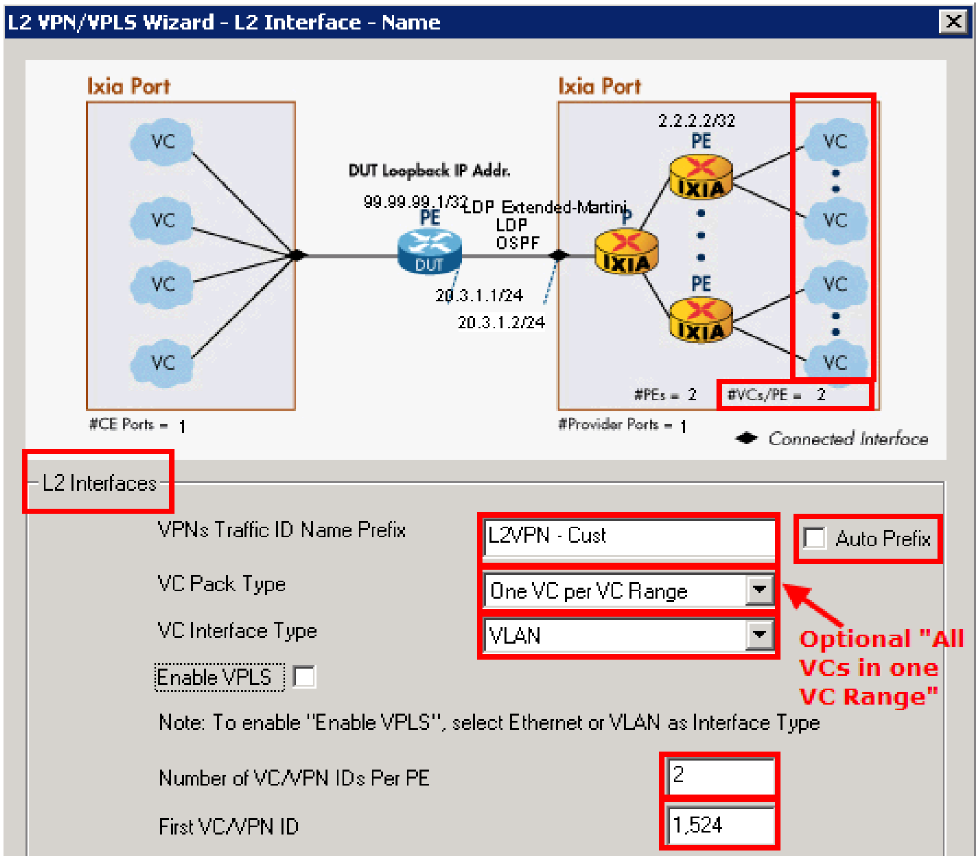


Figure 112. L2 VPN wizard screen 4 of 6

Note: The picture above will update with the number of PEs and the number of VCs per PE. The picture does not change for every emulated topology.

9. This window configures the parameters for P1and P2 and their emulation of **MACs/VLANs.** It also configures the number of MAC addresses that will be used in the test within each VC.
    a. Configure the **Number of MAC Addresses per VC**. By default, 50% of the MACs go on P1 and P2, and 50% on P3 and P4 (this is configurable in **Distribute MAC Address**).
        In this test case, *10***.** 5 MACs will be used on the VCs on P1 and P2, and 5 MACS on the VCs on P3 and P4.
    b. Enter the **First VLAN ID** for the first VC on P1.
        i. In this test it is *1524*.
        ii. The second VC on P1 will use VLAN 1525, and so on.
    c. Click **Next**.

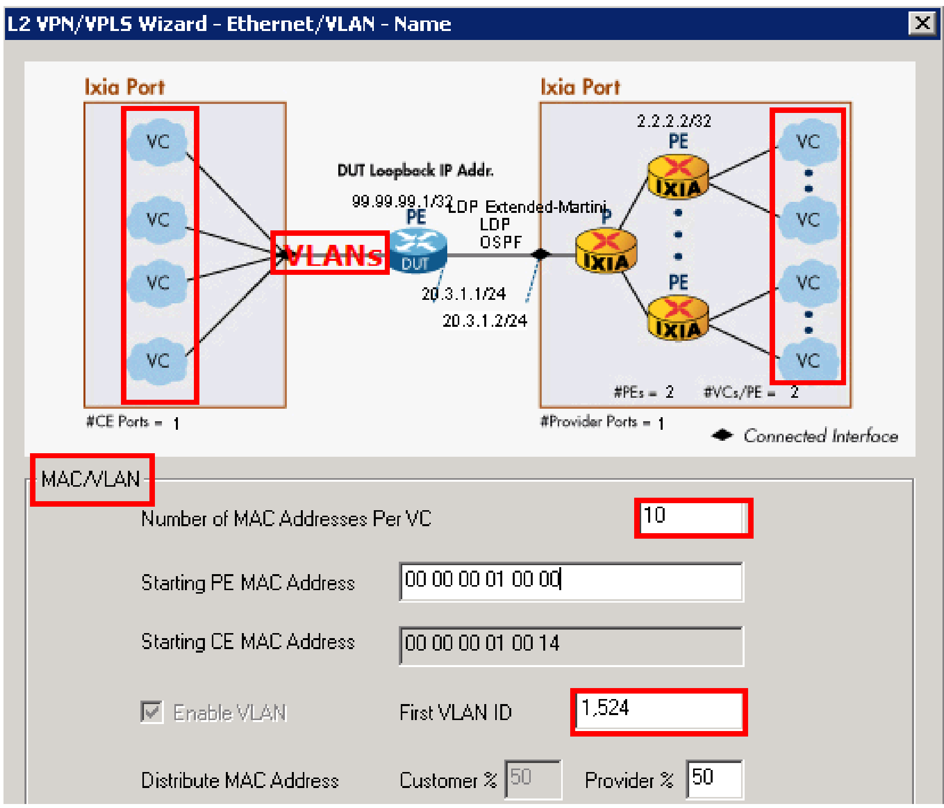


Figure 113. L2 VPN wizard screen 5 of 6

Note: The MAC addresses and VLAN IDs are assigned sequentially across all ports in the test.

10. This window configures the name of the wizard run and the action to take with this run of the wizard.
    a. Use a descriptive name for the wizard. In this test use *L2VPN – PWE.*
    b. Specify what to do with the finished wizard configuration.
       In this test select **Generate and Overwrite All Protocol Configurations**. This will overwrite all previous configurations.

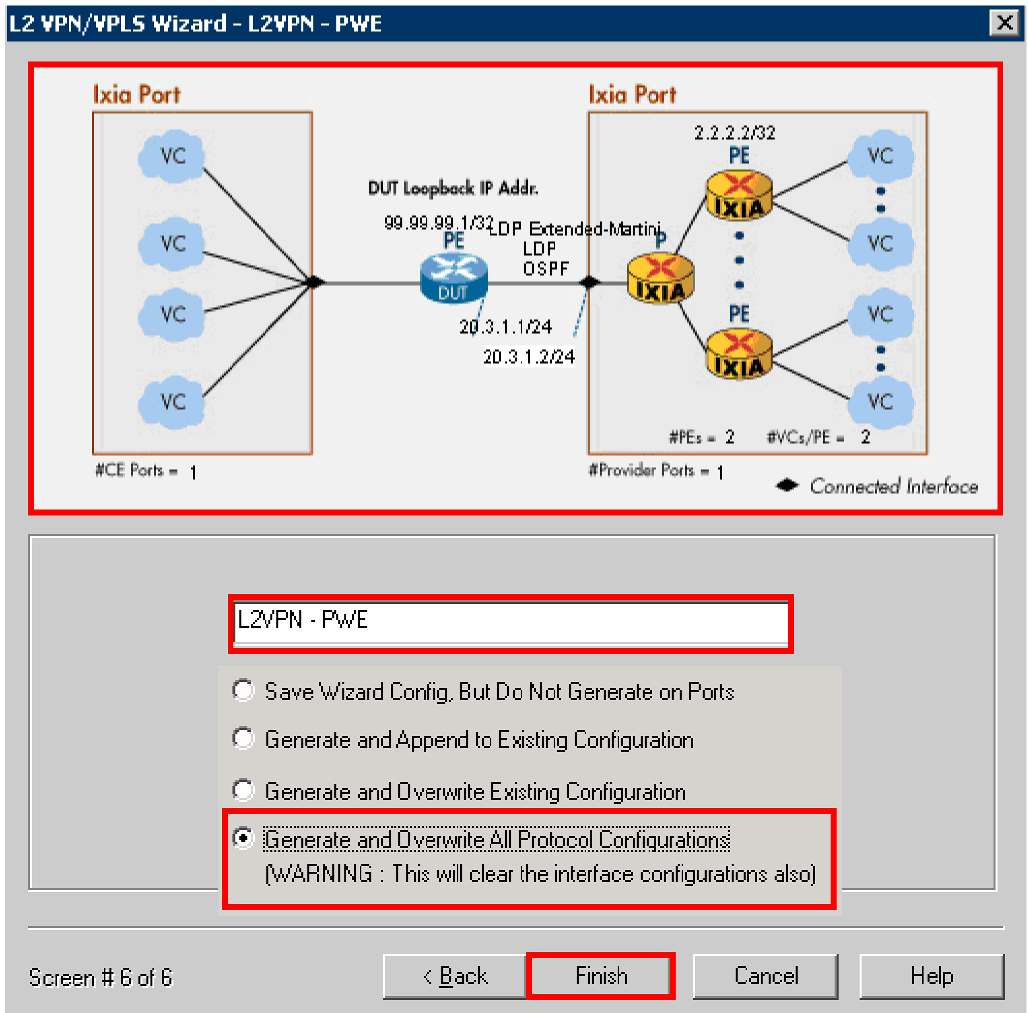


Figure 114. L2 VPN Wizard Screen 6 of 6

11. This window displays the saved wizard template.
    a. Click **Close** to finish the wizard configuration.
    b. ***Optionally***, with saved wizard templates, you may:
        - Come back to the same wizard to (double-click) view and/or modify.
        - Save new or modified wizards with a new name (or overwrite).
        - Create a library of templates for use in different tests.
        - Highlight each template and preview the configuration in the topology below.

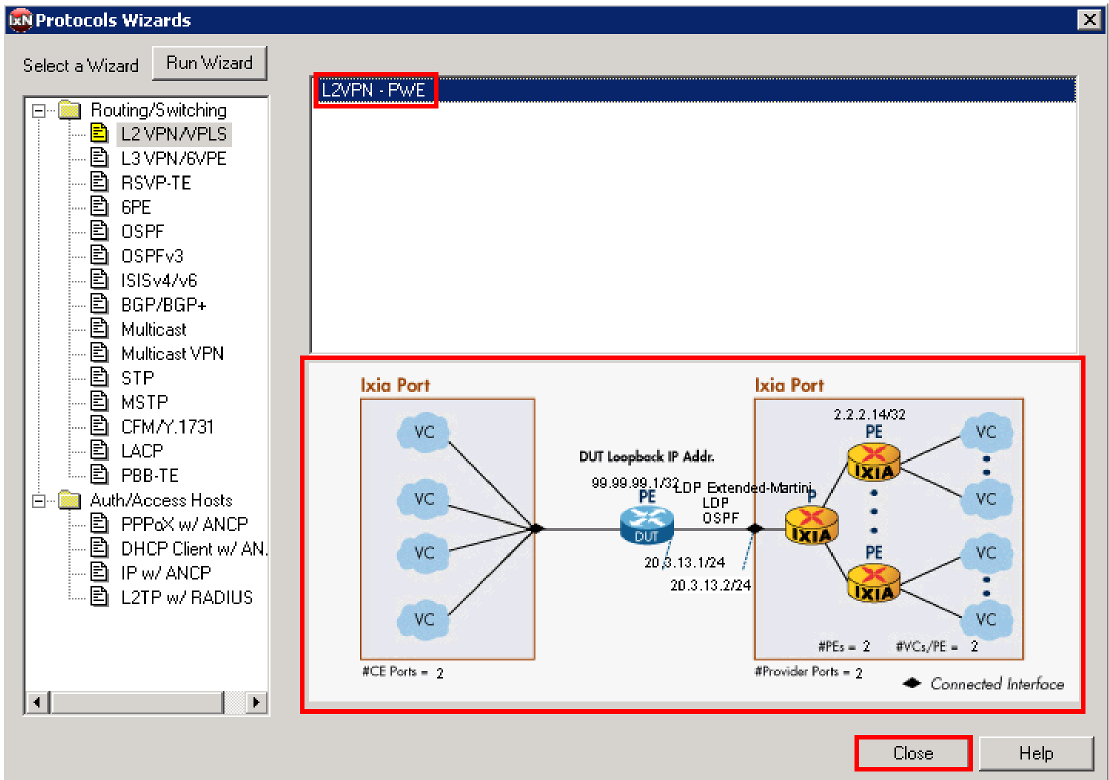
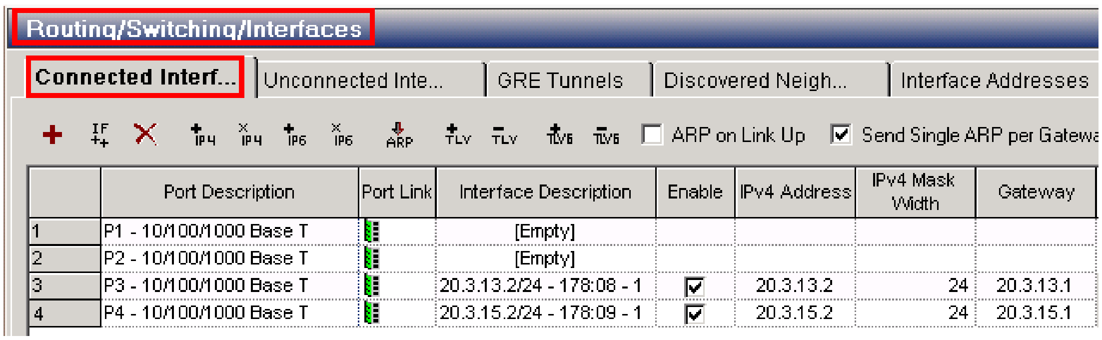


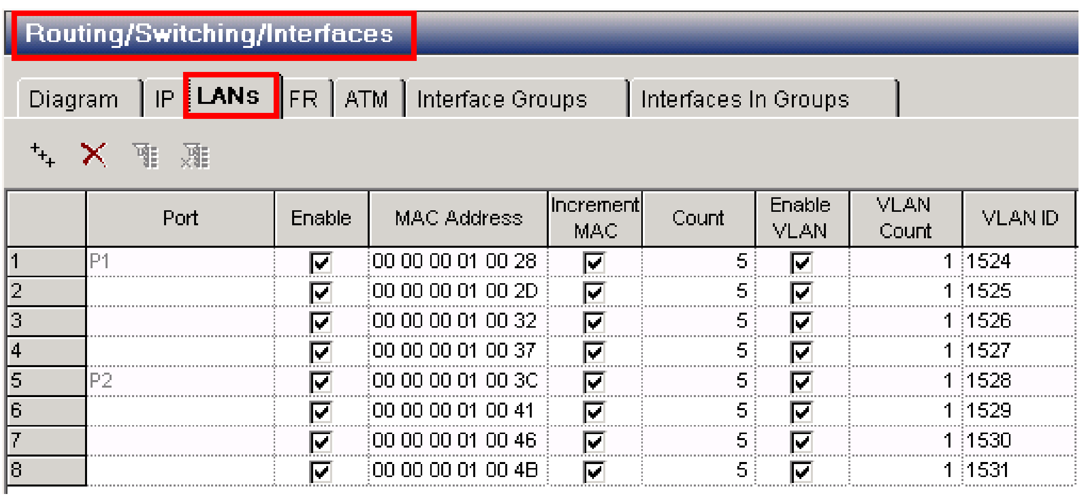
Figure 115. L2 VPN wizard saved wizard template

12. Once the wizard is done, go through the IxNetwork configuration windows to see how the wizard configured them, and verify IP connectivity between the DUT interfaces and the Ixia port interfaces. For example,
    a. Click on the **Routing/Switching/Interfaces** window on the top, and the **Protocol Interfaces** in the middle.
    Verify that the IP addressing/incrementing functions of the wizard properly created IP interfaces to connect to the DUT. If necessary, manually change them to match the DUT.
    b. Click on the **Routing/Switching/Interfaces** window on the top, and the **Static folder** in the middle.
    Verify that the MAC/VLAN addressing/incrementing functions of the wizard properly created the MAC/VLAN values to talk to the DUT. If necessary, re-run the wizard to correct this, or change them manually in this window.



	Port Description	Port Link	Interface Description	Enable	IPv4 Address	IPv4 Mask Width	Gateway
1	P1 - 10/100/1000 Base T		[Empty]				
2	P2 - 10/100/1000 Base T		[Empty]				
3	P3 - 10/100/1000 Base T		20.3.13.2/24 - 178:08 - 1	☑	20.3.13.2	24	20.3.13.1
4	P4 - 10/100/1000 Base T		20.3.15.2/24 - 178:09 - 1	☑	20.3.15.2	24	20.3.15.1

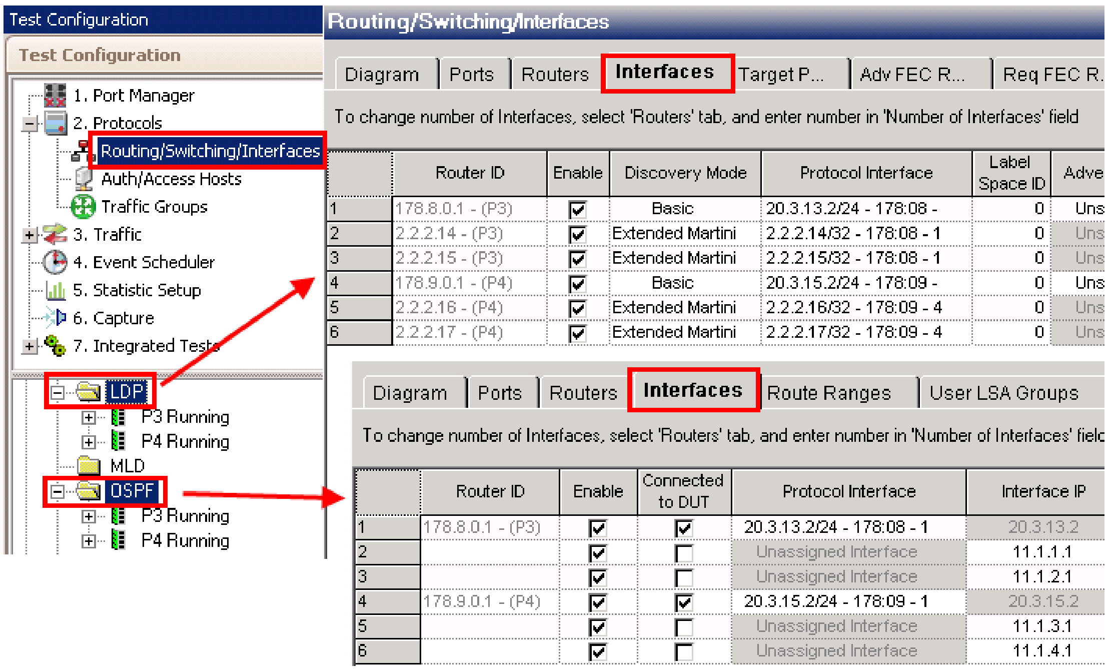
Figure 116. Protocol interface window



	Port	Enable	MAC Address	Increment MAC	Count	Enable VLAN	VLAN Count	VLAN ID
1	P1	☑	00 00 00 01 00 28	☑	5	☑	1	1524
2		☑	00 00 00 01 00 2D	☑	5	☑	1	1525
3		☑	00 00 00 01 00 32	☑	5	☑	1	1526
4		☑	00 00 00 01 00 37	☑	5	☑	1	1527
5	P2	☑	00 00 00 01 00 3C	☑	5	☑	1	1528
6		☑	00 00 00 01 00 41	☑	5	☑	1	1529
7		☑	00 00 00 01 00 46	☑	5	☑	1	1530
8		☑	00 00 00 01 00 4B	☑	5	☑	1	1531

Figure 117. Static MAC window

13. Click on the **Routing/Switching/Interfaces** window on the top, and the **LDP** and **OSPF** protocol in the middle. Make sure the settings will work with the DUT configuration. For example;
    a. On **P3** and **P4**, note the one **Basic LDP** peer and two **Extended-Martini** peers on both going from the emulated P and PEs, respectively, on to the DUT (PE).
    b. Note the two **OSPF** peers going from the emulated P to the DUT (PE).
    c. If necessary, manually change the configuration in the protocol table/grid. Another option would be to highlight columns and right-mouse click to further customize with **Same** or **Fill Increment** options.



	Router ID	Enable	Discovery Mode	Protocol Interface	Label Space ID	Adve
1	178.8.0.1 - (P3)	☑	Basic	20.3.13.2/24 - 178:08 -	0	Uns
2	2.2.2.14 - (P3)	☑	Extended Martini	2.2.2.14/32 - 178:08 - 1	0	Uns
3	2.2.2.15 - (P3)	☑	Extended Martini	2.2.2.15/32 - 178:08 - 1	0	Uns
4	178.9.0.1 - (P4)	☑	Basic	20.3.15.2/24 - 178:09 -	0	Uns
5	2.2.2.16 - (P4)	☑	Extended Martini	2.2.2.16/32 - 178:09 - 4	0	Uns
6	2.2.2.17 - (P4)	☑	Extended Martini	2.2.2.17/32 - 178:09 - 4	0	Uns

	Router ID	Enable	Connected to DUT	Protocol Interface	Interface IP
1	178.8.0.1 - (P3)	☑	☑	20.3.13.2/24 - 178:08 - 1	20.3.13.2
2		☑	☐	Unassigned Interface	11.1.1.1
3		☑	☐	Unassigned Interface	11.1.2.1
4	178.9.0.1 - (P4)	☑	☑	20.3.15.2/24 - 178:09 - 1	20.3.15.2
5		☑	☐	Unassigned Interface	11.1.3.1
6		☑	☐	Unassigned Interface	11.1.4.1

Figure 118. Protocol configuration window

14. Click the **Statistics** window on the bottom left and click the **Start all Protocols** button on the toolbar.

15. Click on the **Global Protocol Statistics** option for a summary of all protocols running on each port.

a. Check if all of the OSPF and LDP sessions are up.

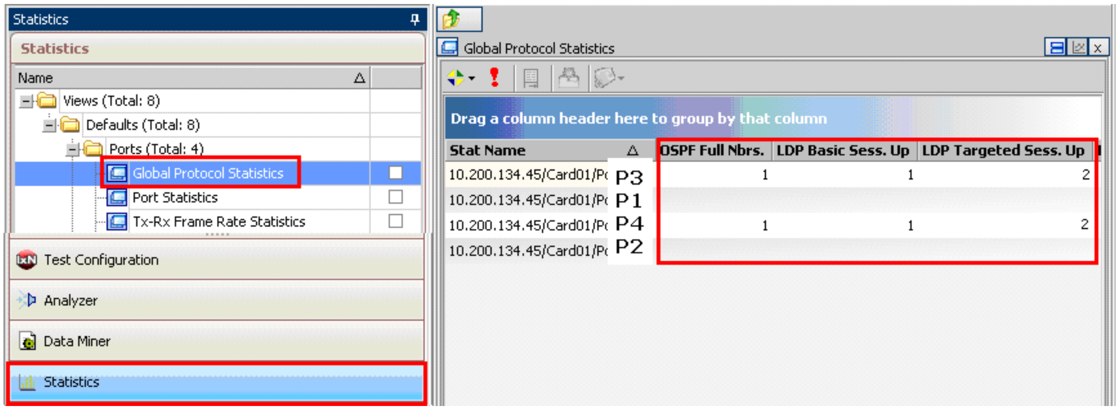


Figure 119. Global Protocol Statistics Window

Note: Optionally click on each of the specific protocol statistics (LDP, OSPF) to see statistics for that protocol (including up/down status as shown in **Global Statistics**).

Troubleshooting tip: If the sessions are not up

a. Go back to the **Test Configuration** window and double check the protocol configuration against the DUT.

b. From the **Test Configuration** window, turn on **Control Plane Capture**, then start the **Analyzer** for a real-time sniffer decode between the Ixia port and the DUT port.

16. Once protocols have been started, use the Ixia learned routes option to verify that each Ixia peer is receiving the correct routes/labels for each peer.
    a. View the MPLS labels learned by the Ixia LDP peers on **P3**.
        i. Click on **Learned Routes** and then **Refresh** to see the labels learned by the Ixia peer. In this test case there should be **two** Martini labels learned from the DUT (PE) to the Ixia PE at 2.2.2.14. Check it against the setup topology.

    Optionally:

    a. View the OSPF routes learned by the Ixia **P1 OSPF** peering sessions and make sure that the BGP routes are being redistributed properly.
    b. View the regular LDP labels coming from the DUT (PE) to the Ixia P routers (on **P3 and P4**).

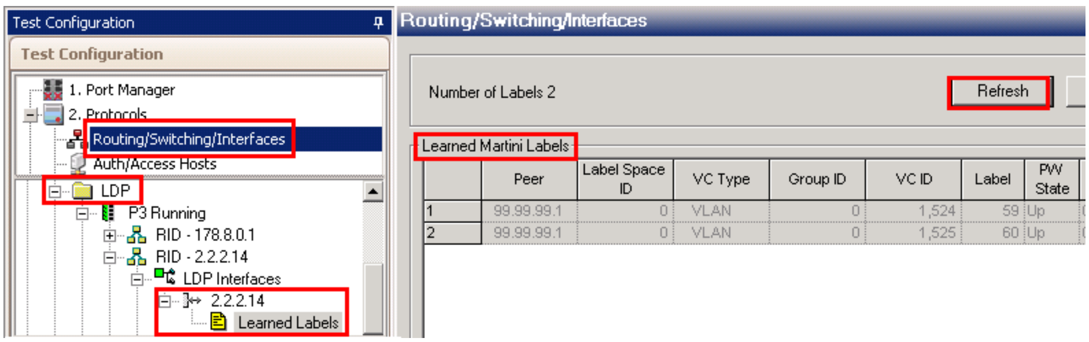


Figure 120. Protocol learned info

17. After all of the sessions are up, you need to build bidirectional traffic from CE-PE, and from PE-CE. Launch the **Advanced Traffic Wizard** by clicking on the **+** sign.

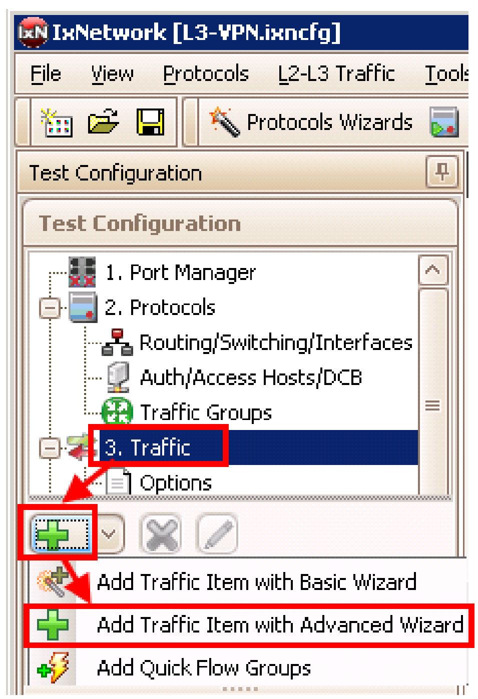


Figure 121. Create traffic

18. First configure the CE-PE traffic
    a. Name the **Traffic Item** to **CE-PE**
    b. Make sure the **Traffic Type** is **Ethernet/VLAN**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select all of them. Click **Apply Filter.**
        i. This will filter the **Source** and **Destination** trees to only display items that belong to these customer/VPNs. It is also possible to select only one Traffic Group ID at a time to see an exact view of all sources/destinations that belong to that customers VPN.
        ii. Even though both Traffic Group ID filters were selected at the same time, IxNetwork is smart enough to only send traffic to/from sources and destinations that belong to the same VPN
    e. Set the source **Encapsulation Type** to **non-MPLS**, and the destination to **L2VPN**. This will further filter the source/destination tree for CE-PE traffic.
    f. Select the **Source – Static Mac VLAN Ranges** checkbox.
       This is a global option that selects all of the static MAC VLANs for the source ports.
    g. Select the **Destination** – **LDP MAC VLAN Ranges** checkbox .
       This is a global option to select ALL of the LDP MAC VLANs for the destination ports.
    h. Click the **down arrow** sign to add the eight sources and eight destinations as a traffic Endpoint Set.
    i. Click **Next.**

Note: It is possible to configure the PE-CE traffic at the same time by selecting the **Bi-Directional** checkbox within this window. However, by creating them in separate Traffic Wizard runs the resources (flows) used can be saved, allowing better use of flow tracking, as selected in the **Flow Tracking** page of this wizard.

Note: Make sure to uncheck the **Merge Destination Ranges** checkbox if the same routes are used on two or more VPNS in the test.

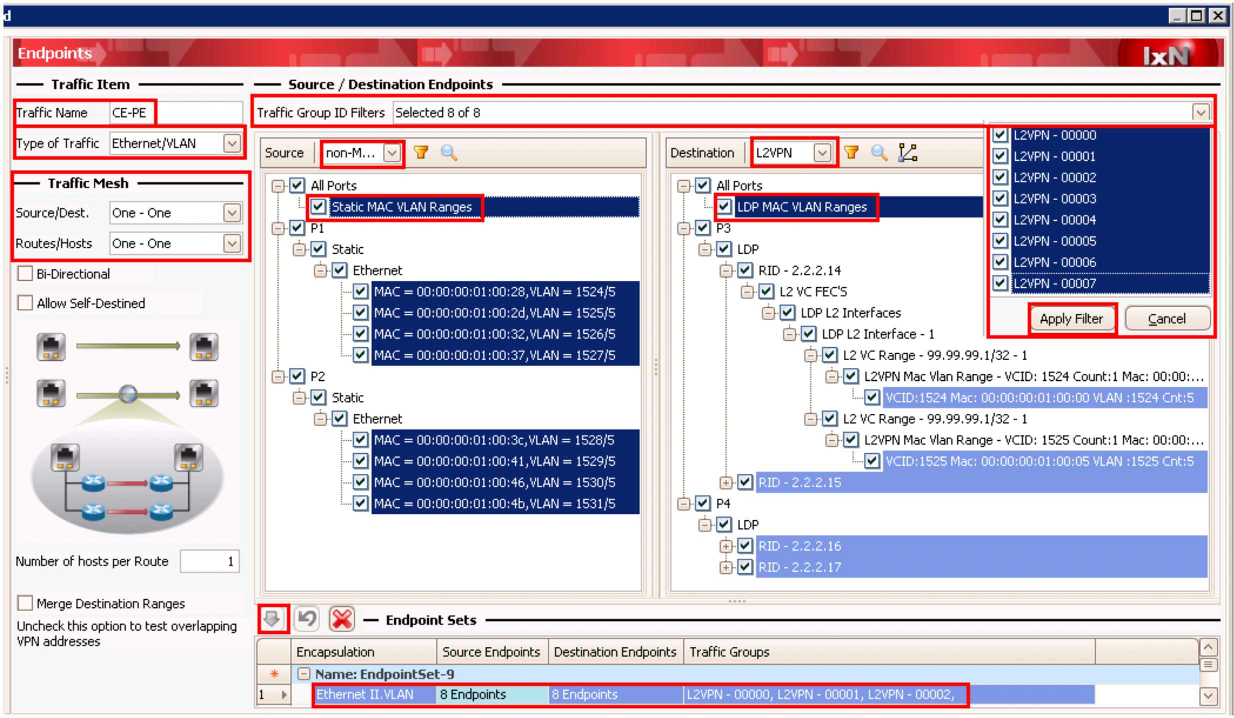


Figure 122. Advanced Traffic Wizard Screen 1

19. Optionally, use the **Packet/QOS** window (not shown) to add an IP/TCP or IP/UDP header, for example.

20. Optionally, use the **Flow Group Setup** window (not shown) to, in this case, separate VLANs/VPNs per port into separate Flow Groups. Each Flow Group uses its own transmit engine and can have unique content, and its own rate/frame size.

21. Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration, such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing the wizard.

22. Select the **Flow Tracking** options for CE-PE traffic.
    a. In this test select **Traffic Item, Source/Dest Value (MAC) Pair, and VLAN-ID**. Selecting these options will create a track able flow for every combination of the selected items. Each Flow will provide full statistics, including rate, loss, and latency.
    b. Click **Next.**

Note: These options will also be available as **Drill-down** views in the Statistics windows. In this case there will be an aggregated **Traffic Item** statistics that shows all of the combined statistics for every flow within this Traffic Wizard. Then, the user can use a right-mouse-click to select the Traffic Item and drill-down per **Src/Dst Value pair** and/or **VLAN-ID** to see the detailed flow statistics within this traffic Item. This helps immensely in pinpointing trouble areas without going through pages of flows.

Note: In large-scale tests, it may not be feasible to select multiple checkboxes. Use the **Resource Bar** at the bottom to see how many resources are used or available when you check each box. Also use the **Validate** window at the end of this wizard to understand the precise number of resources used.

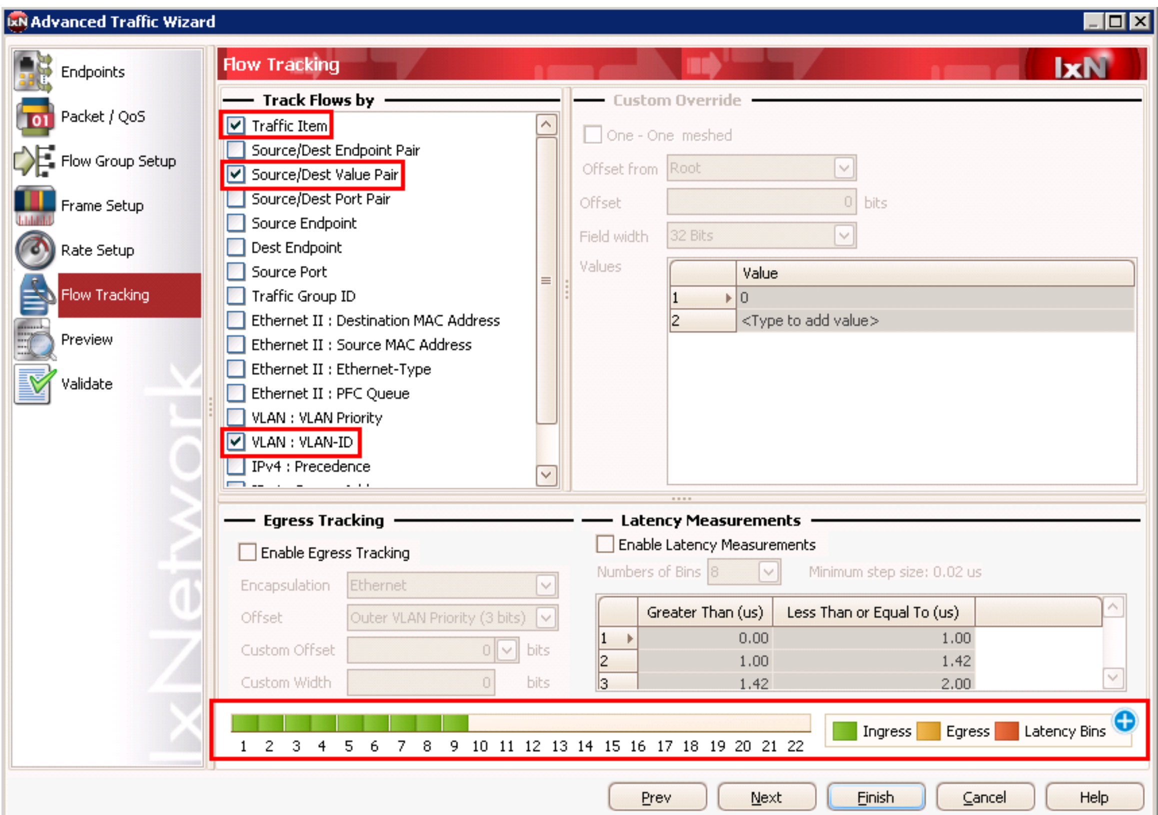


Figure 123. Advanced Traffic Wizard Screen 6

23. Optionally, in the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that be transmitted from each Port/Flow Group.
    a. In this case on P1, Flow Group 1, there are 20 unique packets/flows that will be sent. As shown in the setup topology, five MACs from each of the four VPNs on P1 will send to the five MACs on the same VPN on P3. Clicking on P2, Flow Group 2, will yield the same number of packets/flows to P4.

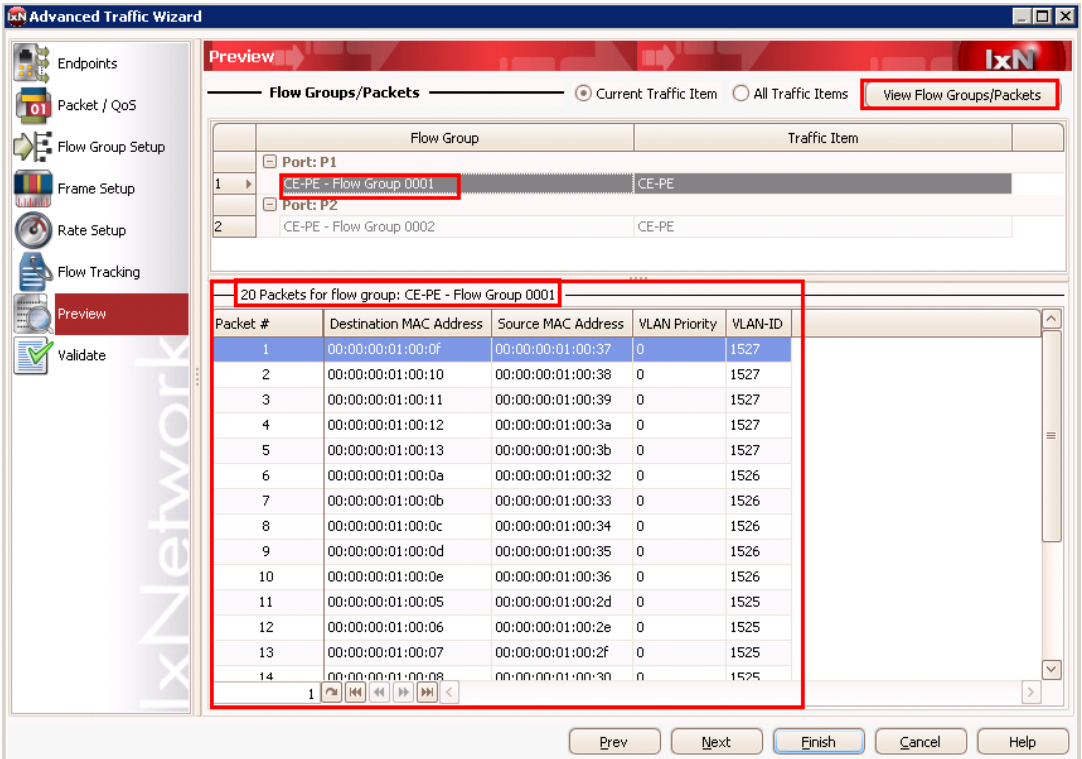


Figure 124. Advanced Traffic Wizard Screen 7

24. Optionally, on the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

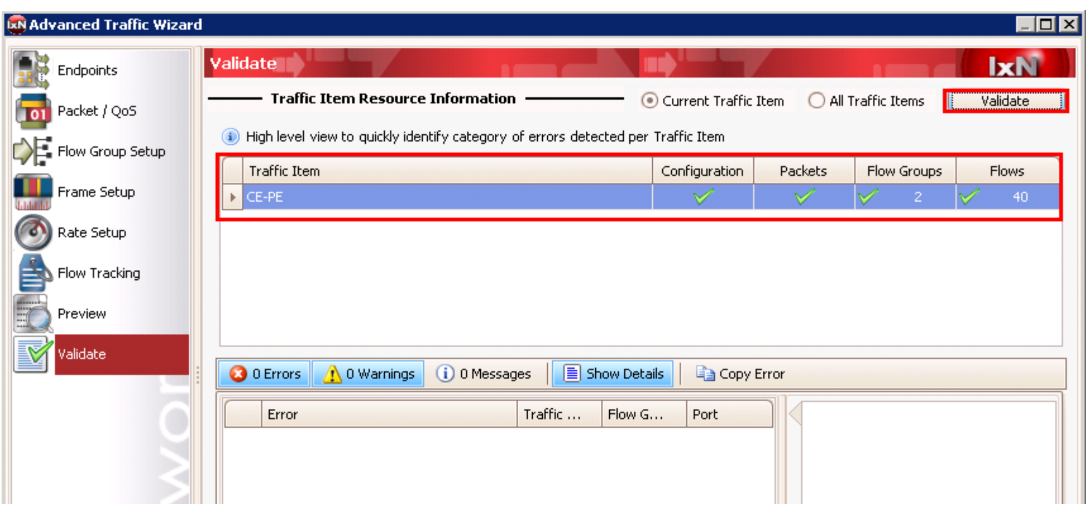


Figure 125. Advanced Traffic Wizard Screen 8

Troubleshooting Tip: If errors are generated after hitting finish, see the **Errors** window at the bottom of the screen. Follow the explanation/steps provided. In this type of test, it is likely the test port cannot create the traffic because the DUT has not sent all the information, usually MPLS labels, on the PE side. Check the protocols and view the Learned information on both the Ixia and DUT side. To finish again, simply right-click on the affected **Traffic Item** and choose **Regenerate.**

Regenerate must also be used if the DUT sends new label information – for example, if a topology change or flapping occurs. The symptom that this has occurred is usually when certain flows are experiencing 100% loss.

25. Now configure the PE-CE traffic. Run the **Traffic Wizard** again by hitting the **+** sign. The steps are practically the same as used for CE-PE, except in the other direction. Here are the shortened steps (screenshot not shown):
    a. Name the **Traffic Item** as **PE-CE**
    b. Make sure the **Traffic Type** is **Ethernet/VLAN**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select all of them. Click **Apply Filter.**
    e. Set the source **Encapsulation Type** to **L2VPN**, and the destination to **non-MPLS**.
    f. Select the **Source – LDP MAC VLAN Ranges** checkbox.
    g. Select the **Destination** – **Static Mac VLAN Ranges** checkbox .
    h. Click the **down arrow** sign to add the eight sources and eight destinations as a traffic Endpoint Set.
    i. Click **Next.**

26. Optionally, use the **Packet/QOS** window (not shown) to add an IP/TCP or IP/UDP header, for example.

27. Optionally, use the **Flow Group Setup** window (not shown) to separate the MPLS labels per port into separate Flow Groups. Each Flow Group uses its own transmit engine and can have unique content, and its own rate/frame size.

28. Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration, such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing the wizard.

29. Select the **Flow Tracking** options for PE-CE traffic (screenshot not shown).
    a. For this direction of traffic it is best to choose **Traffic Item, Traffic Group ID, MPLS Label (1),** and **Source/Dest Value (MAC) Pair.**
    b. All possible combinations from all checkboxes will create a track able flow in the statistics, including rate, loss, and latency.

30. Optionally, in the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that will be transmitted from each Port/Flow Group.
    a. In this case, on P3, Flow Group 1, there are 20 unique packets/flows that will be sent. As shown in the Setup topology, five MACs from each of the four VPNs on P3 will send to the five MACs on the same VPN on P1. Clicking on P4, Flow Group 2, will yield the same number of packets/flows to P2.

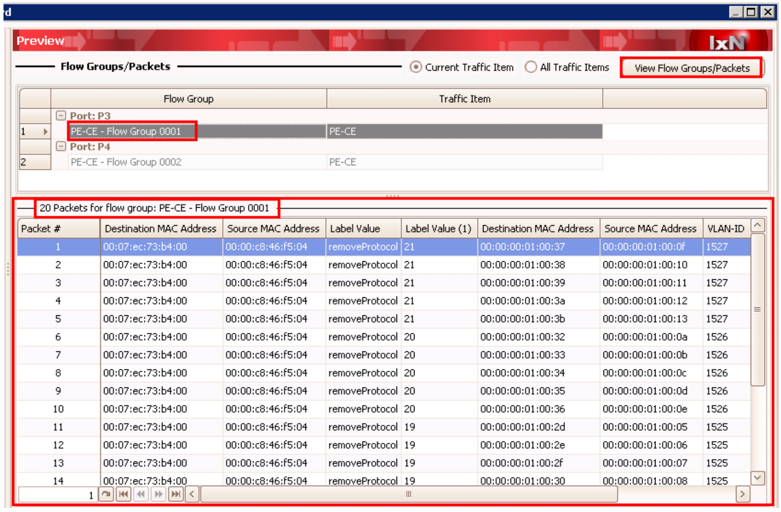


Figure 126. Advanced Traffic Wizard Screen 8

31. Optionally, in the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

32. Optionally, after finishing the Traffic Wizard you will see the Traffic (grid) window. There are many operations that can be done here including:
    - Adding new (tab) views
    - Adding new columns to existing views, including packet contents fields
    - Many grid operation, including multi-select, and copy down/increment.
    - Changing the rate/frame size on the fly without stopping traffic.
    - Double-clicking a flow group to configure its properties/packet contents.

    Performance test variables:
    - Manual performance testing of the data plane can be accomplished by increasing the frame size and data rate.
    - Automatic throughput tests can be accomplished using IxNetwork's integrated tests as discussed in the *Test Variables* section below.

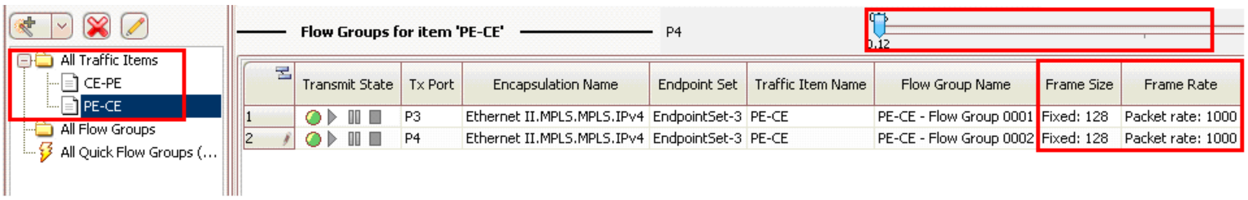
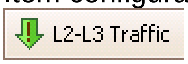


Figure 127. Post-Wizard Traffic Grid

33. **Apply,** and **Start** the traffic.
    a. Click the **Apply Traffic** button at the top of the screen. This will send the Traffic Item configuration to the test port.

    b. Click the **Start** (play) button

34. View the traffic statistics.
    a. Click on **Statistics** -> **Traffic Item Statistics**. This will show the aggregated view of all the traffic of each Traffic Item…from CE-PE, and PE-CE.

    Note: The Traffic Item aggregated view is very helpful to understand the performance of the DUT at a large-scale without having to investigate large amounts of results. If everything looks fine, then is no need to "drill-down" further. However, if there is loss or high latency, drilling down within each traffic item to pinpoint the problem can become very useful.

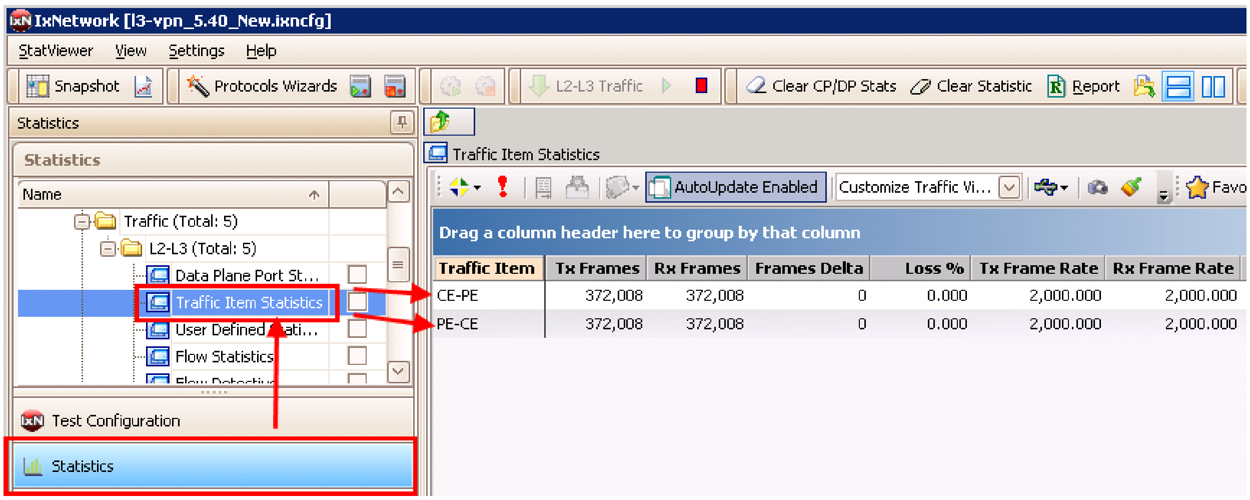


Figure 128. Statistics -> Traffic Item View

Performance test variable: Go back to the **Test Configuration** window and increase the rate, in real time, of one or more flow groups until loss occurs. Then use the following step to *drill down* to find the problem.

    b. Now **Drill Down** on the CE-PE traffic by right-mouse clicking on the CE-PE Traffic Item and finding the **Flow Tracking** options as defined in the Traffic Wizard. In the example below, click on **Drill Down per VLAN ID** to see all the VLAN statistics inside the CE-PE Traffic Item. These are the per-VLAN detailed statistics that make up the aggregated CE-PE Traffic Item stat.

    Note: This is very helpful to see if, or which, particular VLAN (i.e. customer VPN) is having issues.

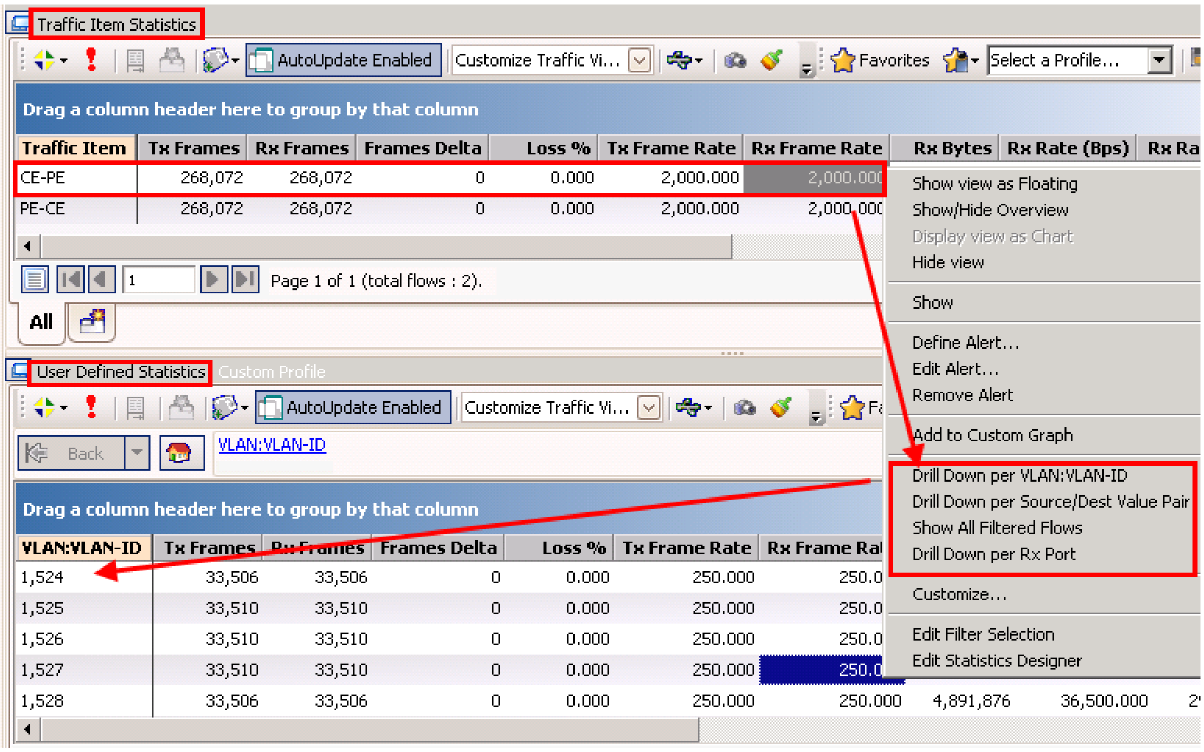


Figure 129. Statistics -> Drill down from Traffic Item View to VLAN ID

c. Now **Drill down** again on VLAN 1524 **(right-click -> Drill down per Src/Dst Value (MaC) Pair).** Here you see all five MAC flows within VLAN 1524 from the CE-PE side

Note: This is very helpful to see if, or which, particular Src/Dst MAC within the given VLAN (i.e. customer VPN) is having issues.

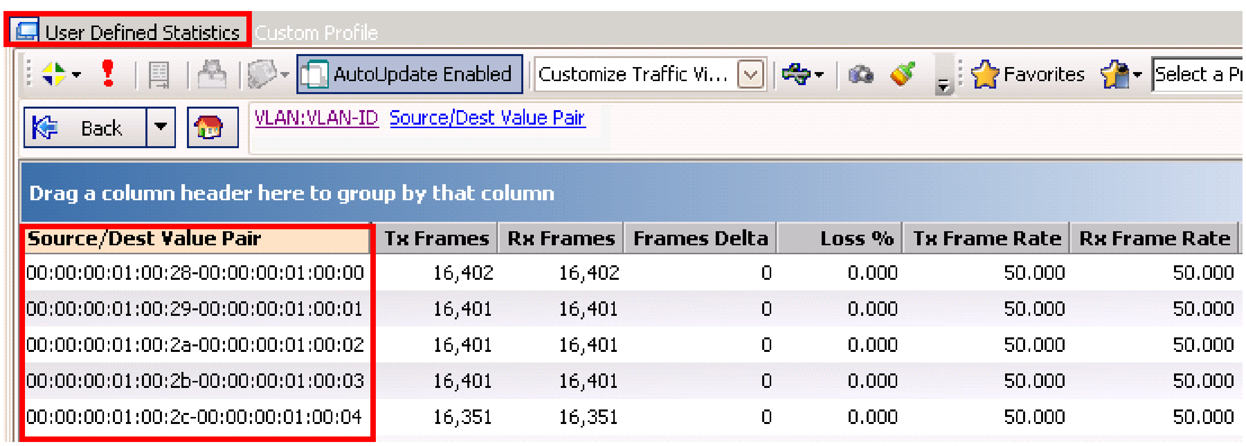


Figure 130. Statistics -> Drill down from VLAN ID to Src/Dst Value (MAC) Pair

d. Likewise, **Drill-down** on the PE-CE Traffic Item to the **Traffic Group ID.**

Note: This is very helpful to understand how the traffic on each VPN (Traffic Group ID) within the PE-CE traffic is performing. The **Traffic Group ID** can also be used in the CE-PE traffic item.

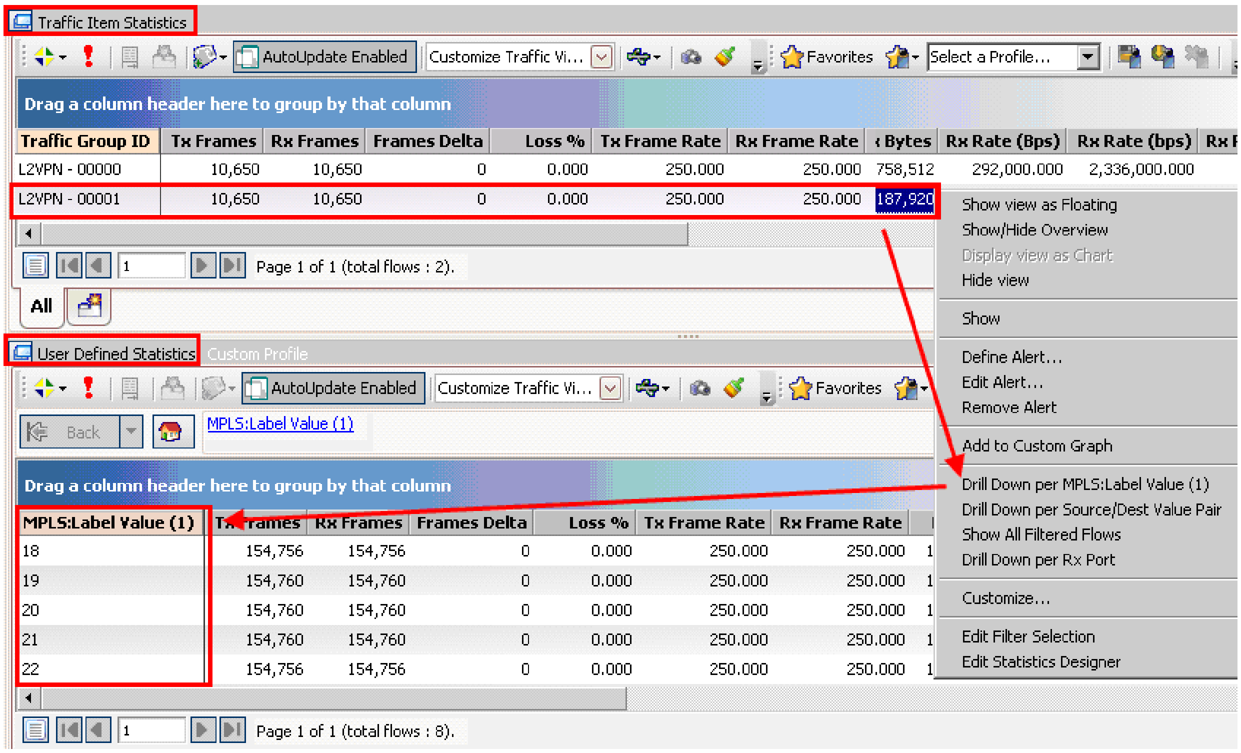


Figure 131. Statistics -> Drill down from Traffic Item to Traffic Group ID

e. Optionally, drill down again from each **Traffic Group ID** to **MPLS label.**

Note: This is very helpful to understand how the traffic on each MPLS label within the given VPN (Traffic Group ID) is performing.

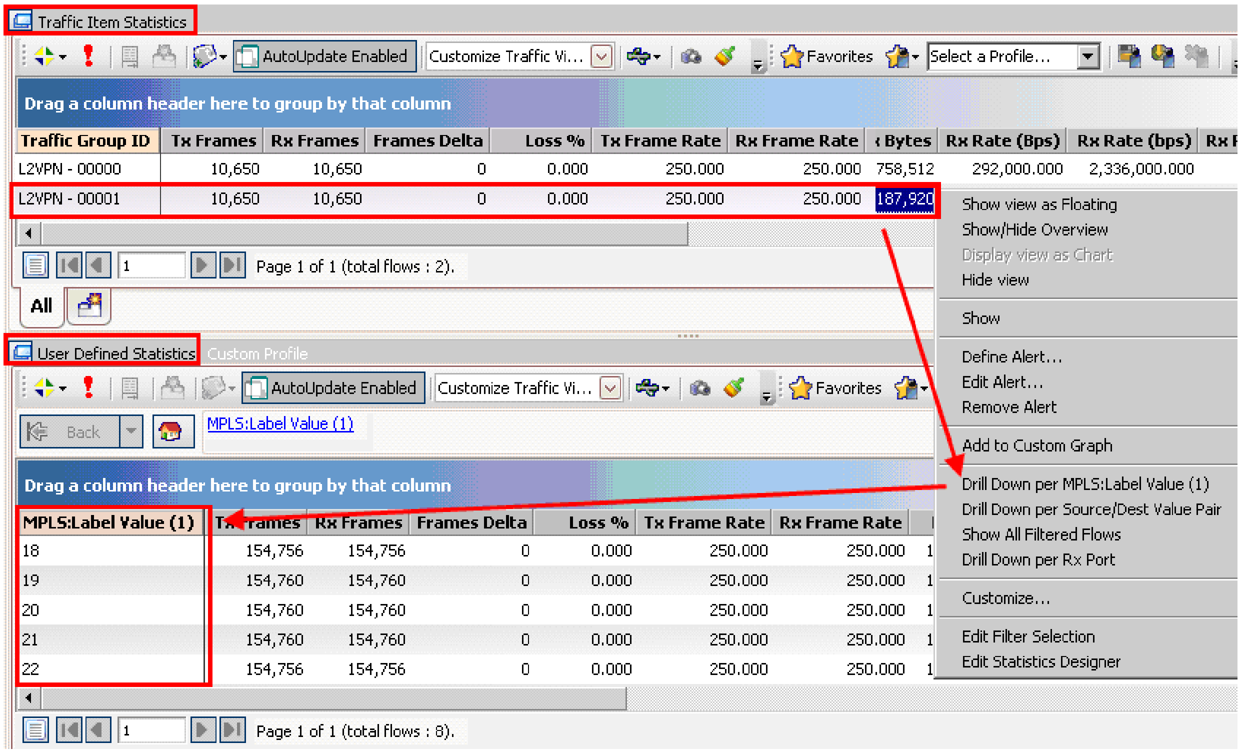


Figure 132. Statistics -> Drill down from Traffic Group ID to MPLS label

f. Optionally, drill down *again* from each **MPLS Label** to **Source/Dest Value (MAC) Pair.**

Note: This is very helpful to understand how the Src/Dst MAC traffic within each MPLS label is performing.

Note: **Drill-down per Rx Port** comes standard by default with every drill-down view. In this case it will help determine which RX port on the CE side is receiving the suspect MPLS traffic from the PE side. It may help determine which VPN is at fault without having to go to the label database and track the label through the network to the CE side.

Troubleshooting tip: In any of the above views, a small frame delta statistic does not necessarily mean that loss is present. Stopping traffic will fully synchronize the results. No test tool can measure Tx and Rx instantaneously, since the traffic must go through the DUT first. If the frame delta is continually increasing, however, there is likely loss.

Test Variables

Each of the following variables can be used in separate test cases to test a PE router in an L2 VPN - PWE network. They all use the test case above as a baseline, modifying a few parameters in the same IxNetwork L2 VPN wizard views shown above. You can create control plane scalability tests from 10x to more than 100x to fully stress the DUT's capability as a PE router and to understand its peering capacity with CEs, Ps, and other PEs. Once control plane scalability is understood, data plane performance can be measured in terms of throughput, latency, and loss for every frame size or IMIX pattern available.

Control Plane Performance Variables

Performance Variable	Description
Increase CE Ports	**Step 5:** On a real PE Router, there will be many more CE ports than P or PE ports, and each CE port will have many CEs/VLANs on it.
Increase PE Ports	**Step 5:** On a real PE Router, there are typically a minimum of two provider ports (one for backup), and it's possible that one or more of these ports will be high speed (10G) and therefore have high control plane scalability requirements.
Increase Emulated Ixia P Routers	**Step 6:** Increasing Ixia P Routers per port will stress the DUT's (PE) ability to peer/run MPLS and IGP protocols. If needed, use VLANs.
Use different IGP, or MPLS Protocol	**Step 6:** Try the other routing/MPLS protocols, such as ISIS and RSVP-TE. These protocols may have higher or lower overhead on the DUT and performance may vary.
Increase Emulated Ixia PE Routers	**Step 7:** This is one area that can grow quite large in a service provider network, in terms of IGP connections and exchanged VPN/VC information. This will test the DUT's ability to store/maintain VPN/VC information without leaking the information to incorrect VPNs/VCs.
Increase VPNs/VCs per PE	**Step 8:** This parameter will test the DUT's maximum number of VCs.
Use different Interface types	**Step 8:** The different interface types have different requirements inside the DUT in terms of power, cooling, memory, and scalability.
Increase the number of MACs per VLAN	**Step 9:** This will test the DUT's ability to handle many MAC addresses over each VLAN.

Data Plane Performance Variables

Performance Variable	Description
Increase Traffic Rate	**Step 21/32:** Manually increase the rate at which traffic is sent. Verify latency and loss levels per flow are as expected**.**
Change Frame Size	**Step 21/32:** Manually change the frame size of the traffic. Smaller frames generate more trouble for switches/routers, so tests running with 64-byte packets at a high frame rate should be tested by the operators. Additionally, select one of the real-world IMIX patterns that Ixia provides**.**
Run Binary-search Throughput tests using Ixia's "Integrated Tests"	Go to IxNetwork Test Configuration Window and look for **7. Integrated Tests**. These tests will automatically run binary-search throughput tests using any/all frame sizes and industry-standard methodologies to determine the maximum amount of throughput (without loss) that the DUT can handle.

Results Analysis

The test described in this booklet proved that the DUT, acting as a PE router, could maintain and run a network consisting of eight customer VPNs/VCs, each with 2 sites. Adding to that was emulation of two P routers, and four PE routers. In addition, the DUT was able to forward 64-byte data traffic at a rate of 10% (of a 1 Gb link) across the network with no loss and low latency.

Even in a small-to-medium size service provider network there can be tens or hundreds of VPNs covering hundreds of locations. These VPNS can use tens or hundreds of ports spanning hundreds or thousands of miles.

Because of this, control plane scalability testing and data plane performance testing is critical to ensure that these devices and networks can handle the load placed upon them in real-world scenarios. Go to the **Test Variables** section for a discussion of the various ways in which the test case can be extended into more extensive scalability and performance tests.

As the control plane variables are increased to the DUT's maximums, special attention must be paid to the detailed protocol statistics, including up/down sessions, and protocol counters. On the data plane side, each and every MAC address should be inspected for loss and latency as it flows through the DUT.

Lastly, long duration tests at maximum scale are required with optional simulated outages to ensure expected behavior in a volatile environment.

Troubleshooting Tips

Issue	Troubleshooting Solution
Can't ping from DUT to the Ixia Emulated P	**Step 12:** Check the protocol interface window and look for red exclamation marks (!). If any are found, an IP address/gateway mismatch is likely.
Sessions won't come up	**Step 15:** • Go back to the **Test Configuration** window and double check the protocol configuration against the DUT. • From the **Test Configuration** window, turn on **Control Plane Capture**, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.
No "Learned" info	**Step 16:** There is likely a mismatch in the VPN/VC configuration on the Ixia port or the DUT. Also check to make sure your VLAN IDs are correct.
Traffic 100% Loss from PE-CE	**Step 24/31:** Check the **Warnings** columns in the **Traffic** view (step 24) and make sure that there are no streams that say *VPN label not found*. The DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then **Apply** traffic.
Stop/Start Protocols or Link Down/Up has Traffic 100% Loss from PE-CE	**Step 24/31:** Check the **Warnings** columns in the **Traffic** view (step 24) and make sure there are no streams that say *VPN label not found*, and then the DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then **Apply** traffic.

Conclusions

This test verified that the DUT can perform with four ports of scale as a PE Router in a L2 VPN - PWE network.

However, scalability and performance are of paramount importance when testing a DUT acting as a PE router. Follow the **Test Variables** section above to test the PE at its maximum capability before deploying into a real-world L2 VPN – PWE Network.

Layer 2 MPLS VPNs – VPLS Testing

Virtual private LAN services (VPLS) are layer 2 Ethernet services offered by service providers. Unlike pseudo-wire emulation (PWE) layer 2 VPN circuits that only provide L2 point-to-point services, VPLS allows multiple sites to be connected in a single L2 switched domain over a provider managed IP/MPLS network.

All customer sites that belong to a VPN (i.e. an enterprise customer) will appear to be on the same Local Area Network (LAN), regardless of their locations. VPLS uses an Ethernet interface with the customer, simplifying the LAN/WAN boundary. A VPLS-capable network consists of three types of devices:

- **Customer edge (CE) routers** – The CE is a router or switch located at the customer's premises. It connects to a PE router. Unlike L2 PWE that can interface to the PE over various L2 technologies, with VPLS only Ethernet is supported between the CE and the PE for VPLS.
- **Provider edge (PE) routers** – The PE is where the intelligence of the customer's VPN originates and terminates. All of the necessary virtual circuits (VCs) are set up to connect to all the other PEs within the provider MPLS network. Unlike L3 VPN networks that require a routing protocol session between the CE and PE, this does not matter with VPLS since the PE is only required to keep the MAC table of each VPN. It switches the packets to other PEs in the core belonging to the same VPN. The PE routers run an IGP protocol (such as OSPF or ISIS) to the service provider core as well as a VPLS signaling protocol (either LDP Extended-Martini or MP-iBGP) to the other PEs to exchange VPN information.
- **Provider (P) router** - The P interconnects the PEs and runs the provider MPLS core network. It does not participate in the VPN functionality. It simply switches the VPN traffic using MPLS labels. The P routers run an IGP protocol (such as OSPF or ISIS) to other Ps and PEs within the service provider network, along with LDP or RSVP-TE for MPLS signaling.

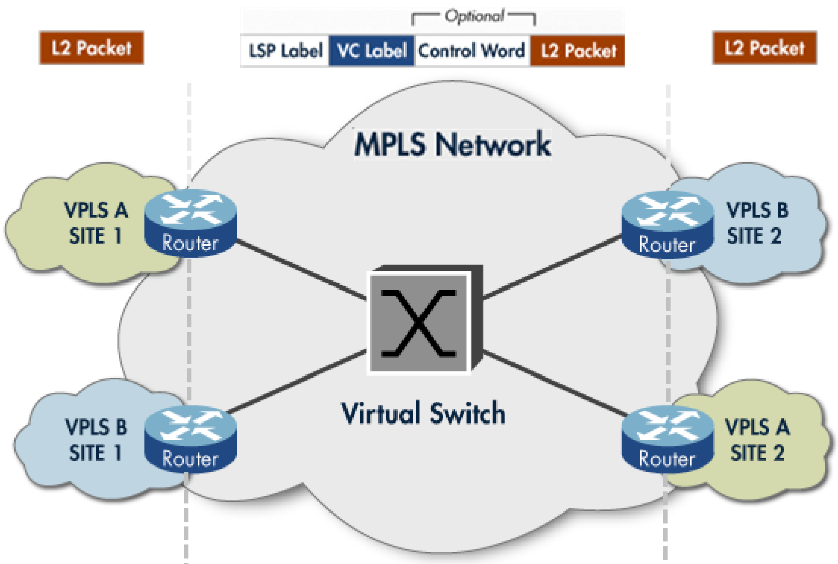


Figure 133. Typical Layer 2 VPN - VPLS network

Testing an L2 VPN - VPLS network is largely concerned with the PE routers.

The PE routers need to maintain separate MAC forwarding tables for each CE that belongs to a unique VPN. These MAC tables must be maintained by the PE router without leakage to other customer VPNs. The uncertainty of MAC table sizes, number of CEs for a given customer/VPN, flooding of traffic to un-learned MAC destinations, CE flapping, and MAC-based router security threats create the requirement for a plethora of functional and performance tests for the PE.

On the service provider side of the PE router, an IGP such as ISIS or OSPF must be chosen, as well as a core MPLS protocol – either LDP or RSVP-TE. Combinations of these protocols must be tested to ensure efficient operation in a service provider network.

Besides choosing either LDP or RSVP-TE for the outer MPLS label, the inner MPLS VPN labels need to be exchanged between all PEs in the provider network using LDP Extended-Martini or MP-iBGP. These two protocols are the brains of VPLS networks and require significant testing.

All of these PE router aspects need initial testing at the functional level, but more importantly at the performance level, including:

- Scaling CEs (over VLANs) with a varied number of MACs per CE.
- Scaling PEs in the provider network. All PE neighbors must peer with each other, and many VPN/VC MAC tables are exchanged. Flapping is another key test case. It is also very important to test the scalability of both LDP Extended-Martini and MP-iBGP signaling protocols.
- Tests should scale the Ps in the core of the provider network to test with massive amounts of MPLS and (in some case) non-MPLS packets. When using MP-iBGP, these Ps are also sometimes called upon to assume the role of I-BGP route reflectors.

- Data plane performance should be tested at the maximum CE, PE or P scale. Testing should not only include throughput, but verify that MAC/VPN leakage is not present.

Further performance test cases using Ixia's IxNetwork can be verified with the following step-by-step test case, along with the *Test Variables* section below.

Relevant Standards

- The PE Router LDP Specification – RFC 3036
- LDP Applicability – RFC 3037
- LDP State Machine – RFC 3215
- Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling – RFC 4761
- Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling – RFC 4762
- Transport of Layer 3 Frames Over MPLS – draft-martini-l2circuit-trans-mpls-09.txt
- Virtual Private LAN Services (VPLS) over MPLS – draft-ietf-ppvpn-vpls-ldp-01.txt
- Pseudo-wire emulations:
    - draft-martini-ethernet-encap-mpls-01.txt
    - draft-martini-ppp-hdlc-encap-mpls-00.txt
    - draft-ietf-pwe3-frame-relay-02.txt
    - draft-martini-atm-encap-mpls-01.txt
    - draft-malis-sonet-ces-mpls-05.txt

Test Case: Layer 2 MPLS VPN – VPLS Scalability and Performance Test

Overview

Although L2 MPLS VPNs - VPLS networks are becoming widely available, router vendors and service providers should carefully consider a number of scalability issues.

Service Provider PE routers need to allow for the partitioning of their resources between unique customer VPNs, and at the same time partition their Internet routing resources. The PE router in an L2 MPLS VPN - VPLS network must:

- Maintain separate, unique MAC tables for each customer/VPN.
- Run MPLS, IBGP and IGP protocols into the core of the SP network, usually connecting to faster P/PE routers on high-speed links.
- Peer with all other MP-iBGP or LDP Extended-Martini PE neighbors and exchange VPN/VC info with them.
- Make forwarding decisions at microsecond speeds while bi-directionally adding/popping MPLS and VC labels.
- Keep enterprise customers' VPN traffic and Internet traffic separate.

Because of this, the focus of the tests is largely centered on the PE, as all the unique customer/VPN intelligence is implemented within the PE routers. Layer 2 MPLS VPN – VPLS technology takes advantage of the emerging MPLS technology for tunneling data packets from different VPNs over the same service provider network. LDP Extended-Martini or MP-iBGP is extensively used for VPN exchange and for the distribution of VPN reachability information. The combination of MPLS and BGP working together make up this exciting technology.

The best methodology in performance testing a PE is to create a scalable baseline test, and then modify it in different ways to test the control plane and data plane performance. This testing will verify the PE's ability prior to being deployed in a real-world, revenue generating, service provider network.

Objective

The objective of this test is to baseline the scalability of a single DUT acting as a PE router in a Layer2 VPN – VPLS network.

At the end of this test other test variables will be discussed that will provide many more performance test cases, using the topology described below as the baseline.

Setup

The test consists of a DUT acting as a PE router, and four Ixia ports.

One Ixia test port will emulate two customer (CE) devices. Each of these CE devices belongs to a different customer/VPN.

The other three Ixia port emulate the entire service provider network, which includes three Ps, six PEs, and twelve additional CEs.

In total, this test will emulate three Ps, six PEs, and fourteen CEs (that consist of two VPNs each with seven sites), as shown in the Figure 134 below.

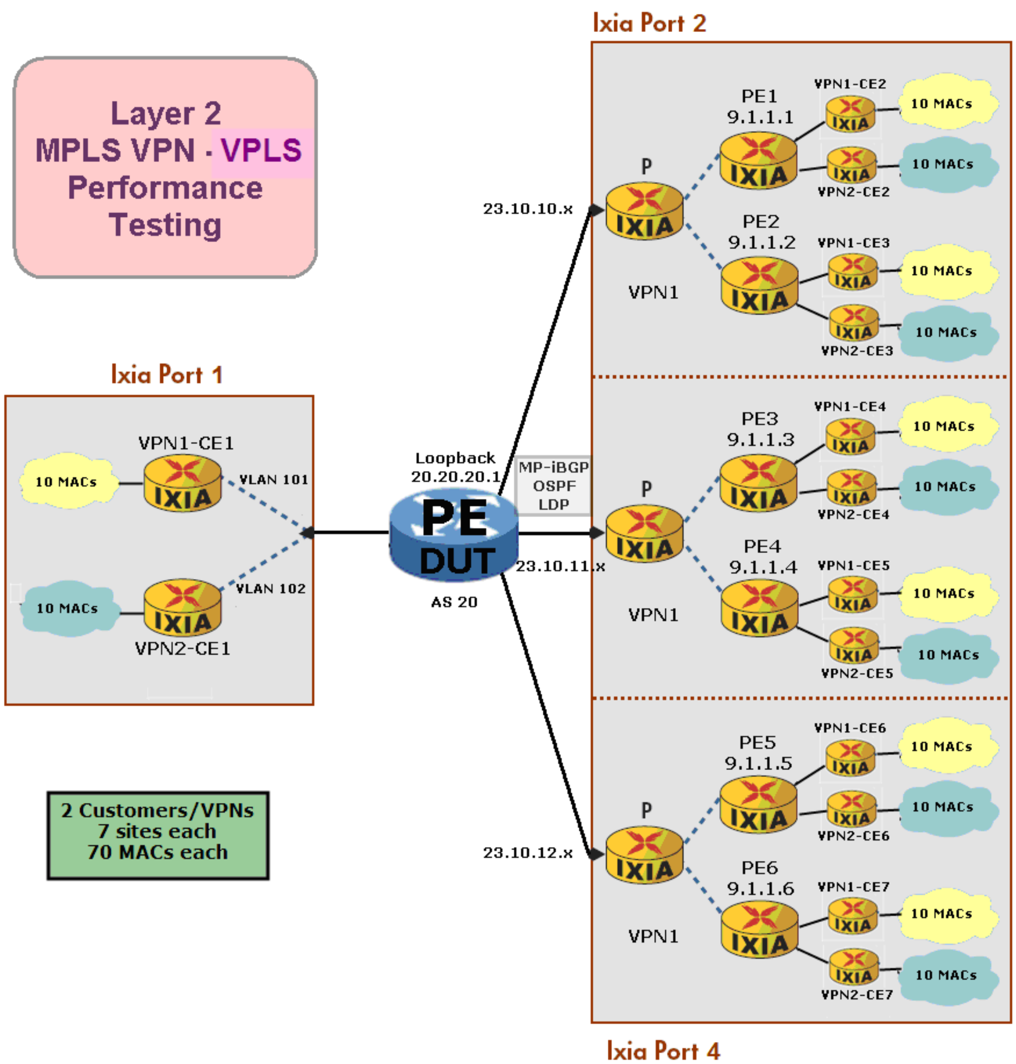


Figure 134. Ixia emulated layer 2 VPN - VPLS network

Step-by-Step Instructions

These instructions will result in a Layer2 VPN – VPLS performance test for the topology in Figure 135. Optionally, use the steps below as a guide to building other Layer2 VPN – VPLS performance test scenarios.

1. Reserve four ports in IxNetwork.

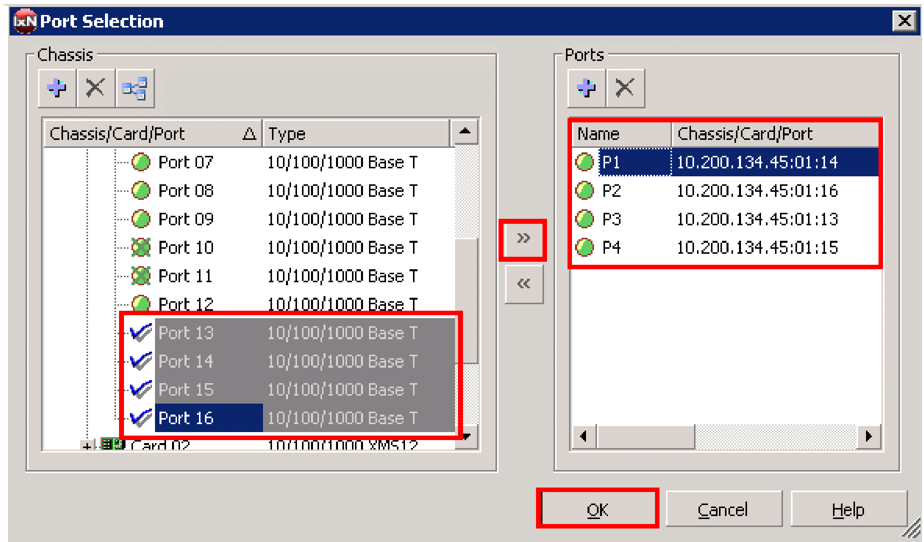


Figure 135. Port reservation

2. Rename the ports for easier use throughout the IxNetwork application.

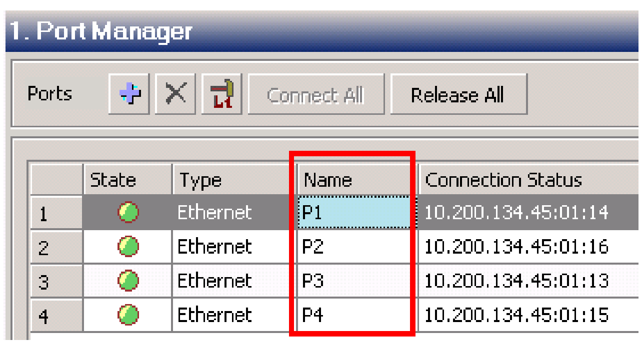


Figure 136. Port naming

3. Click the **Protocol Wizards** button on the top toolbar in the IxNetwork application.

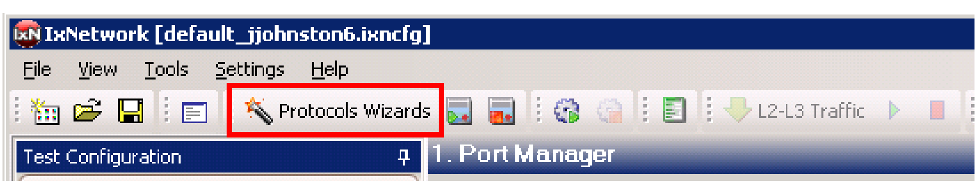


Figure 137. Protocol wizards

4. Run the **L2 VPN/VPLS** protocol wizard.

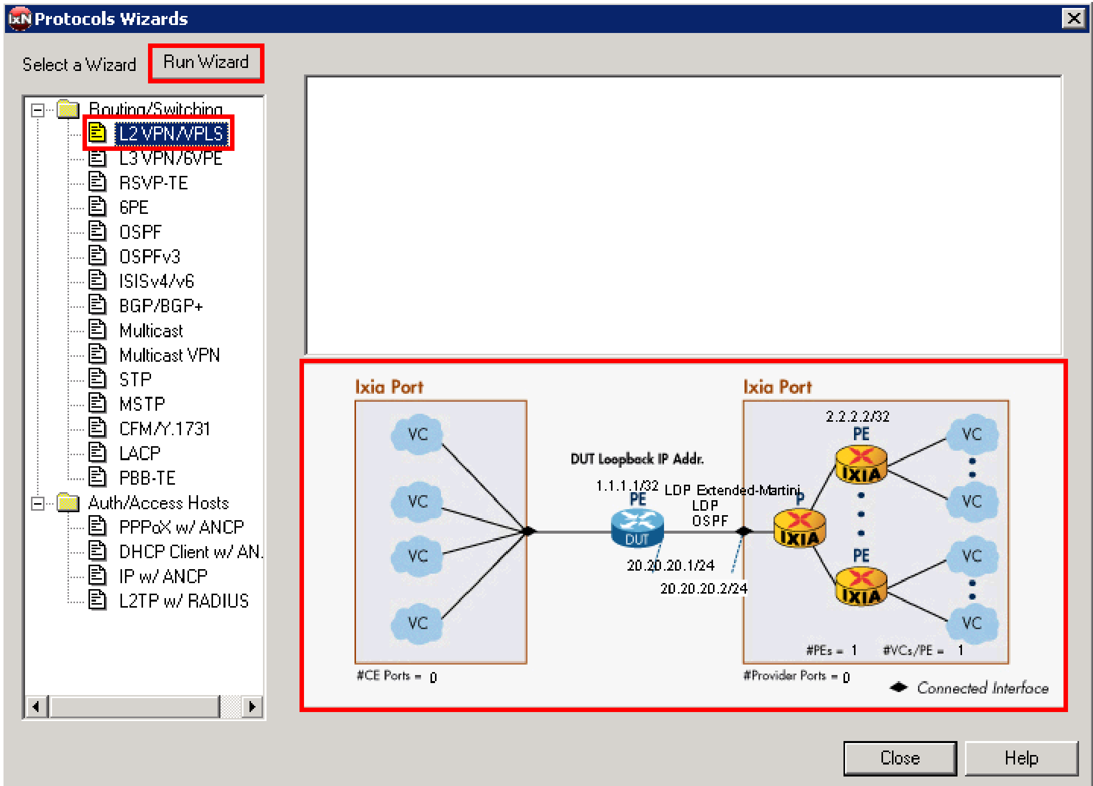


Figure 138. L2 VPN wizard

Note: the Wizard supports **both** L2 VPN – PWE and L2 VPN – VPLS. In brief, L2 VPN – PWE runs point-to-point virtual circuits across the MPLS core, and L2 VPN – VPLS supports use of MPLS as an effective layer 2 switch for point-to-multipoint.

Note: the figure above represents a typical test case for testing a PE router in an L2 VPN network.

5. Configure **P1** to emulate the CE (left) side of the topology, and **P2, P3,** and **P4** the SP (right) side of the topology, then click **Next**.

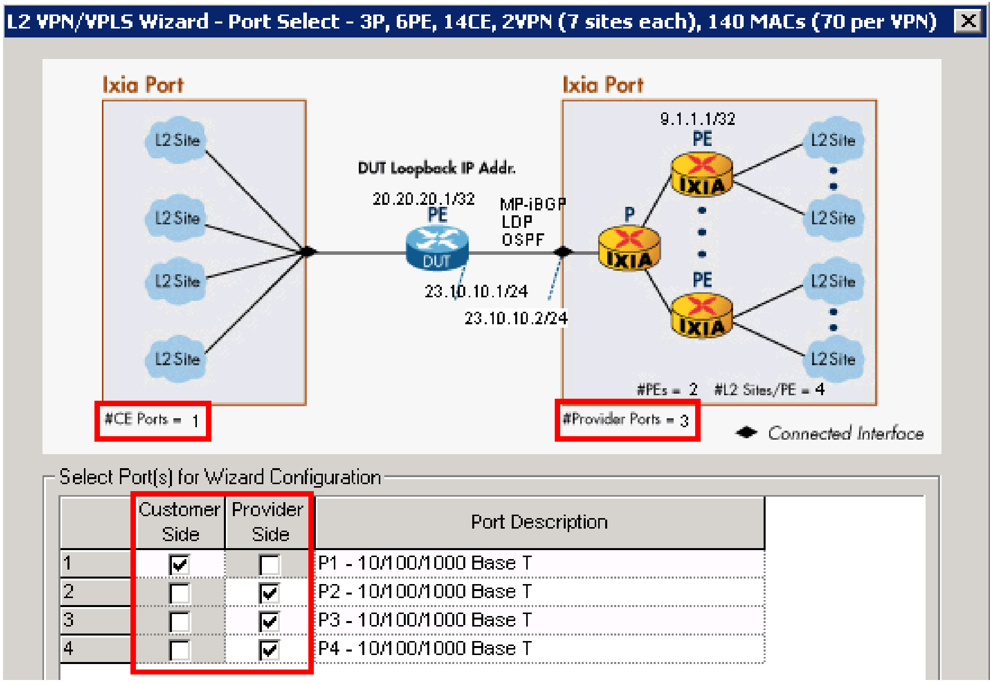


Figure 139. L2 VPN Wizard Screen1 of 6

Note: The screen above updates with the number of customer-side ports as well as the number of provider-side ports.

Performance test variable: Increase the number of customer and provider ports to test the DUT's (PE's) ability to scale at a port level. In a real-world network, there are more customer ports than provider ports.

6. This window configures **P2, P3,** and **P4** with emulations of one or more P routers. These ports are configured to talk directly to the DUT (PE) router.
   a. Keep the default of **1** P router. This is a per-port setting.
   b. Configure a starting subnet between the Ixia P router and the Ixia PE routers. Any subnet will work. In this case use *11.1.1.0/24.*
   c. Configure the **IGP Protocol** and **MPLS Protocol** running in the SP core.
      - In this test use the defaults of **OSPF** and **LDP**, respectively.
   d. Configure the **L2 VPN Signaling Protocol** running in the SP core
      - In this test use **MP-iBGP**.
   e. Configure the Ixia **P Router IP address** on **P2** and the **DUT IP Address**
      - In this test they are *23.10.10.2/24* and *23.10.10.1/24*, respectively
   b. Configure the **Increment per port** option to support **P3** and **P4** IP addresses.
      - In this test it is *0.0.1.0.*
   f. Click **Next**.

   Optionally:
   a. Disable (uncheck) **Enable P Routers**. In this case, Ixia ports(s) would then only emulate PE routers (i.e. no P router emulation), and will test the DUT in a PE-to-PE scenario.

   Performance test variables:
   - Increase the **number of Emulated P Routers** to test the DUT's ability to peer with many P routers, all running an IGP/MPLS protocol.
   - Check the **Enable VLAN** checkbox (not shown) to run these protocols over VLANs. Enter the first **VLAN ID** and choose to increment.

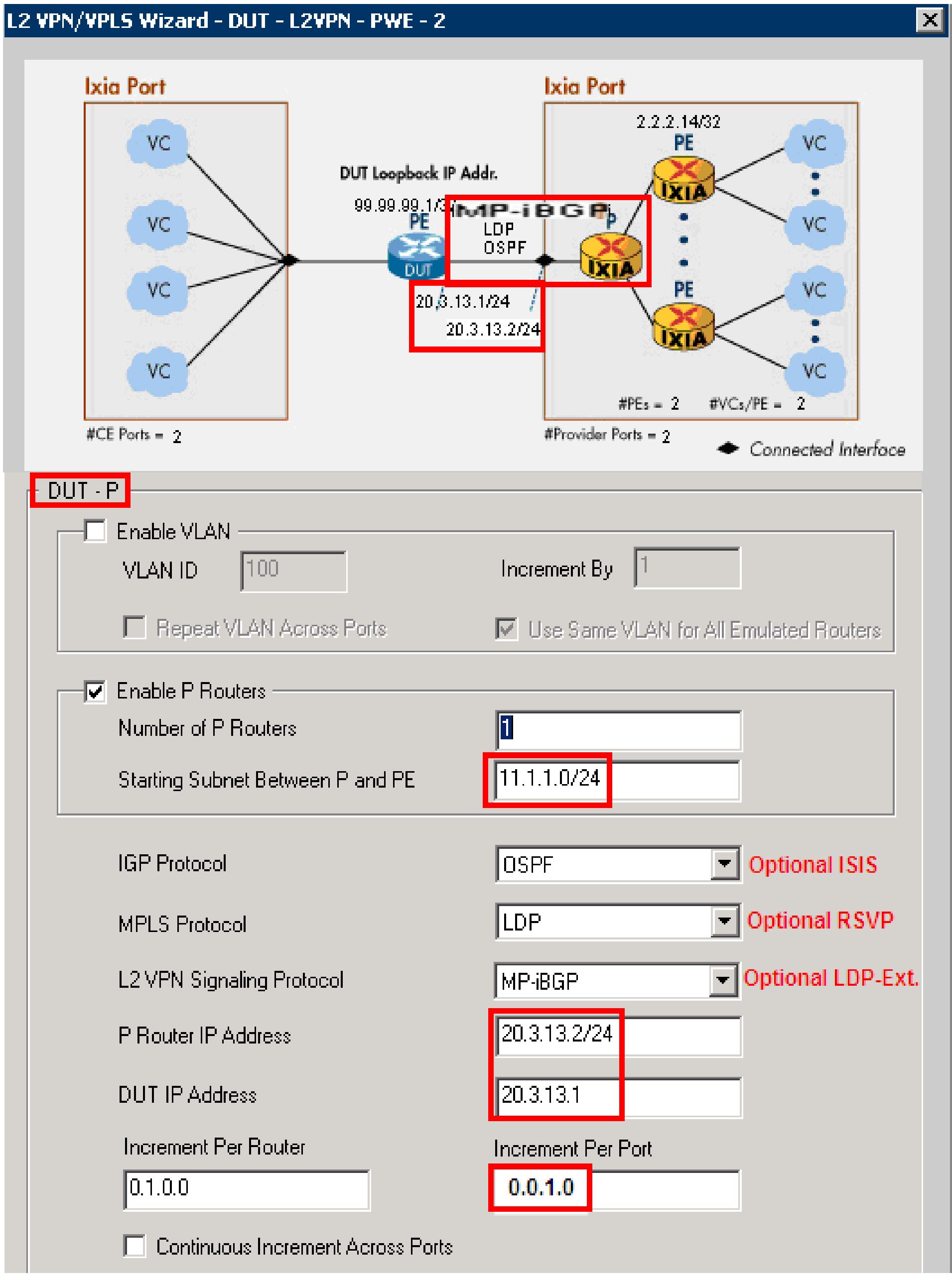


Figure 140. L2 VPN wizard screen 2 of 6

Note: The screen above updates with the configured protocols/IP addresses.

7. This window configures **P2, P3,** and **P4** with emulations of one or more **PE routers** that work directly behind the emulated P router(s).
   a. Configure the **Number of PE Routers Connected to the P Router**. This is a per-port setting.
      - In this test it is *2* PEs (per P).
   b. Configure **Emulated PE Loopback Address** (and its incrementing function for the additional PEs).
      - In this test it is *9.1.1.1* (the second to sixth will get *9.1.1.2 – 9.1.1.6*)
   c. Configure **DUT Loopback IP Address**.
      - In this test it is *20.20.20.1.*
   d. Click **Next**.

   Performance test variable*:* Increase the number of PE routers per P router. This will test the DUT's ability to peer with many PE routers with potentially many VPNs/VCs.

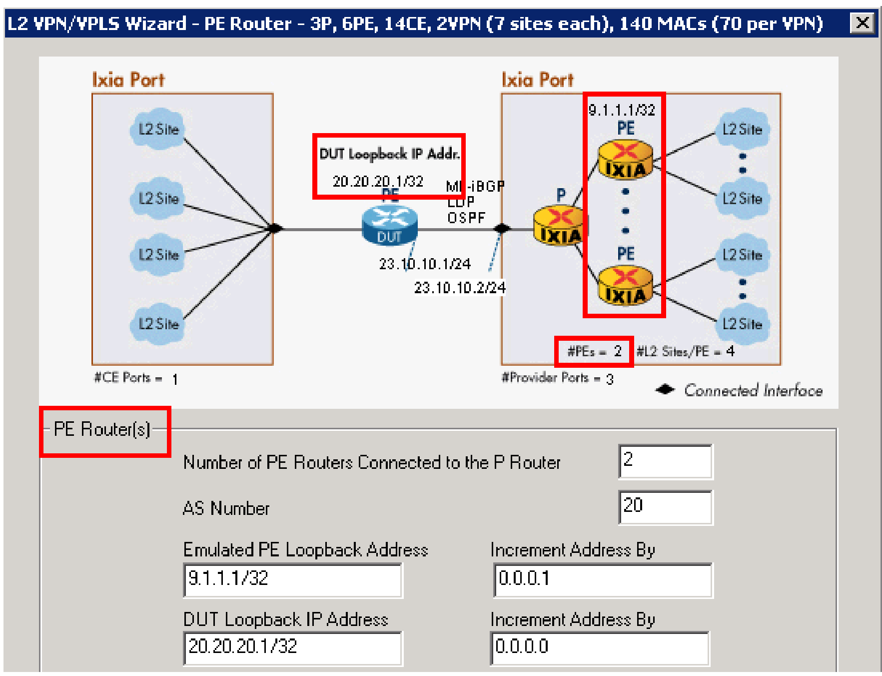


Figure 141. L2 VPN wizard screen 3 of 6

8. This window configures the BGP VPLS VPNs for all provider side ports in the test.
   a. Configure the **VPN Traffic ID Prefix**.
      For most L2 VPN test cases use *L2VPN.*
   b. Configure the **Route Target** for the first VPN/VRF. In most test cases this is a combination of the AS # and a unique identifier. The **Route Distinguisher** is the same.
      In this test it is *151:1*. The second VPN will use 151:2.
   c. Configure the **Number of VPNs per PE Router**. This will partially determine the number of customers/VPNs that will be used in the test. This number will also determine the number of CE routers that are in used in *Step 9*.
      In this test it is *2*.

d. Configure the **DUT Side – Start L2 Site ID** and the **Ixia Side - Start L2 Site ID**. The site ID must be unique for each circuit within a given VPN.
   i. In this test they are *101* and *201*, respectively
   ii. Increment by 1.
e. Change the **Label Block Offset** and **Block Offset Step** to *1* and *0* respectively.
f. Click **Next**.

Performance test variable: Increase the **Number of VPNs per PE Router**. This will test the DUT's maximum ability for number of VPNs.

Troubleshooting tip:

- Make sure the site IDs and label block values are consistent with the DUT's.

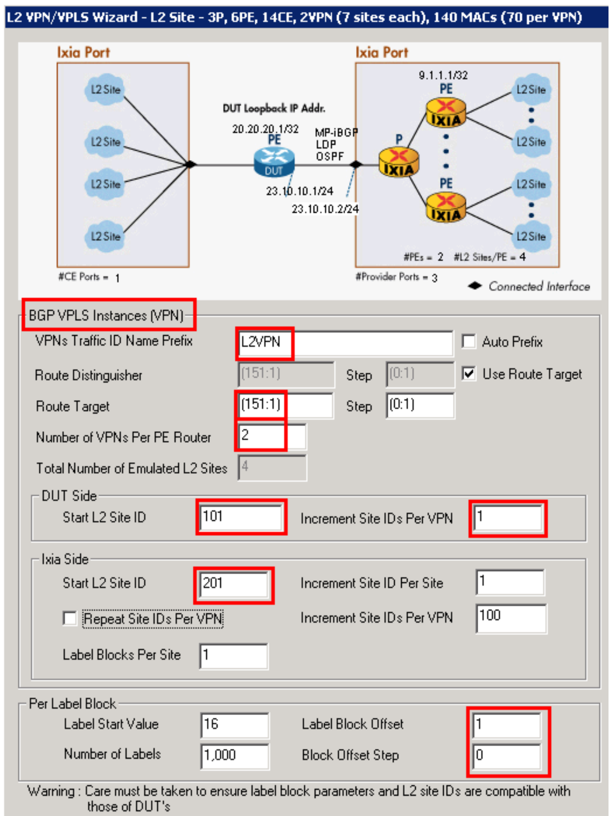


Figure 142. L2 VPN wizard screen 4 of 6

9. This window configures the number of MACs used per VPLS VPN and the VLAN ID for the CE side.
    a. Configure the **Number of MAC addresses per VPLS instance**. By default, 50% of the MACs go on P1 and P2, and 50% on P3 and P4 (this is configurable in **Distribute MAC Address**).
    In this test case it is *20***.** 10 MACs will be used per VPN site (70 MACs per VPN total).
    b. Enter the **First VLAN ID** for the first VPN on P1.
        i. In this test it is *101*.
        ii. The second VC on P1 will use VLAN 102.
    c. Click **Next**.

Performance test variable*:* Increase the number of MACs per VPLS Instance. Unlike PWE, the DUT using VPLS needs to maintain unique MAC tables for each VPN so it can switch the packets to the appropriate site. Therefore, increasing the number of MACs will stress the DUT's ability to handle many MAC addresses on each VPN.

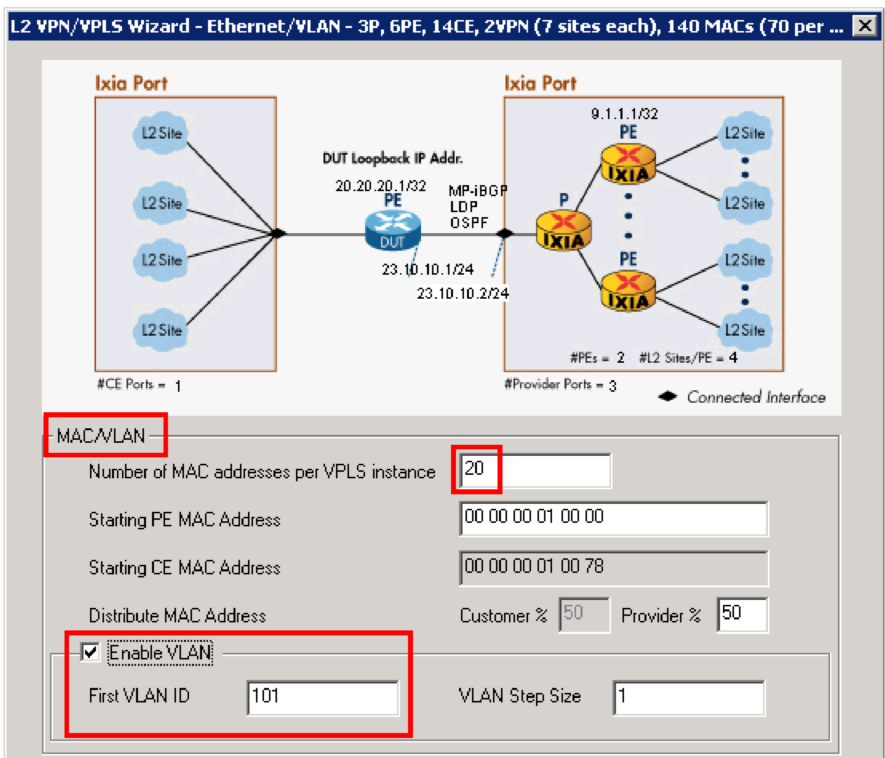


Figure 143. L2 VPN Wizard Screen 5 of 6

Note: The MAC addresses are assigned sequential across all ports in the test. The VLAN IDs have a **Step** function as shown above.

10. This window configures the name of the wizard run and the action to take with this run of the wizard.
    a. Use a descriptive name for the wizard. In this test use *3P, 6PE, 14CE, 2VPN (7 sites each), 140 MACs (70 per VPN).*
    b. Specify what to do with the finished wizard configuration.
       In this test select **Generate and Overwrite All Protocol Configurations**. This will overwrite all previous configurations

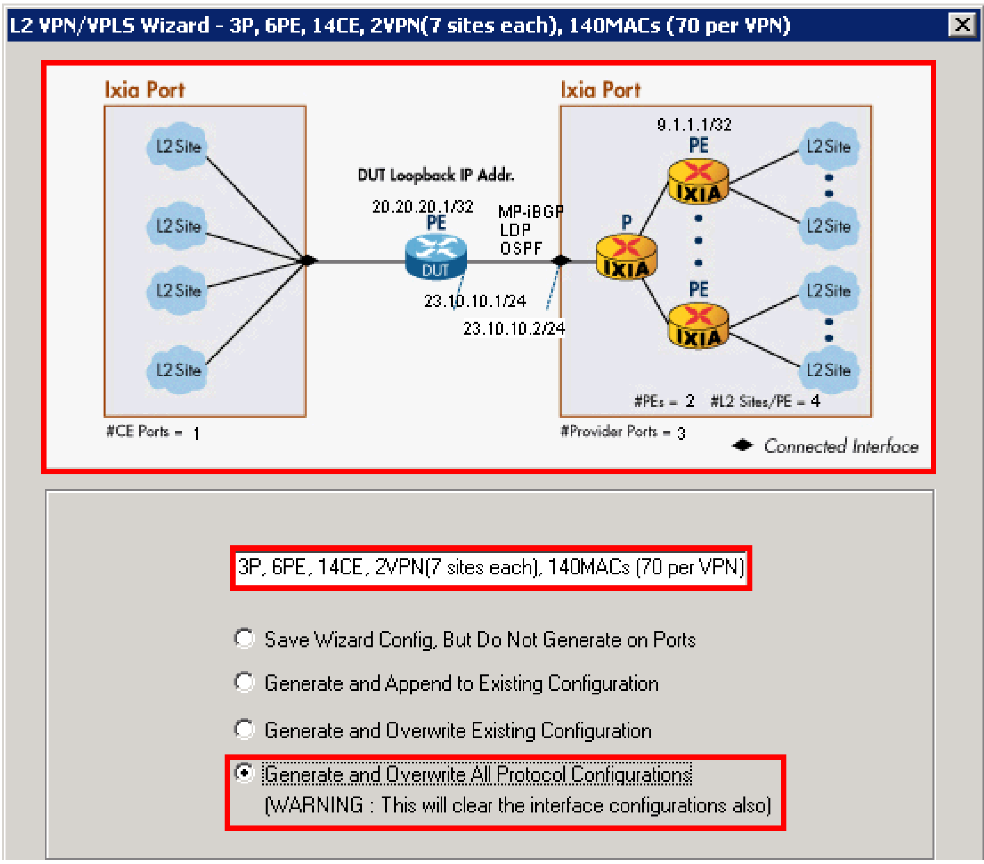


Figure 144. L2 VPN Wizard Screen 6 of 6

11. This window shows the saved wizard template.
    a. Click **Close** to finish the wizard configuration
    b. ***Optionally***, when using saved wizard templates, you may:
        - Come back to the same wizard to (double-click) view and/or modify.
        - Save new or modified wizards with a new name (or overwrite).
        - Create a library of templates for use in different tests.
        - Highlight each template and preview the configuration in the topology below.

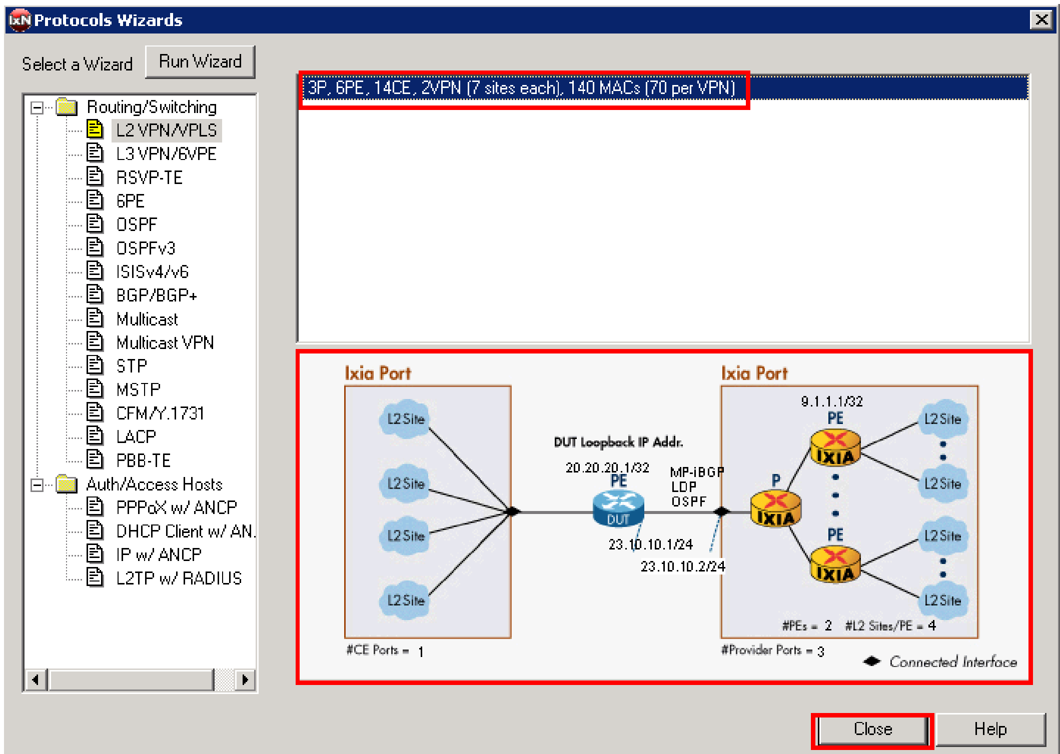


Figure 145. L2 VPN wizard saved wizard template

12. Click on the **Routing/Switching/Interfaces** window on the top, and the **BGP** protocol in the middle. Note how the wizard incremented the fields and check that the settings will work with the DUT configuration. For example:
    a. On **P2, P3, P4**, see the **Local IP** (aka the **Ixia PE**) and make sure the DUT configuration is peering with these addresses.
    c. On **P2, P3, P4**, see the **Site IDs** and **Route Distinguisher/Target** and check that the DUT is configured the same.
    d. If necessary, manually change the configuration in the protocol table/grid to your liking. Another option is to highlight columns and right-mouse click to easily customize with **Same** or **Fill Increment** options.

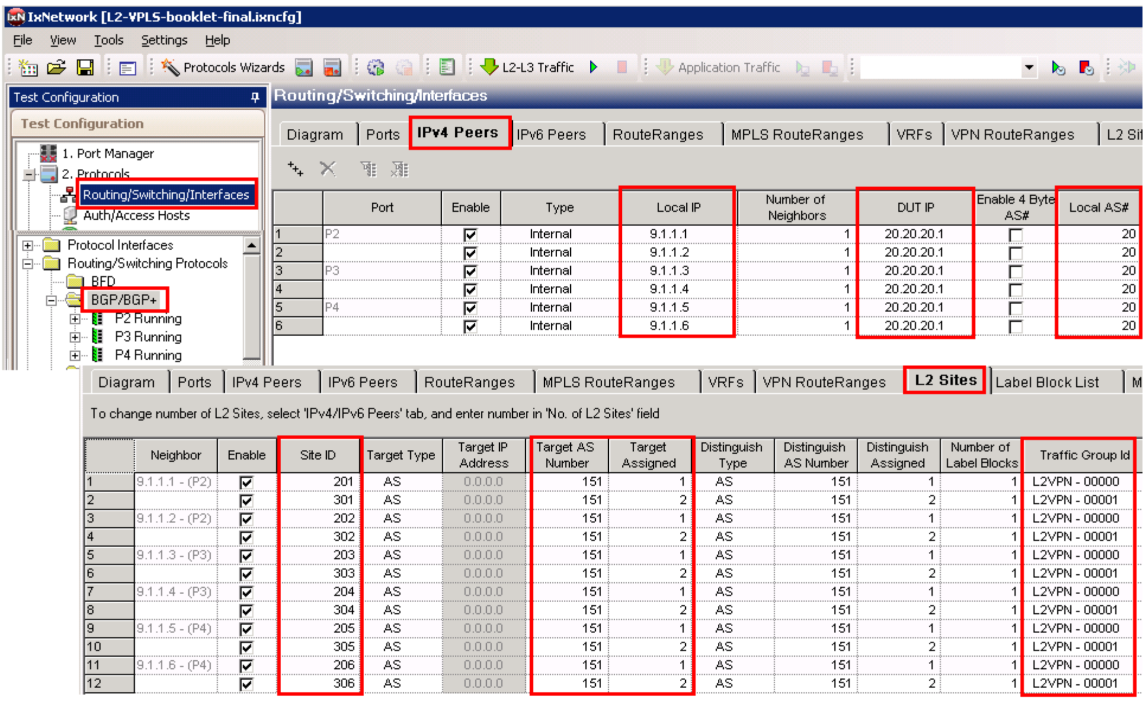


Figure 146. Protocol configuration window

13. Click the **Statistics** window on the bottom left and click the **Start all Protocols** button on the toolbar.

14. Click on the **Global Protocol Statistics** option for a summary of all protocols running on each port.
    Check whether all of the BGP, OSPF and LDP sessions are up.

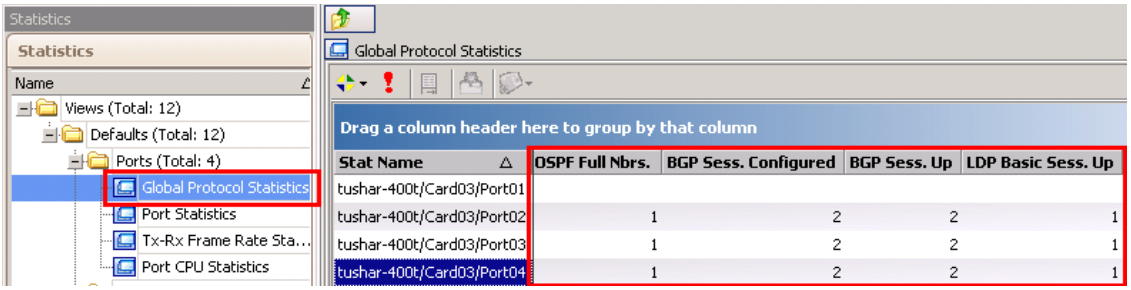


Figure 147. Global protocol statistics window

Optionally:
Click on each of the specific protocol statistics (LDP, OSPF, and BGP) to view statistics for that protocol (including up/down status as shown in **Global Statistics**).

Troubleshooting Tip: If the sessions are not up:

- Go back to the **Test Configuration** window and double check the protocol configuration against the DUT.
- From the **Test Configuration** window, turn on **Control Plane Capture**, then start the **Analyzer** for a real-time sniffer decode between the Ixia port and the DUT port.

15. After protocols have been started, use the Ixia **Learned Routes** option to verify that each Ixia peer is receiving the correct routes/labels for each peer.
    a. View the MPLS labels learned by the Ixia BGP peers on **P2**.
        i. Click on **Learned Routes** and then **Refresh** to see the labels learned by the Ixia peer. In this test case there should be **two** BGP-VPLS labels learned from the DUT (PE) to the Ixia PE at 9.1.1.1. Check it against the DUT.

    Optionally:

    a. View the LDP labels learned (these are the outer labels).
    b. View the OSPF Routes Learned.

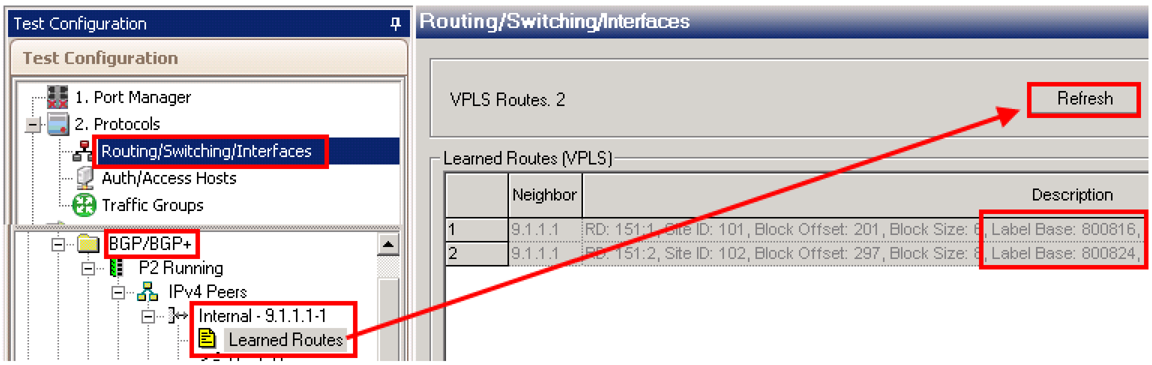


Figure 148. Protocol learned info

16. After all of the sessions are up, you need to build bidirectional traffic from CE-PE, and from PE-CE. Launch the **Advanced Traffic Wizard** by clicking on the **+** sign.

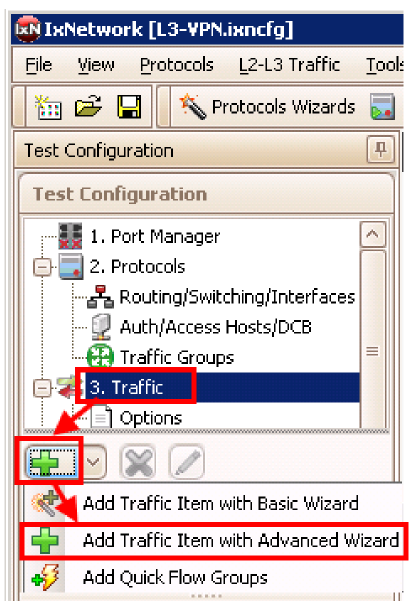


Figure 149. Create traffic

17. First Configure the CE-PE traffic
    a. Name the **Traffic Item** as **CE-PE**
    b. Make sure the **Traffic Type** is **Ethernet/VLAN**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select both of them. Click **Apply Filter.**
        i. This will filter the **Source** and **Destination** trees to only display items that belong to these customer/VPNs. It is also possible to select only one Traffic Group ID at a time to see an exact view of all sources/destinations that belong to that customers VPN.
        ii. Even though both Traffic Group ID filters were selected at the same time, IxNetwork is smart enough to only send traffic to/from sources and destinations that belong to the same VPN .
    e. Set the source **Encapsulation Type** to **non-MPLS**, and the destination to **L2VPN**. This will further filter the source/destination tree for CE-PE traffic.
    f. Select the **Source – Static Mac VLAN Ranges** checkbox.
    This is a global option to select all of the Static MAC VLANs for the source ports.
    g. Select the **Destination –BGP VPLS MAC Ranges** checkbox .
    This is a global option to select ALL of the LDP MAC VLANs for the destination ports.
    h. Click the down arrow sign to add the 2 sources and 12 destinations as a traffic Endpoint Set.
    i. Click **Next**

Note: It is possible to configure the PE-CE traffic at the same time by selecting the **Bi-Directional** checkbox within this window. However, by creating those in separate Traffic Wizard runs the resources (flows) used will be separately saved, allowing better use of flow tracking as selected in the **Flow Tracking** Page of this wizard.

Note: Make sure to uncheck the **Merge Destination Ranges** checkbox if the same routes are used on two or more VPNS in the test.

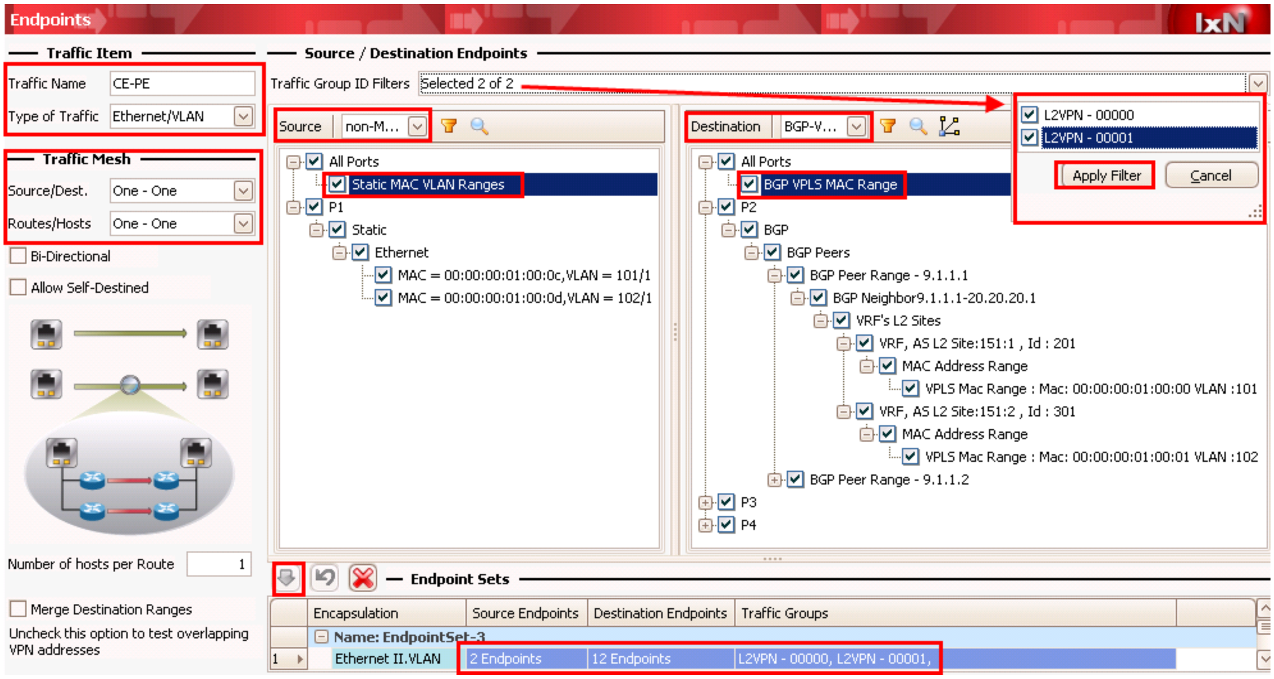


Figure 150. Advanced Traffic wizard screen 1

a) Optionally, use the **Packet/QOS** window (not shown) to add an IP/TCP or IP/UDP header, for example.
b) Optionally, use the **Flow Group Setup** window (not shown) to; in this case, separate VLANs/VPNs per port into separate Flow Groups. Each Flow Group uses its own transmit engine and can have unique content, and its own rate/frame size.
c) Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration, such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing the wizard.

18. Select the **Flow Tracking** options for CE-PE traffic.
    - In this test select **Traffic Item, Source/Dest Value (MAC) Pair, and VLAN-ID**. Selecting these options will create a track able flow for every combination of the selected items. Each flow will provide full statistics (rate, loss, latency, etc.)
    - Click **Next.**

    Note: These options will also be available as **Drill-down** views in the **Statistics** windows. In this case there will be an aggregated **Traffic Item** statistics that shows all of the combined statistics for every flow within this Traffic Wizard. Then, the user can use the right-mouse-click select the Traffic Item and drill-down per **Src/Dst Value pair** and/or **VLAN-ID** to see the detailed flow statistics within this traffic Item. This helps immensely in in pinpointing trouble areas without going through pages of flows.

    Note: In large-scale tests, it may not be feasible to select multiple checkboxes. Use the **Resource Bar** at the bottom to see how many resources are used or available when you check each box. Also use the **Validate** window at the end of this wizard to understand the precise number of resources used.

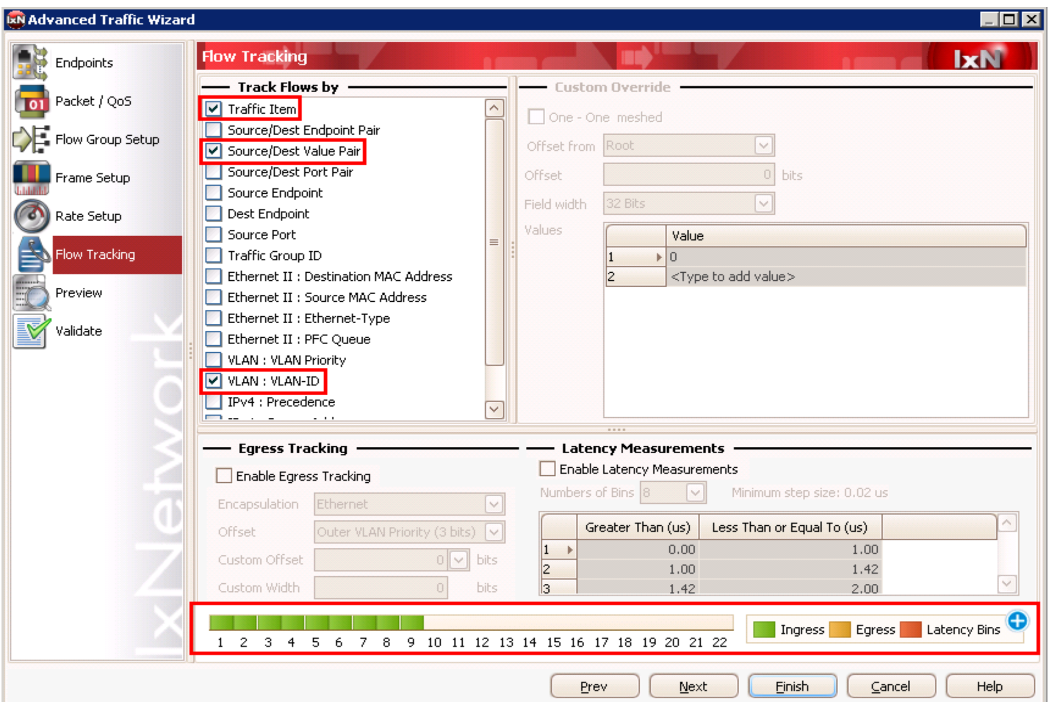


Figure 151. Advanced Traffic wizard screen 6

19. Optionally, on the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that will be transmitted from each Port/Flow Group.
    a. In this case on P1, Flow Group 1, there are 12 unique packets/flows that will be sent. As shown in the Setup topology, 10 MACs from each of the two VPNs on P1 will send to the 60 MACs on the same VPN on P2, P3, amd P4.

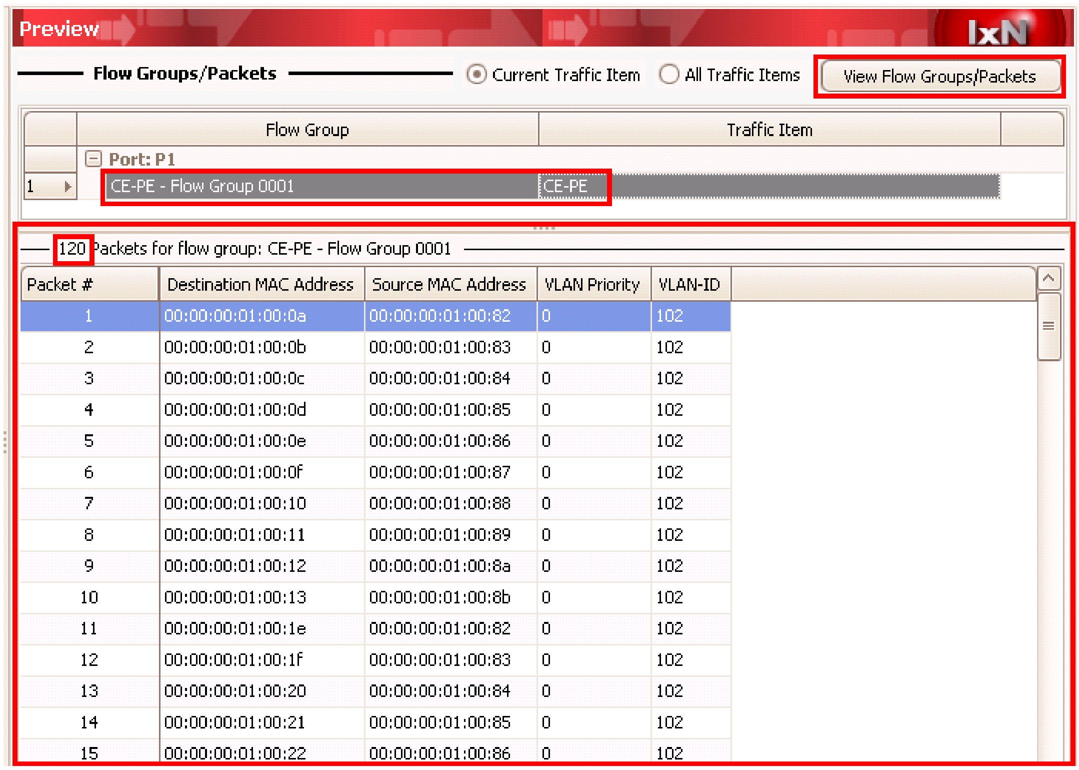


Figure 152. Advanced Traffic wizard screen 7

20. Optionally, on the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

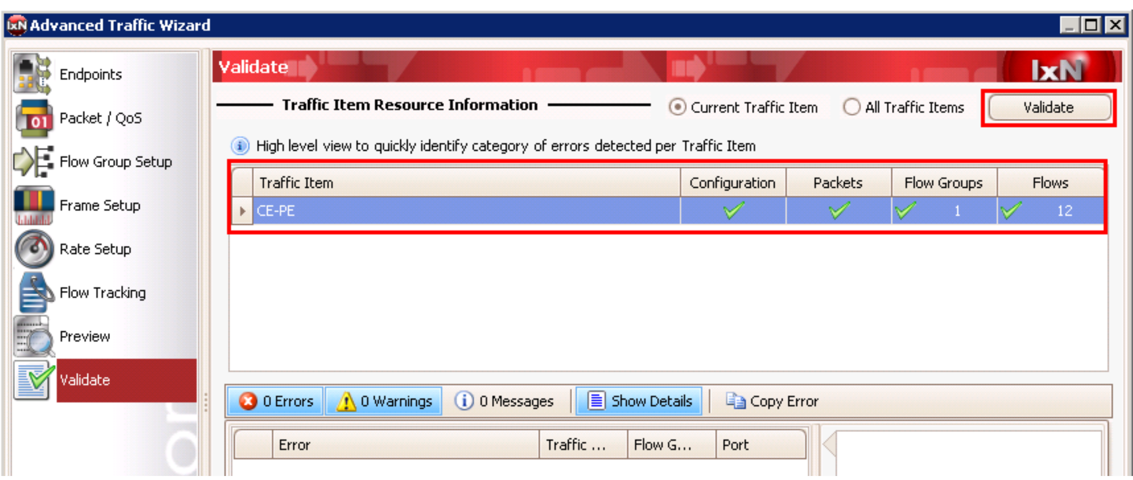


Figure 153. Advanced Traffic wizard screen 8

21. **Troubleshooting Tip**: If errors are generated after hitting finish, see the **Errors** window at the bottom of the screen. Follow the explanation/steps provided. In this type of test, it is likely the test port cannot create the traffic because the DUT has not sent all the information (usually MPLS labels) on the PE side. Check the protocols and view the Learned information on both the Ixia and DUT side. To Finish again, simply right-click on the affected **Traffic Item** and choose **Regenerate.**
Regenerate must also be performed if the DUT sends new label information – for example if a topology change or flapping occurs. The symptom that this has occurred is usually when certain flows are experiencing 100% loss.

22. Now configure the PE-CE traffic. Run the **Traffic Wizard** again by hitting the **+** sign. The steps are practically the same as used for CE-PE, except in the other direction" Here are the shortened steps (screenshot not shown).
    a. Name the **Traffic Item** as **PE-CE**
    b. Make sure the **Traffic Type** is **Ethernet/VLAN**
    c. Change the **Traffic Mesh** to **One-to-One.**
    d. Pull down the **Traffic Group ID Filters** and select both of them. Click **Apply Filter.**
    e. Set the source **Encapsulation Type** to **BGP-VPLS**, and the destination to **non-MPLS**.
    f. Select the **Source – BGP VPLS MAC VLAN Ranges** checkbox.
    g. Select the **Destination** – **Static Mac VLAN Ranges** checkbox .
    h. Click the **down arrow** sign to add the 12 sources and 2 destinations as a traffic Endpoint Set.
    i. Click **Next.**

23. Optionally, use the **Packet/QOS** window (not shown) to add an IP/TCP or IP/UDP header, for example.

24. Optionally, use the **Flow Group Setup** window (not shown) to separate the MPLS labels per port into separate Flow Groups. Each Flow Group is its own transmit engine and can have unique content, and its own rate/frame size.

25. Set the **Frame Setup** and **Rate Setup** windows (not shown) to the desired settings. Start with a simple configuration such as 128 byte frames and 1000 pps rate. These two parameters can also be easily changed in the **Traffic Grid** window after completing the wizard.

26. Select the **Flow Tracking** options for PE-CE traffic (screenshot not shown).
    b. For this direction of traffic it is best to choose **Traffic Item, Traffic Group ID, MPLS Label (1),** and **Source/Dest Value (MAC) Pair.**
    c. All possible combinations from all checkboxes will create a track able flow in the statistics, including rate, loss, and latency.

27. Optionally, in the **Preview** window, click the **View Flow Group/Packets** to see the exact packets that will be transmitted from each Port/Flow Group.
    d. In this case on P2, Flow Group 1, there are 40 unique packets/flows that will be sent. As shown in the Setup topology, 20 MACs from each of the two VPNs will send to the 10 MACs on the same VPN on P1.

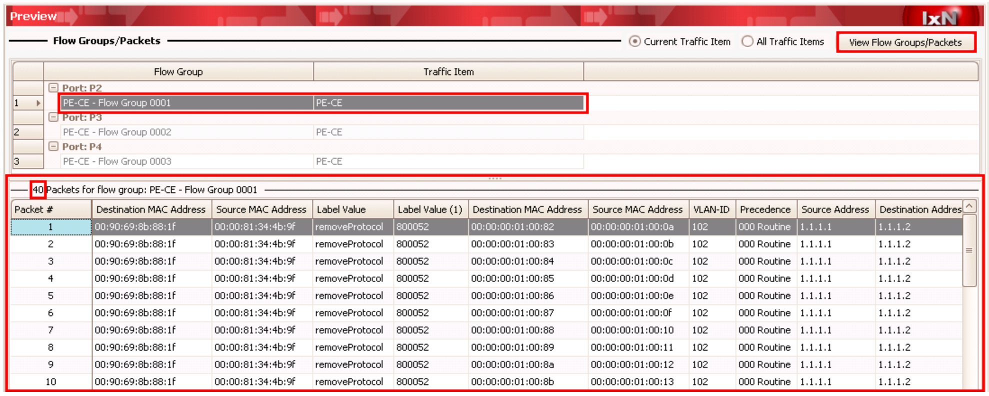


Figure 154. Advanced Traffic wizard screen 7

28. Optionally, on the **Validate** window, click the **Validate** button to understand the resources used for the traffic item you are configuring, or all traffic items. Click **Finish.**

29. Optionally, after finishing the Traffic Wizard you will see the Traffic (grid) window. There are many operations that can be done here including:
    - Adding new (tab) views
    - Adding new columns to existing views, including packet contents fields.
    - Many grid operation, including multi-select, and copy down/increment.
    - Changing the rate/frame size on the fly without stopping traffic.
    - Double-clicking a flow group to configure its properties/packet contents.

    Performance test variables:
    - Manual performance testing of the data plane can be accomplished by increasing the frame size and data rate.
    - Automatic throughput tests can be accomplished using IxNetwork's integrated tests as discussed in the *Test Variables* section below.

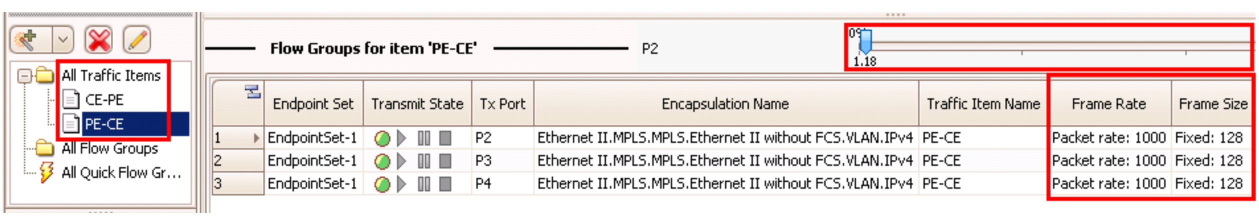
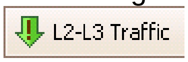


Figure 155. Post-Wizard Traffic Grid

30. **Apply,** and **Start** the traffic.
    a. Click the **Apply Traffic** button at the top of the screen. This will send the Traffic Item configuration to the test port.



    b. Click the **Start** (play) button

31. View the traffic statistics.
    a. Click on **Statistics** -> **Traffic Item Statistics**. This will show the aggregated view of all the traffic of each Traffic Item from CE-PE, and PE-CE.

Note: The Traffic Item aggregated view is very helpful to understand the performance of the DUT at a large-scale without having to investigate large amounts of results. If everything looks fine, then is no need to “drill-down” further. However, if there is loss or high latency, drilling down within each traffic item to pinpoint the problem can become very useful.

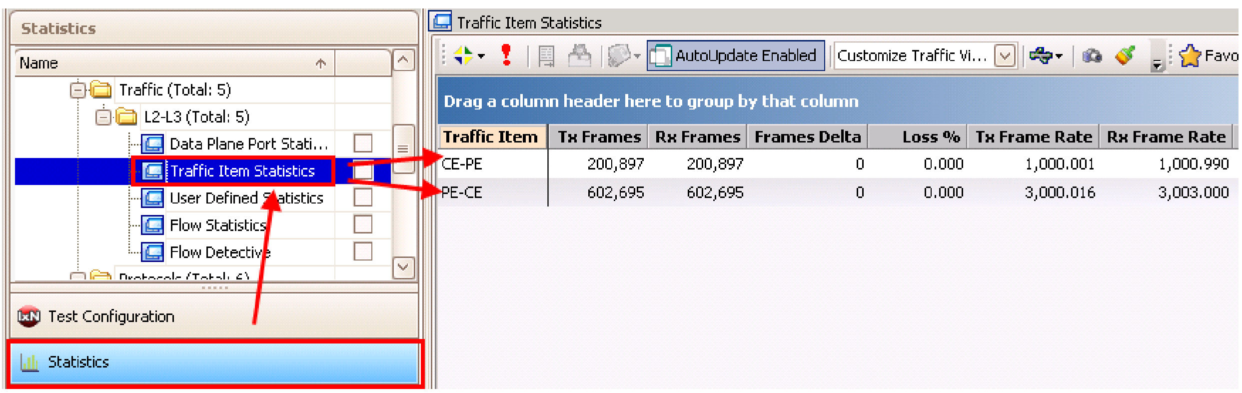


Figure 156. Statistics -> Traffic Item View

Performance test variable*:* Go back to the **Test Configuration** window and increase the rate in real time of one or more flow groups until loss occurs. Then use the following step to drill -down and find the problem.

    b. Now **Drill Down** on the CE-PE traffic by right-mouse clicking on the CE-PE Traffic Item and finding the **Flow Tracking** options as defined in the Traffic Wizard. In the example below click on **Drill Down per VLAN ID** to see all the VLAN statistics inside the CE-PE Traffic Item. These are the per-VLAN detailed statistics that make up the aggregated CE-PE Traffic Item statistic.

    Note: This is very helpful to see which particular VLAN (i.e. customer VPN) may be having issues.

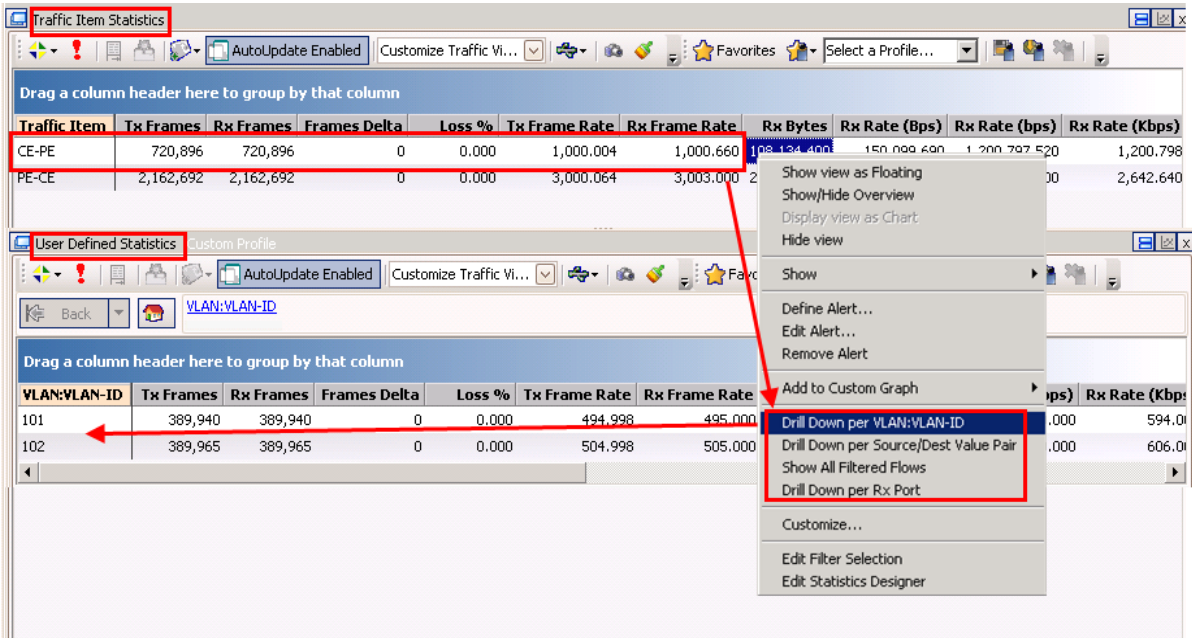


Figure 157. Statistics -> Drill down from Traffic Item to VLAN ID

c. Now **Drill down** again on VLAN 101 (right-click -> **Drill down per Src/Dst Value (MaC) Pair**). You see all 60 MAC flows within VLAN 101 from the CE-PE side.

Note: This is very helpful to see which particular Src/Dst MAC within the given VLAN (i.e. customer VPN) may be having issues.

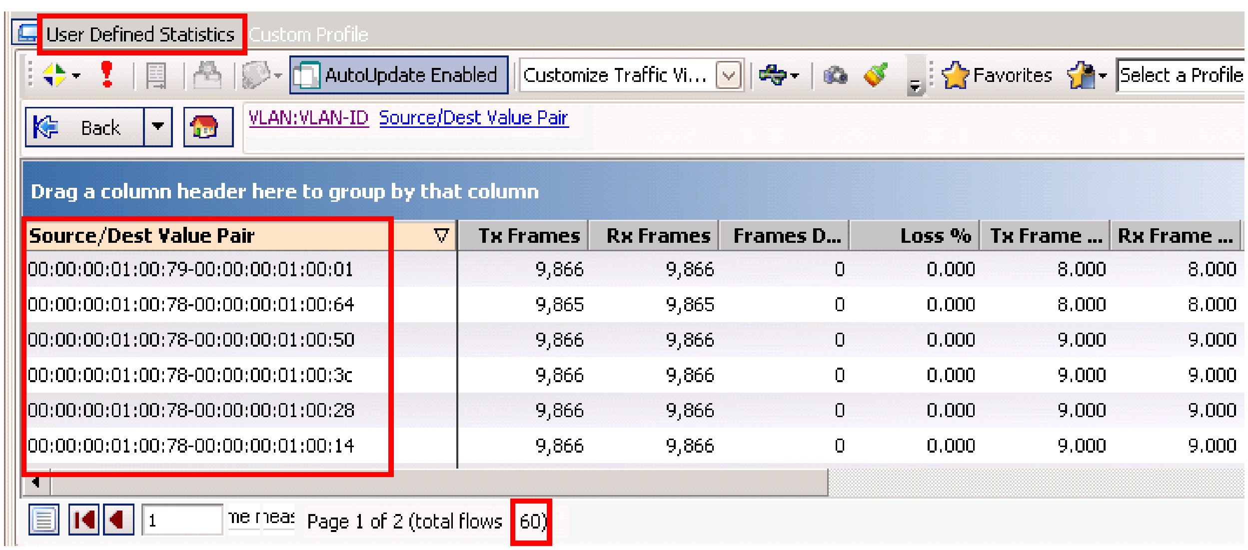


Figure 158. Statistics -> Drill down from VLAN ID to Src/Dst Value (MAC) pair

d. Likewise, **Drill-down** on the PE-CE Traffic Item to the **Traffic Group ID**.

Note: This is very helpful to understand how the traffic on each VPN (Traffic Group ID) within the PE-CE traffic is performing. The **Traffic Group ID** can also be used in the CE-PE traffic item.

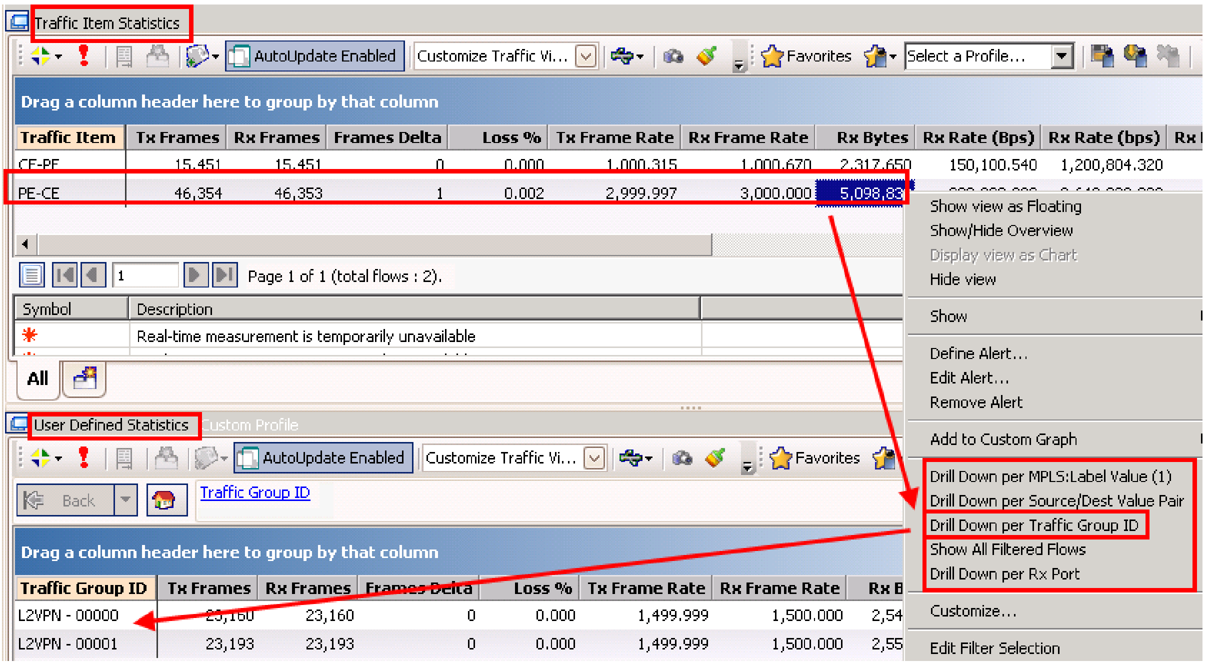


Figure 159. Statistics -> Drill down from Traffic Item to Traffic Group ID

e. Optionally, drill down *again* from each **Traffic Group ID** to **MPLS label.**
Note: This is very helpful to understand how the traffic on each MPLS label within the given VPN (Traffic Group ID) is performing.

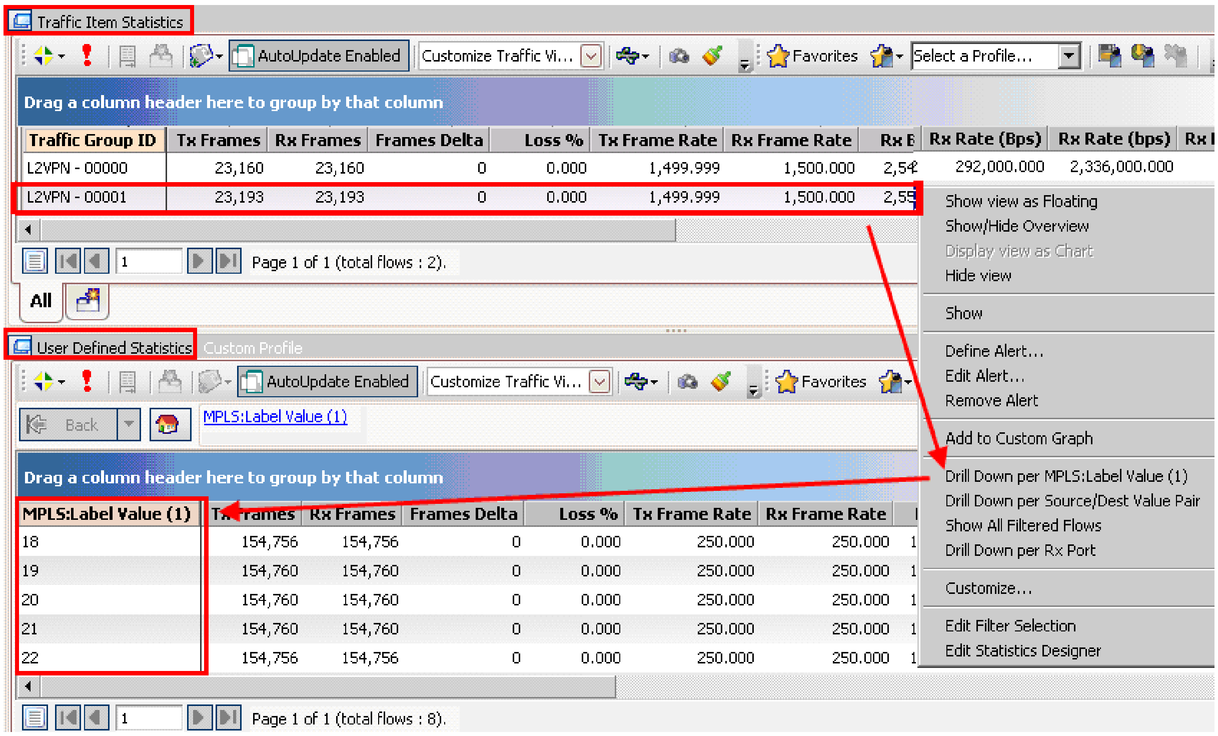


Figure 160. Statistics -> Drill down from Traffic Group ID to MPLS label

f. Optionally, drill down again from each **MPLS Label** to **Source/Dest Value (MAC) Pair.**

Note: This is very helpful to understand how the Src/Dst MAC traffic within each MPLS label is performing.

Note: **Drill-down per Rx Port** comes standard by default with every drill-down view. In this case it will help determine which RX port on the CE side is receiving the suspect MPLS traffic from the PE side. It may help determine which VPN is a fault without having to go to the label database and track the label through the network to the CE side.

Troubleshooting tip: In any of the above views, a small frame delta statistic does not necessarily mean that loss is present. Stopping traffic will fully synchronize the results. No test tool can measure Tx and Rx instantaneously, since the traffic must go through the DUT first. If the frame delta is continually increasing, however, there is likely loss.

Test Variables

Each of the following variables may be used in separate test cases to test a PE router in an L2 VPN - VPLS network. They all use the test case detailed above as a baseline, modifying a few parameters in the same IxNetwork L2 VPN wizard views shown above. You can create control plane scalability tests from 10x to over 100x to fully stress the DUT's capability as a PE router and understand its peering capacity with CEs, Ps, and other PEs. Once control plane scalability is understood, data plane performance can be measured in terms of throughput, latency, and loss for every frame size or IMIX pattern available.

Control Plane Performance Variables

Performance Variable	Description
Increase CE Ports	**Step 5:** On a real PE router, there will be many more CE ports than P or PE ports, and each CE port will have many CEs/VLANs on it.
Increase PE Ports	**Step 5:** On a real PE router, there is a minimum of two provider ports (one for backup), and it's possible that one or more of these ports will be high speed (10G) with high control plane scalability requirements.
Increase Emulated Ixia P Routers	**Step 6:** Increasing Ixia P routers per port will stress the DUT's (PE) ability to peer/run MPLS and IGP protocols. If needed, use VLANs.
Use different IGP, MPLS, or L2 VPN Protocols	**Step 6:** Try other routing protocols, such as ISIS, RSVP-TE, and LDP-Extended-Martini. These protocols may have higher or lower overhead on the DUT, and performance may vary.
Increase Emulated Ixia PE Routers	**Step 7**: This is one area that can grow quite large in an service provider network in terms of IGP connections and exchanged VPN/VC information. This will test the DUT's ability to store/maintain VPN/VC information without leaking the information to incorrect VPNs/VCs.
Increase VPNs per PE Router	**Step 8:** This parameter will test the DUT's maximum capacity for VPNs attached to one or more PE routers. Increase this number along with the number of PEs to expand the test substantially**.**
Increase the number of MACs per VPLS instance	**Step 9:** Unlike PWE, a DUT using VPLS needs to maintain unique MAC tables for each VPN so it can switch the packets to the appropriate site. Therefore, increasing the number of MACs will stress the DUT's ability to handle many MAC addresses on each VPN. Forward traffic to all MACs and track all MACs to truly test performance of each/every MAC per VPLS instance.

Data Plane Performance Variables

Performance Variable	Description
Increase Traffic Rate	**Step 18-23:** Manually increase the rate at which traffic is sent. Verify that latency and loss levels per flow are as expectations.
Change Frame Size	**Step 18-23:** Manually change the frame size of the traffic. Smaller frames typically cause more trouble for switches/routers, so tests running with 64-byte packets at a high frame rate should be tested by operators. Additionally, select one of the real-world IMIX patterns that Ixia provides.
Run Binary-search Throughput tests using Ixia's "Integrated Tests"	Go to the IxNetwork **Test Configuration** window and look for **7. Integrated Tests**. These tests will automatically run binary-search throughput tests using any/all frame sizes, and apply industry-standard methodology to determine the maximum amount of throughput without loss that the DUT can handle.

Results Analysis

The baseline test demonstrated that the DUT, acting as a PE router, could maintain and run a network consisting of two customer VPNs, each with eight sites, and each site having ten MAC addresses. Think of these MAC addresses as hosts/PCs. Additional emulation of three P routers and six PE routers was added. Finally, the DUT was able to forward 64-byte data traffic at a rate of 10% of a 1Gb link. The DUT maintained performance across this network with no loss and low latency.

However, even in a small-to-medium size service provider network there can be tens or hundreds of VPNs covering hundreds of locations. These VPNS may use tens or hundreds of ports spanning hundreds or thousands of miles.

Because of this, control plane scalability testing and data plane performance testing are critical to ensure that these devices and networks can handle the load placed upon them in real-world scenarios. Go to the **Test Variables** section for a discussion of the various ways in which the test case can be extended into more extensive scalability and performance tests.

As the control plane variables are increased to the DUT's maximums, special attention must be paid to the detailed protocol statistics, including up/down sessions, and protocol counters. On the data plane side, each and every MAC address should be checked for loss and latency as it flows through the DUT. Packet/MAC leakage is another critical check, to make sure that one VPN customer's traffic/forwarding table is not mixed with others. Lastly, long duration tests at maximum scale are required with and without real-world outage situations to ensure expected behavior in a volatile real-world network environment.

Troubleshooting Tips

Issue	Troubleshooting Solution
The VCs are not coming up Can't Ping from DUT to the Ixia Emulated P	**Step 8:** Make sure the site IDs and label block values are consistent with the DUTs. **Step 12:** Check the protocol interface window and look for red exclamation marks (!). If any are found, an IP address/gateway mismatch is likely.
Sessions won't come up	**Step 14**: • Go back to the **Test Configuration** window and double check the protocol configuration against the DUT. • From the **Test Configuration** window, turn on **Control Plane Capture**, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.
No "Learned" info	**Step 16:** There is likely a mismatch in the VPN/VC configuration on the Ixia port or the DUT. Also check to make sure your VLAN IDs are correct.
Traffic 100% Loss from PE-CE	**Step 24-25:** Check the **Warnings** columns in the **Traffic** view (step 24) and make sure there are no streams that say *VPN label not found*. The DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then **Apply** traffic.
Stop/Start Protocols or Link Down/Up has Traffic 100% Loss from PE-CE	**Step 24-25:** Check the **Warnings** columns in the **Traffic** view (Step 24) and make sure there are no streams that say *VPN label not found*. The DUT may have sent new label info. If so, regenerate traffic by right-mouse-click on the traffic item. Then Apply traffic.

Conclusions

This test verified that the DUT can perform with four ports of scale as a PE router in a layer 2 VPN - VPLS network. However, scalability and performance are of paramount importance when testing a DUT acting as a PE router. Follow the **Test Variables** section above to test the PE at its maximum capability before deploying into a real-world L2 VPN – VPLS Network.

Test Case: Impairment Testing of Layer 2 MPLS VPN

Overview

WAN networks typically suffer from network conditions such as drop, delay and jitter because of slow WAN links. It is important for service providers to measure the VPN service performance when their network uses WAN links. Impairment modules emulate WAN link impairment conditions by introducing drop, delay and jitter in the traffic, thus providing a solution for impairment testing. Ixia's Impairment solution also allows impairing traffic in each direction independently, emulating the asymmetric WAN link configuration.

Testing Layer 2 MPLS VPNs is discussed in the previous test case. This test case simulates real world network impairments, thereby adding another dimension to the Layer 2 MPLS VPN performance testing. Service providers can observe the impact of network impairments on VPN services and roll out their revenue-generating network accordingly to meet the SLA agreements. The PE Router being the key component in the provider network, the focus of this test is to impair the traffic on PE router ingress, and provide impairment measurements.

Objective

The objective of this test is to introduce drop, delay and jitter in the traffic flowing from the Ixia emulated Service Provider Network to DUT PE. The traffic is classified for impairments, based on outer and inner MPLS Labels.

Impairment module can be inserted in any link where impairment is needed. The steps used in this test case can be applied equally well for Layer 3 VPN, multicast VPN and NG multicast VPN.

At the end of this test, other test variables will be discussed that will provide many more performance test cases.

Setup

The test setup requires

- a DUT acting as a PE router,
- a pair of Ixia impairment ports, and
- four Ixia test ports

This test topology follows the topology of Layer2 MPLS VPN, which means, one Ixia Test port emulates the CE routers and the other three ports emulate the entire service provider network. A pair of Impairment ports is connected to emulated service provider network on one side and to the DUT PE on the other. The lightning icon denotes impaired traffic on the link.

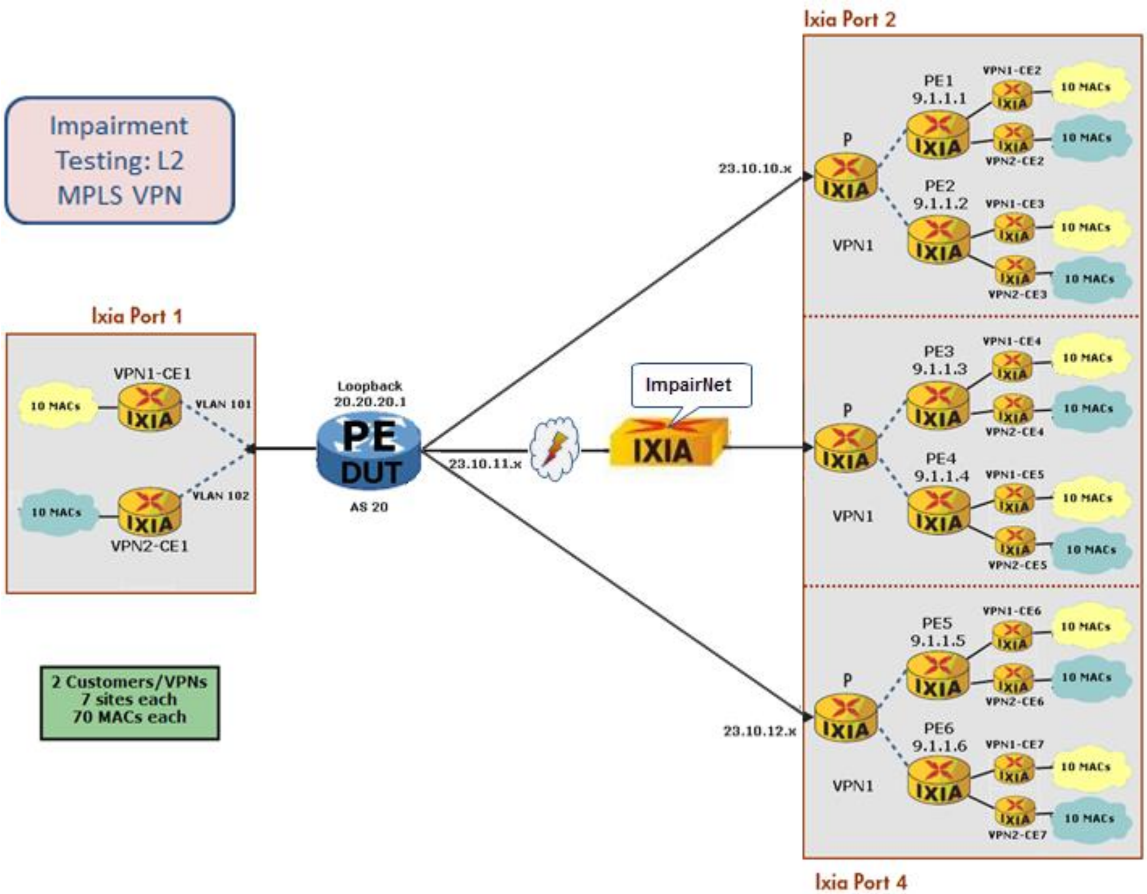


Figure 161. Impairment testing - Ixia emulated layer 2 MPLS VPN network

Step-by-Step Instructions

These instructions will result in Delay, Jitter, Drop and Rate Limit Impairment testing of Layer2 MPLS VPN topology similar to the one shown in Figure 161. You may also use these steps as a guide to build other Impairment test scenarios.

1. Follow the steps in the section **Test Case: Layer 2 MPLS VPN – VPLS Scalability and Performance TestError! Reference source not found.** to configure Layer 2 MPLS VPN Topology. Note that the L2 VPN configuration parameters in this test case are different from those of Layer 2 MPLS VPN test case, and accordingly there will be differences in the traffic and impairment statistics. For example, the traffic rate is set to 2% in this test setup.

2. Reserve two impairment ports in IxNetwork. The Impairment ports are added in the same way as other Ixia test ports with the exception that Impairment Ports are always selected as a port pair.

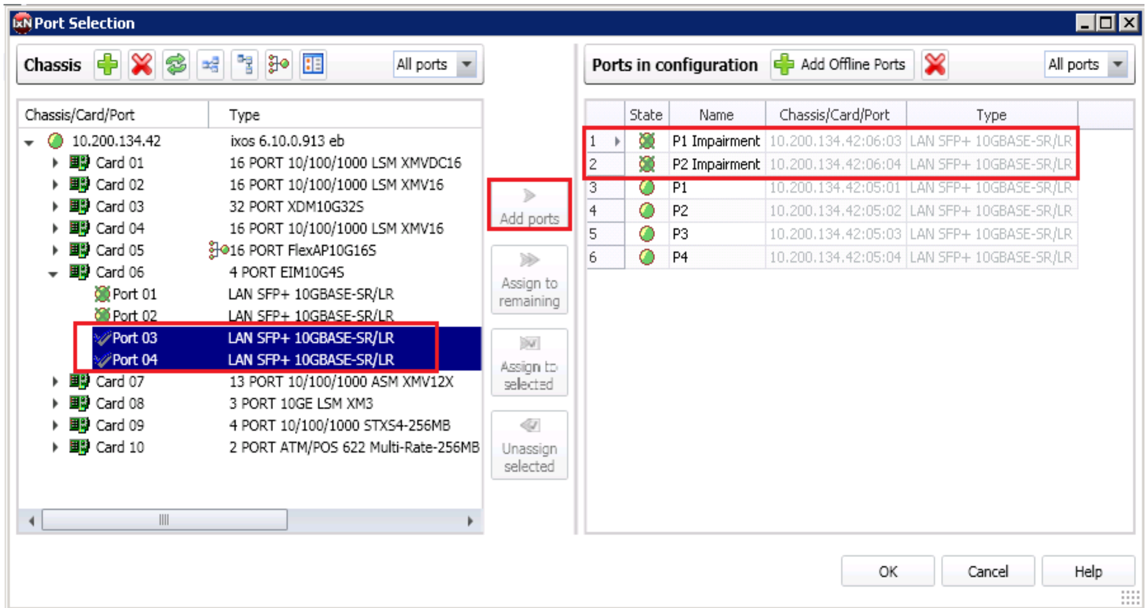


Figure 162. Impairment Port Selection

Optionally, rename the ImpairNet ports just like any other test ports. You can then refer to impairment ports throughout the IxNetwork application.

3. Ixia's IxNetwork Impairment GUI provides an easy to use one click option to create an impairment profile directly from the traffic flow group. Right click on the desired flow group in L2-3 Flow Groups view and choose Create Impairment Profile from the menu.

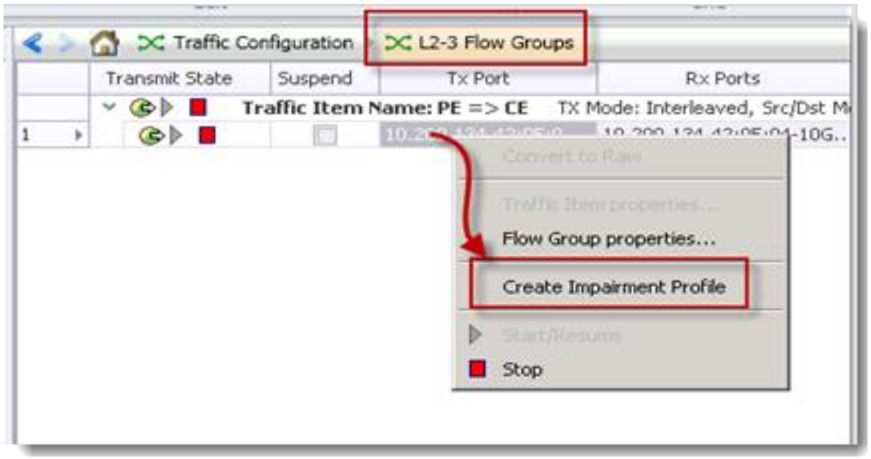


Figure 163. Impairment Profile Creation

Creating impairment profile directly from the traffic flow group has the advantage that all the L2-3 traffic classifiers are automatically added in the list of classifiers for this profile.

Note: The view changes from L2-3 Flow Groups view to Network Impairment view on clicking **Create Impairment Profile**.

4. The Network Impairment view has three tabs: Diagram, Profiles and Links. The Diagram tab is chosen by default. Select the **Profiles** tab to see the list of all the impairment profiles.

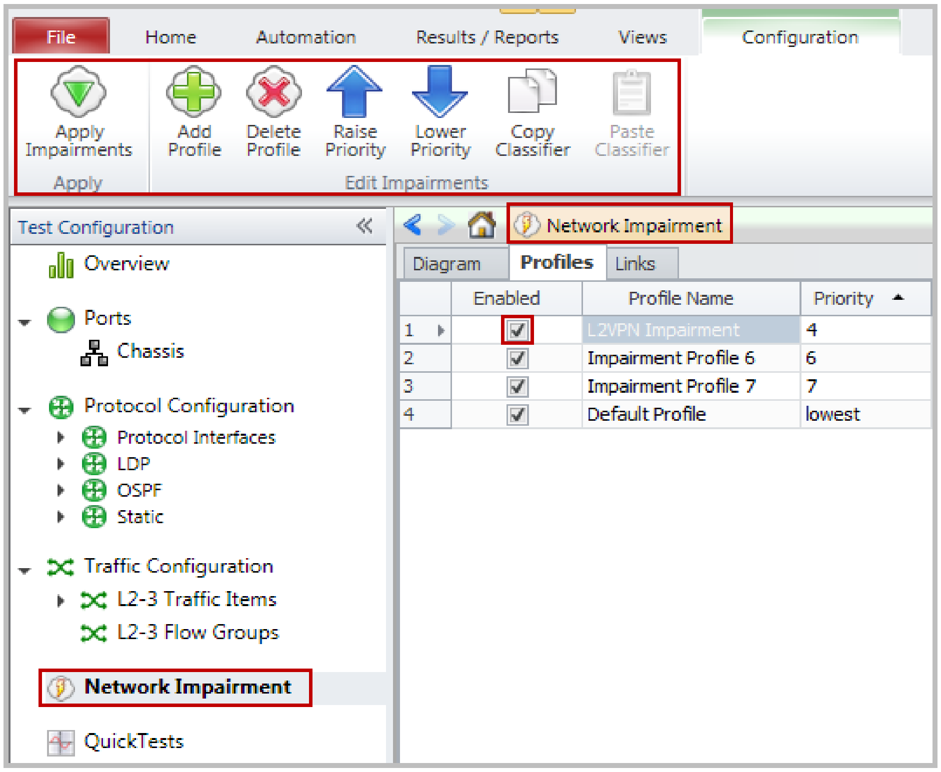


Figure 164. Network Impairment view

Optionally, change the name of the impairment profile. A named profile can be easily referenced throughout the IxNetwork application.

Note:

- The Network Impairment view has commands for creation, deletion, and raising or lowering priority of impairment profiles as shown in Figure 164.
- When the impairment profile is created, it is enabled by default. Each profile has a check box next to it to disable/enable the profile.

5. To see the list of available traffic classifiers, click on the **Classifier** grid in the **Network Impairment -> Profiles** tab.

There are two MPLS label value; the first is the LDP or RSVP-TE transport label, and the second is the VPLS instance label. Select the second MPLS Label Value from the list of patterns.

The classifier pattern value has hexadecimal format and is aligned to an octet boundary. The unused bits in the value can be ignored by using don't care bits in the mask.

An MPLS label value contains the first 20 bits out of 32 bits (4 bytes) field, set the mask to *FFFFF0* to ignore the last 4 bits. The TTL byte is ignored in this setting. In this test case, the traffic for the VPLS instance with label value 19 is being impaired. The label value *19* translates to hex value *00 01 30.*

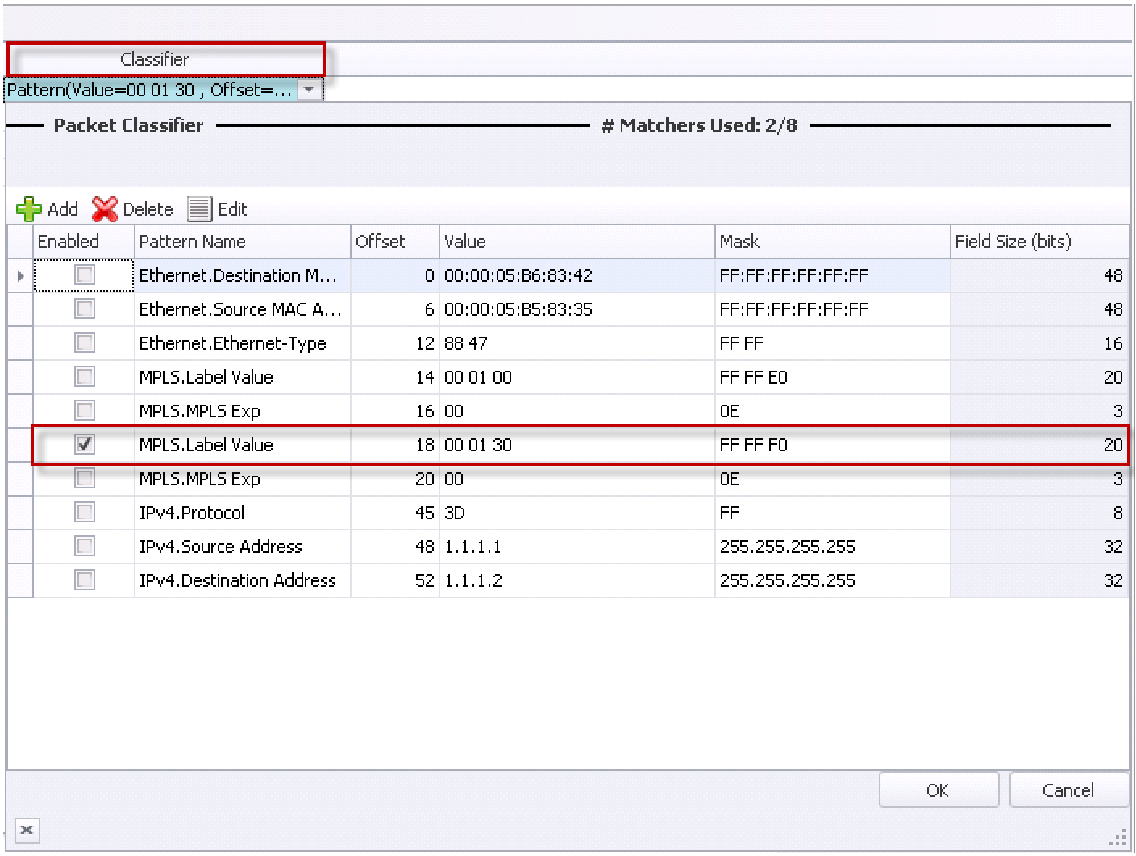


Figure 165. Traffic classifiers

6. Each impairment port pair has two links that denote the direction of traffic flow between the two impairment ports. Click the **Links** grid of the desired impairment profile. Select the appropriate link to impair the traffic flow from the Service Provider to the PE DUT.

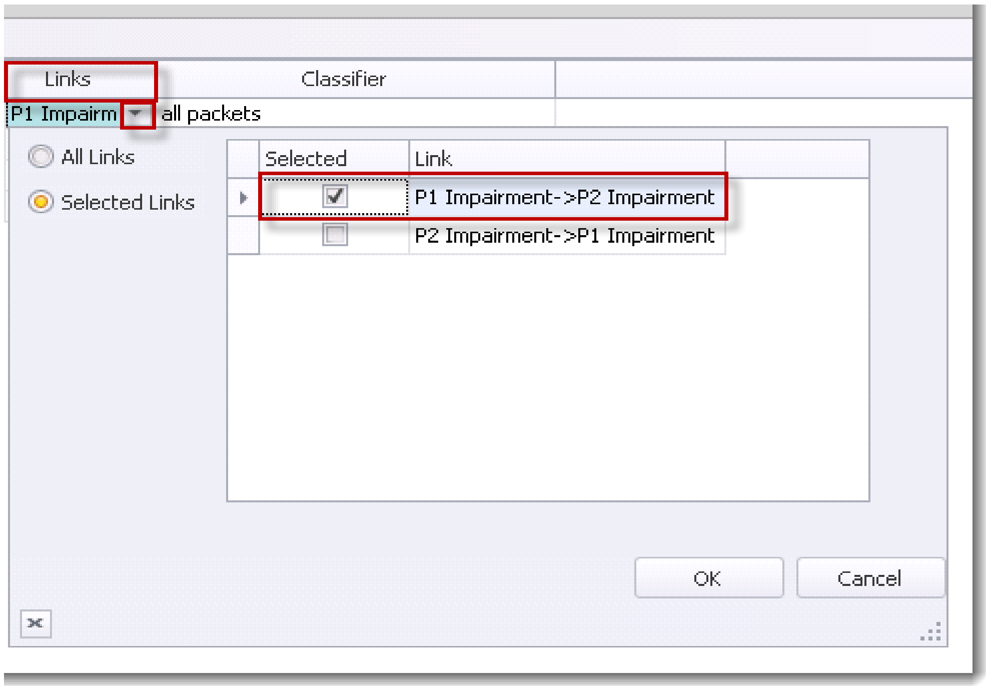


Figure 166. Network Impairment Link Selection

7. Right click the Drop grid of the desired impairment profile to apply drop impairment. Tick the **Enabled** check-box and set the drop percentage to *50%.*

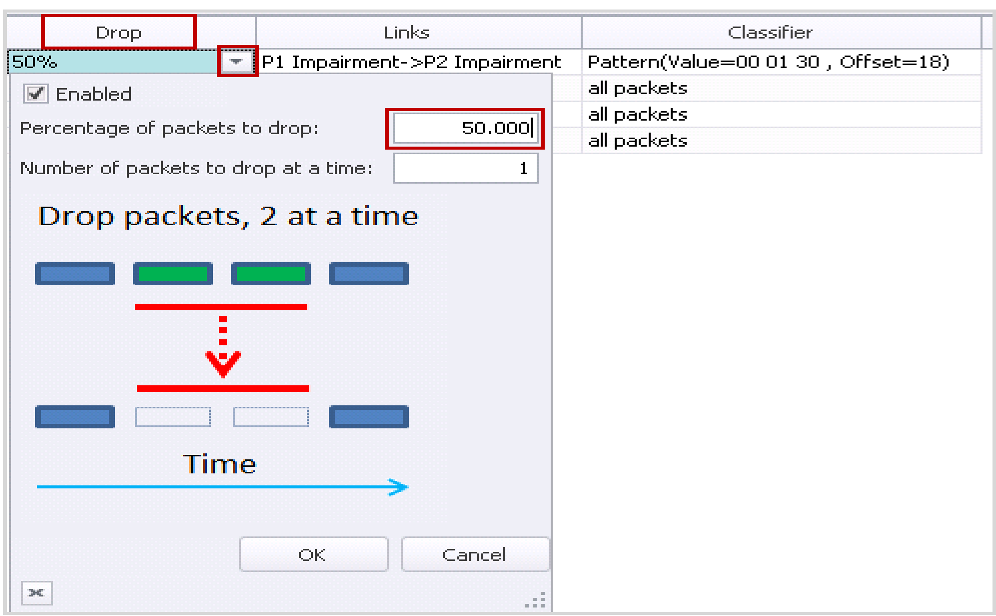


Figure 167. Drop Impairment Configuration

8. Change the bottom tab to **Delay** in **Network Impairment -> Profiles** tab, to apply delay and delay variation impairments. Select the impairment profile and right click on the **Delay**. Tick the **Enabled** checkbox and enter *100 microseconds.*

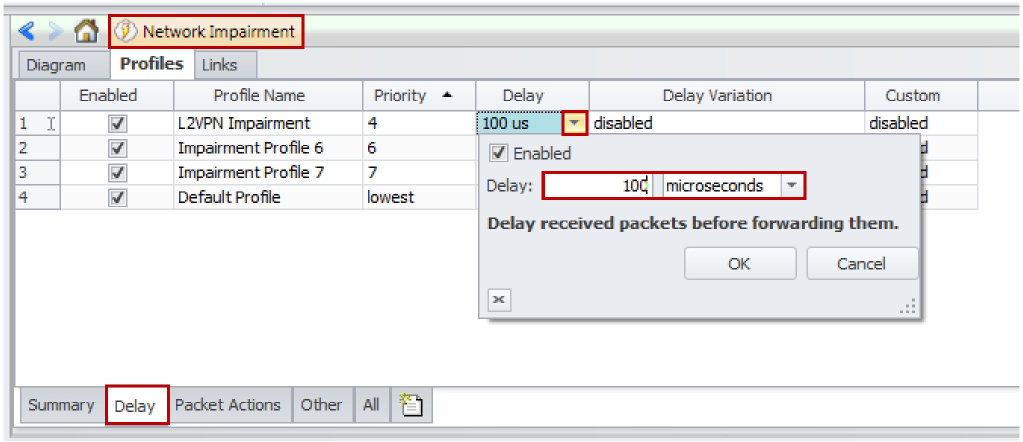


Figure 168. Delay Impairment Configuration

9. Select the impairment profile and right click **Delay Variation** grid. Tick the **Enabled** check-box and select the radio button *Gaussian*. Set **Standard Deviation** to *10 microseconds*.

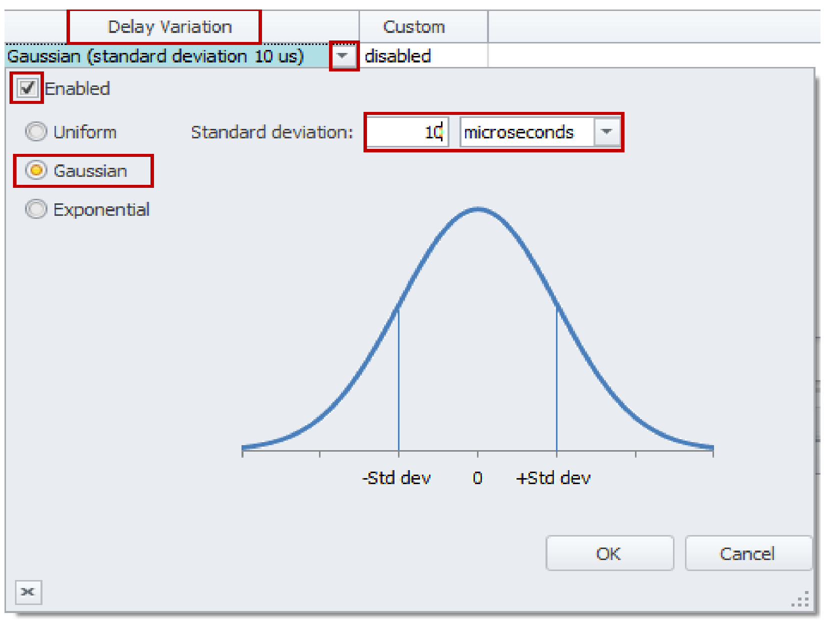


Figure 169. Jitter Impairment Configuration

10. To apply the impairment profile in the hardware, click **Apply Impairments** icon in the configuration ribbon. If applying impairment profile changes is successful, then the exclamation mark on the **Apply Impairment** icon will disappear.

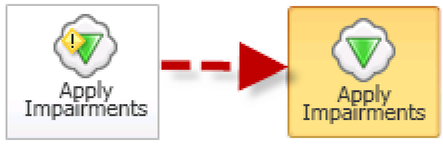


Figure 170. Apply Impairment Icon Change

Note:
- Only the enabled profiles are applied to the hardware.
- If the impairment profile contains configuration errors, the exclamation mark will not disappear and a pop-up window will appear on the right hand side bottom corner of the IxNetwork GUI. For further troubleshooting, follow the instructions in the Troubleshooting Tips section.

11. After applying impairments, the impairment statistics starts updating. Select **Impairment Profile Statistics** and click the **Dropped** tab at the bottom in the impairment statistics view.

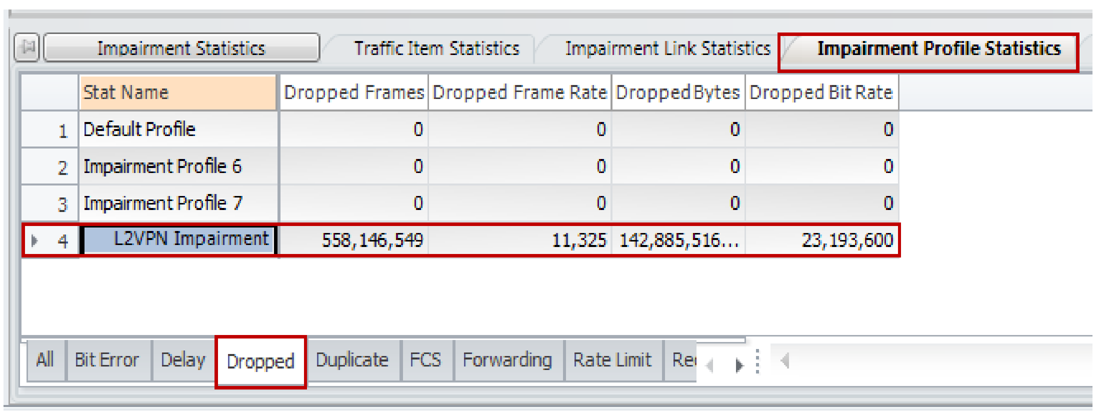


Figure 171. Drop Impairment Profile Statistics

12. Only the profiles with drop impairment enabled will drop the packets. Ensure that the packets are dropped at the configured rate. To view the dropped packet statistics for each link direction of the Impairment module, select the **Impairment Link Statistics** tab and then select the **Dropped** tab at the bottom.

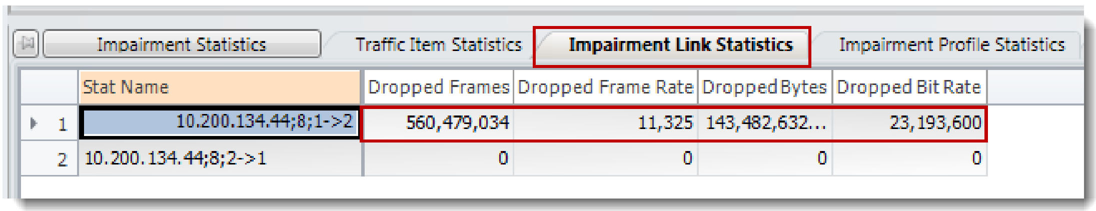


Figure 172. Drop Impairment Link Statistics

Note: In this test case, only packets from P1 Impairment -> P2 Impairment link direction are dropped because of the **Links** configuration.

13. To view the packet delay/jitter statistics for L2VPN Impairment profile, select **Impairment Profile Statistics** tab and select **Delay** tab at the bottom.

    Note: Two profiles show delay statistics: L2VPN Impairment profile and Impairment Profile 6. Based on the profile priority value, Impairment Profile 6 is applied to all the traffic that is not classified under L2VPN Impairment profile. Since ImpairNet module has an intrinsic delay of 30 us, all the traffic classified under Impairment Profile 6 experiences a delay of 30 us.

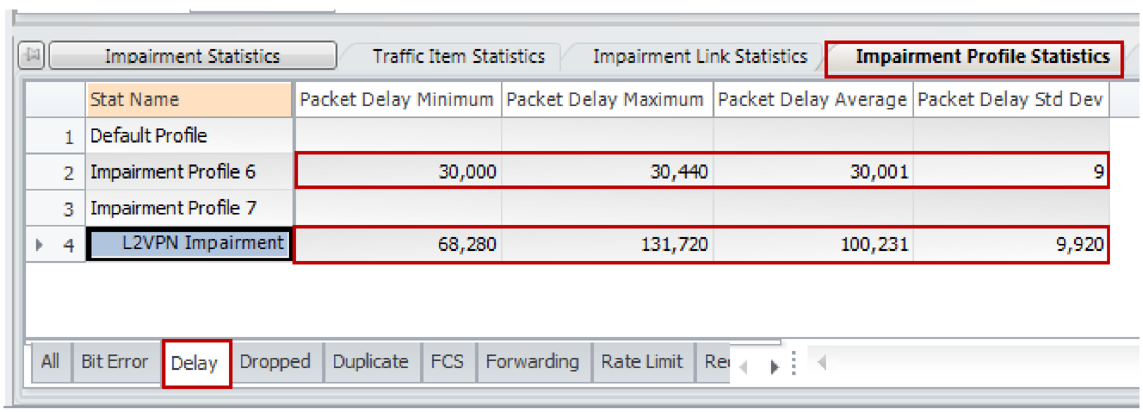


Figure 173. Delay Impairment Profile Statistics

14. To view the packet delay/jitter statistics for impairment links, select **Impairment Link Statistics** tab in the Impairment Statistics view and select the **Delay** tab at the bottom.

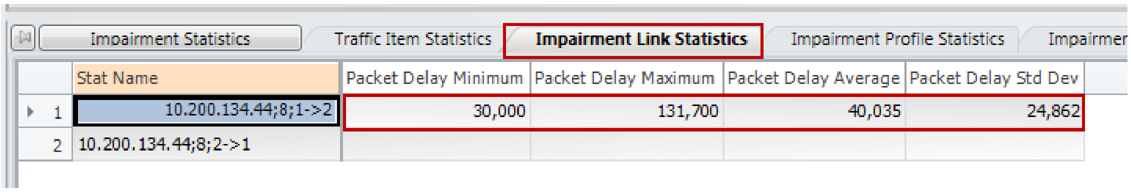


Figure 174. Delay Impairment Link Statistics

Note: Unlike impairment profile statistics, impairment link statistics show the delay statistics for all the packets passing through the impairment links and hence there is a minimum delay of 30 us. Hence the Standard Deviation is also centered on ~25 us.

15. This step demonstrates how to configure a 100% drop when the traffic for MPLS Label 19 exceeds 4 Mbps.

    Go to Profiles Tab in Network Impairment view and select **Summary** or **All** tab. Tick the **Enabled** check-box in the **Rate Limit** grid and set the rate limit to *4 Mbps*.

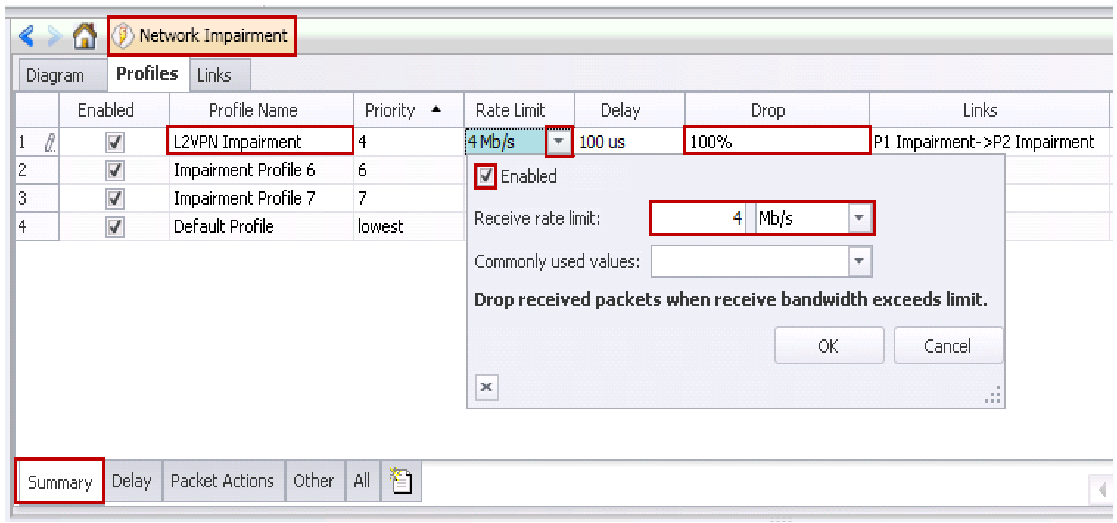


Figure 175. Rate Limit Impairment configuration

Note: For this test setup, L2 MPLS VPN parameters have been configured such that more than 4 Mbps traffic is flowing through the ImpairNet module for L2VPN impairment profile. If in your L2 MPLS VPN configuration, traffic for the MPLS Label selected for impairment is less than 4 Mbps, then choose a different rate limit. The steps below are still applicable although Impairment measurements will vary.

16. Click the **Drop** grid for **L2VPN Impairment** Profile and set the **Drop rate** to *100%* without opening the configuration dialogue as the impairment is already enabled. When the impairment profile is changed, the Apply Impairment icon will show an exclamation mark as shown in Figure 170. Click on Apply Impairment icon again to apply the impairment profile changes.

17. **Note**: Impairment profile changes can be applied without disrupting the traffic flowing through the ImpairNet module. To view how much of traffic is dropped due to rate limit setting, select **Rate Limit** tab from the bottom of Impairment Profile Statistics view.

    The statistics show a total of ~23 Mbps traffic dropped with 50% drop enabled, which means, 23 Mbps * (100% / 50%) = ~46 Mbps traffic with MPLS label 19 enters ImpairNet module. The rate limit being set to 4 Mbps, ~42 Mbps traffic is dropped at the ingress of the ImpairNet module.

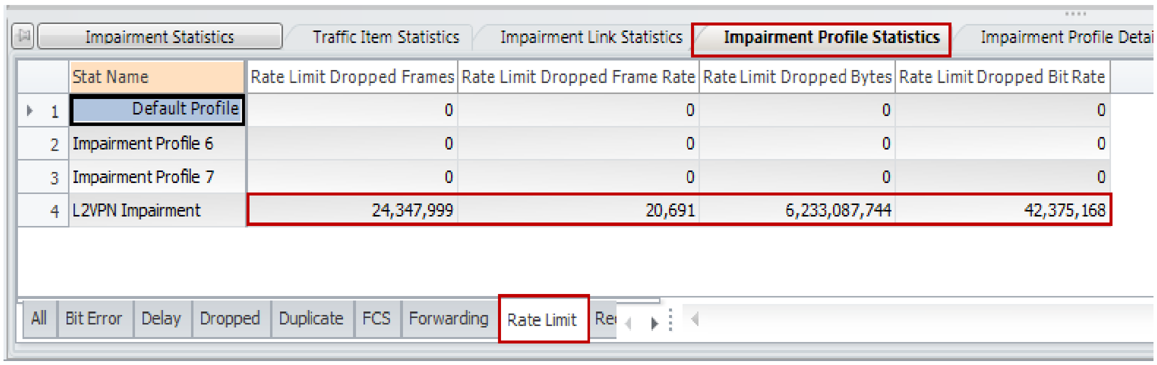


Figure 176. Rate Limit Statistics for Impairment Profile

18. To view the rate limited traffic for the Impairment Links, select the **Rate Limit** tab at the bottom of the **Impairment Link Statistics** view. The link dropped statistics is the aggregation of all impairment profile dropped statistics.

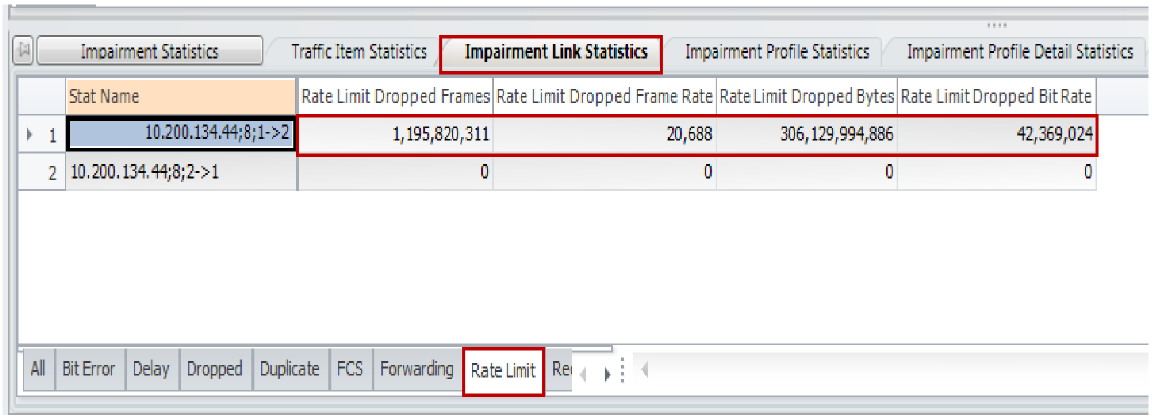


Figure 177. Rate Limit Statistics for Impairment Link

19. To view the dropped packets statistics for the impairment profile, select the **Dropped** tab at the bottom of the Impairment Profile Statistics tab. A total of ~4 Mbps traffic is being dropped as per the drop configuration.

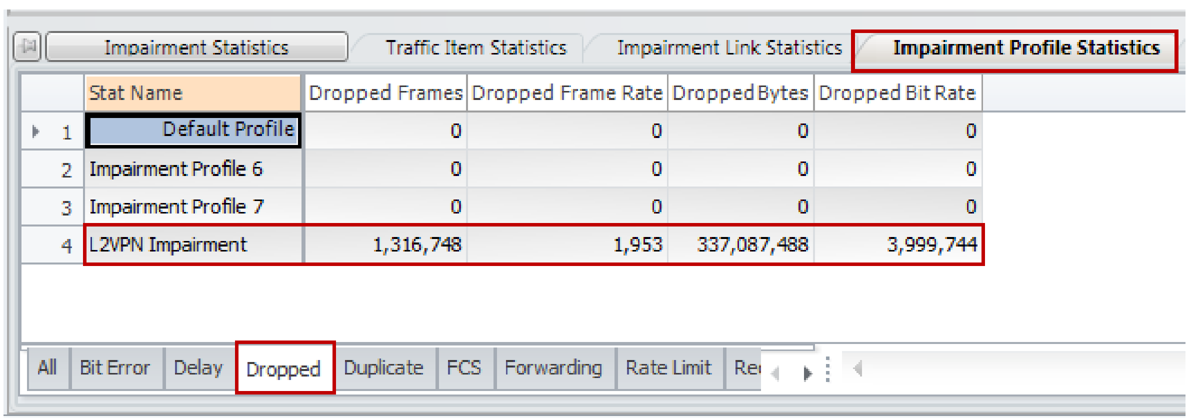


Figure 178. Dropped Statistics with Rate Limit for Impairment Profile

20. To view the Dropped statistics for impairment links, select the **Dropped** tab at the bottom of the Impairment Link Statistics view.

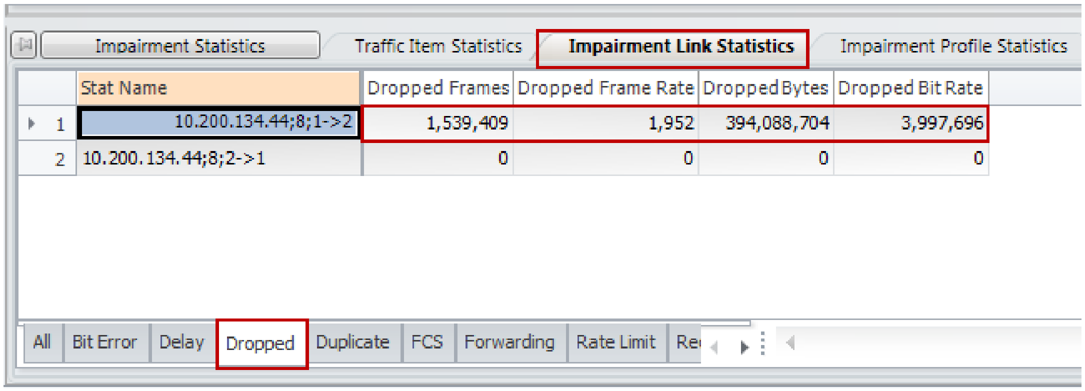


Figure 179. Dropped Statistics with Rate Limit for Impairment Link

Test Variables

Each of the following variables may be used in separate test cases to test a PE router in an L2 VPN - MPLS network with impairments. These variables use the test case detailed above as a baseline, with a few modifications in the parameters. You can create various scalability tests to stress the DUT's capability to the fullest in presence of real-world network impairments.

Performance Variable	Description
	You can create up to 32 bidirectional or 64 unidirectional impairment profiles per impairment port pair.
Use multiple classifiers	You can introduce multiple classifiers in a single impairment profile. Classifiers can also be copied and pasted across impairment profiles by using Copy Classifier and Paste Classifier commands in the Network Impairment Configuration tab. A maximum of 16 classifiers can be added for each link direction.
Apply impairments in both link directions	You can choose to impair either one or both the links.
Apply different drop rates	Apply drop rates from 0-100% in clusters to a maximum of 65535 packets.
Apply different packet impairments	Apply reorder and duplicate and BER impairments in addition to drop impairment. Reorder and duplicate impairments are present in the Packet Actions tab at the bottom of the Profiles tab.
Increase Delay	Introduce delay up to 6s for every impairment profile on a 1G impairment module and up to 600ms for a 10 G impairment module.

Performance Variable	Description
Apply different kind of delays	Introduce delay in us, ms or km. 1 km of WAN Link causes a delay of 5 us.
Apply different delay variations	You can apply uniform, exponential and customized delay variations.
Apply different packet impairments	Apply rate limit to a maximum of the full line rate. Optionally, choose the most commonly used rate limits from the drop-box.
Apply BER impairment	Apply BER impairment in the **Other** tab. Optionally, you can choose to enable: *Correct L2 FCS error* and *Drop the packet with L2 FCS errors* in the **Checksum** grid.

Results Analysis

The baseline test demonstrated the DUT's capability of handling common impairments like drop, delay and jitter. Finally, you can observe the traffic statistics at the Ixia emulated CE router to check the impact on VPN service performance. Consider each MPLS Label classifier as a LSP for a set of customer sites. Test the performance under stress and impairment conditions to understand the DUT's capabilities.

A medium to large sized VPN network has thousands of PE and CE routers. Divide the PE routers into a small number of categories based on their types, and impairment-test a few PE routers under each category. This can help you plan the VPN service roll-out.

The rate-limit testing is an important aspect of service provisioning. This testing helps to ascertain that the SLA agreements are met and network bandwidth is utilized properly.

Finally, impairment testing can also help in planning service restoration during severe network conditions.

Troubleshooting Tips

Issue	Troubleshooting Solution
Impairment profiles are enabled but impairment statistics are not updated.	Ensure that the **Apply Impairments** icon does not have any exclamation mark. Ensure that 100% drop is not configured for all impairment profiles.
No traffic is flowing through the impairment links.	To check that the traffic is flowing through the impairment module, disable all the impairment profiles except the default profile, which cannot be disabled. Apply Impairments and ensure that Rx/Tx Frames statistics for the impairment link corresponds to the traffic. Also make sure that both the links for the impairment port pair are forwarding, which means that the check-boxes for **Interrupt Forwarding** are unchecked in the **Links** tab. Look for impairment profile configuration error. Ensure that the impairments are applied with in the configuration limits. You can look into ImpairNet module specifications for the configuration limits. Ensure that the classifier value, mask and offset are set correctly. Also see that a profile with more generic classifier does not have a lower priority than that of the desired impairment profile. Ensure that the **Enabled** checkbox is ticked for the configured impairments.

Conclusions

This test verified that the DUT can perform in a layer 2 VPN - MPLS network with impairments. However, scalability and performance are of paramount importance when testing a DUT, which is acting as a PE router. Follow the **Test Variables** section above to test the PE at its maximum capability before deploying into a real-world L2 VPN – MPLS Network

Introduction to MPLS OAM

Operation, Administration and Management (OAM) is an essential part of any service-carrying network – from the old days of TDM network to the current days of global Internet. It is meant to provide failure detection and diagnostics for potential connectivity issues such as congestion, routing loops, bad addresses, black holes, and possible misbehaved nodes. An effective OAM not only means a better network reliability, but also it means potential savings of big money in terms of Opex.

In the context of MPLS, MPLS OAM is a set of tools that provides error detection for an MPLS data forwarding path (either LSP or PW). A data forwarding path could be completely broken but the control plane (LDP, RSVP-TE, or BGP) can work correctly. It is because that the control plane messages (for example LDP Hello and RSVP-TE SRefresh) are not going through the same path as the data plane packets (label forward).They are typically forwarded based on destination IP address which is controlled by an IGP protocol such as OSPF.

The following are the top reasons why a data forwarding path in an MPLS network can be broken:

- Intermittent wrong label value because of a faulty hardware
- Label/Port mismatch in a node due to software bugs
- Mismerge of multiple ingress routers towards the same egress due to human mis-configuration
- Accidental disable of MPLS functions in one or more nodes due to user error

To detect data plane forwarding path failure, a new approach can be taken. Send the control plane packets in-band – using the exact MPLS labels as used by the data plane packets. If MPLS OAM own messages are not responded to by the far end, it can be understood that there is a broken link in the data forwarding path.

The ‘black hole’ in the network can be determined, when an MPLS OAM toolset determines that MPLS OAM messages are lost or negatively responded to. The ability to simulate black holes in an MPLS network is an important requirement for test tools, since network operators use fall-out strategies such as Fast ReRoute (FRR) to protect revenue generating traffic when black holes are detected in a live network. These fall-out strategies must be thoroughly tested in the lab to ensure that it is working before putting it in service.

LSP Ping/Traceroute (MPLS Echo Request/Reply)

One of the key building blocks of MPLS OAM for data forwarding failure detection is the LSP Ping and Traceroute (MPLS Echo Request and Reply). LSP Ping/Traceroute operates in similar way as of IP Ping and Traceroute but with distinctive differences. the following is a brief description about how IP Ping/Traceroute works.

IP Ping relies on ICMP Echo Request or Reply messages to achieve connectivity verification. The optional field in an ICMP message carries Echo Request departure timestamp and Echo Reply arrival timestamp. The Round Trip Time (RTT) can be calculated for each request or reply pair, and an average, minimum and maximum can be computed based on many samples.

IP Traceroute extended the IP Ping by encapsulating the ICMP Echo Request inside IP/UDP payload with a predefined UDP port number (33434). This is done to have extra IP header so that the TTL field is open for write. The IP header TTL field for the traceroute message (or IP/UDP encapsulated ICMP echo request) is gradually incremented for each successive request sent by the source host. All the intermediate nodes between source host and destination hosts will perform two actions:

1) Decrease the TTL by one (or some other values) and if it is <= zero, send back to the source host an ICMP message with message type = TTL Expiry (11)

2) Else, continue the encapsulated ICMP Echo request to its next hop to the final destination.

Given a max hop count of x, the source host will send x number of IP/UDP encapsulated ICMP Echo request with TTL=1, 2, … x. Based on received ICMP message with TTL Expiry, the source host will have a complete picture of all the intermediate nodes from the source host to the destination host.

The LSP Ping/Traceroute or the MPLS Echo Request/Reply works in a similar way but with a few differences.

The diagram below explains how LSP Ping works.

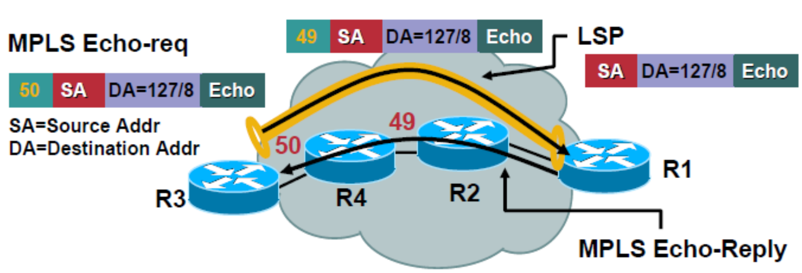


Figure 180. How a LSP Ping (MPLS Echo) Works

Step 1: The source router (R3) establish an MPLS LSP between R3 and R1

Step 2: The source router (R3) constructs an LSP Ping (or MPLS Echo-Req) message and then encapsulate the message using the LSP label. Send the MPLS Echo Request in-band so that it can flow on the exact path as the data packets.

Step 3: All the intermediate nodes (R4 and R2) will perform label swap on the MPLS Echo Request as if it is real data.

Step 4: When the destination router (R1) receives the label encapsulated MPLS Echo-Request, it pops out the label and processes it further. Echo Requests must be replied with an Echo-Reply. The Echo-Reply can be in plain IP/UDP, or IP/UDP plus Router Alert bits in the IP header, with or without MPLS label for the reversing path. The reply mode is configurable and carried in the Echo-Request, set by the source router. The source node can demand the destination node to perform FEC verification, and in such a case, the verification result is returned to the source.

Step 5: When the source router finds a positive Echo-Reply, it understands that the LSP forwarding plan is error free – The nodes (R3, R4, R2, and R1) are not malfunctioning.

The following paragraphs explain the key difference between an MPLS Echo Request and an ICMP Echo Request.

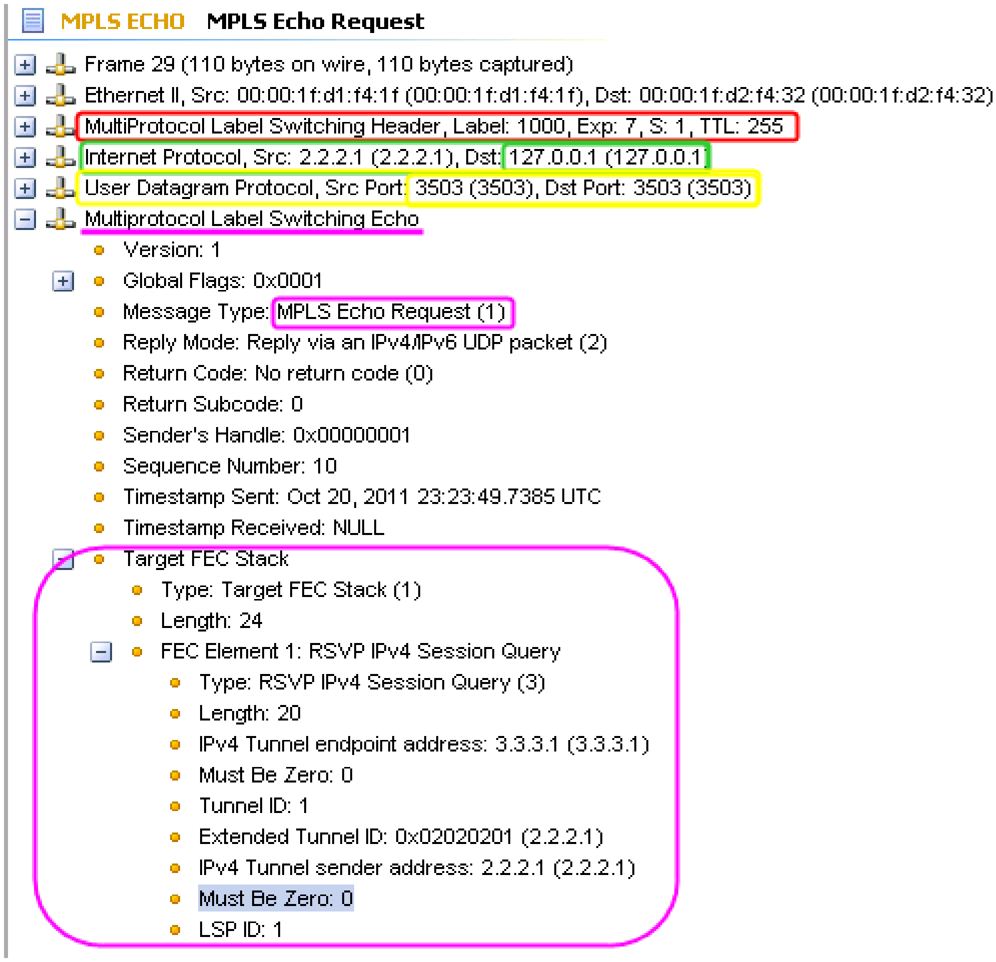


Figure 181. How a LSP Ping Differs from an IP Ping

The above figure shows the decode of an MPLS Echo Request. It has the following distinctive properties that distinguish it from ICMP Echo.

1. It carries the same LSP label as the regular data packets - indicating that it is an in-band MPLS Echo Request.

2. The destination IP address 127/8 is quite unique. From the RFC 1122, it says that 127/8, it is an 'Internal host loopback address' and it must not appear outside a host. This is a precautionary measure: If LSP in question gets broken, chances of an ICMP Echo Request being delivered to a user of an MPLS service is minimized. Any node that spots the packet, intended or not, will consume it internally without forwarding. The broken node is guaranteed to receive the LSP Ping request and returns a negative match since it is not the correct egress node of the LSP under test. The source node will immediately know which node is broken based on negative reply by the broken node. It has a two way advantage: it detects whether a destination node can be pinged, if not, the exact place from where it is broken.

3. UDP port number 3503 is reserved for MPLS Echo and further message type identifies if it is a request or a reply. The reply mode is also specified at the source. Sequence number of timestamps works in a similar way as ICMP Request.

4. The MPLS Echo Request carries a 'Target FEC Stack' which is different from a regular ICMP Echo Request. The 'Target FEC Stack' specifies the nature of the LSP under test so that the destination node can perform independent verification whether or not it is the egress node of the said LSP. The MPLS Echo Request does not remain just a connectivity tool but also a LSP verification tool. The latter is not a feature of the ICMP Echo Request. It is the verification part of the MPLS Echo Request that makes it extremely effective tool for trouble shooting, in the occasion that an LSP is broken. This makes the LSP Ping is complex and it gets more difficult to scale it to hundreds or even thousands of LSP and PW (as explained later).

LSP BFD

You are now aware of MPLS Echo Request and fathomed its power in detecting LSP failures, the relative complexity and hence limit of scale. The following explains a better way to detect and monitor many LSPs in an MPLS network. BFD is used exclusively for failure detection by all known protocols, and it is similar in case of LSP.

BFD control packets ride over known UDP port (3784). It's also carried in-band using the same MPLS labels as the actual data packets. The packet decode is shown below.

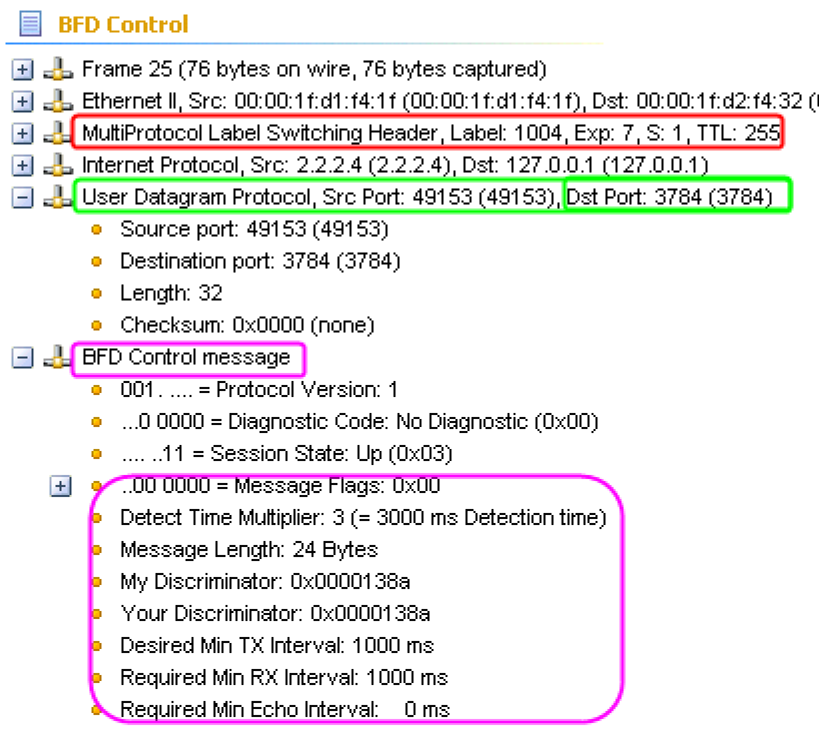


Figure 182. LSP BFD Packet Encoding

One of the key advantages of using BFD over LSP Ping is that that BFD is light weight and most vendors have it in the BFD messages in their hardware therefore it is extremely scalable. Furthermore, BFD offers different Continuity Check Interval (CCI); offering the user flexible options to run BFD control packets: faster for high paying services (LSPs or PWs) and slower for less important services. You need not issue any command to activate BFD sessions, since they start as soon as the LSPs are up.

BFD is a lightweight tool and does not act as a verification tool. In an actual network, BFD runs in parallel with the LSP Ping/Traceroute. BFD runs in an auto mode while LSP Ping/Traceroute runs on-demand or periodically, on selected LSP or PW.

PW VCCV Ping VCCV BFD

L2VPN Peduowire (PW) is a popular way to transport difference services (legacy and new) over the MPLS infrastructure. A PW works like TDM circuit and is popular among traditional transport community. An area where PW is widely adopted is mobile backhaul transport. The OAM associated PW, as defined in 'Pseudowire Virtual Circuit Connectivity Verification (VCCV) – RFC 5085', is an integral part of the overall L2VPN service. Essentially, we need to extend the "LSP Ping" capability for an MPLS LSP to a L2VPN PW – it is termed as VCCV Ping. We do not need the 'LSP traceroute' for the PW because, by definition, a PW is a point to point connection and therefore the other end is only one hop away. All the intermediate nodes (P router) in an L2PVN network are transparent to the PW service; they are strictly between two PE routers. Similar to LSP Ping, the VCCV Ping can be issued on-demand or periodically., It must, like the LSP Ping, include the PW verification part to work reliably. The verification aspect of VCCV Ping does not make it scalable to large number of PWs; therefore, BFD is needed as an add on – therefore came the VCCV BFD. BFD is light weight, and typically sits in the hardware making it extremely scalable. In a typically L2VPN network where there are thousands s of PW or VPLS being deployed, a combination of VCCV Ping and VCCV BFD is usually deployed.

The fact that there are thousands or even more PWs riding over a single LSP, and both user data and OAM messages flows on the same path (they share the same LSP and PW labels), the question remains as to how you can separate a control plane message (OAM) from up to line rate of user data. There has to be a mechanism so that when an MPLS OAM message arrives at a far end PE router, it can be delineated from the wire from a pile of actual user data, and deliver to the CPU for processing and responding.

The following points discuss the three ways (called Control Channel, or CC, options)

1. Use in-band method with ACH encoding with ChannelType = IP. MPLS Echo Request will then be IP/UDP encoded like a standard LSP Ping, following the ACH header;
2. Use an out-of-band way called Router Alert Label (RAL, value=1) which is inserted in the middle of a total three label stack (LSP Label, RAL, PW Label);
3. PW Label carries TTL=1 to force expiry.

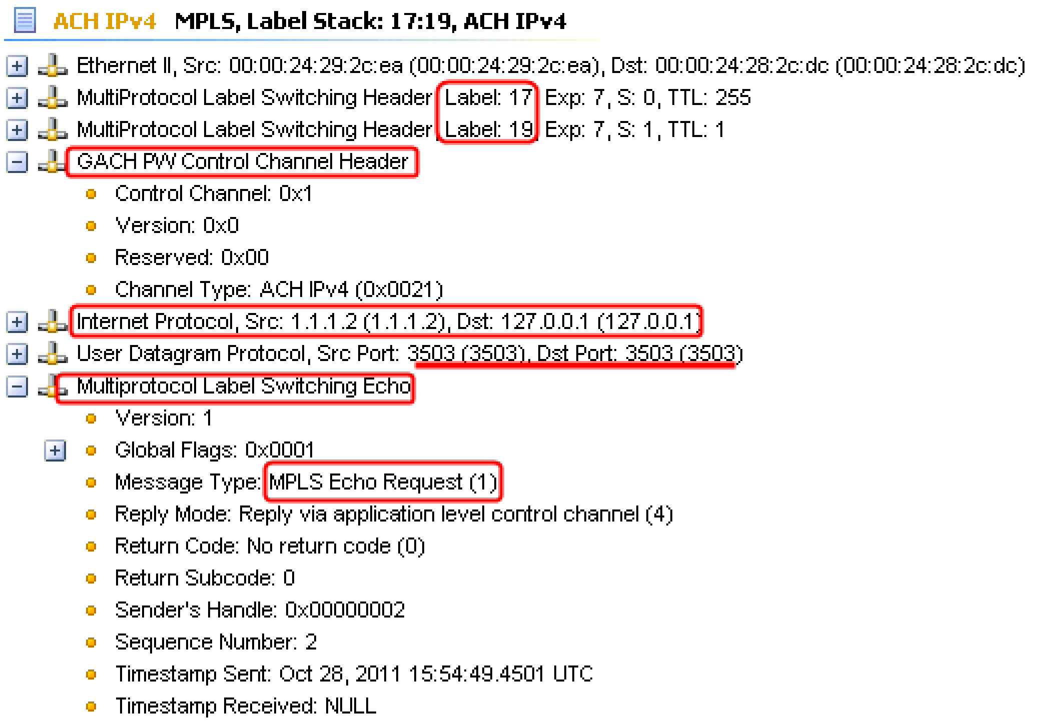


Figure 183. VCCV Ping using In-Band ACH Encoding

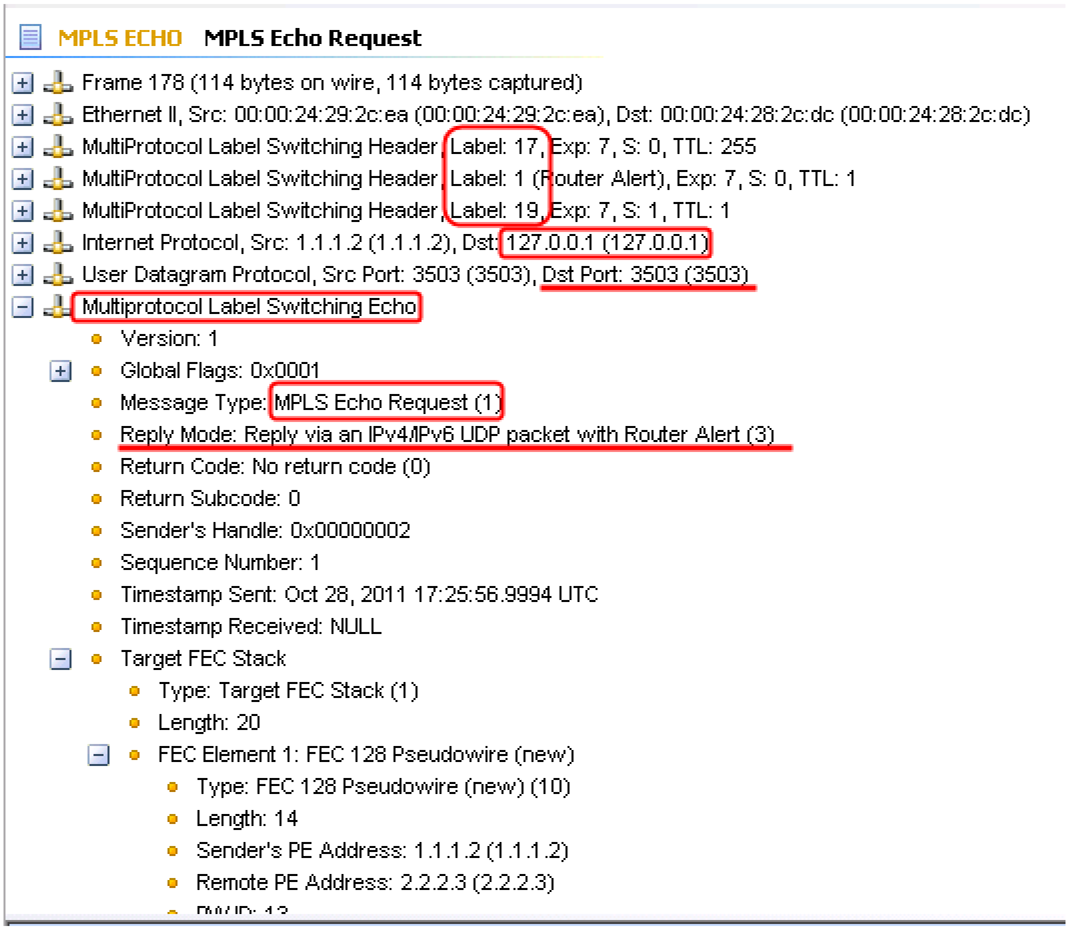


Figure 184. VCCV Ping using Out-of-Band RAL

To add to more flexibility to the Echo Request/Reply, the standard allows both ICMP Echo Request and the MPLS Echo Request to be supported (called Connectivity Verification, or CV options). Availability of various options raises a question as to how you can ensure that two devices can talk immediately without much of user configuration. Can this be automated?

Fortunately, for some protocols like LDP, it has the ability to negotiate CC/CV options in the beginning, during the PW establishment phase. A sub interface TLV can be specified in the LDP Label Mapping Message, which clearly indicates the preferred CC and CV types.

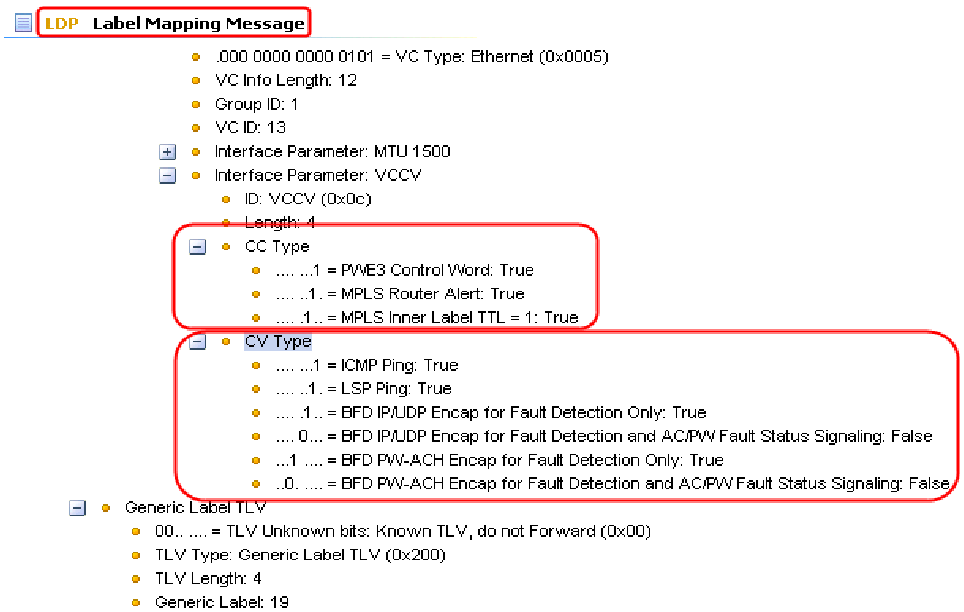


Figure 185. LDP Signaling for CC/CV Capability

Protocol like LDP has defined procedures on how to negotiate the CC/CV capability during PW establishment; other protocol such as BGP does not have this. In such cases, operators have to reply on manual configuration of CC/CV mode. It is important for test tools to support both the auto negotiation and the manual configuration.

In VCCV BFD, the encoding and operation is straightforward. BFD has its own ACH ChannelType (value=07), it is therefore easy to support either in-band or out-of-band (via RAL) for VCCV BFD to operate.

To summarize, MPLS OAM encompasses many different flavors for both MPLS LSP and MPLS PW services. They are an integral part of a healthy MPLS network. Network operators need all the flexibility to troubleshoot and proactively maintain an MPLS network.

Relevant Standards

- RFC 4379 – Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 5884 – Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)
- RFC 5085 – Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Psedowires
- RFC 5885 – Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

Test Case: Troubleshoot LDP or RSVP-TE LSPs with LSP Ping/Traceroute, and LSP BFD

Overview

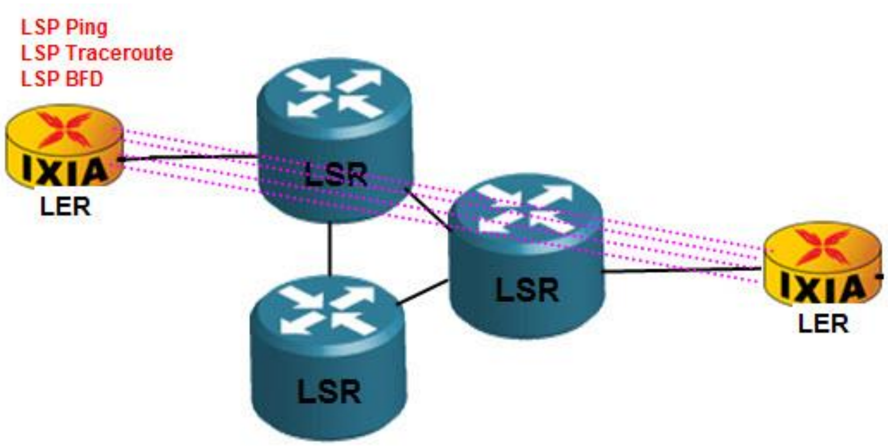
LDP and RSVP-TE are two MPLS signaling protocols that they are the basic building blocks of an MPLS network. There is usually a large number of LSPs in an MPLS network. To troubleshoot LDP or RSVP-TE, created LDP requires both on-demand LSP Ping and the automatic LSP BFD running in the background to monitor each LSP's liveliness and their long term health.

Objective

The objective of this test is to create some (10 for example) LDP (or RSVP-TE) LSPs , and run the LSP Ping on selective LSP and observe whether LSP Ping responds per the reply mode settings. Repeat the same for LSP Traceroute. Finally, enable the LSP BFD auto sessions on all configured LSP and ensure BFD sessions are running. Capture packet for detail analysis.

Setup

The test consists of two Ixia test ports. Any number of DUT can be connected in between the two test ports and the procedure for conducting the test as detailed in the test steps are the same and are not likely to change, regardless of the number of P routers. Both Ixia ports will be Label Edge Routers (LER) while DUT or DUTs, if any, will be acting as the Label Switch Router (LSR). If there are LSRs in the test setup, LSP traceroute works better, since they create multiple hops for the selected LSP of interest.



Step-by-step Instructions

The operation of LSP Ping/Traceroute and LSP BFD over LDP created LSP is similar to the LSP created by RSVP-TE, the procedure below use LDP as an example. RSVP-TE LSPs needs to use the RSVP-TE wizard.

Follow the step-by-step instructions to create 10 LDP LSPs and issue LSP Ping and Traceroute on selected LSPs to observe response. Capture control packets to ensure correct encoding of packets. Enable LSP BFD on all LSPs to observe the statistics of the BFD session.

1. Reserve two ports in IxNetwork.

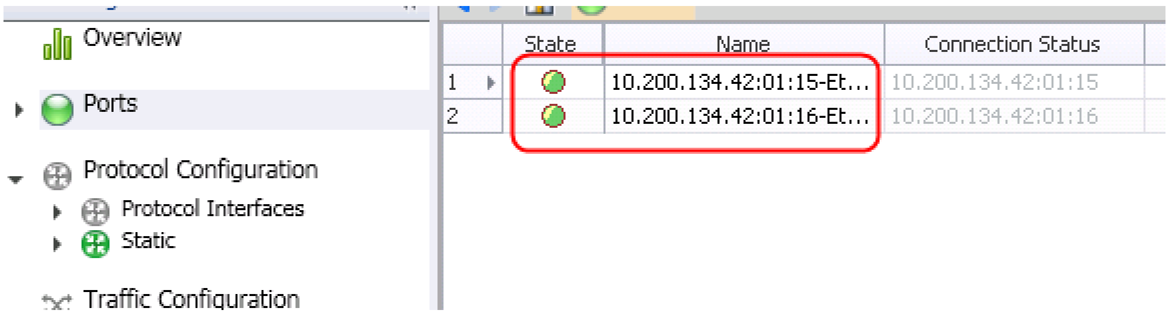


Figure 186. Port Reservation

2. Click **Add Protocols** button on the ribbon area of the IxNetwork application and then select **LDP** wizard.

3. Double click to open the wizard.

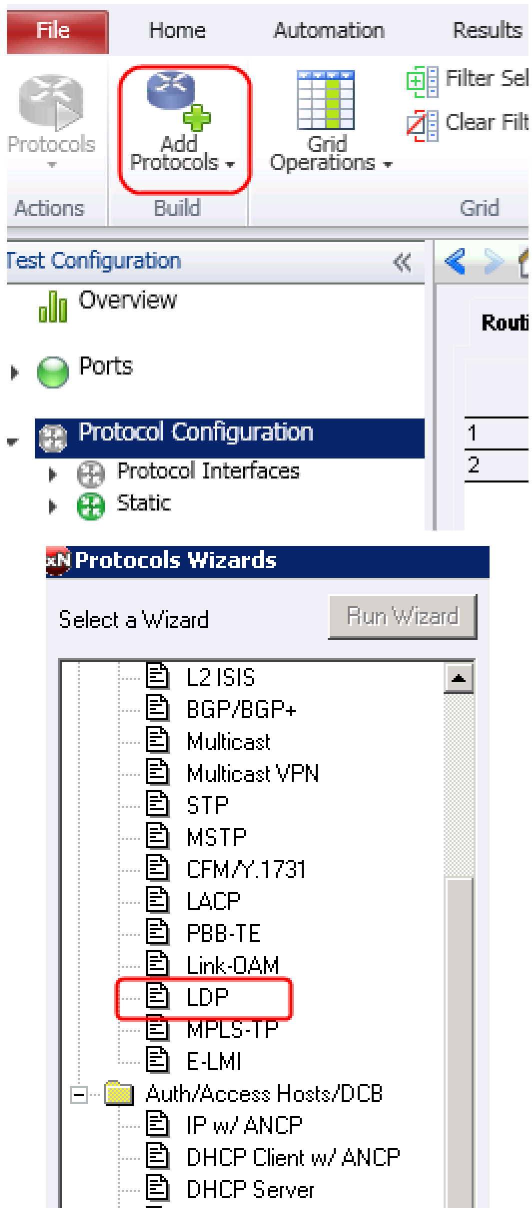


Figure 187. Launch Protocol Wizard and Open LDP Config Wizard

4. Select the port to run the LDP protocol.

   Note: The LDP wizard is designed for both P2P and P2MP tunnels. P2MP parameters are ignored since P2P LSP is tested.

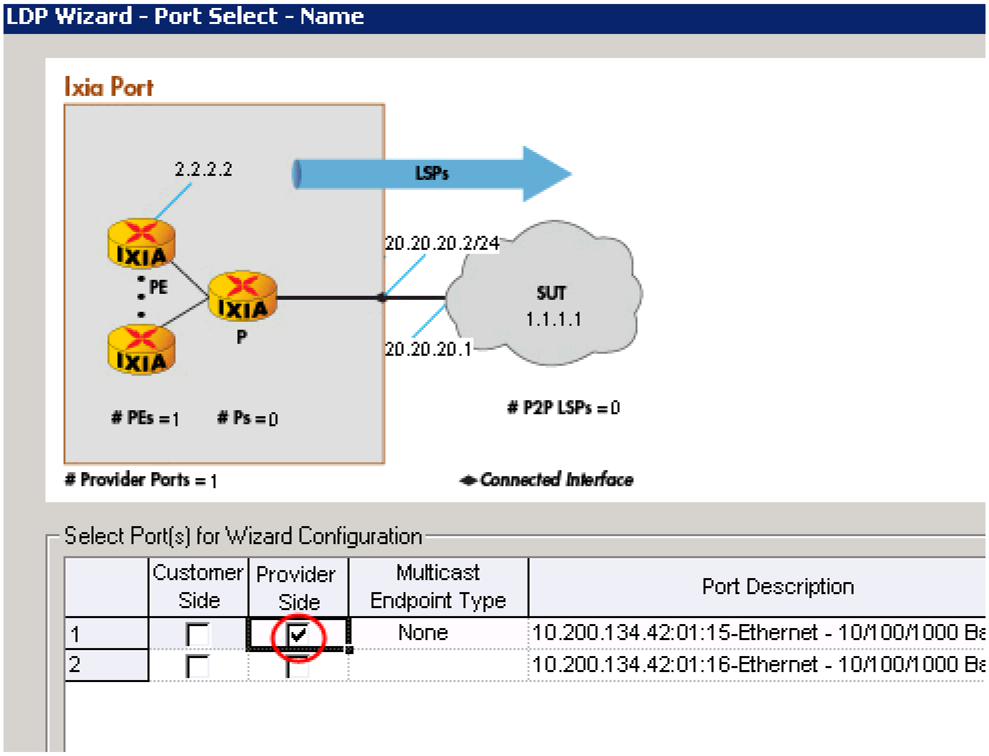


Figure 188. Select the First port to Join LDP Emulation

5. In next page, enable the P router and keep the default parameters for number of P, IGP and IP addresses. Go to the MPLS OAM section to enable both LSP Ping and Reply to LSP Ping option. Leave the LSP BFD out . LSP BFD can be enabled later by manually.

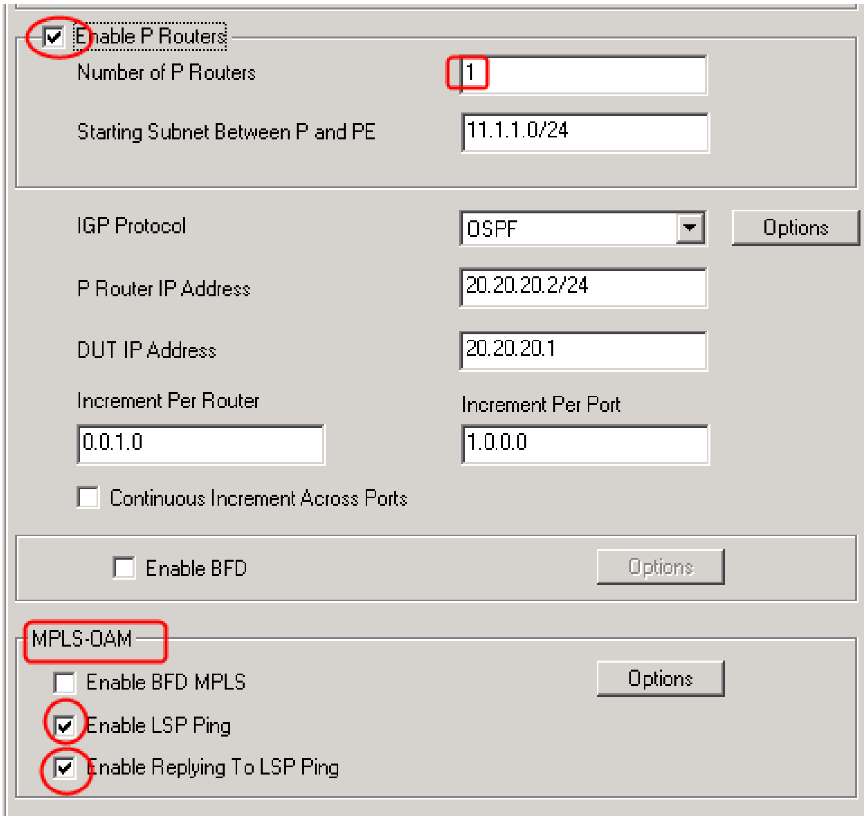


Figure 189. The Second Page of the LDP Wizard

6. The next page in the LDP wizard configures the number of FECs or LSPs to be established by the LDP protocol, and the label start.

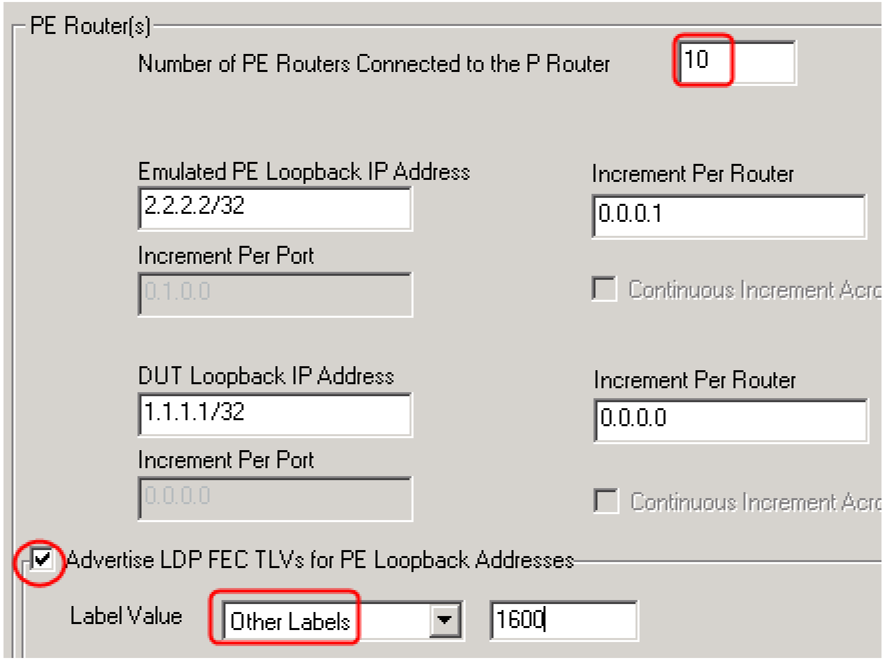


Figure 190. The Third Page of the LDP Config Wizard

7. In the last page of the wizard, provide a name to the configuration and select the save to overwrite existing configuration option.

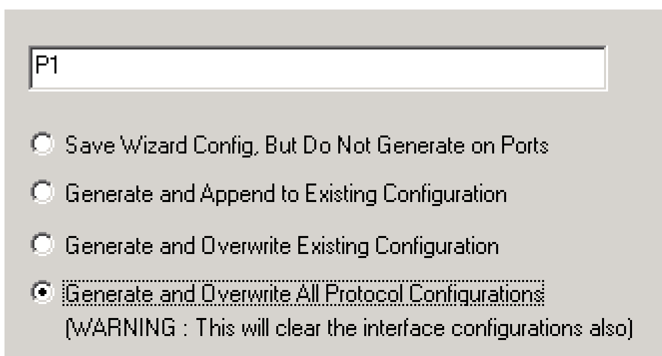


Figure 191. The Last Page of the LDP Wizard

8. Configure the second port to run the LDP protocol in a similar way**.** The configuration steps for the first port, except the P router address and DUT address that is reversed, keep the other configuration the same. Optionally, you can configure a different LDP start label value.

    Note: If you are not using Ixia back-to-back ports, then simply rerun the wizard for ports 2 through *n*, following the steps above with appropriate address.

    It is also possible to run this wizard only once for all ports by selecting all of them as shown in Step3.

9. Click the **Protocols** icon to start to run all protocols including LDP, OSPF, and MPLS OAM.
    Note: By default OSPF uses Broadcast interface type. You can change both ports to Point-to-Point type to make the icon green.

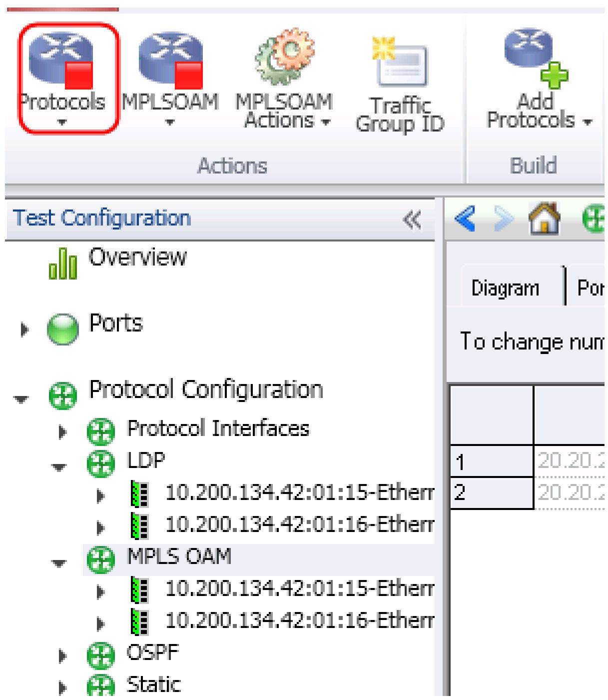
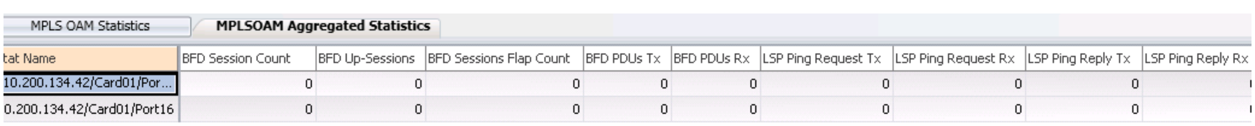


Figure 192. Run All Configured Protocols

10. The LDP stats show that a basic session is running. The MPLS OAM statistics however will show no record. This is because the BFD auto session is not enabled, and periodic LSP Ping is not enabled. No OAM messages are therefore going on the LSPs.



tat Name	BFD Session Count	BFD Up-Sessions	BFD Sessions Flap Count	BFD PDUs Tx	BFD PDUs Rx	LSP Ping Request Tx	LSP Ping Request Rx	LSP Ping Reply Tx	LSP Ping Reply Rx
10.200.134.42/Card01/Por...	0	0	0	0	0	0	0	0	
0.200.134.42/Card01/Port16	0	0	0	0	0	0	0	0	

Figure 193. MPLS OAM Initial Stats

11. Go to the MPLS OAM **Learned Information** and click on the **Refresh** button in the ribbon. The learned info area will display a total of 20 LSPs – 10 Ingress and 10 Egress. It also displays other information related to the LSP and the Ping related statistics for the selected LSP.

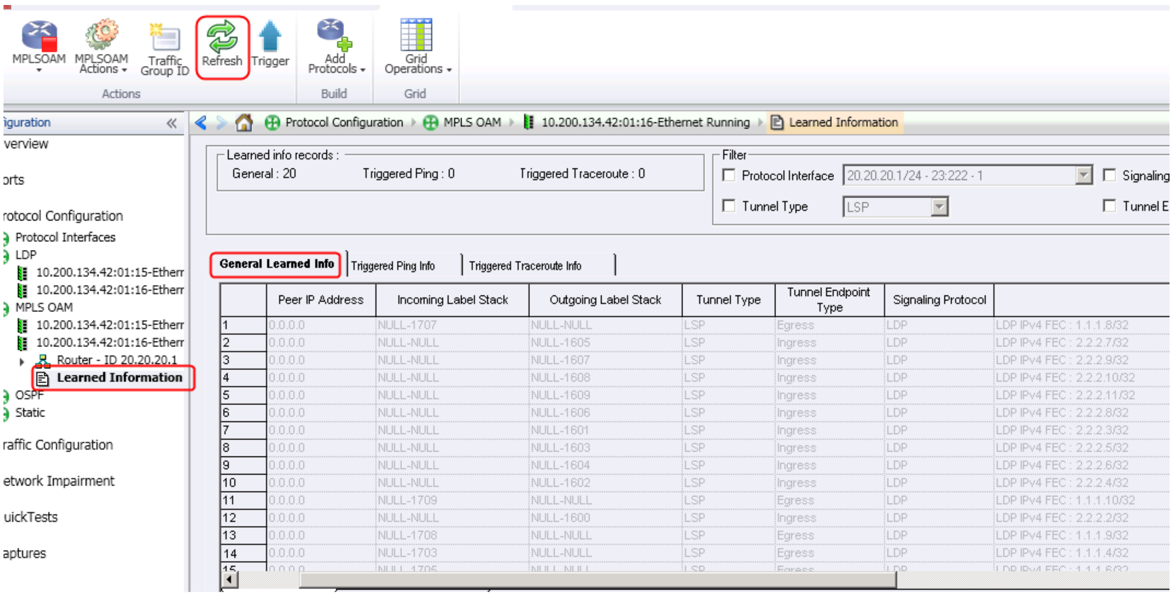


Figure 194. MPLS OAM Learned Information

12. Now follow these sub steps to issue a LSP Ping
    a. Click the row and select an Ingress LSP for injecting LSP Ping.
    b. Click the **Trigger** button.
    c. Select **Send Triggered Ping/Traceroute** tab.
    d. Select **Send Triggered Ping.**
    e. Select **Advanced Options** and select *Do not reply* as the **Reply Mode.**
    f. Click **OK** to send the triggered LSP Ping.

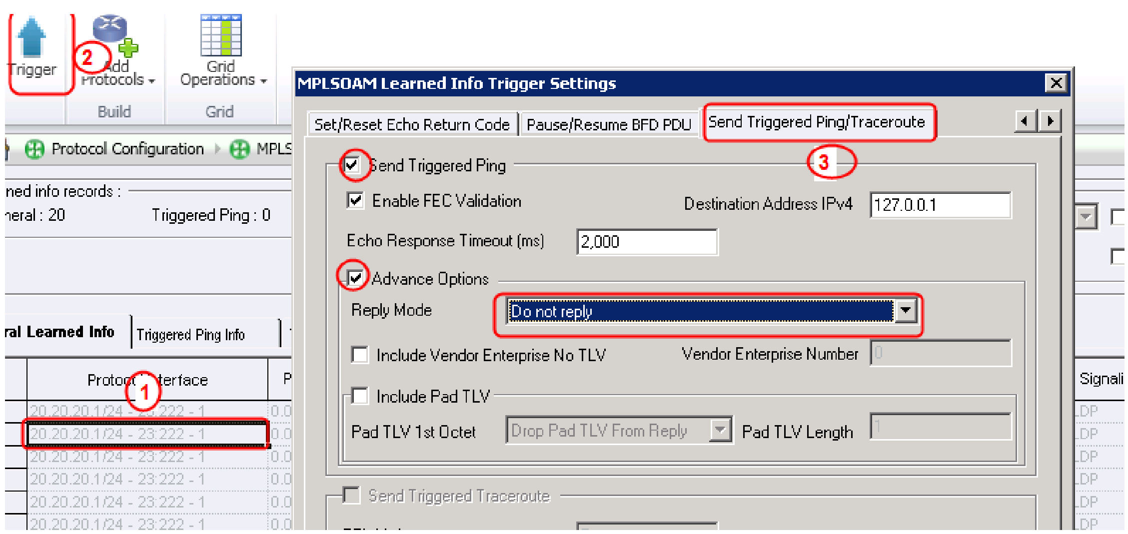


Figure 195. Steps to Issue LSP Ping

13. Click **Triggered Ping Info** to display *unreachable* as the status, and the MPLS OAM statistics shows a LSP Ping sent by the second port and received by the first port.

Figure 196. Trigger Ping Info and Corresponding MPLS OAM Stats

14. Repeat the process and change the **Reply Mode** to *Reply via an IPv4/IPv6 UDP packet*.
    Note: The **Triggered Ping** Information shows the LSP as *reachable* and the MPLS OAM stats shows 2 tx 1 reply.

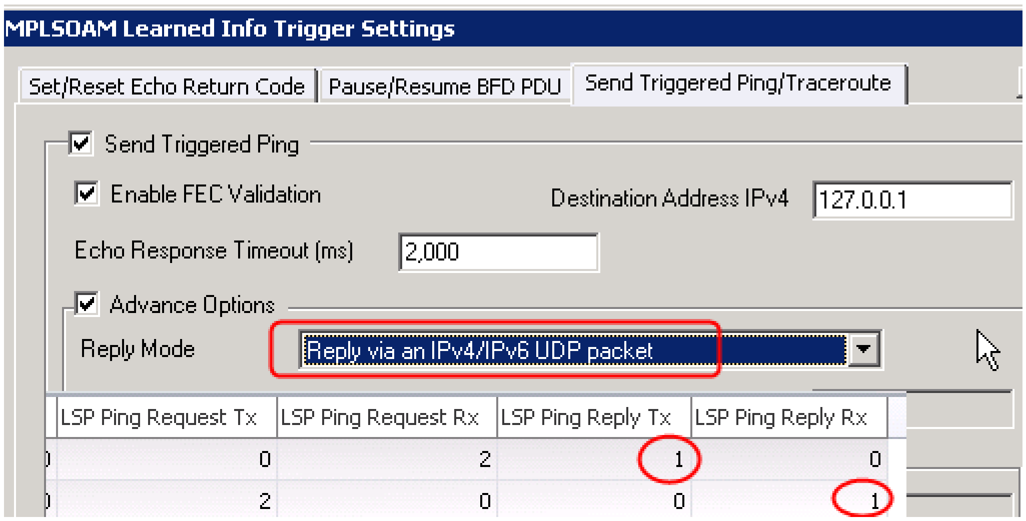


Figure 197. Set up Return Code for Negative Test

15. Select Reply Mode and see other responses. Capture the LSP Ping and LSP Ping Reply to make sure they are encapsulated correctly.
    For example, the LSP Ping should be encoded in the right LSP label, while the LSP Ping Reply is native IP with correct IP/UDP/MPLS Echo Reply encapsulation.
16. You can perform the on-demand LSP on multiple selected LSPs simultaneously and observe the response.
    Note: The Route Trip Time min/max/average are reported for the LSPs that is Pinged and has replied.
17. Enable LSP Traceroute. If there are DUTs in the setup, the number of LSP pings issued by LSP traceroute will be the number of DUTs in the setup plus one (Ixia egress).
18. Go to the MPLS OAM router level and toggle to enable the periodic Ping. Configure the right reply mode, and the interval for the periodic Ping. Disable and then enable the router and restart the protocols again.
    Note: The MPLP OAM LSP Ping Tx/Tx and the Reply Tx/Rx will increase continuously.

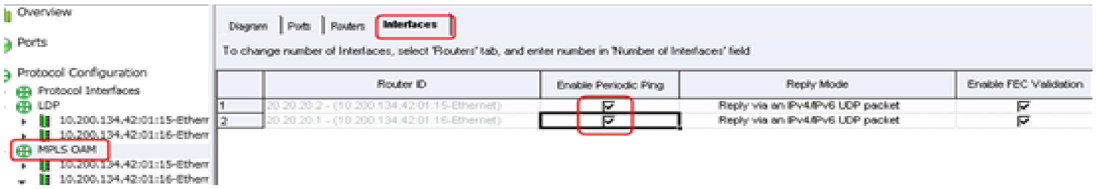


Figure 198. Enable Periodic Ping

19. The last step of the exercise is to enable the LSP auto BFD session. To do this, you need to go to the LDP protocol tree and select **Routers** tab. Toggle to check the option **Enable BFD MPLS for Learned LSPs**.

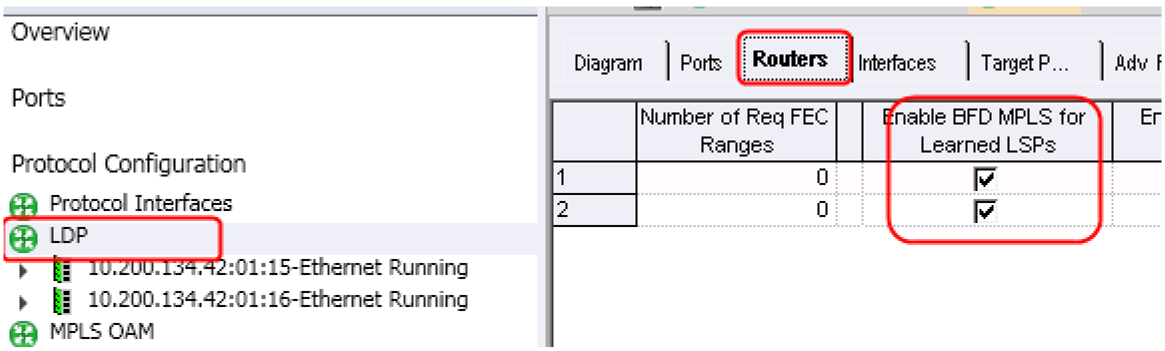


Figure 199. Manual Enabling of BFD Sessions over LSP

20. To configure BFD intervals and the other BFD specific parameter, you need to go to **MPLS OAM** -> **Interface** -> **BFD MPLS.**

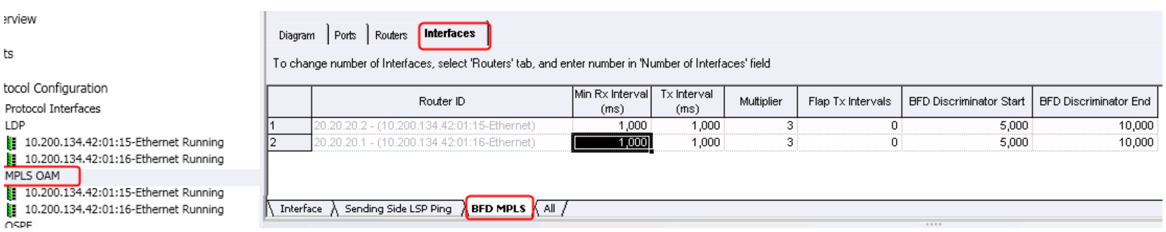


Figure 200. BFD Protocol Configuration

21. To check BFD statistics and ensure that all BFD sessions are running, you can verify the MPLS OAM statistics.

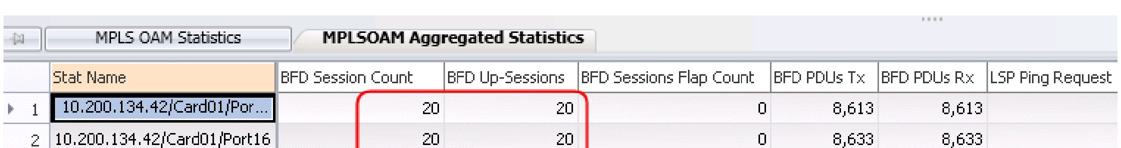


Figure 201. MPLS OAM BFD Stats

You can also verify individual LSP BFD statistics by navigating to the MPLS OAM **Learned Information** -> **General Learned Info** -> **BFD MPLS OAM Sessions.**

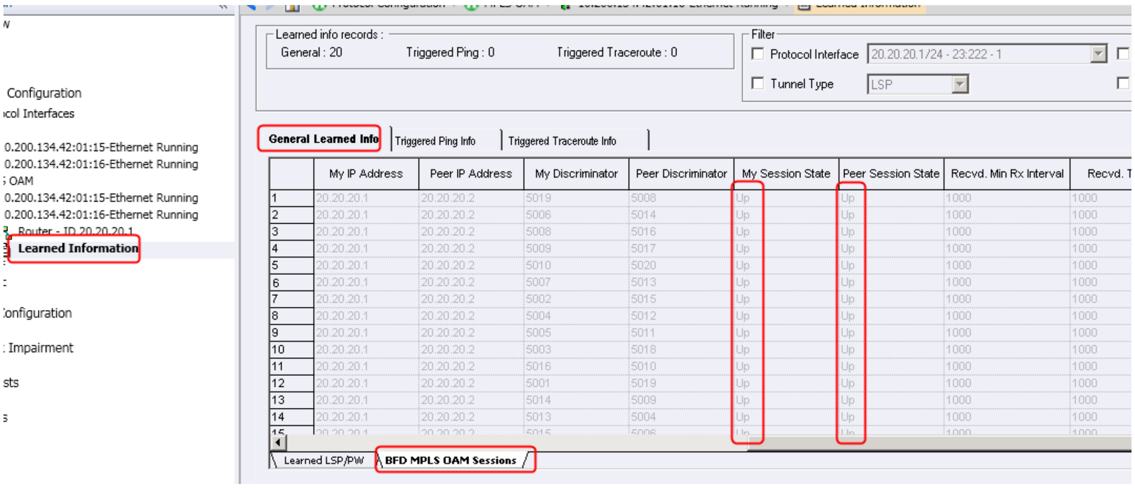


Figure 202. MPLS OAM BFD Learned Info

22. You can create black holes on selected LSPs by creating BFD disparity and data plane forwarding. Navigate to the BFD learned information display and select one or more BFD sessions. Click the **Trigger** button to inject BFD abnormality. The figure displays how to Pause tx/rx BFD PUDs. Once activated, BFD sessions become inactive instantly and the MPLS OAM statistics show BFD flapped sessions.

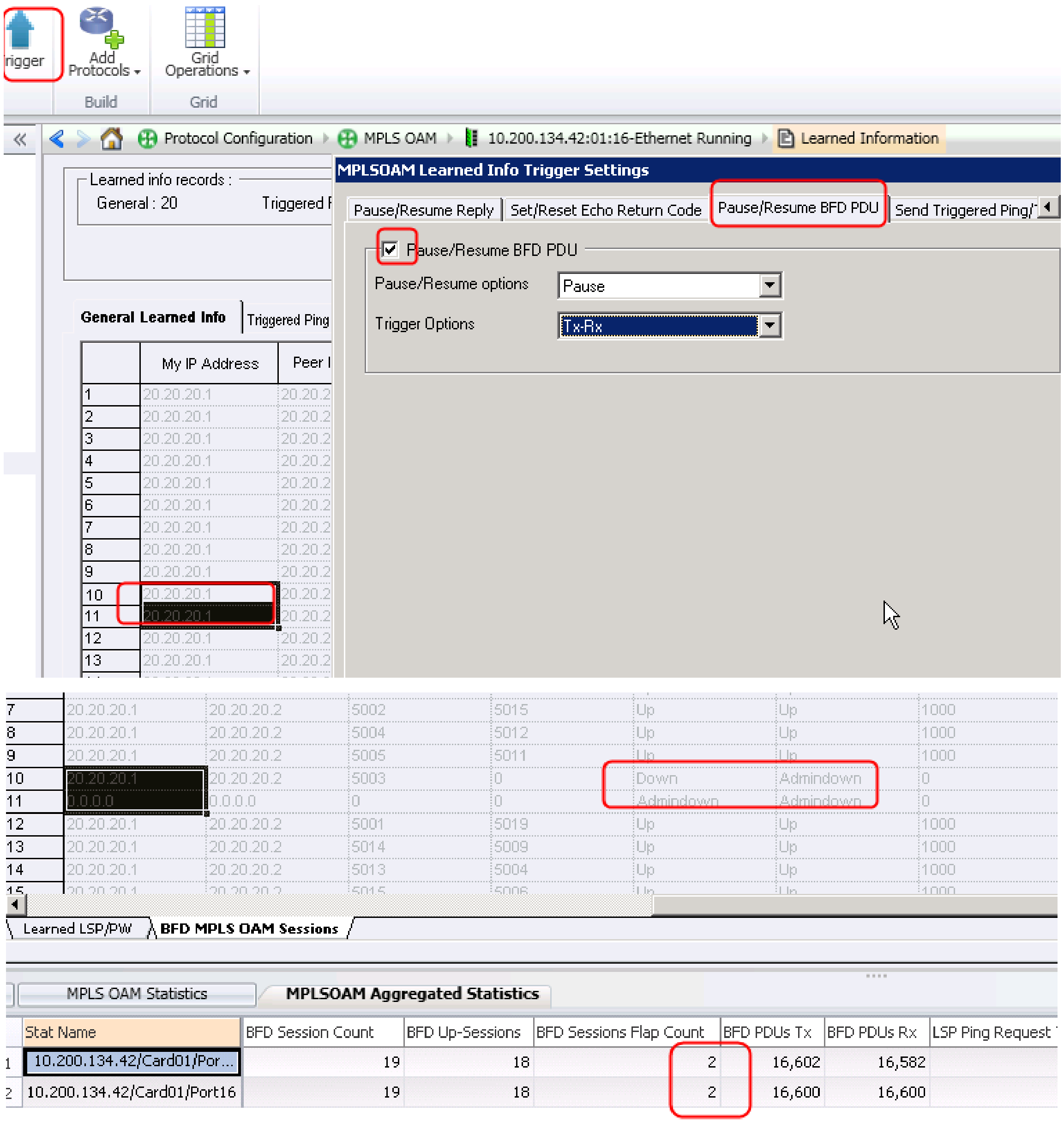


Figure 203. Inject Black Hole to Test DUT's Reaction

Test Variables

The following list of variables can be considered to be added in the test to add more weight to the overall test plan.

Performance Variable	Description
Data plane traffic	You can introduce data plane traffic to verify LSP Ping/Traceroute and LSP BFD functions. Note that that they are in-band and hence are sharing the same pipe. The more OAM overhead it consumes the less bandwidth is available for user data. It is always interesting to test if line rate traffic at smaller packet size will have negative impact on the OAM operation; especially when the auto BFD sessions are enabled.
BFD Tx/Rx Intervals	BFD interval affects the performance. Some DUTs cannot handle many sessions when BFD is running at high rate (smaller interval). It is interesting to observe how a real DUT behave with respect to BFD intervals, and the total number of LSPs running BFD.
Mix LSP BFD and Periodic LSP Ping	A mixture of periodic LSP ping and LSP BFD is more useful in an actual network. You must know that LSP Ping has the ability to force LSP verification and BFD does not. LSP Ping is therefore more stressful to the DUT. A mix mode is ideal to achieve assurance and scalability.
Long Term Soaking with LSP BFD (or/and LSP Ping)	It is important to run LSP BFD over a long period of time to observe if the MPLS forwarding engine experiences any abnormal condition. Most hardware of today works fine over a few hours but with increased temperature over time the hardware's behavior may change. In such a case BFD session flap count would be an indication of any abnormal behavior.

Conclusions

LSP Ping/Traceroute and LSP BFD offers flexible and effective trouble shooting, and network diagnostic tool to support and maintain an MPLS network. IxNetwork offers all key features with scalability.

Test Case: Maintain and Support a live BGP VPLS Network Using VCCV Ping and VCCV BFD

Overview

BGP VPLS is one of the earliest flavors of VPLS in use hence it enjoys its popularity among service providers. In a typical service provider's network, there are 4,000to 8,000 BGP VPLS instances running in parallel to deliver revenue generating traffic. The operator needs test tool to support and maintain such a large network.

Objective

The objective of this test is to use IxNetwork to create 4,000 to 8,000 BGP VPLS instances that correspond to a typical service provider's network, and use VCCV Ping and VCCV BFD to troubleshoot and detect if there are any instances in which are in a bad state. This approach can be deployed in a live network. Care must be taken when running VCCV BFD, since it may generate large number of control packets that may negatively cause performance issues.

Setup

The test consists of one or more Ixia test ports connected to a live network. All sites belonging to the same VPLS instance have any to any connectivity. If Ixia's simulated VPLS sites for all the VPLS instances can perform VCCV Ping or VCCV BFD to one or more PE routers in the network, the network then can be assumed to be working correctly. If, however, any VPLS sites does not get VCCV Ping reply or the VCCV BFD sessions go down, there is an indication that the network has errors.

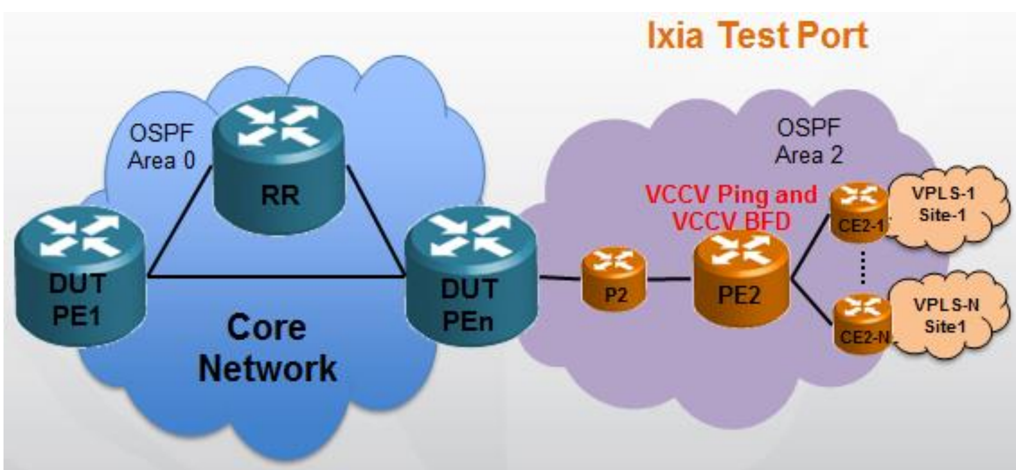


Figure 204. Test Setup

Step-by-step instructions

Follow the step-by-step instructions to create 100 BGP VPLS instances and issue on-demand VCCV Ping for reply from the Device Under Test (DUT). Capture control packets to ensure correct encoding of packets per MPLS OAM configuration. Enable periodic VCCV Ping on selected VPLS, and also enable VCCV BFD to ensure BFD sessions are maintained over the VPLS instances. Inject BFD errors to observe DUT's response to black hole conditions.

1. Reserve two ports in IxNetwork.

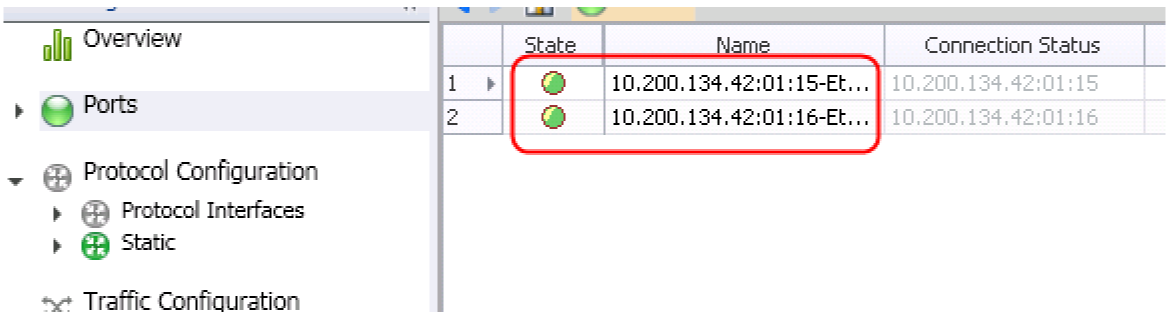


Figure 205. Port Reservation

2. Click **Add Protocols** button on the ribbon area of the IxNetwork application and then select **L2VPN/VPLS** wizard. Double click to open.

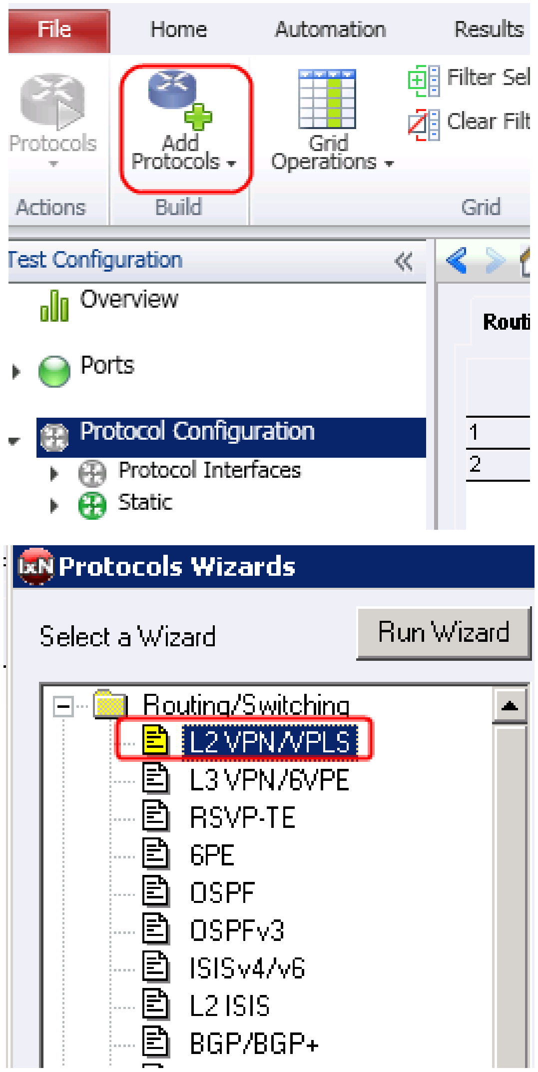


Figure 206. Launch Protocol Wizard and Open L2VPN/VPLS Config Wizard

3. Once **L2VPN wizard** is open, select the port to emulate VPLS PE and VPLS instances.

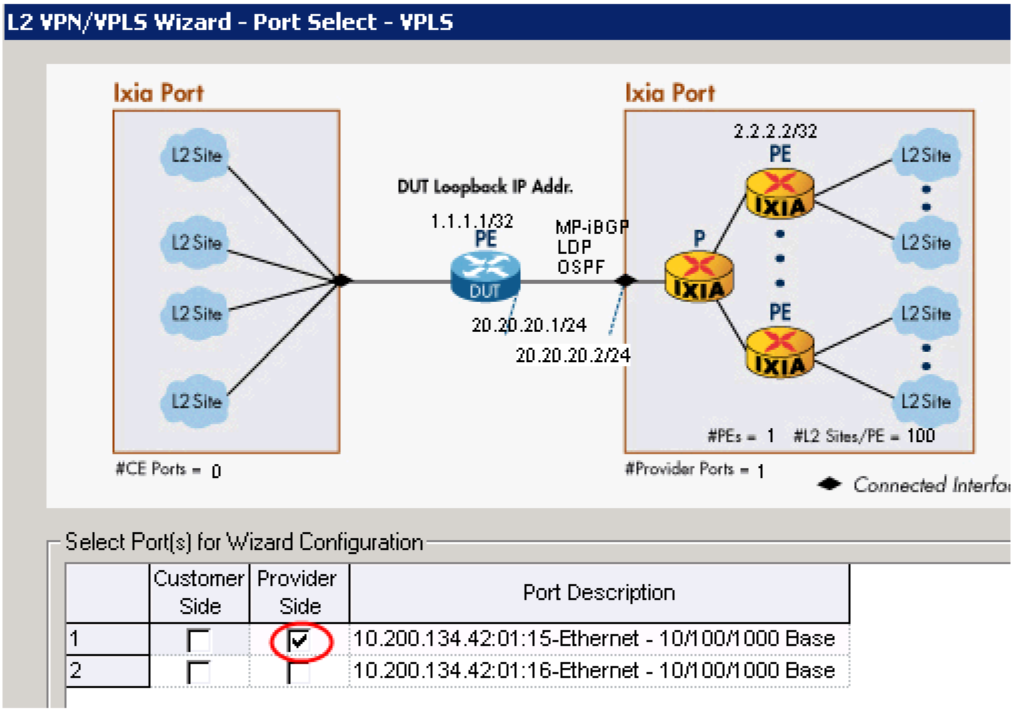


Figure 207. Select the First port to Join L2VPN/VPLS Emulation

4. In next page of the wizard, enable P router and keep the default parameters for number of P, IGP and IP addresses. Select *"MP-iBGP* as the **L2VPN Signaling Protocol**. This is known as BGP based VPLS.

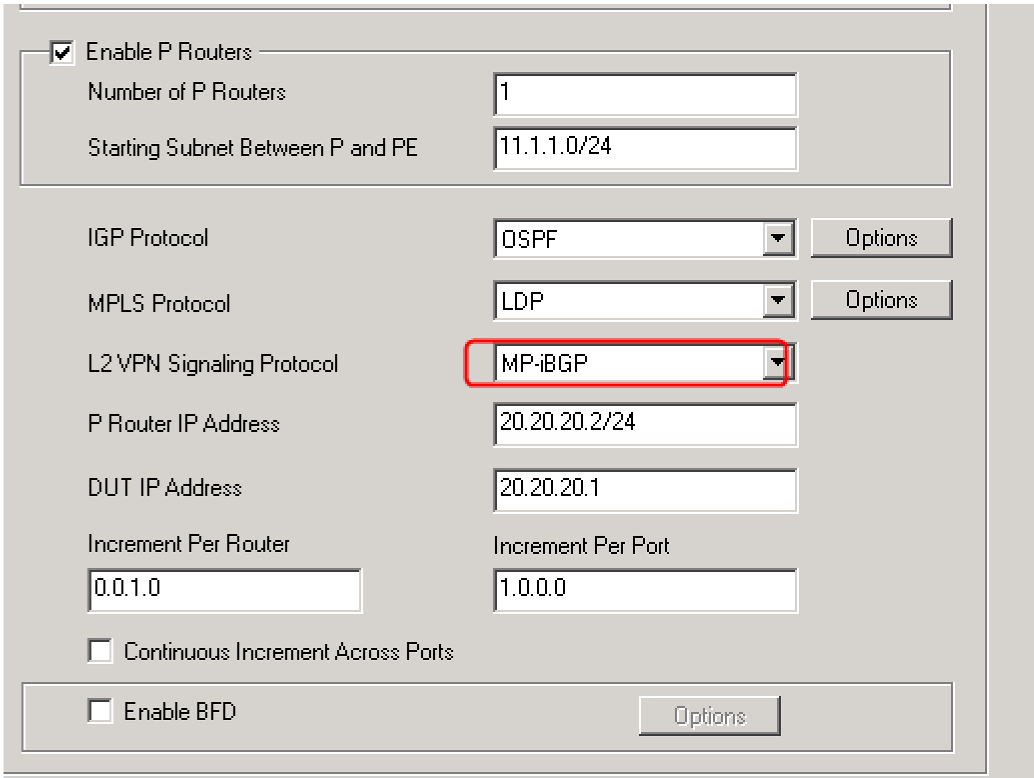


Figure 208. The Second Page of the L2VPN/VPLS Wizard

5. The next page in the L2VPN/VPLS wizard is to configure the number of PEs to emulate. The test objective being monitoring and troubleshooting VPLS instances, one emulated PE is enough to start.

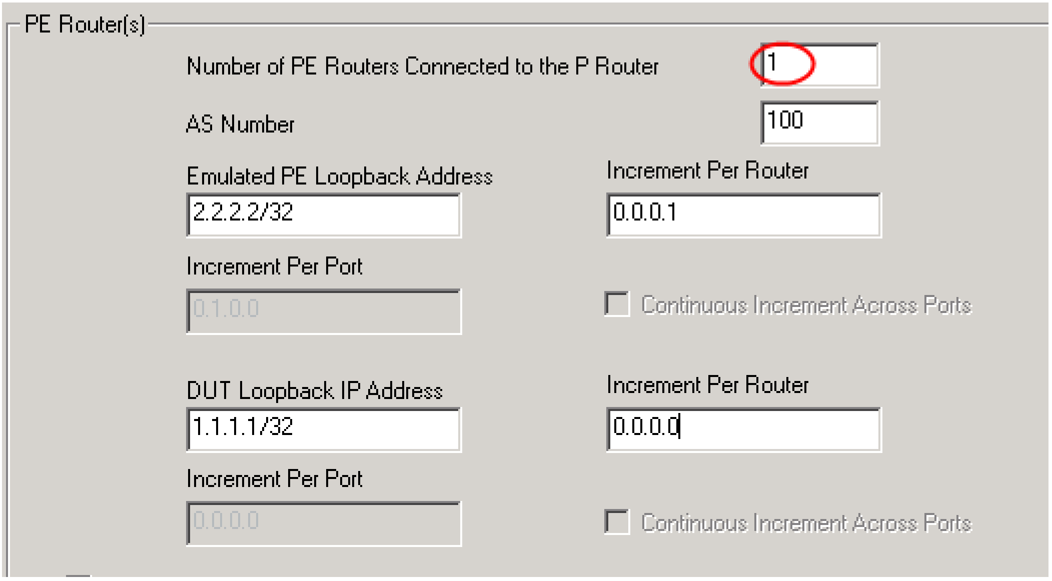


Figure 209. The Third Page of the L2VPN/VPLS Config Wizard

6. Next page of the L2VPN/VPLS wizard is the key to configure VCCV Ping and VCCV BFD. Toggle to enable both *Enable BFD VCCV* and -*Enable VCCV Ping* options. Click **Options** to configure BFD intervals, the discriminators for the BFD sessions to run over the VPLS instances. Enable the on-demand Ping and manually enable the automatic Ping. A number of VCCV parameters are disabled because we are using BGP as the L2VPN signaling protocol. As of now, BGP doesn't have procedures to negotiate CC or CV options. LDP is the one that has clearly defined procedures to advertise and negotiate CC and CV options. These options are for LDP based VPLS or PW.

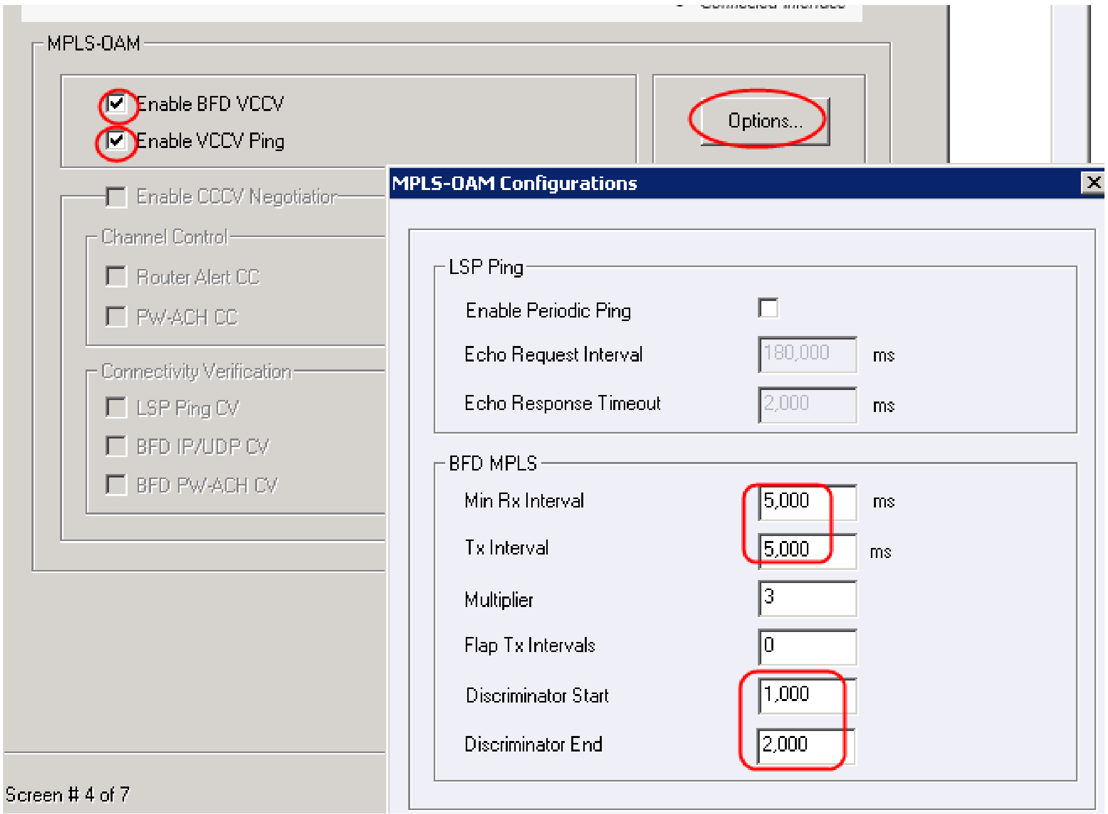


Figure 210. VCCV Ping and VCCV BFD config page

7. Next page of the L2VPN/VPLS wizard defines the number of VPLS instances, and all the parameters for the VPLS instances. Here 100 VPLS instances have been defined.
   Note: The L2 Site ID for both Ixia and DUT must match with the actual value configured in the DUT. Site ID can be the same for VPLS instances defined. The corresponding label blocks and the block offset needs to match the DUT configuration.

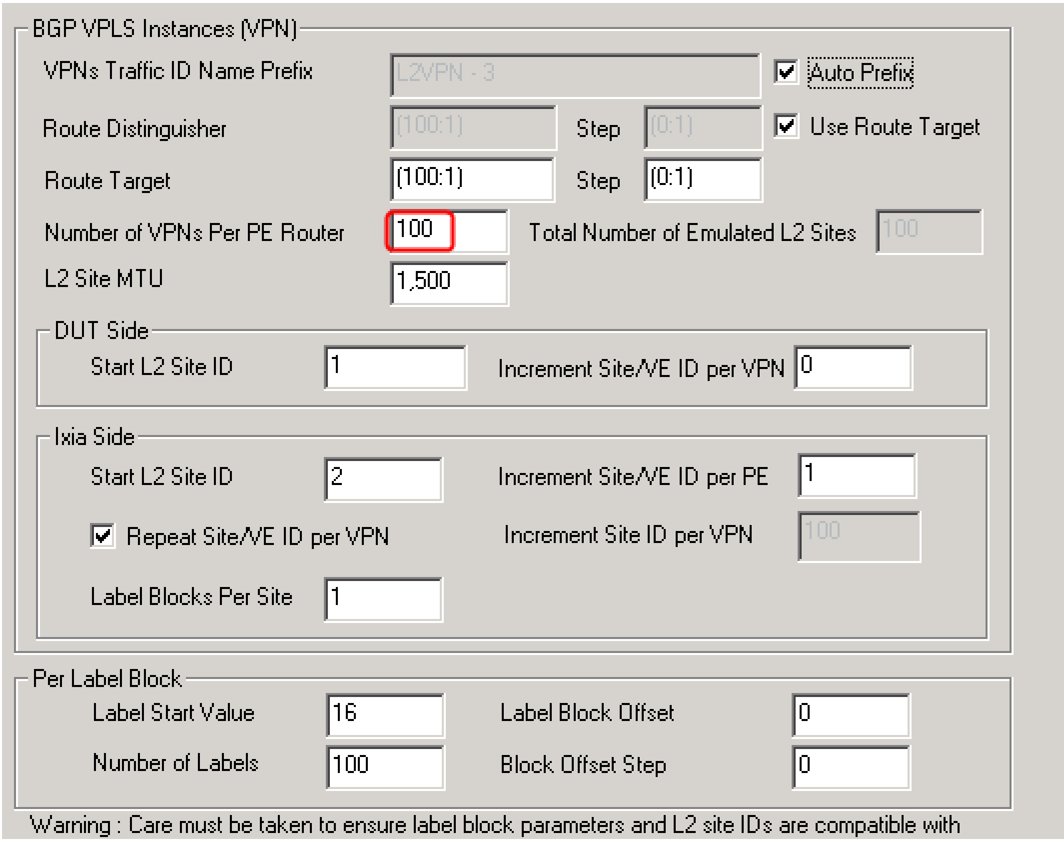


Figure 211. BGP VPLS Instance Configuration Page

8. Skip the next page of the wizard. In the last page of the wizard, name the configuration properly and generate and overwrite existing configuration.

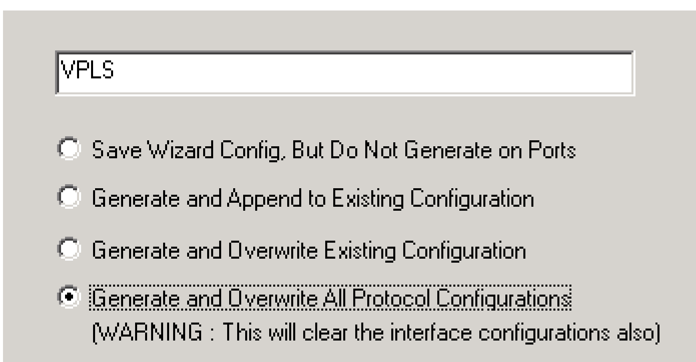


Figure 212. The Last Page of the L2VPN/VPLS Wizard

9. Click the **Protocols** icon to start to run all protocols including LDP, OSPF, and MPLS OAM. If the configuration is right, you should see a total of 100 BFD configured sessions and the running sessions. You can go to the BGP learned information for the learned VPLS instances if the BGP related configuration is configured correctly.

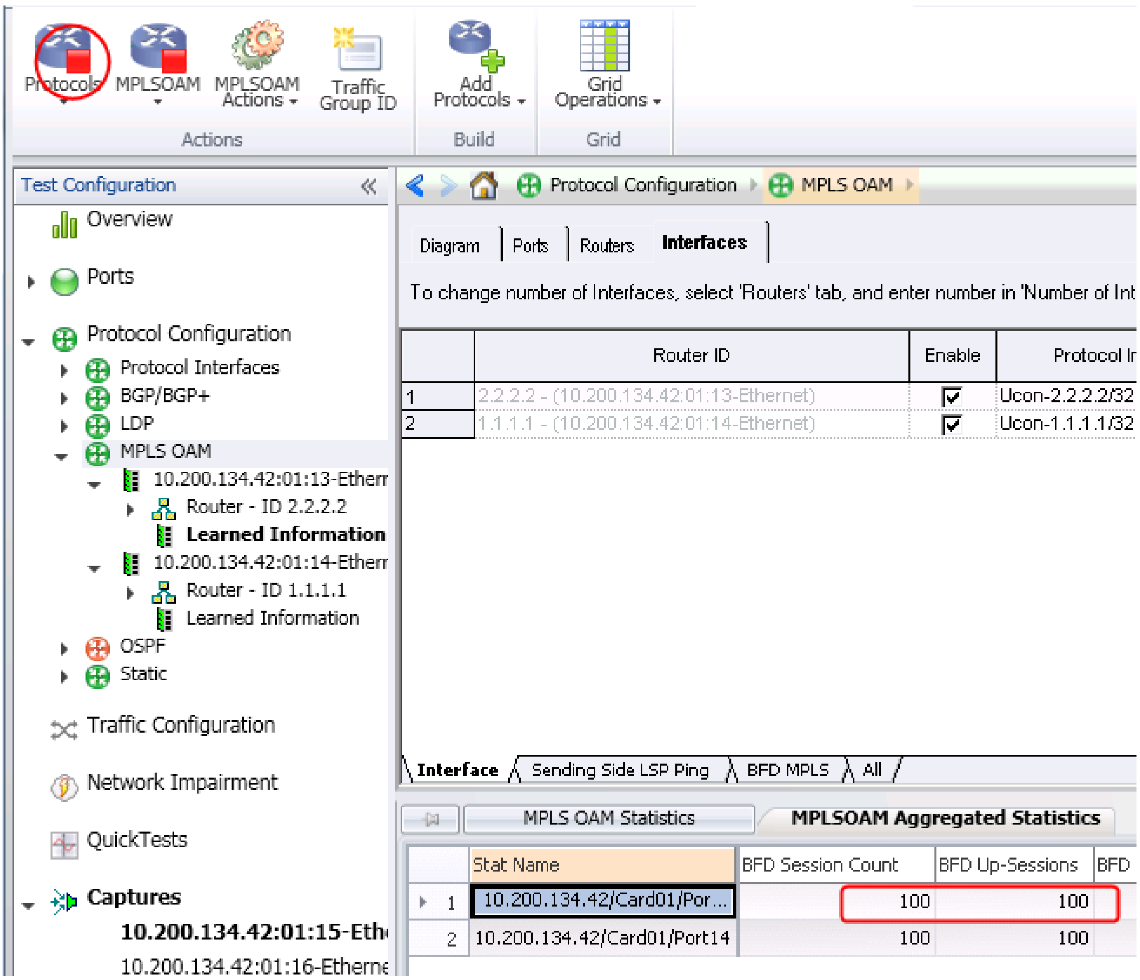


Figure 213. Start All Protocols and Observe MPLS OAM Stats

10. To inject on-demand VCCV Ping to selected VPLS instances, follow these sub steps:
    a. Select the MPLS **Learned Information**
    b. Click **Refresh**
    c. Click interested VPLS instances from **General Learned Info** tab
    d. Click **Trigger.**

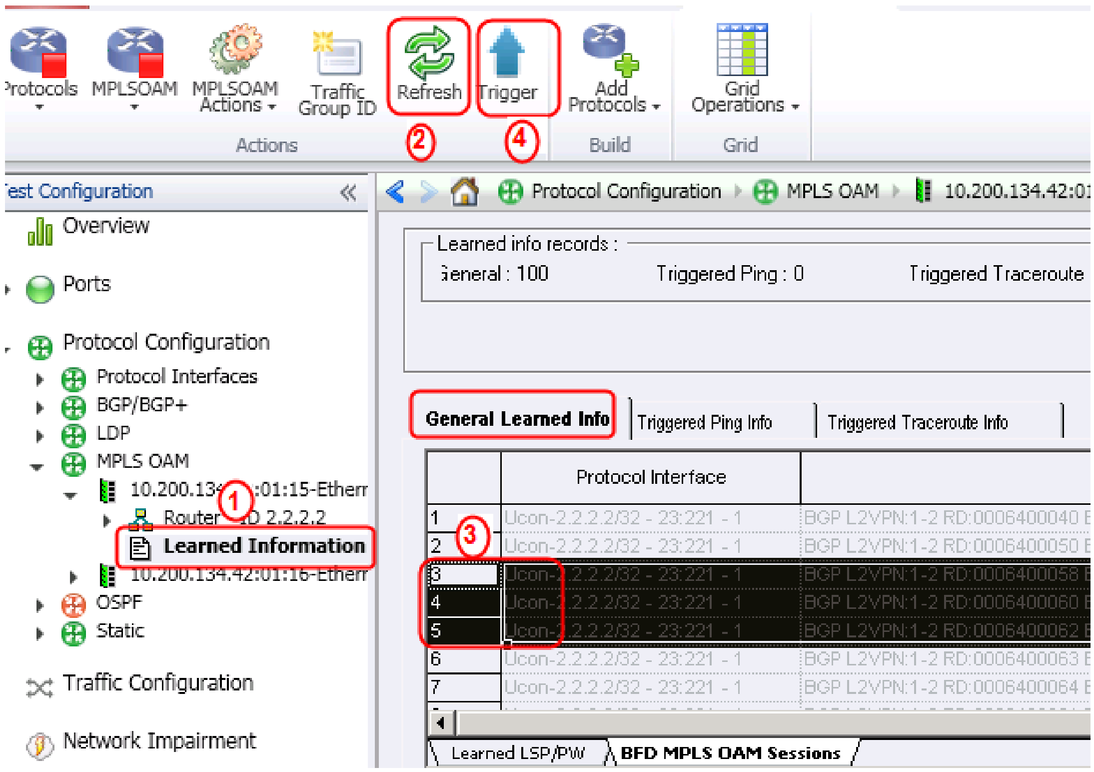


Figure 214. Steps to Inject On-Demand VCCV Ping

11. Once the trigger setting page is open, follow these sub steps to send triggered VCCV Ping:
    a. Click **Send Triggered Ping/Traceroute**
    b. Toggle to enable **Advanced Options**
    c. Select the appropriate **Reply Mode**
    d. Send the VCCV Ping on the selected VPLS
    e. View the MPLS OAM statistics of **LSP Ping Request Tx** and **LSP Ping Reply Rx**

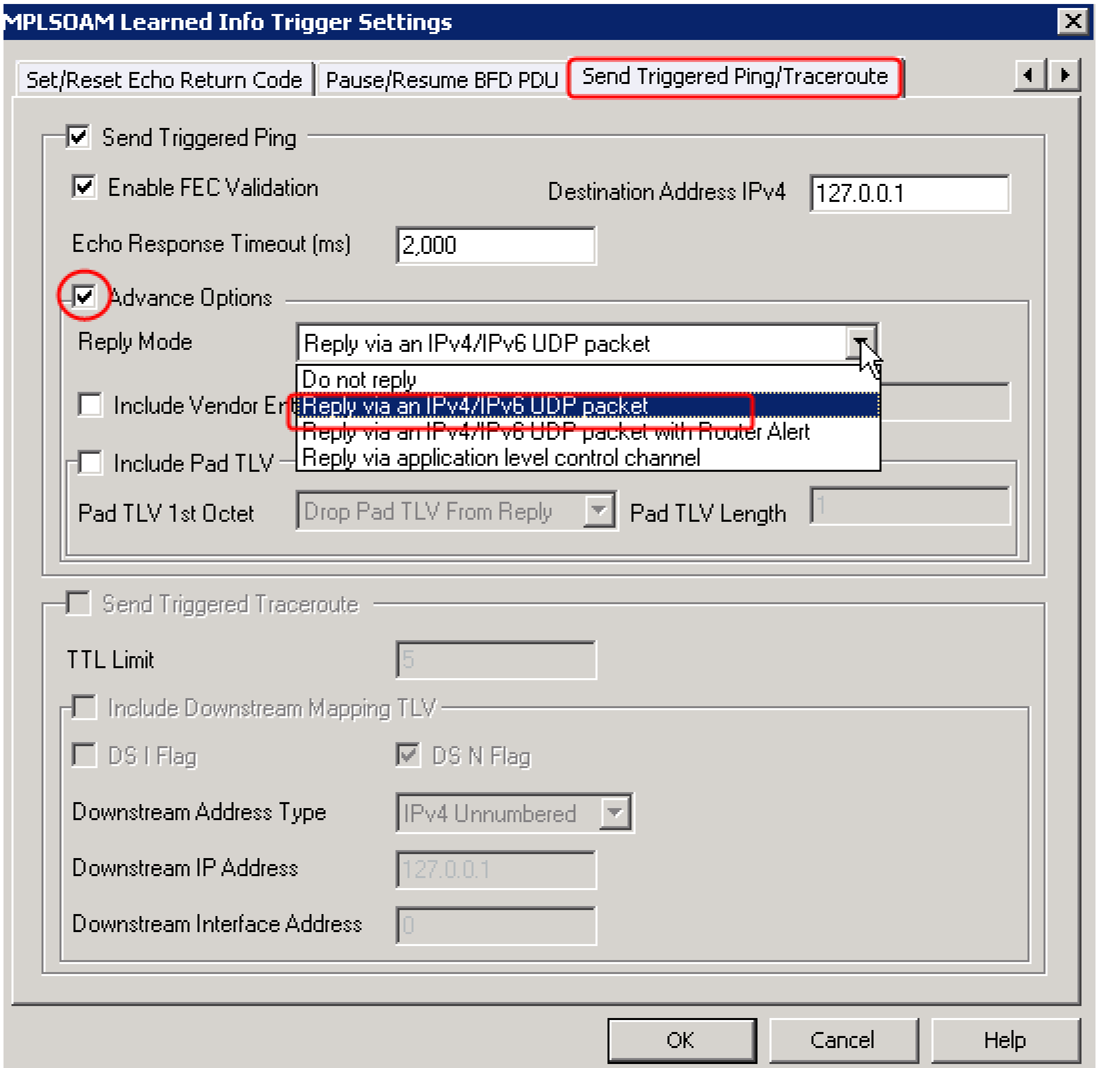


Figure 215. Configure VCCV Ping

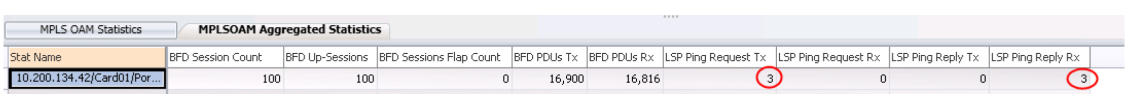


Figure 216. MPLS OAM Stats After On-Demand VCCV Ping

12. To activate the periodic VCCV Ping, go to click the port then click the **Interface** top tab and **Sending Side LSP Ping** tab. Select **Enable Periodic Ping**.

    Optionally:

    You can configure the interval, reply mode and a other parameters. After all parameters configured, either Disable orEnable the router or restart the protocol emulation.

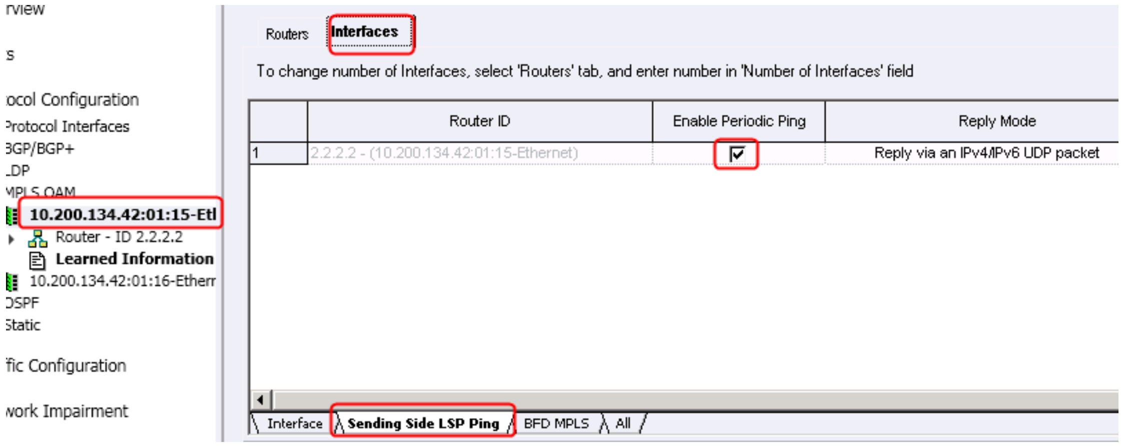


Figure 217. Configuring Periodic VCCV Ping

13. To force the emulator to reply with a particular error code on selected VPLS, you can go to the trigger setting page and select **Set/Reset Echo Return Code** and set the trigger type to be **Forced Return Code**. Click the exact return code from the list.

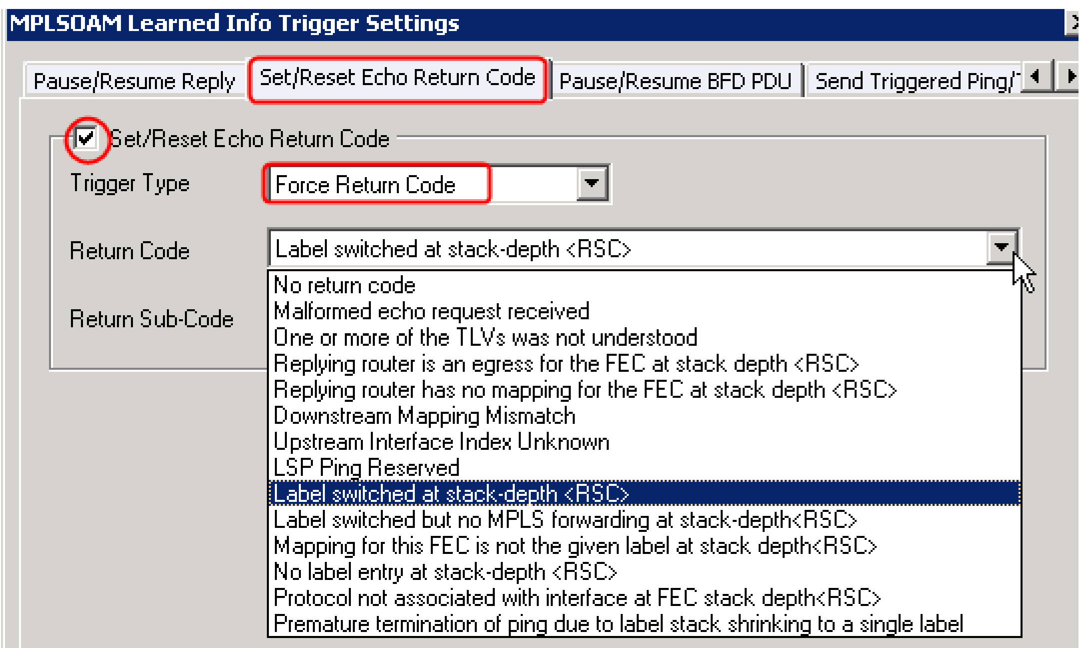


Figure 218. Set Specific Return Code for Negative Test

14. To change BFD intervals and the other BFD specific parameter, go to **MPLS OAM** -> **Interface** -> **BFD MPLS**

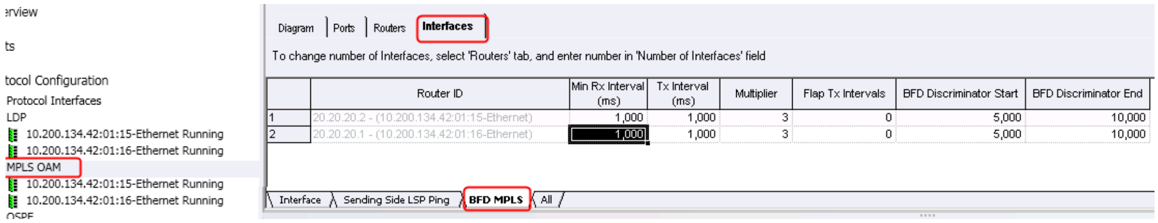


Figure 219. BFD Protocol Parameters

You can also verify individual LSP BFD stats by going to the MPLS OAM **Learned Information** -> **General Learned Info** -> **BFD MPLS OAM Sessions.**

15. To create VPLS black hole based on BFD sessions, you can go to the trigger setting page and select *Pause/Resume BFD PDU*. If Tx-Rx are paused, BFD session flaps appear. View DUT to ensure that right action is taken in order to cope with the black holes.

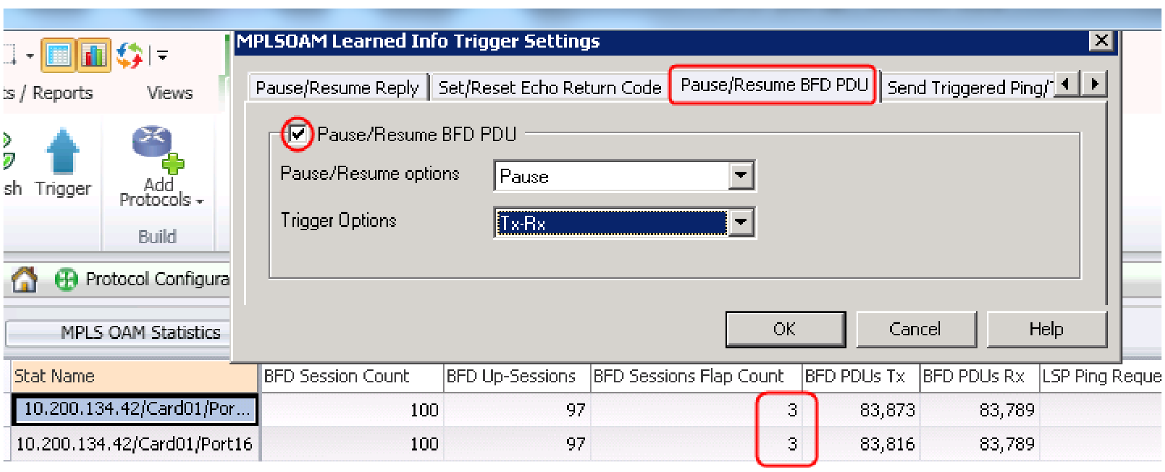


Figure 220. Creating BGB VPLS Black Holes

Test Variables

The following list of variables can be considered to be added in the test to make the overall test plan better.

Performance Variable	Description
Different L2VPN technologies: LDP based PW or VPLS created by FEC 128 or FEC 129	BGP VPLS is used as an example in the illustration on how VCCV Ping and VCCV BFD can be used to maintain an MPLS network. There are other types of L2VPN types, such as the LDP based VPLS, or LDP based PW created by FEC 128 or FEC 129. Note that FEC 129 is specifically used for VPLS using BGP as Auto Discovery (AD) and LDP as signaling protocol. The operation of VCCV Ping and VCCV BFD are almost the same as illustrated in the example. LDP has the ability to advertise CC/CV capabilities, and has more options in the wizard, and in the LDP protocol folder for enabling or disabling these options.
Data plane traffic	You can introduce data plane traffic to verify VCCV Ping and VCCV BFD functions. Note that since they are in-band, they are sharing the same pipe. The more OAM overhead it consumes, the less bandwidth is available for user data. It is interesting to test if line rate traffic at smaller packet size would have any negative impact on the OAM operation; especially when the auto BFD sessions are enabled.
BFD Tx/Rx Intervals	BFD interval affects performance.. Some of the DUT cannot handle many sessions when BFD is running at a high rate (smaller interval). It is interesting to observe how a real DUT behaves with respect to BFD intervals and the total number of VPLS instances running BFD.
Mix VCCV BFD and Periodic VCCV Ping	A mixture of periodic VCCV ping and VCCV BFD makes sense in an actual network. VCCV Ping has the ability to force PW verification and BFD does not. VCCV Ping is more stressful to the DUT. Mixture mode is ideal to achieve assurance and scalability.
Long Term Soaking with VCCV BFD (or/and VCCV Ping)	It is important to run VCCV BFD over a long period of time to observe if the MPLS forwarding engine experiences any abnormal condition. Most of the hardware today works over a few hours but with increased temperature over time the hardware’s behavior may change. In this case, BFD session flap count offers a good indication if there is an error.

Conclusions

VCCV Ping and VCCV BFD offers flexible and effective trouble shooting and network diagnostic tool to support and maintain an BGP based VPLS network. IxNetwork offers all key features with scalability.

Introduction to MPLS Inter-AS VPN Options

Three options exist in accordance with RFC 4364 section 10 for extending MPLS VPN beyond a single Autonomous System (AS), as summarized by the following diagram.

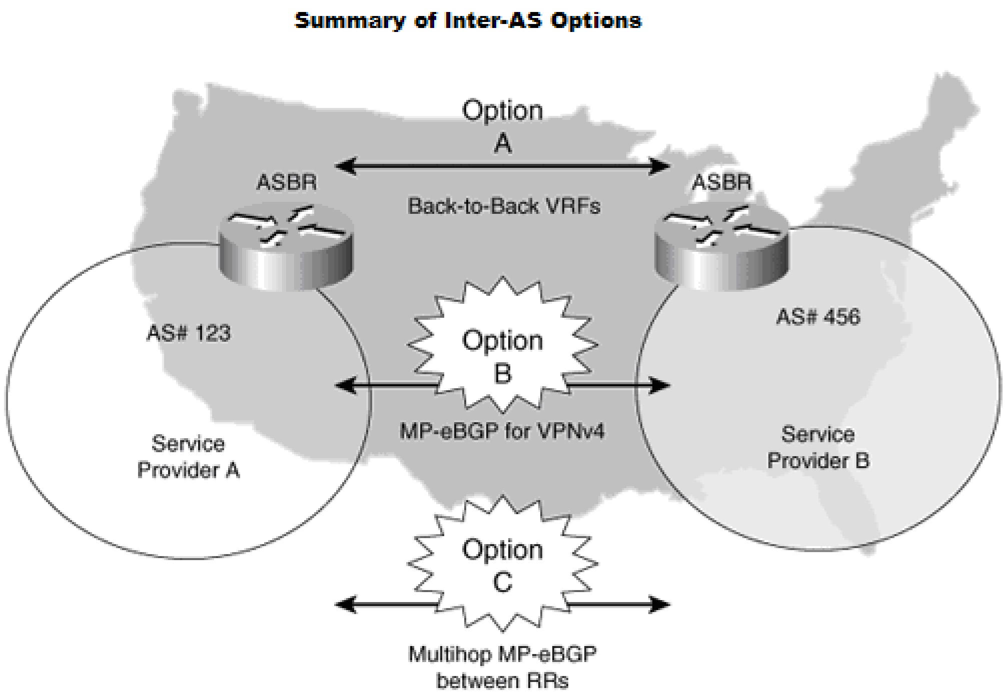


Figure 221. Various Options for Inter-AS VPN Route Distribution

Option A, also known as back-to-back VRF, is the simplest case in which each ASBR PE router is treated as if it is a CE router. VRF routes are converted back to their regular IPv4 or IPv6 routes and are then advertised to the neighbouring AS through the regular BGP. To maintain uniqueness of routes in each VRF, sub-interfaces are commonly used at the connecting interface to provide hard separation between routes belonging to different VPNs. Each VPN requires a separate BGP session to communicate the routes in the same VPN to neighbouring AS. This limits the scalability of the solution as it requires the same number of BGP sessions as the number of VPN or VRFs supported by an ASBR router.

Option B improves the efficiency and scalability over Option A in two aspects. First, it does not require VRF routes being converted back to regular route format. Hence, the VPN concept is kept all the way through across different ASes. Secondly, there is no need for as many BGP (more precisely MP-eBGP) sessions between two adjacent ASBRs; because VRF routes are kept in its native format. A single session is enough if it can satisfy other requirements per inter-AS policy. However, the problem with this option is that the ASBR has to maintain all VRF routes in its database in order for them to be distributed across ASes – a job usually belonging to a router known as Router Reflector (RR). This puts extra burden on the ASBR router, which is already busier than others in the network. Additionally, when packets are entering the network, they must pass through MPLS label (transport label – provided either by LDP or

RSVP-TE), imposition (ingress PE), and deposition (egress PE) twice; one at the ingress/egress PEs that belong to the same AS, the other at the ASBR where they enter the other AS.

Option C improves the efficiency and scalability over option B also in two aspects. First, a multi-hop BGP (MP-eBGP) is established between the two RRs in the two neighbouring ASes. This MP-eBGP session is used to exchange VRF routes, in much the same way as in the case of Option B to relieve the ASBR routers from learning and storing VRF routes and labels. Secondly, there is a need for another MP-eBGP session between the two ASBRs to exchange the loopback addresses of all the PE routers in both of the ASes, along with the MPLS label assignment for these loopback addresses. These labels for the PE loopback addresses are propagated by the ASBR towards the other AS, and subsequently reach the RR and made known (reflected) to all the other PEs in the other AS. These labels will be used as the middle label in a total of three labels encapsulation at the ingress PE, when packets first enter the MPLS network from a CE router.

Ixia's IxNetwork has supported both Option A and Option B in as early as version 5.20. In its latest release 6.30, the option C is finally supported with not only control plane emulation, but also scalable data plane with auto resolution of 2 labels or 3 labels stack, depending on Ixia's role to play in a multiple DUT setup environment.

The following diagram illustrates the idea how the IxNetwork is used to test both the functionality and scalability of Inter-AS option B, and Option C. A minimum of two test ports are required, one to act as regular MPLS VPN CE/PE and the other as PE/ASBR/RR from the other AS. The MP-eBGP peers between the emulated ASBR and the DUT/ASBR exchanges PE loopbacks and their associated labels, while the emulated RR and the DUT RR exchanges VRF routes and VRF labels. Traffic form the emulated CE/PE has a three labels encapsulation, while the traffic by the emulated ASBR/RR has two labels. Most importantly, one can easily scale the test by emulating a large number of PE routes in each AS, and a large number of VRF in each AS. The data plane traffic can encapsulate either 2 labels or 3 labels with correct label binding based on control plane learned info, all without user intervention. This concept makes the solution extremely scalable – a focused solution for system test engineers to test Inter-AS VPN without the need for many real DUTs in the test topology.

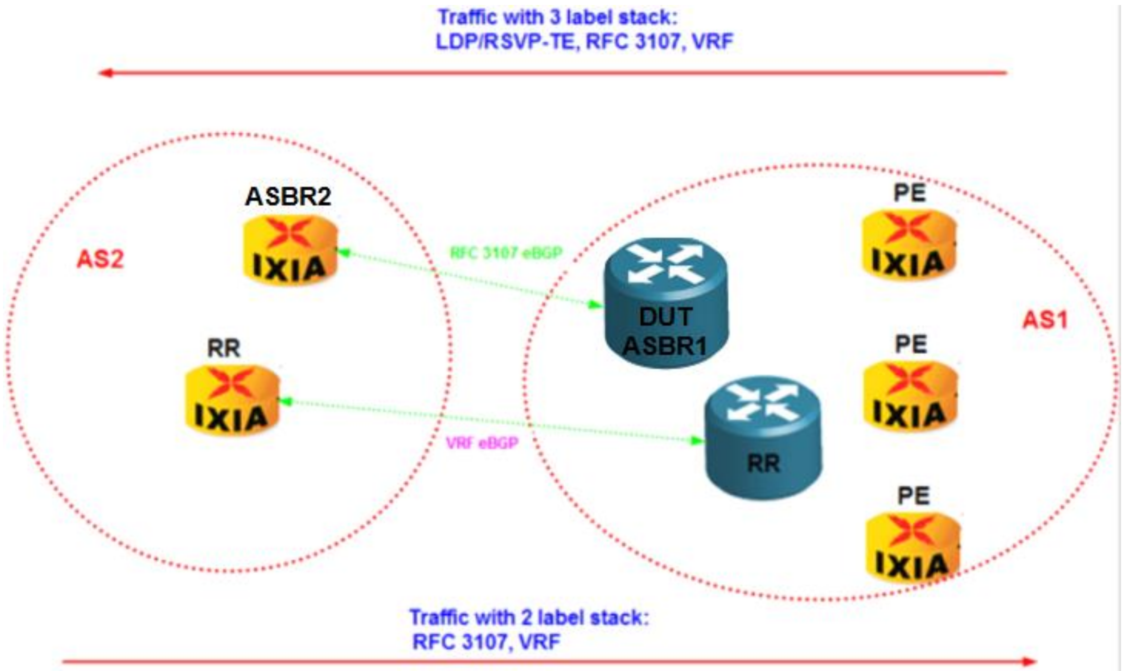


Figure 222. How Inter-AS Option B and C Work

Relevant Standards

RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs)

Test Case: How to Test L3VPN Inter-AS Option B

Overview

Inter-AS option B refers to the two ASBRs residing in two ASes exchanging the VRF info. Hence, VPN information can be kept across ASes. Traffic leaving one ASBR contains only VRF label (transport LDP or RSVP-TE labels are removed) and the ASBR at the other AS is responsible for inserting the transport label of its own AS in order to move the packets across the network to reach far end PE/CE. See the above introductory section for more description and a comparison between different options.

Objective

This is to test DUT Inter-AS option B functionality and scalability as an ASBR router.

Setup

Two Ixia test ports are required to carry out the test. One test port is to emulate one entire AS including PE/CE routers, and the ABSR router. The other test port emulates either CE routers, or both the CE and PE routers in the other AS to test DUT as ASBR, and optionally a regular PE rotuer.

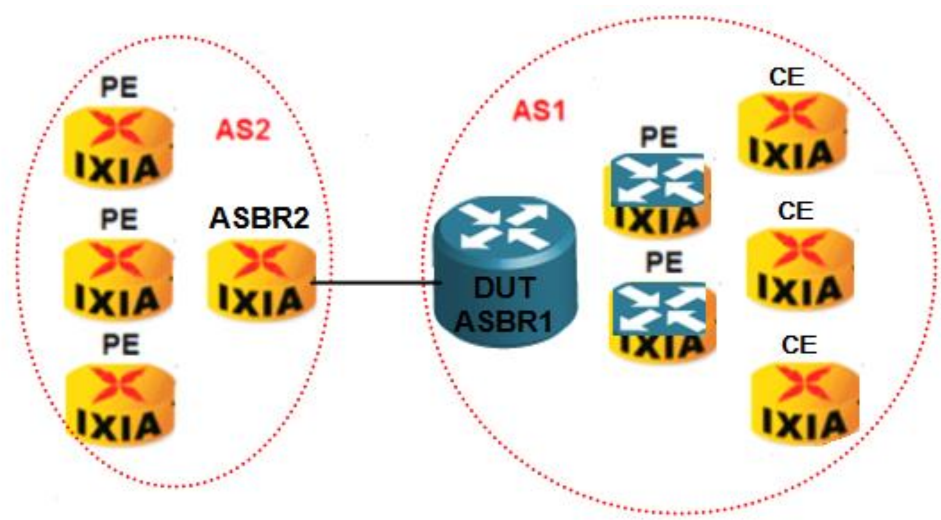
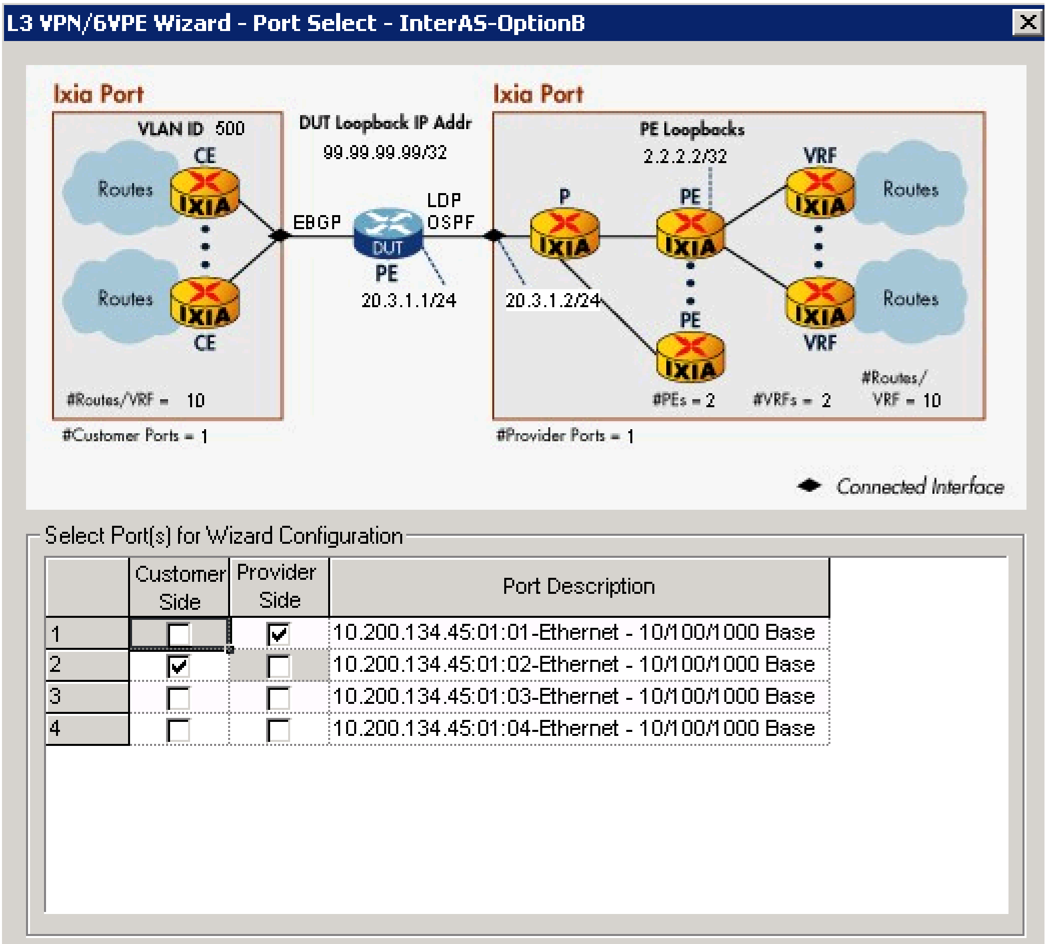


Figure 223. Test Setup for Option B

Step-by-Step Instructions

1. Launch the IxNetwork L3VPN/6VPE Wizard and navigate throughout it. First designate which Ixia test port(s) to participate PE at remote AS (es) (AS2) and which is to participate at CE, or optionally both CE and PE side.



	Customer Side	Provider Side	Port Description
1	☐	☑	10.200.134.45:01:01-Ethernet - 10/100/1000 Base
2	☑	☐	10.200.134.45:01:02-Ethernet - 10/100/1000 Base
3	☐	☐	10.200.134.45:01:03-Ethernet - 10/100/1000 Base
4	☐	☐	10.200.134.45:01:04-Ethernet - 10/100/1000 Base

Figure 224. Select Test Port

2. Configure the physical port address of the DUT that is connected to Ixia Port 1 (simulating PE/ASBR routers at AS2). Keep default OSPF as the MPLS IGP and LDP as the MPLS signaling protocol. Note that neither OSPF nor LDP is actually used in the inter-AS scenario. You can later manually remove the configured OSPF and LDP session by the wizard.

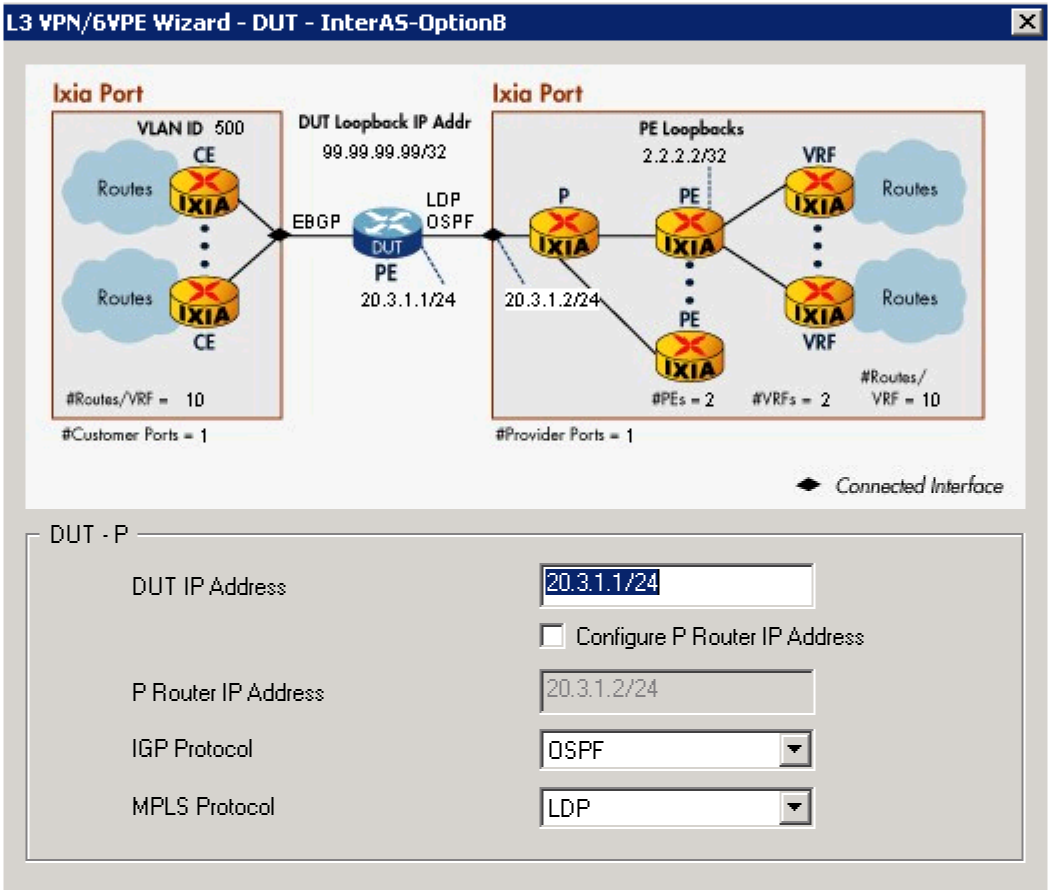


Figure 225. Configure the P Router

3. In the next window, enter 2 as the number of PEs to be emulated by Ixia test port 1 (simulating PEs from AS2), and enter the AS number used by the Systems Under Test (SUT) for now. We use manual method to change the iBGP to eBGP as well as the correct AS number for the eBGP session later on. Also, enter loopback addresses for the two emulated PE router and the DUT loopback address.

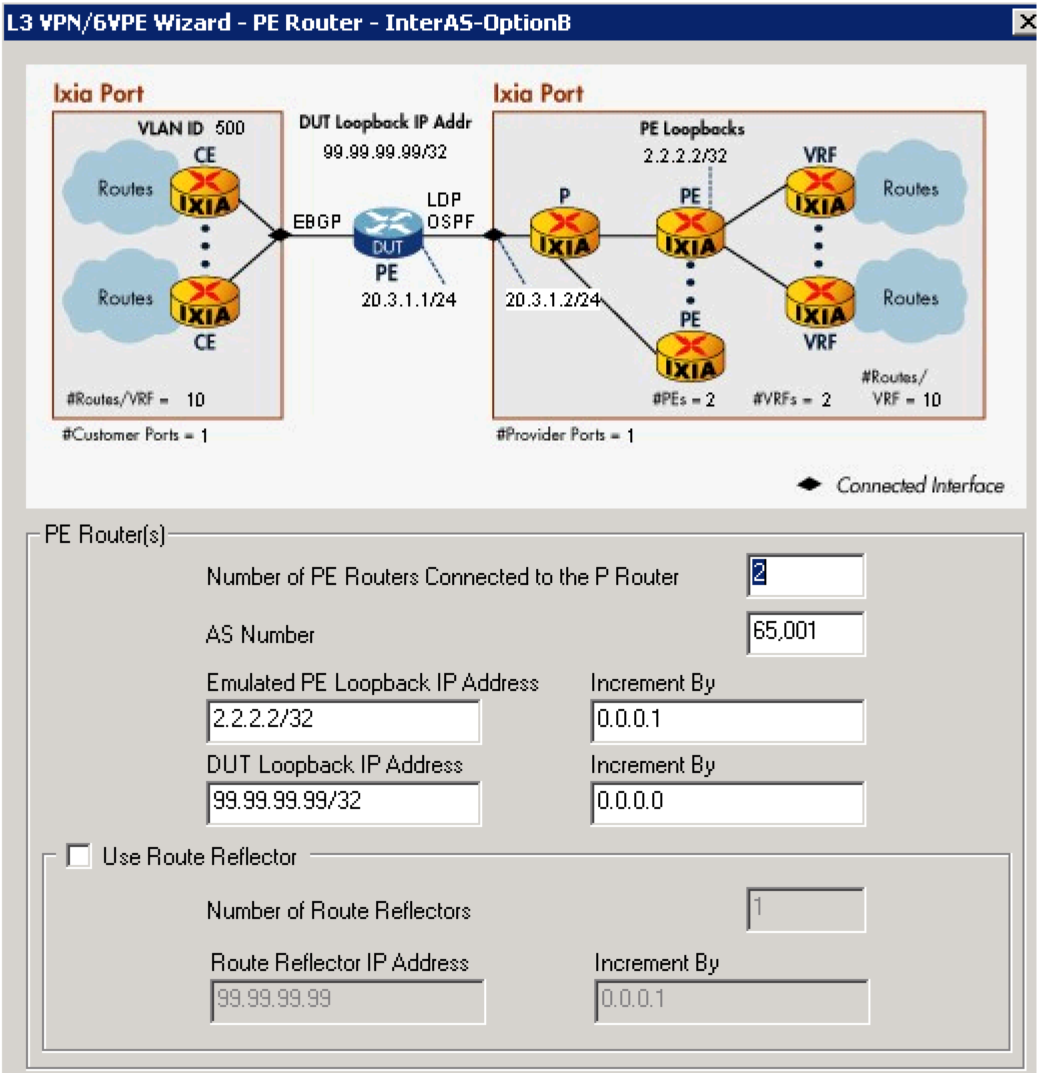


Figure 226. Configure the PE Routers

4. The next window of the configuration wizard contains VRF definitions. Enter the correct RD value and the number of VRFs behind each PE. Select a start value of routes behind each VRF. By default, routes are split between CE and PE side equally as 50%.

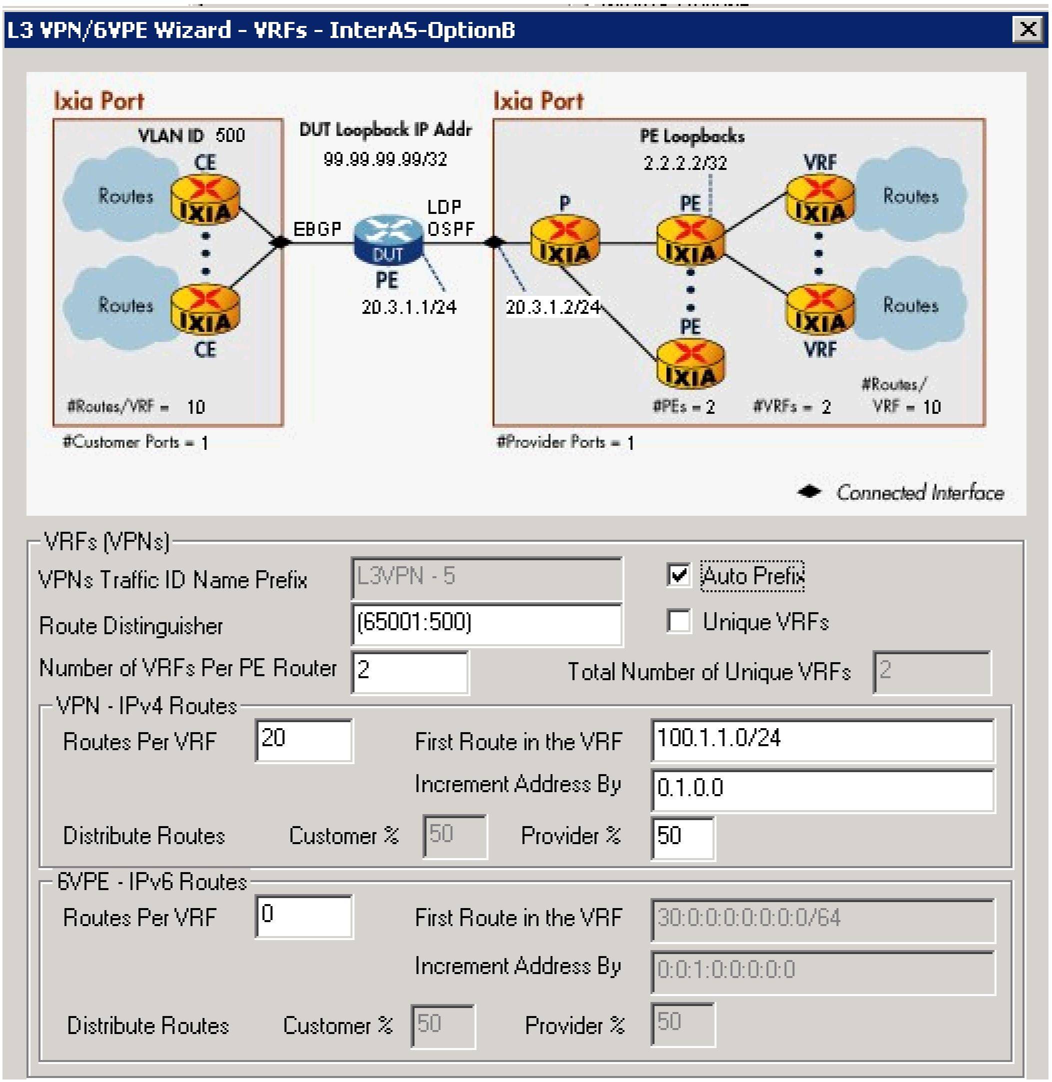


Figure 227. Define L3VPN Info

5. In the next window CE side parameters are setup. Like in a typical VPN deployment scenario, EBGP is chosen as an example between CE and PE. Each CE for different VPN is separated by VLAN.

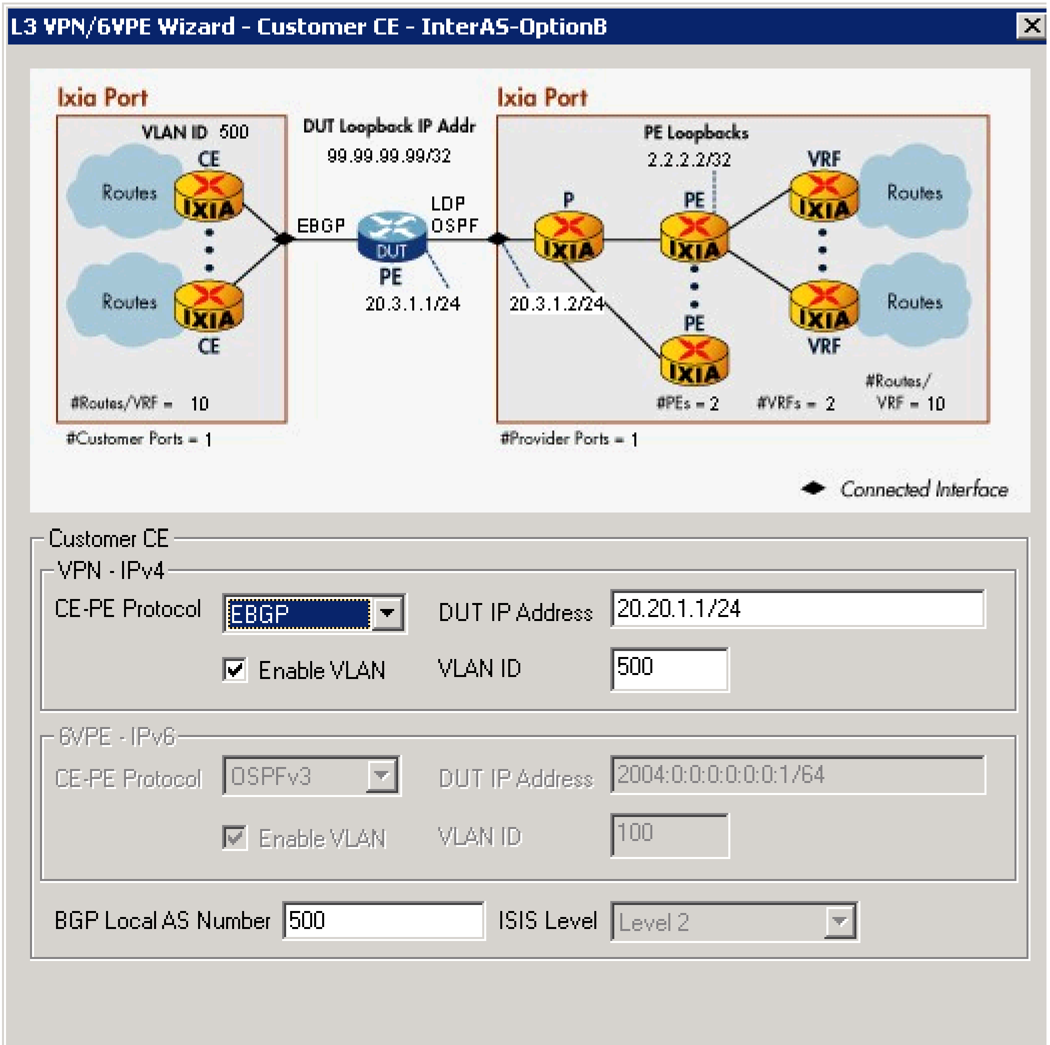


Figure 228. Configure the CE Router

6. The last step of the configuration wizard is to either save the configuration without configuring the ports, or simply save and configure the ports at the same time. This approach is same for all the other wizards supported by Ixia's IxNetwork.

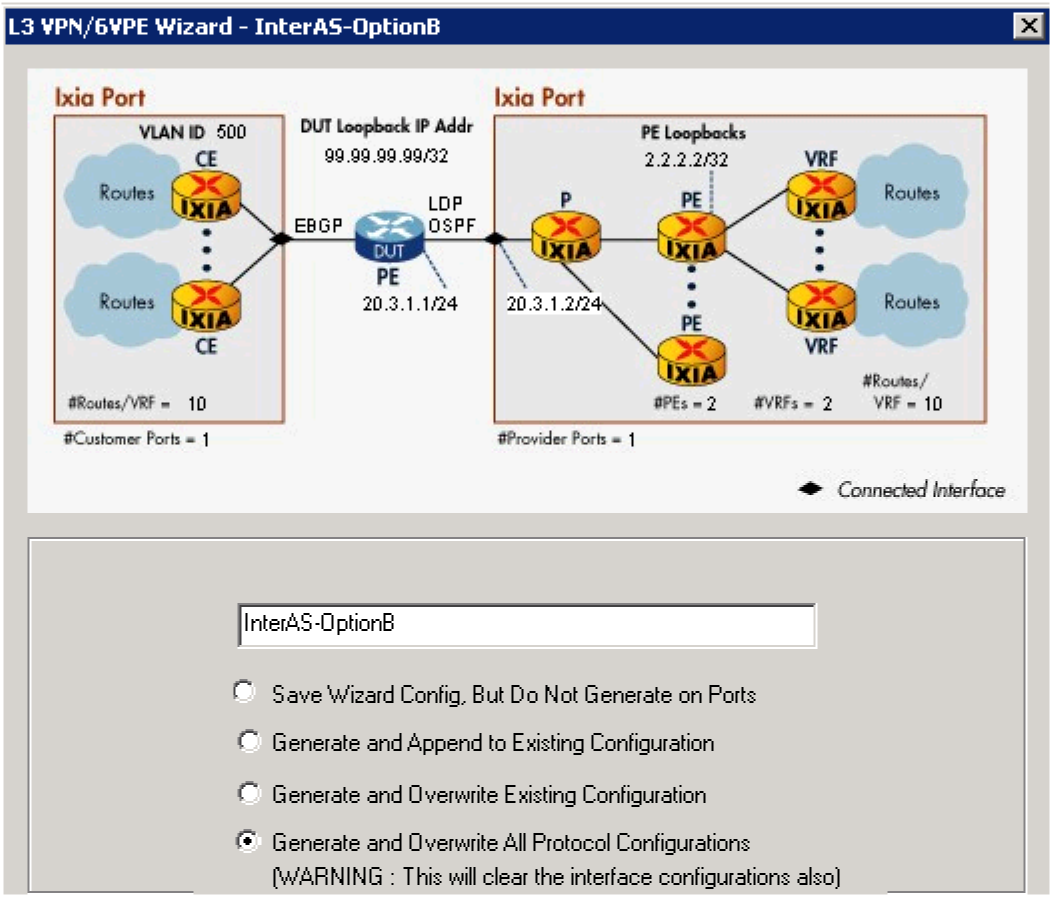


Figure 229. Save and Overwrite the Config

7. Manually modify the configuration created by the protocol wizard. First and foremost, disable OSPF and LDP on the provider port. Neither is required for Inter-AS Option B testing.

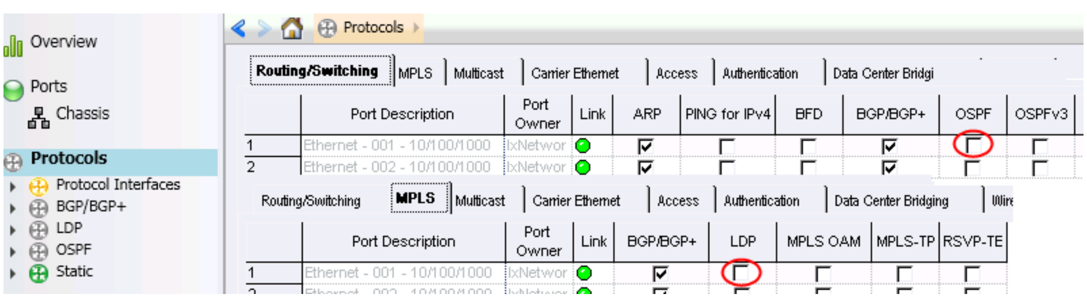


Figure 230. Disable Unwanted Protocols

8. Further, change the MP-iBGP sessions to MP-eBGP sessions. First, click BGP on the protocol tree to access all BGP sessions followed by selecting Peers tab on top and All tab at the bottom. As shown below, the two internal BGP sessions are as a result of the protocol wizard in step 1. We need to change both Internal sessions to External sessions. Change the Local AS number according to your network design.

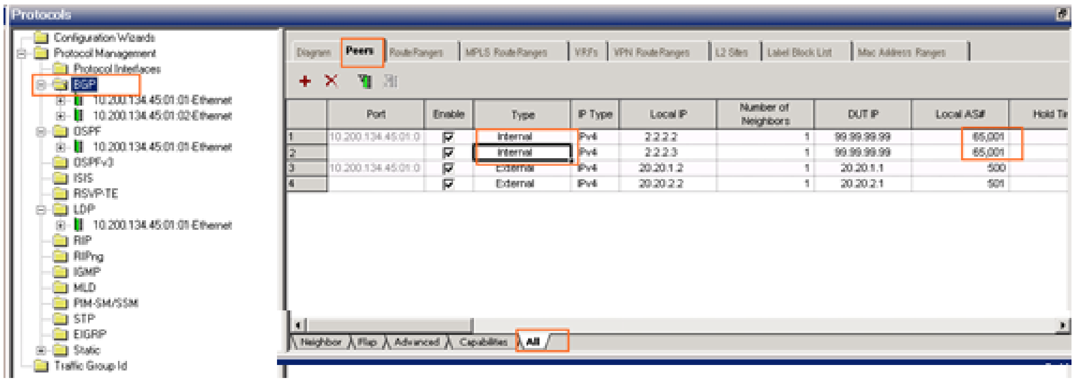


Figure 231. Change Internal BGP to External BGP

9. The following image reflects the parameters to modify. Make sure you select the check boxes in the **Is ASBR** column for the eBGP peers for the Provider port(s). The option **Is ASBR** is used by the traffic wizard to construct data plane traffic with correct amount of labels.

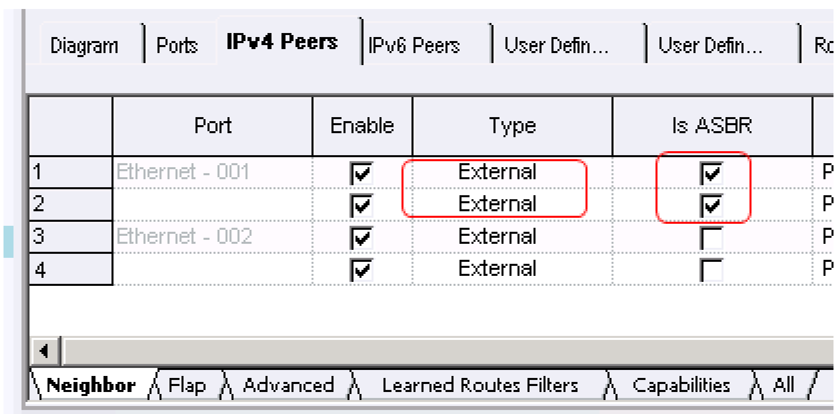


Figure 232. External Peers with ASBR Option

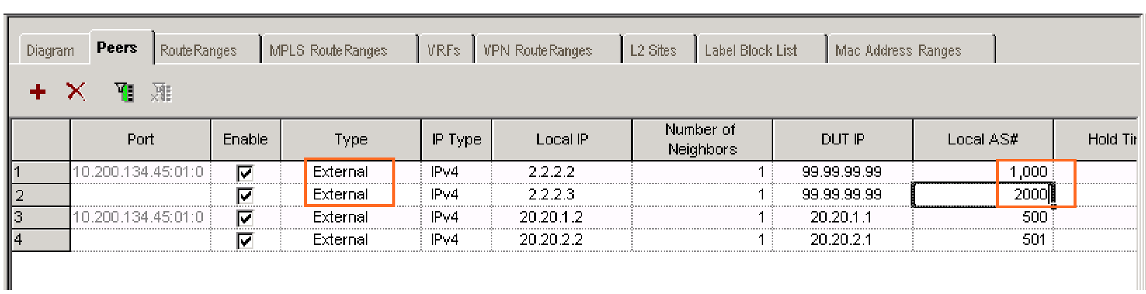


Figure 233. Change the AS

10. Once BGP sessions are changed from Internal to External, modify the VRF routes attributes. By default, the wizard excludes any AS Path info in the VRF routes advertisement, because the BGP sessions are considered as Internal. As they are external sessions, modify the attribute to include correct AS Path info. To access the attributes, click BGP on the protocol tree, followed by click VPN Route Ranges tab on the top and Attributes tab at the bottom, as shown below:

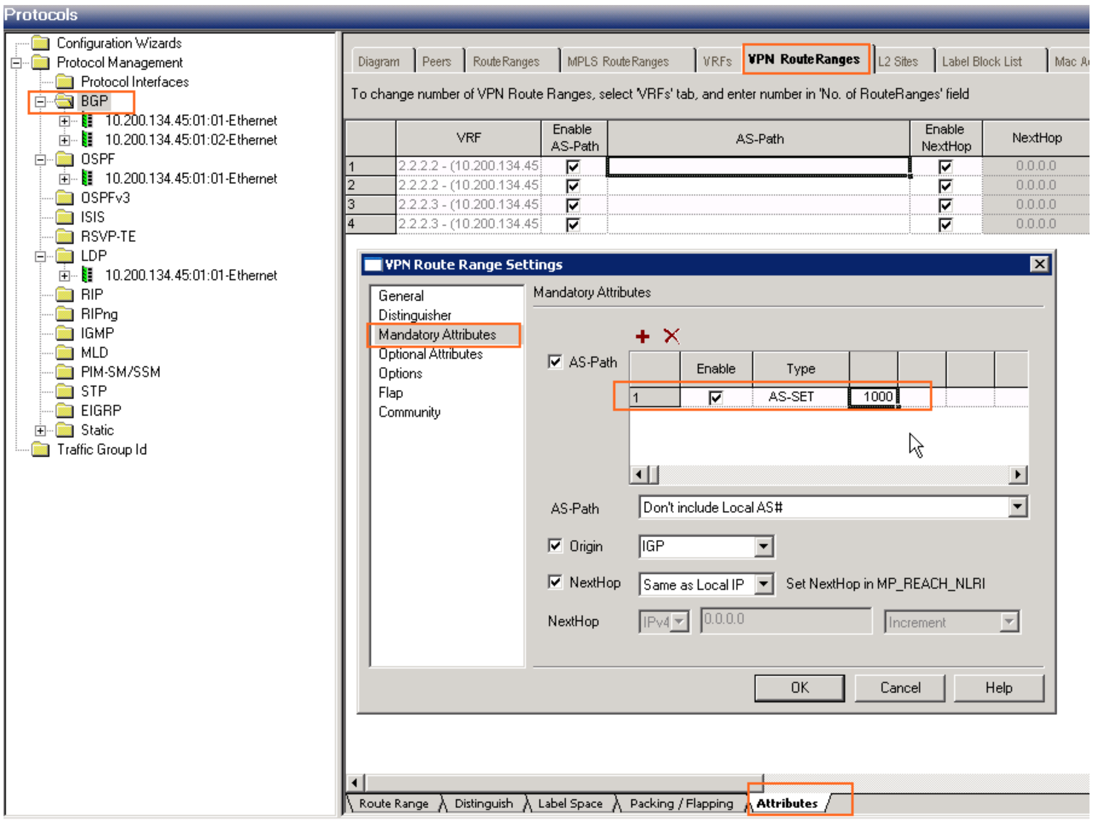


Figure 234. Change AS Set to Reflect Hops

11. Double click the **AS-PATH** field (empty created by the wizard) to open Add AS-Path window. Click the **+** symbol and enter the correct AS number. Click **Ok** and this enters a correct AS-PATH attribute to indicate that the VPN routes are arriving from another AS. Below is the image depicting the change in values. When the number of PEs or number of ASes increse, use copy and paste for easy modification.

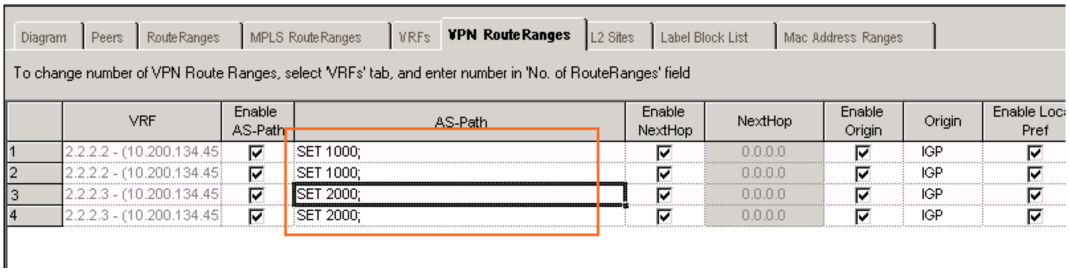


Figure 235. Make Changes for All External Peers

12. Before starting the BGP sessions at both the CE and PE ports, send a few ping commands from the DUT to test reachability to the emulated PE loopback addresses (enable Ping on the Ixia side first). Once Ping is successful, start BGP sessions on both the CE port and PE port. Make sure all protocols are entering stable state, as indicated below.

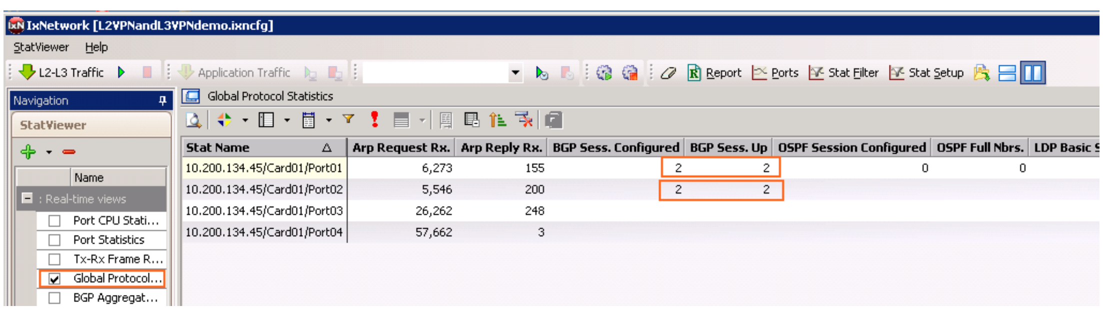


Figure 236. BGP Protocol Stats

13. To verify the VRF routes exchange over the MP-eBGP session, click **Learned Routes** on the Ixia's emulated PE router and as shown below. It displays all the VPN routes learned from DUT.

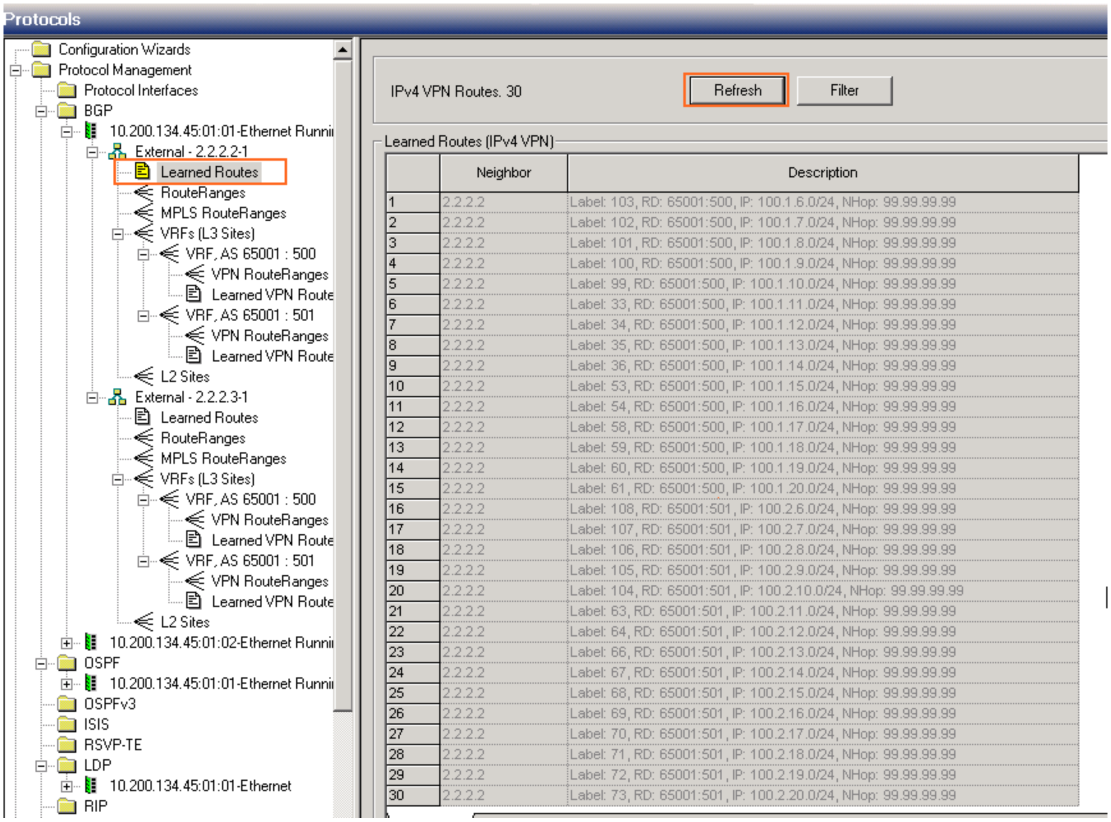


Figure 237. BGP Learned VRF Routes

14. To further verify the emulated PE routers are also advertising the VPN routes to the DUT, go to the DUT, click and verify if the DUT has received the advertisement, as indicated below.

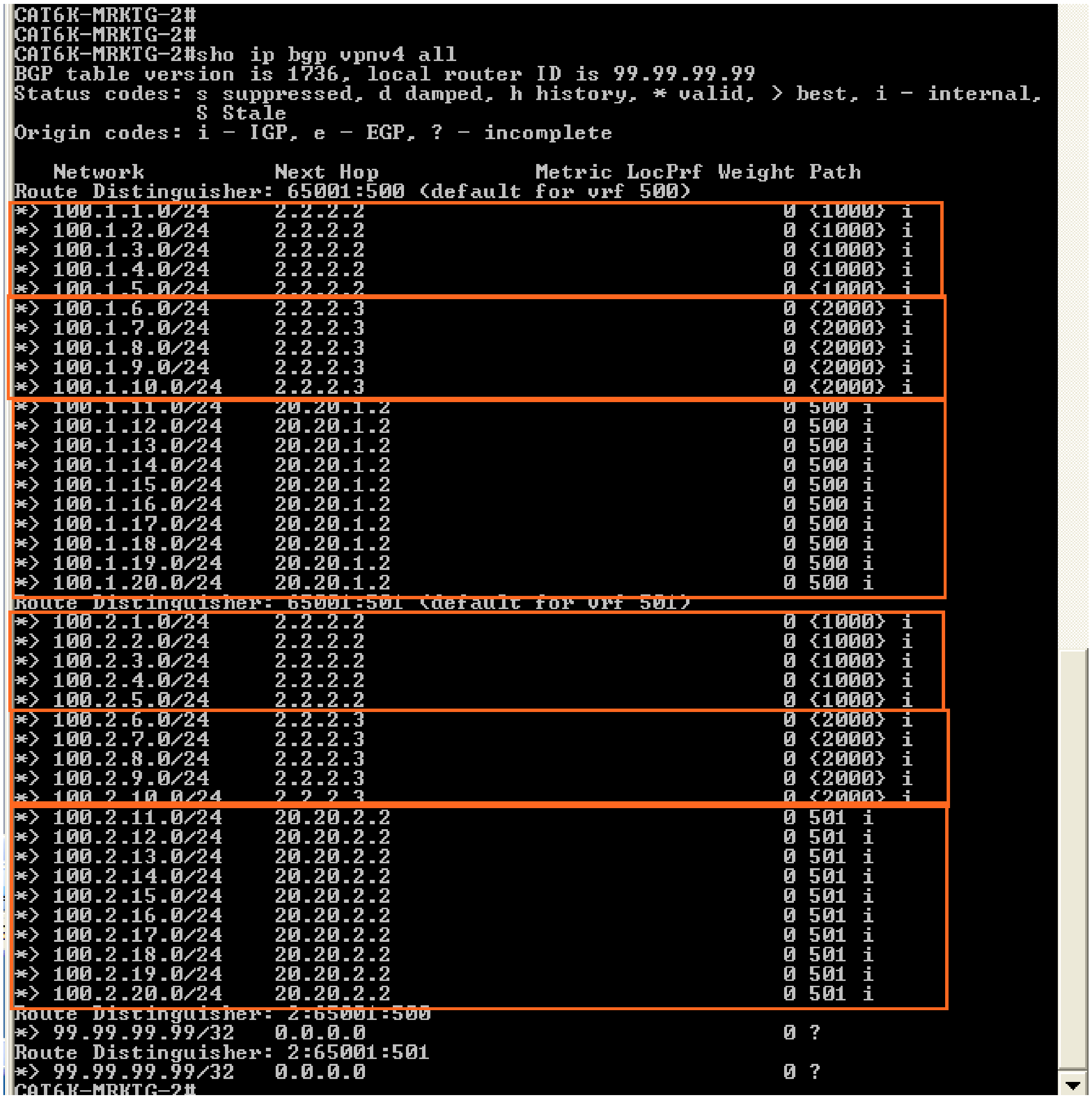


Figure 238. DUT Learned Info

15. Now that the control plane is up and functioning as expected, we must build traffic sending from both directions. To build the traffic from PE->CE direction, launch the traffic wizard first and select the **L3VPN** as the Encapsulation Type. Next, select the Traffic Group ID as assigned by the protocol wizard. There might be many traffic group IDs existing every time you run the protocol wizard. The IDs automatically increment by one to avoid duplicate traffic group ID. The traffic group ID is simply the VPN color and the intention is for intelligent filtering so that no VPN cross-talking traffic is built by default. Click **Apply Filter** in order to associate the traffic group ID with the VPN routes appropriately.

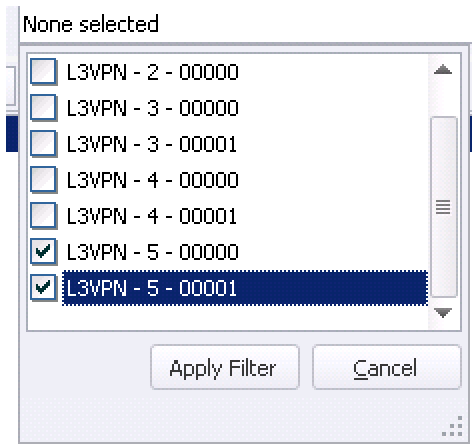


Figure 239. Apply Filters

16. Once the VPN routes are associated with proper traffic group id, select all VPN routes by clicking on BGP as indicated below. This action selects all the routes available on the source list. Also select the same for the destination. Click the green arrow to add the traffic source and destination pairs.

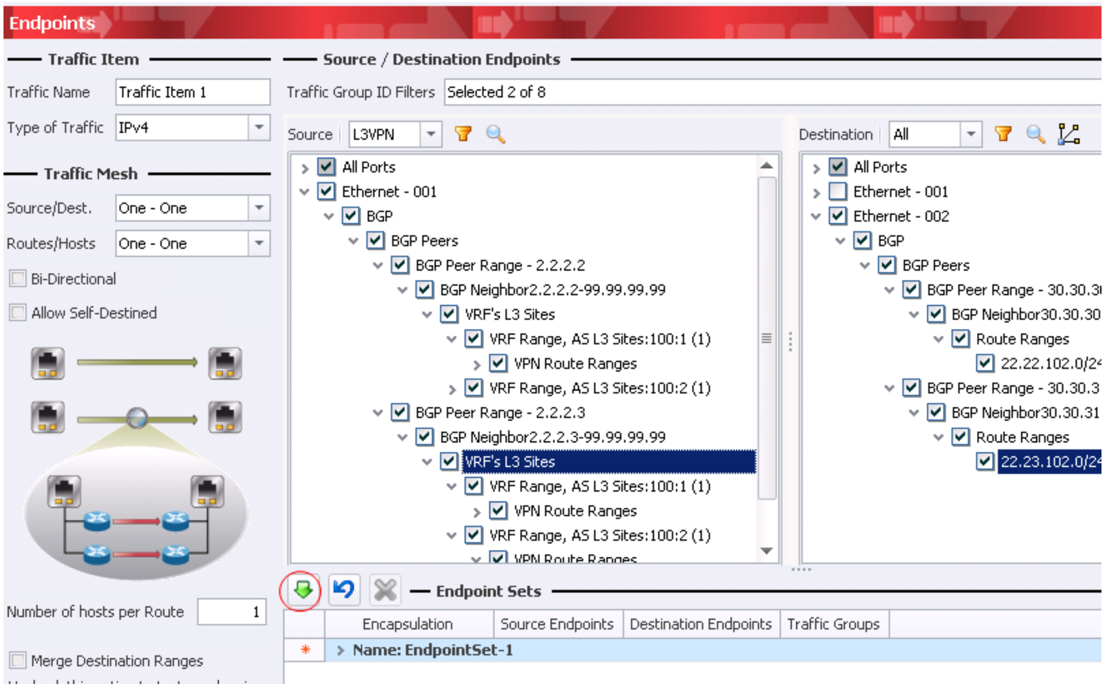


Figure 240. Traffic End Points Selection

17. By now you should understand the advantage of using traffic group id for quick and easy traffic pair construction. In the case of large number of VPNs/VRFs, this is extremely efficient.

18. As an extra step, confirm whether a single label is used by the traffic wizard to build the traffic from PE->CE direction or not, as required by Option B.

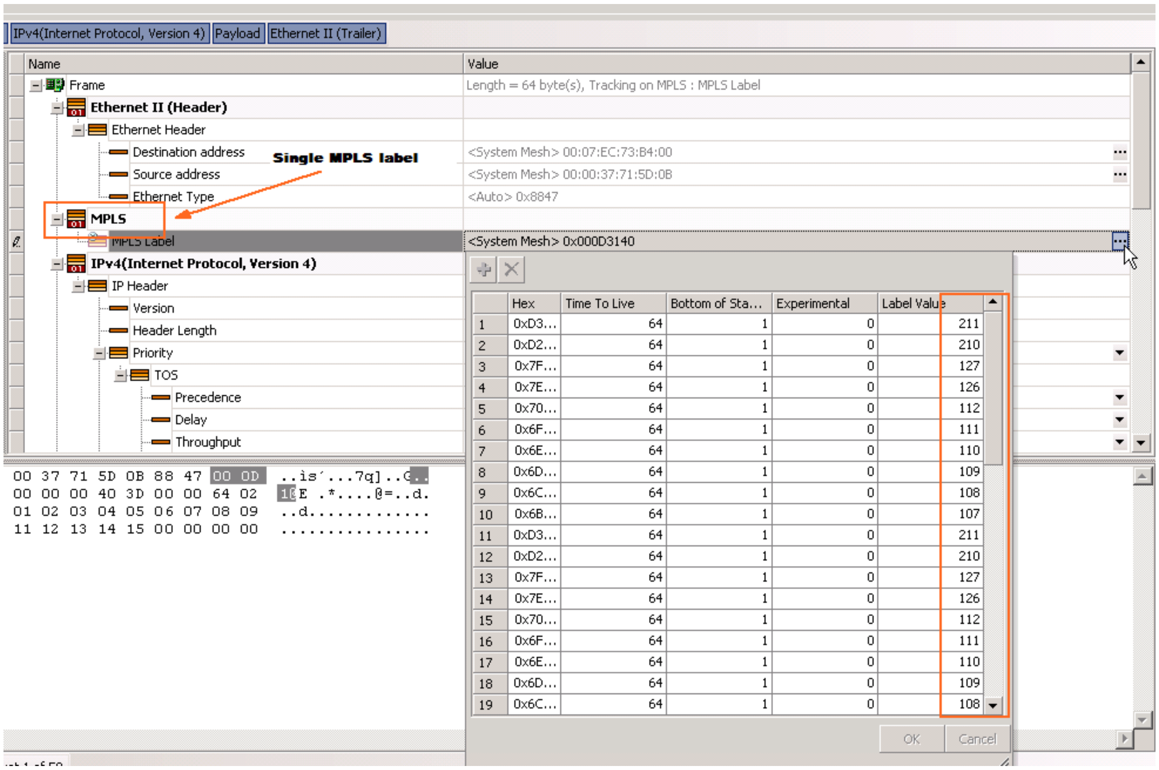


Figure 241. Packet Editor View

19. Similarly, build the traffic pairs for CE->PE direction as shown below. Again, use the traffic group ID to bind VPN routes appropriately to their respective VPNs.

20. As expected, traffic is passing the DUT without any problems.

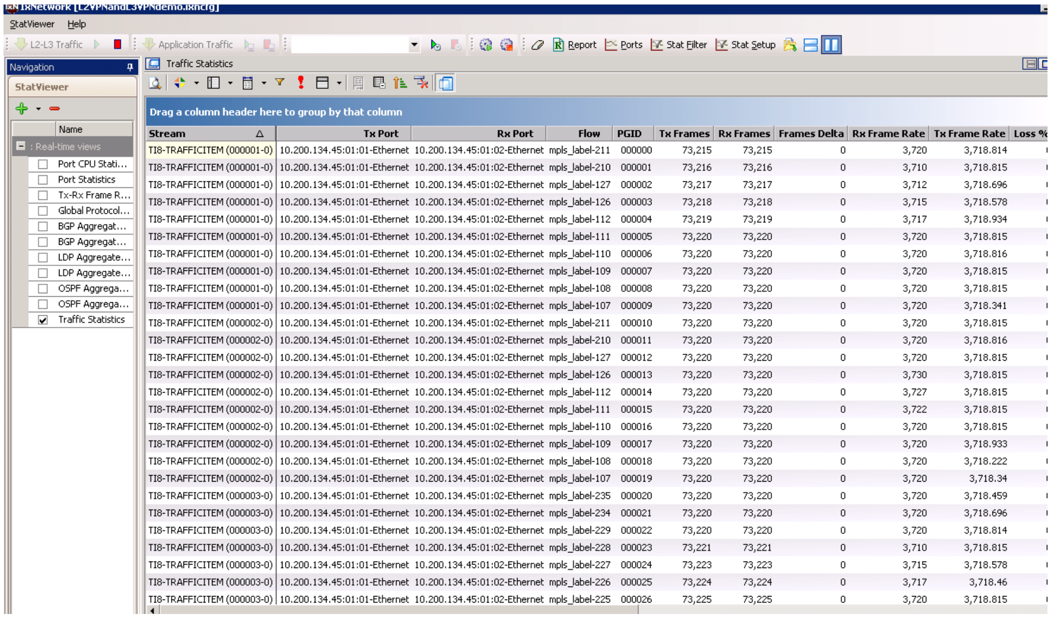


Figure 242. Traffic Per Flow Stats

Test Variables

Consider the following list of variables to add in the test to make the overall test plan better.

Performance Variable	Description
The number of PE routers and the number of VPNs in the AS2 emulated by Ixia test port 1	Functionality and scalability are two different test types. It is common practice to ensure functionality working before expanding the test config for scalability test. Two most obvious dimensions one can scale test into is the number of PE routers and the total number VPNs emulated by Ixia test port in AS2.
The number of PE or CE routes in the AS1, collocated with DUT as ASBR	To fully stretch the DUT, scale the test not only from another AS, but also the number of PE or CE routers in the same AS as the DUT.
Bidirectional traffic with various frame size and rate; optionally running RFC 2544 methodology to cycle thru packet sizes and auto find the maximum throughput/latency	Traffic is also important to test inter-AS options. Due to extra label encapsulation/de-capsulation, throughout and latency do matters to inter-AS traffic, in addition to frame size and traffic rate.

DUT Configuration Excerpt

```
!
version 12.2
!
hostname CAT6K-MRKTG-2
!
boot system sup-bootflash:s72033-pk9sv-mz.122-18.SXD4.bin
enable password ixia
!
no ip domain-lookup
!
ip vrf 500
 rd 65001:500
 route-target export 65001:500
 route-target import 65001:500
!
ip vrf 501
 rd 65001:501
 route-target export 65001:501
 route-target import 65001:501
!
interface GigabitEthernet3/1
 ip address 20.3.1.1 255.255.255.0
 tag-switching ip
!
interface GigabitEthernet3/2
 ip address 20.3.2.1 255.255.255.0
 tag-switching ip
```

```
!
interface GigabitEthernet3/2.1
 encapsulation dot1Q 500
 ip vrf forwarding 500
 ip address 20.20.1.1 255.255.255.0
 no cdp enable
!
interface GigabitEthernet3/2.2
 encapsulation dot1Q 501
 ip vrf forwarding 501
 ip address 20.20.2.1 255.255.255.0
 no cdp enable
!
router bgp 65001
 no synchronization
 bgp router-id 99.99.99.99
 bgp cluster-id 1684275457
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1000
 neighbor 2.2.2.2 ebgp-multihop 3
 neighbor 2.2.2.3 remote-as 2000
 neighbor 2.2.2.3 ebpg-multihp 3
 no auto-summary
 !
 address-family ipv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 neighbor 2.2.2.3 activate
```

```
 neighbor 2.2.2.3 send-community extended
 exit-address-family
!
 address-family ipv4 vrf 501
 neighbor 20.20.1.2 remote-as 501
 neighbor 20.20.2.2 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf 500
 neighbor 20.20.1.2 remote-as 500
 neighbor 20.20.2.2 activate
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route 2.2.2.2 255.255.255.255 20.3.1.2
ip route 2.2.2.3 255.255.255.255 20.3.1.2
```

Test Case: How to Test L3VPN Inter-AS Option C

Overview

Inter-AS option C refers to the scenario where the routers in one AS exchange VPN routes and labels as well as PE loopback address and their associated labels with routers in another AS. VPN info is exchanged between two routers known as Router Reflector (RR), which is typically multi-hops away from the area border routers. The PE loopback address as their associated labels are exchanged between two ASBR routers, which usually are directly connected to each other. Traffic leaving one ASBR and heading to the other AS contains the VRF labels as well as the label corresponding to the egress PE loopback address, which is exchanged between the two ASBR routers. However, there is no transport LDP or RSVP-TE labels as traffic is leaving current AS and transport label is performed with what it is meant for. As traffic enters the other AS, the ingress ASBR at that AS is responsible for inserting the transport label of its own AS in order to move the packets across the network to reach far end PE/CE. See the introduction section for more description and a comparison between different Inter-AS options.

Objective

The objective of the test is to use Ixia to emulate many components in an Inter-AS option C. The setup is to test DUT as ASBR and RR the functionality as well scalability, when surrounded by hundreds or even thousands of PE routers, tens of thousands of VPNs, and millions of VRF routes.

Setup

Two test ports are needed in order to test fully the DUT’s ability as ABSR and RR to bridge L3VPN across two separate ASes. Once test port emulates ASBR and RR in one area, and lots of PE routers behind; the other port emulates large number of PEs in the same AS because the DUT (as ABSR/RR). Traffic for either direction is automatically resolved with correct number of labels, and the correct learned labels.

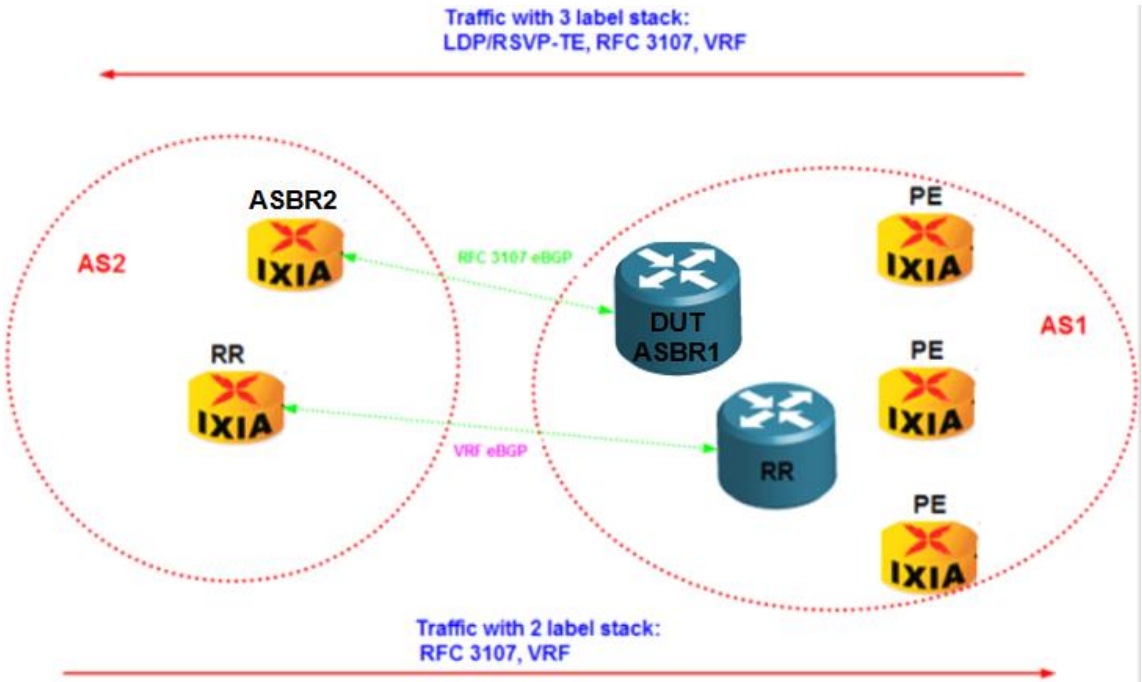


Figure 243. Test Setup for Inter-AS Option C

Step-by-Step Instructions

1. Launch the **L3VPN/6VPE** protocol wizard and perform the tasks in sequence as depicted in the below images to configure BGP peer between Router Reflectors to advertise VPN routes with correct next-hop address.

   Select only the first port to configure.

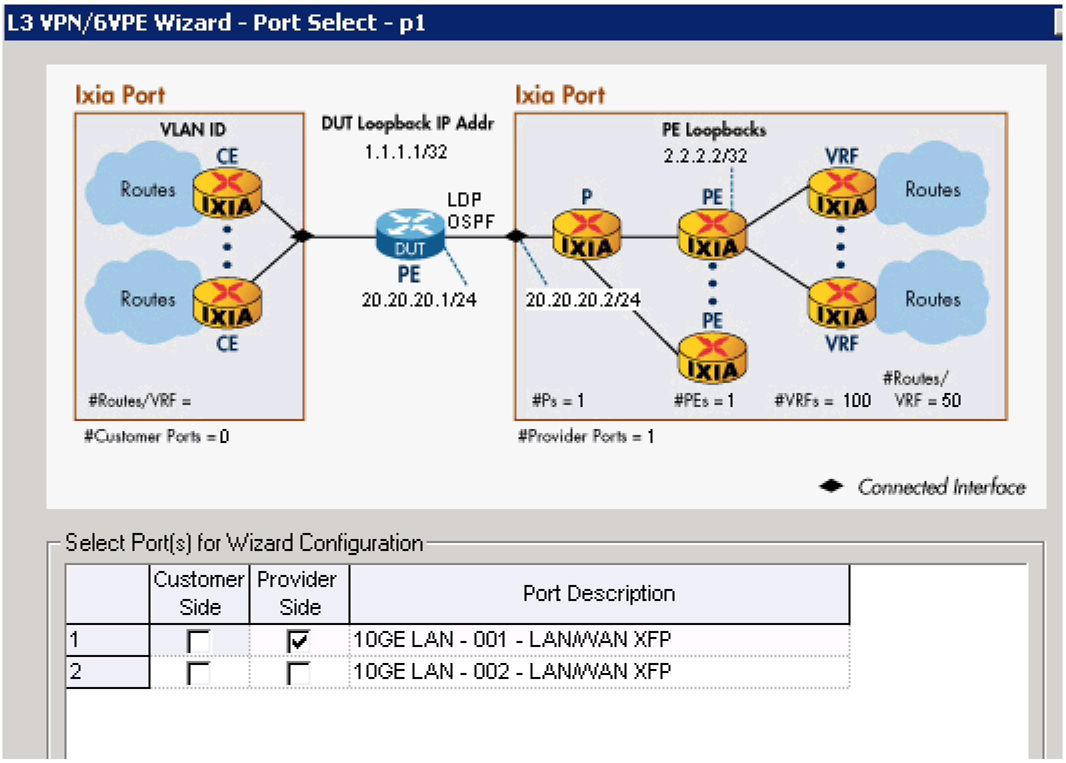


Figure 244. Select Test Port(s)

Enter the emulated P router (ASBR) information

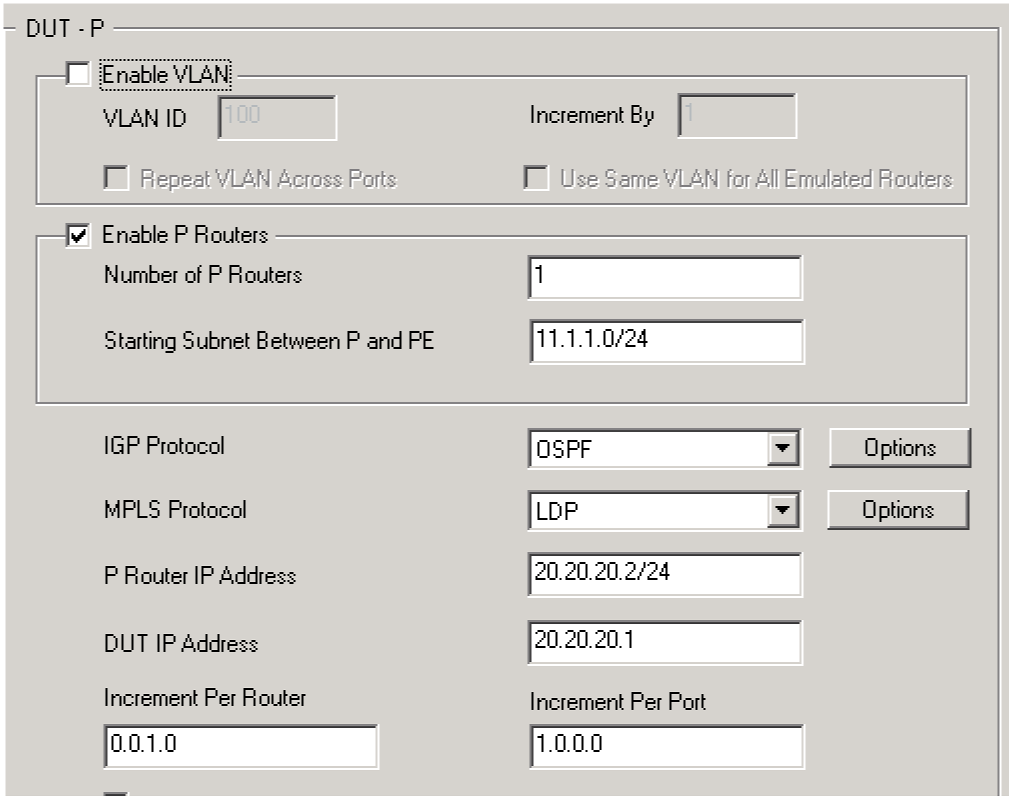


Figure 245. Configure P Router

Enter 1 PE router behind the P – the PE will be the emulated RR

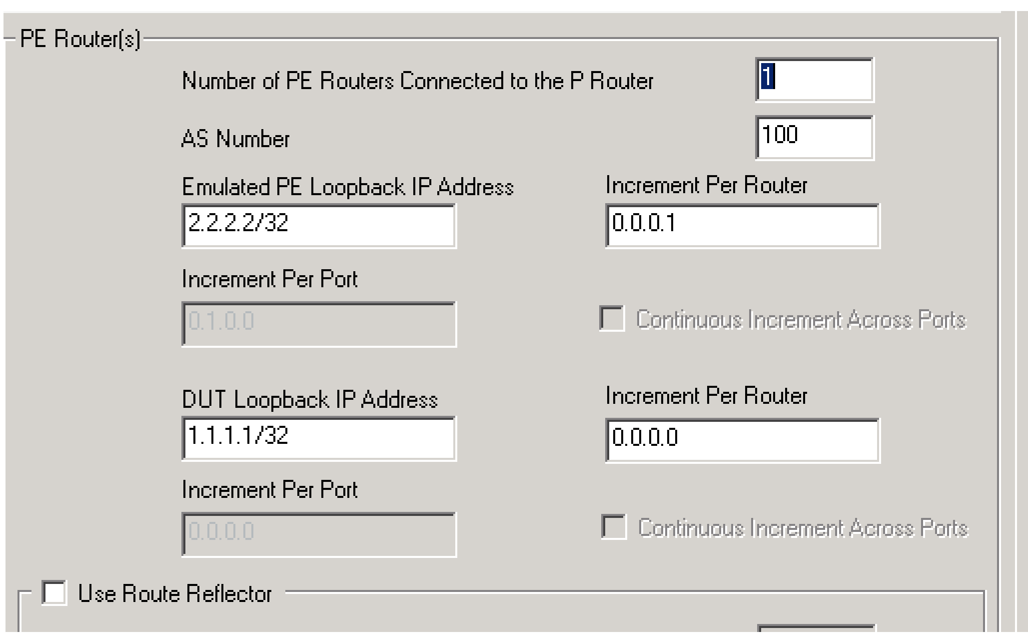


Figure 246. Configure the PE Router

For example, enter total number of VPNs to advertise to DUT as 100. Also input the number of VRF routes per VPN and its start value. In the VRF Configure Mode drop-down list, select **One VRF per VRF Range**.

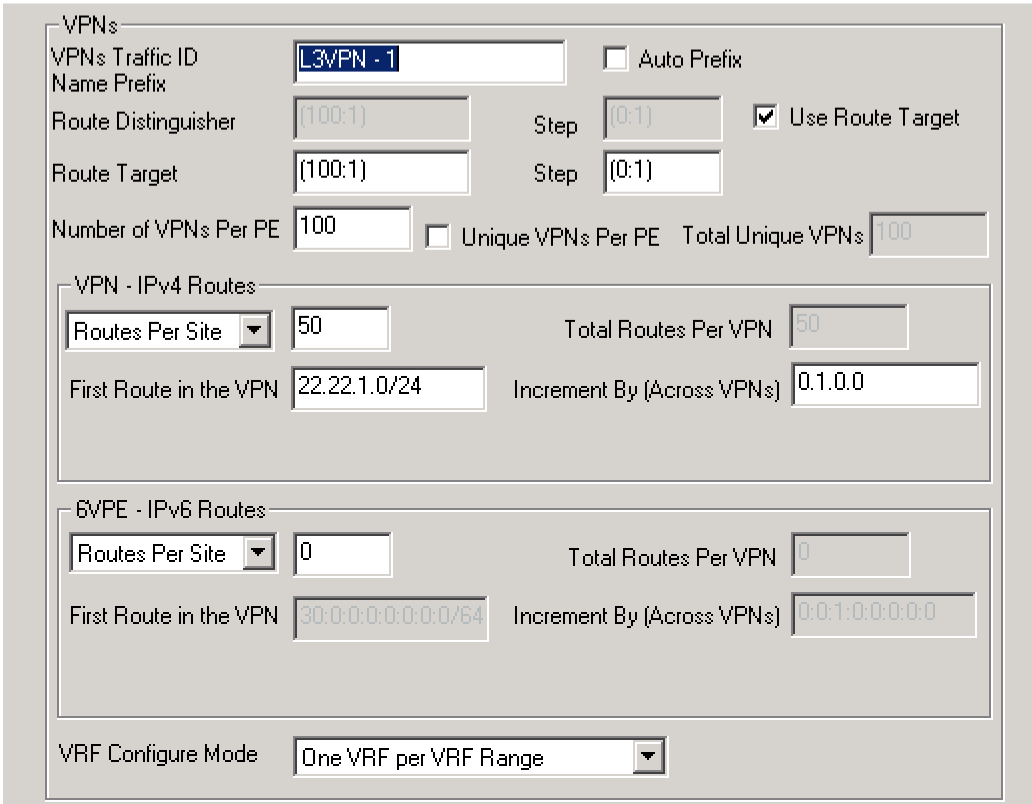


Figure 247. Configure the Number of VPNs and VPN Parameters

Give a name and overwrite the configuration as depicted below.

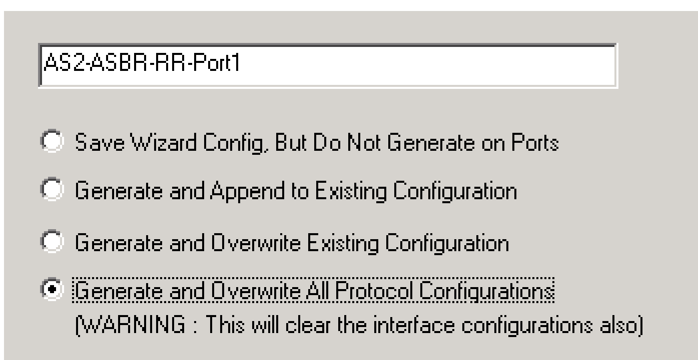


Figure 248. Save and Overwrite the Config

2. Manually modify the wizard generated configuration. First, disable OSPF and LDP – Inter-AS VPN does not require LDP or OSPF.

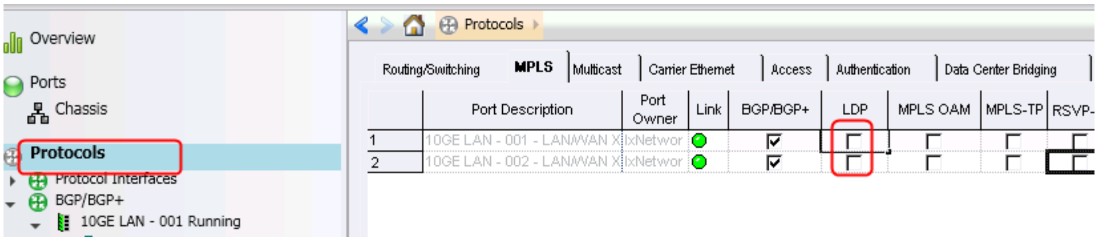


Figure 249. Disable All Unwanted Protocols

3. Now change the number of BGP peers to 2 from 1. The wizard only generated the BGP peer for VRF route exchange, not the BGP between ASBR.

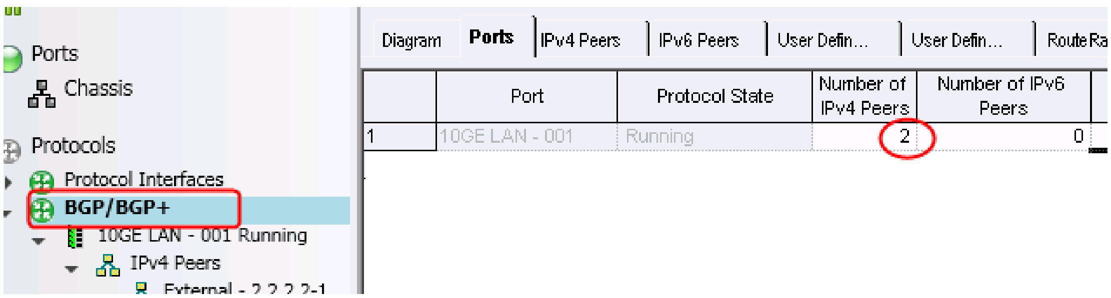


Figure 250. Increase the Number of BGP Peers

4. Change the two BGP peers to be **External** from Internal as generated by the wizard. Select the BGP peer between the ASBR (P) routers as **IS ASBR**. Enter DUT IP for the ASBR peer, and input the correct AS number per your test setup. Also enter 1 for **No. of MPLS RouteRanges** for advertising PE loopback addresses with labels. Make sure the **Learned Routes Filters** is enabled with **Filter IPv4 MPLS** for ASBR peer and **Filter IPv4 MPLS/VPN** for the RR peer.

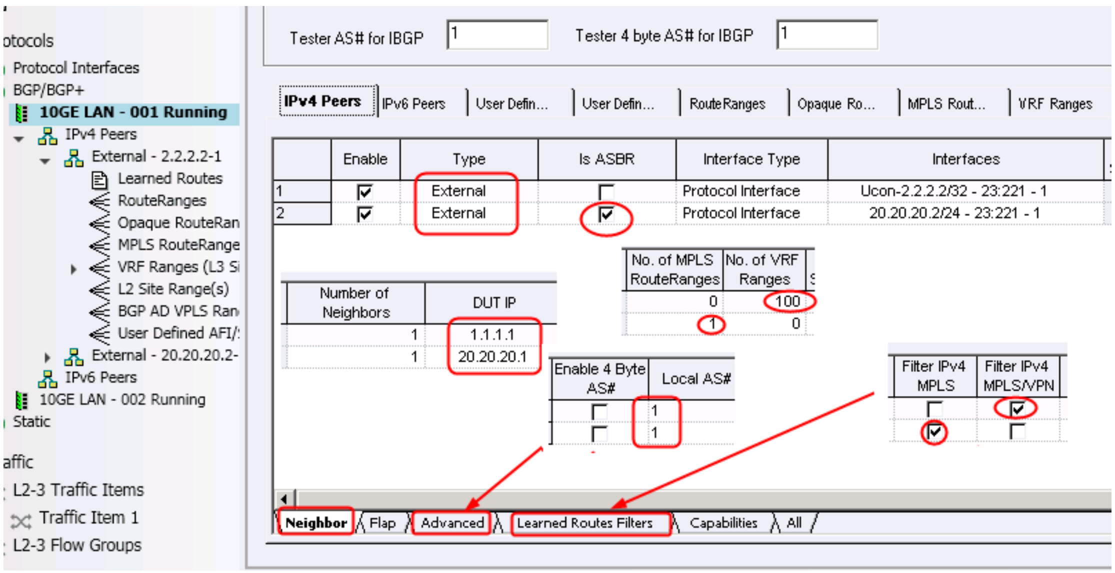
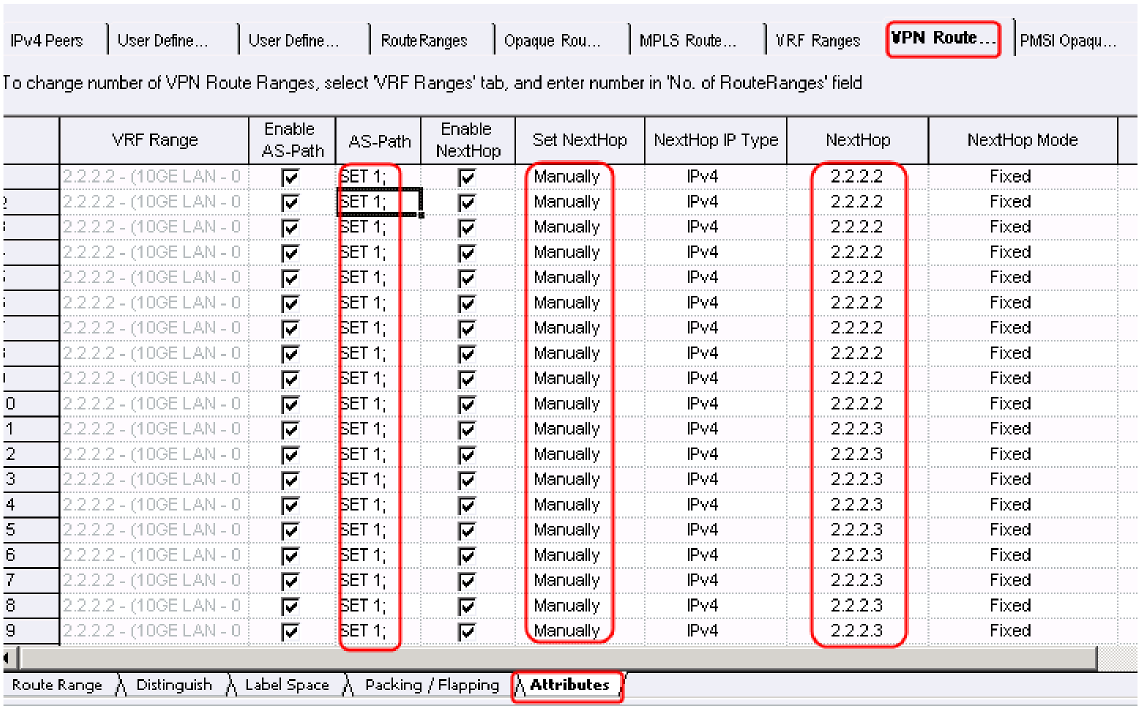


Figure 251. Manual Tweak on BGP Peers

5. Go to RR peer and modify **AS-PATH**, **Set NextHop**, and **NextHop** value; and the **NextHop Mode** as depicted in the following image.



	VRF Range	Enable AS-Path	AS-Path	Enable NextHop	Set NextHop	NextHop IP Type	NextHop	NextHop Mode
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
0	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.2	Fixed
1	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
2	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
3	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
4	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
5	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
6	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
7	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
8	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed
9	2.2.2.2 - (10GE LAN - 0	☑	SET 1;	☑	Manually	IPv4	2.2.2.3	Fixed

Figure 252. Make VRF Route Changes

Use the following tips to perform large scale configuration: to simulate 10 PE routers that have advertised those 100 VPNs. Click the **NextHop** header to highlight the entire column, and then right click to select **Increment By**. Enter **Step Size** as 1, select **Enable Repeat Value** check box, and enter value as 10. This configuration results in first 10 VPN to have next hop as 2.2.2.2, and then the next 10 VPN to have next hop as 2.2.2.3, and so on.

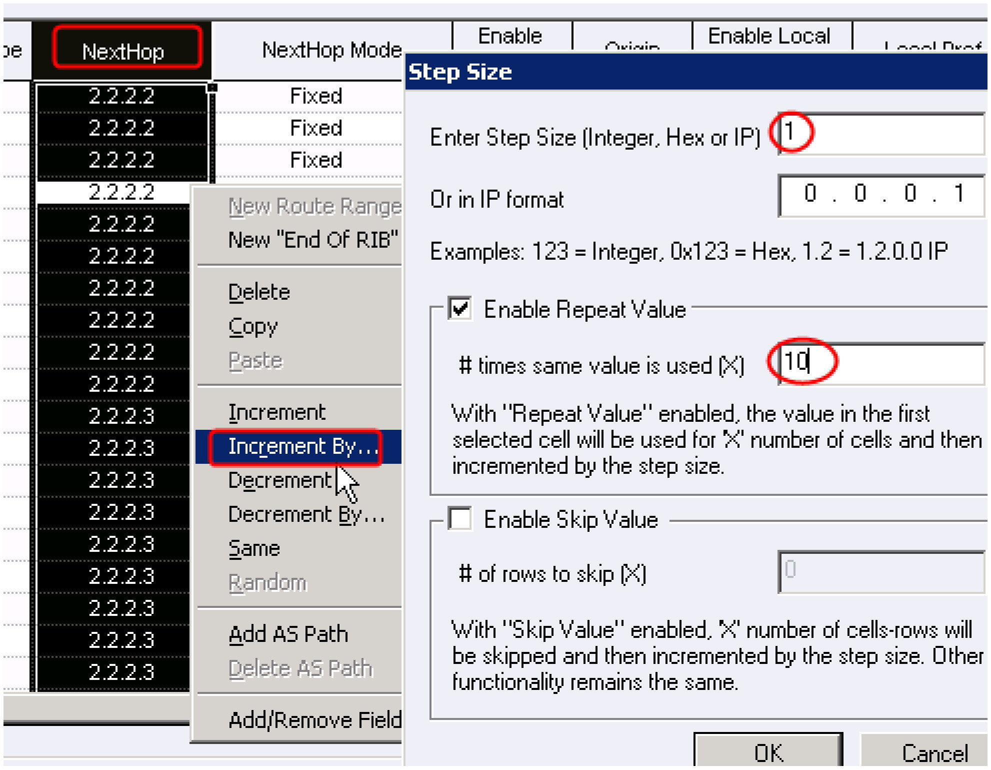


Figure 253. Flexible Increment By Options

6. In the final step, change the MPLS route advertisement to match the PE router loopback. A total of 10 PE routers are emulated. Thus, a total of 10 MPLS Routes are advertised with labels.

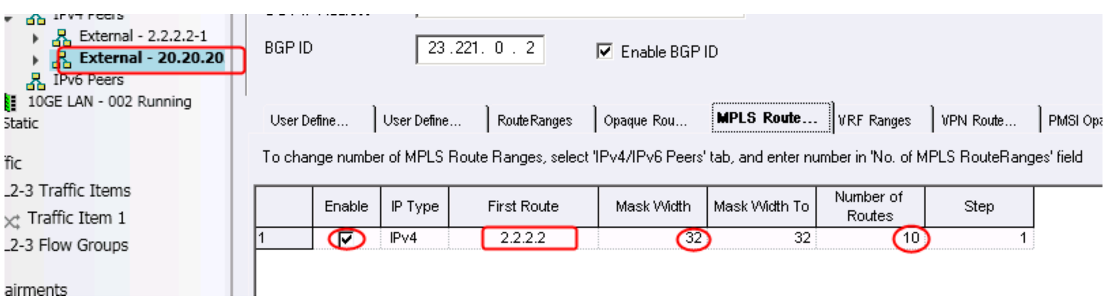


Figure 254. Advertise PE Loopbacks

7. Start both BGP sessions and ensure that the control plane stats as well as the Learned Info display correct info before proceeding with traffic.

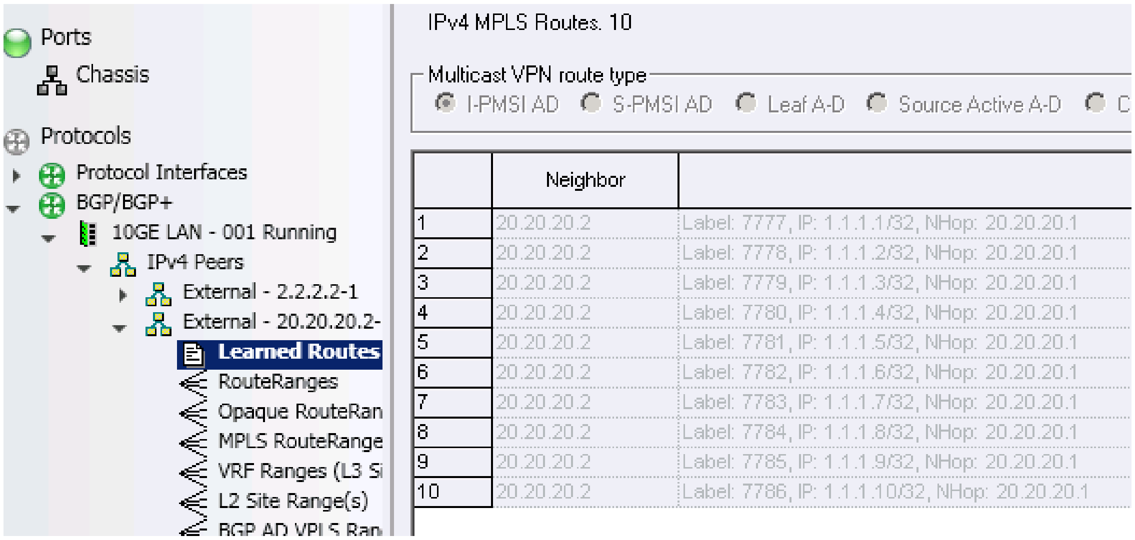


Figure 255. ASBR Learned Loopbacks

8. Once the control plane works as expected, it's time to build and send traffic. Launch the traffic wizard and select the VRF routes for both Source and Destination. Keep One-One mapping if the number of VRFs in each test port is symmetric. Otherwise, use Traffic Group ID to avoid cross-talk – a technique well documented in the L3VPN test case of this book. Make sure the "Max # of VPN Label Stack" is 2 (or 3). The traffic wizard is equipped with intelligence to resolve the right amount of labels.

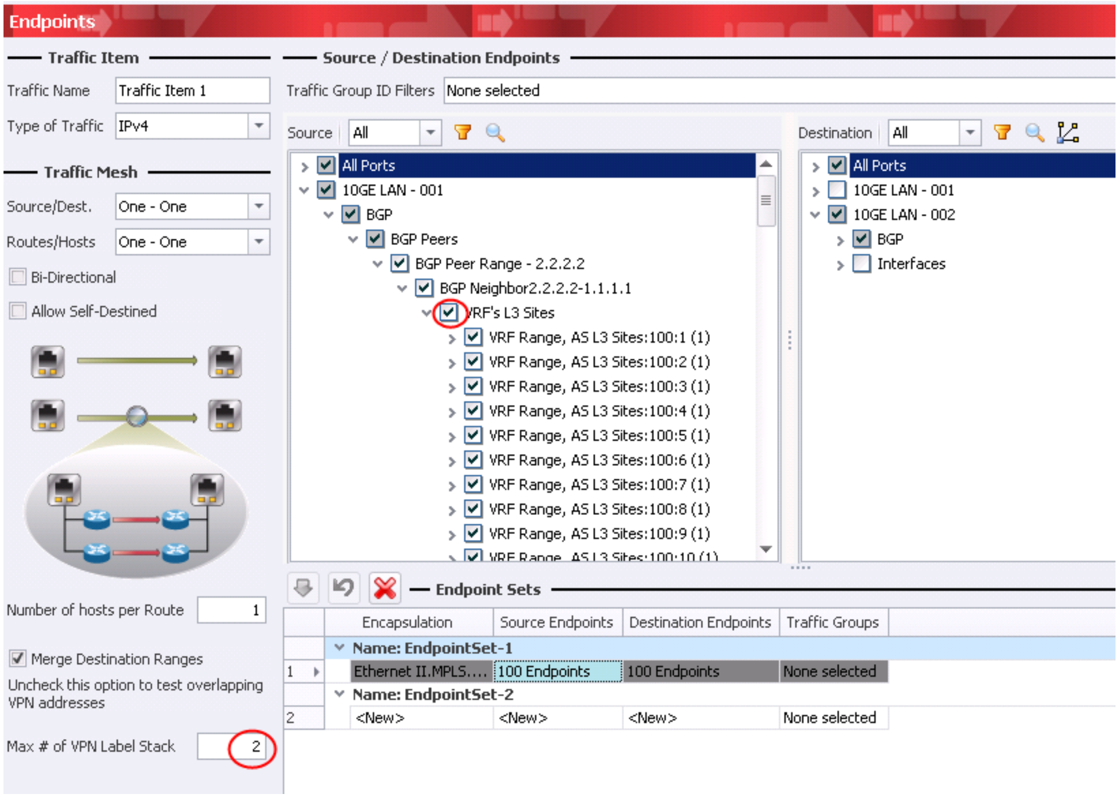


Figure 256. Select Traffic End Points

9. In the **Flow Tracking** page, it's recommended using "**MPLS Flow Descriptor**"

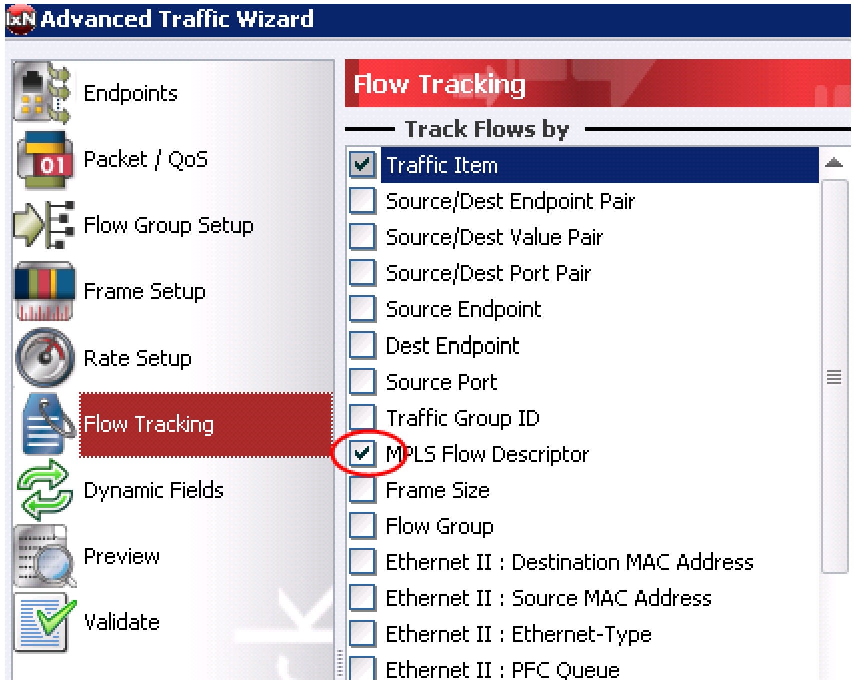


Figure 257. Set Tracking Option

10. In the **Dynamic Fields** page, keep the default **Transport LSP Label Provider Preference**, and the **Inter AS/Reigion LSP Label Provider Preference.**

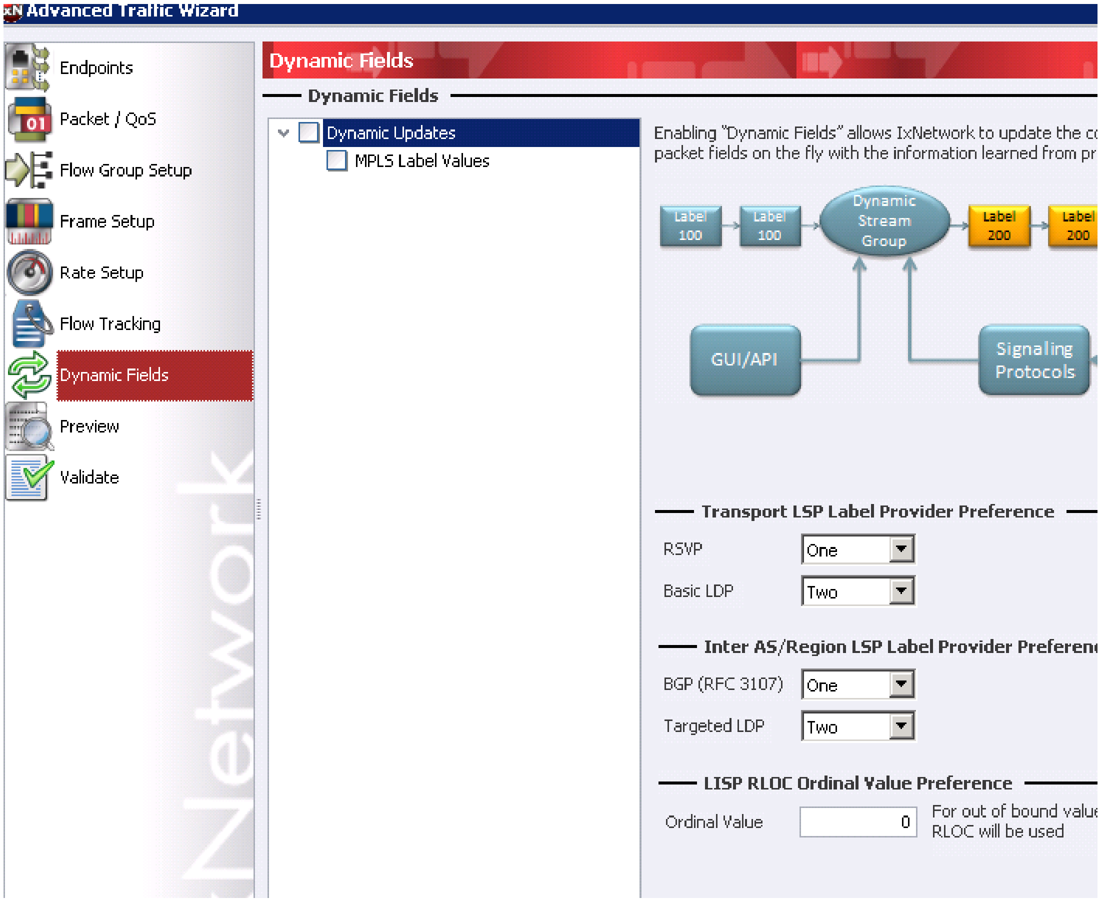


Figure 258. Default Label Preference List

11. Finish the traffic wizard and go to flow editor to manually examine generated packets to ensure they contain 2 labels with the outer label from ASBR advertisement, and the inner from RR advertisement.

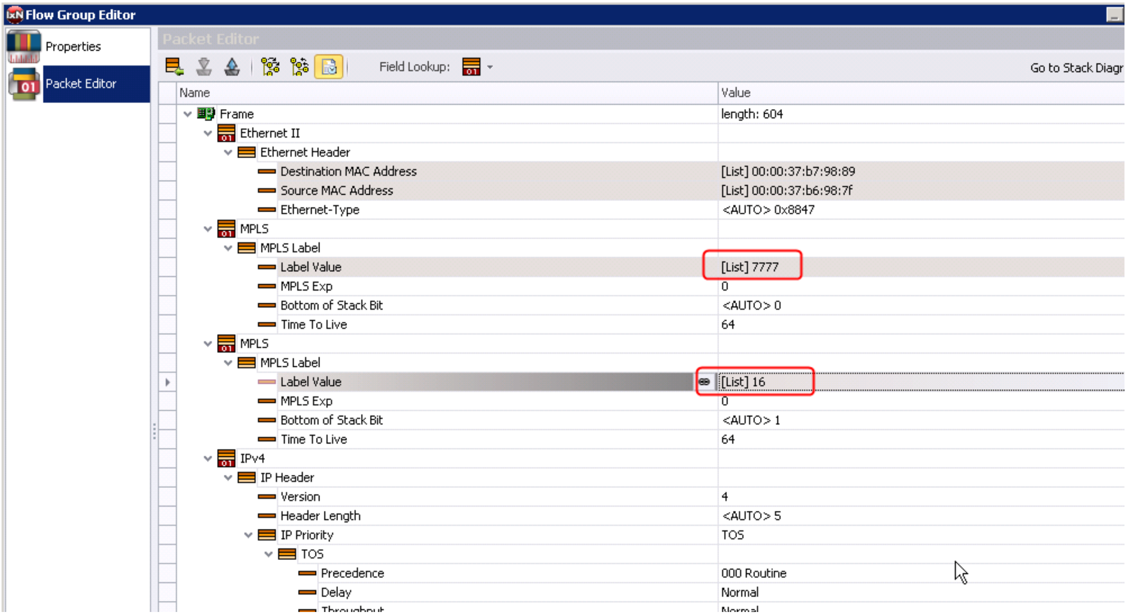


Figure 259. Verify Label Binding via Packet Editor

12. The configuration of the second test port to emulate regular L3VPN PE router is fairly straightforward and need no extra description. Refer to L3VPN test case for example configuration. The difference between a PE in a regular L3VPN case and a PE in an L3VPN environment with RR that connects to another AS, and an ASBR to advertise and receive PE loopback addresses is that the regular PE router not only receives VRF route advertisement, but also the PE loopback with labels from the other AS. In building traffic as an ingress PE, it must build the label stack according to following sequence: Outer label from LDP or RSVP-TE, middle label from RR advertised as MPLS routes and inner label from RR as VRF routes. This can be easily verified from the flow editor:

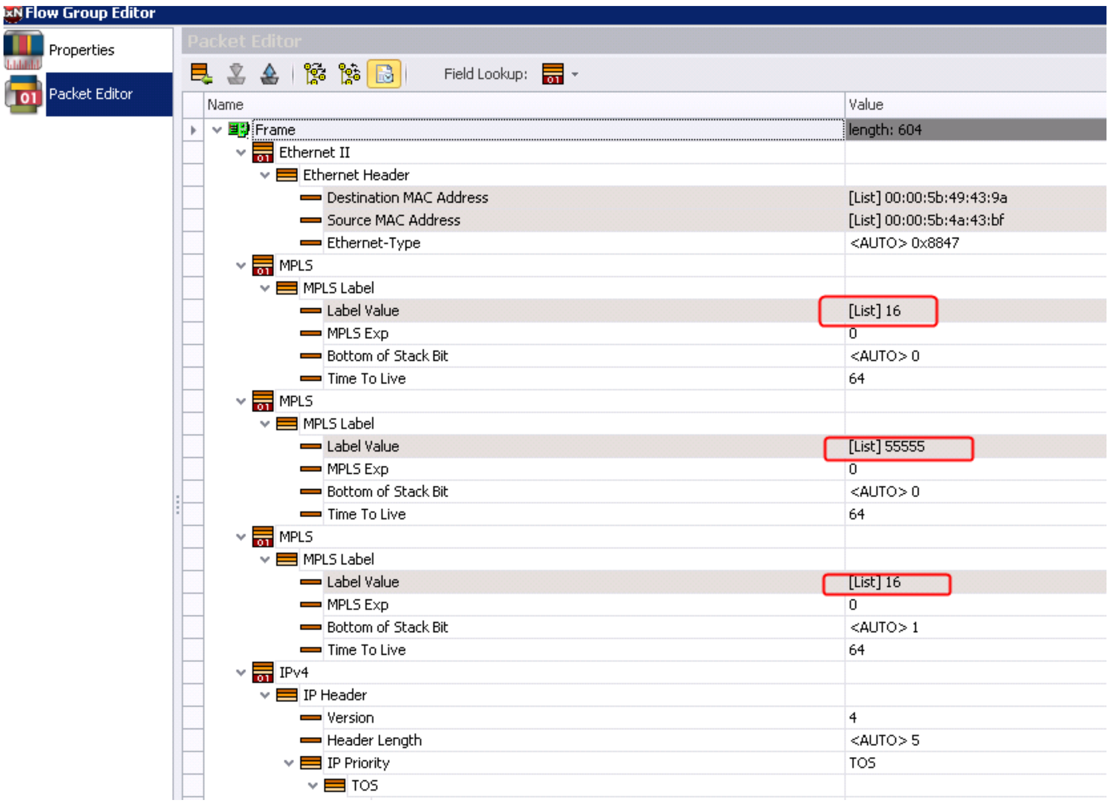


Figure 260. Verify Label Binding on The Other Test Port

Test Variables

Consider the following variables to add in the test to make the overall test plan better.

Performance Variable	Description
The number of PE routers and the number of VPNs in the AS2 emulated by Ixia test port 1	Functionality and scalability are two different test types. It is common practice to ensure functionality working before expanding the test config for scalability test. Two most obvious dimensions one can scale the test into is the number of PE routers and the total number of VPNs emulated by Ixia test port in AS2. This stretches not only the control plane but also the data plane.
The number of PE or CE routes in the AS1, collocated with DUT as ASBR	To fully stretch the DUT, scale the test not only from another AS, but also the number of PE or CE routers in the same AS as the DUT. In the case of CE emulation by Ixia, DUT performs the label binding for up to three labels and the more of VPN routes, the more stressful to the DUT.
Bidirectional traffic with various frame size and rate; optionally running RFC 2544 methodology to cycle thru packet sizes and auto find the maximum throughput/latency	Traffic is also important to test inter-AS options. Due to extra label encapsulation/de-capsulation, throughout and latency do matter to inter-AS traffic, in addition to frame size and traffic rate.

Conclusions

Ixia's IxNetwork offers the comprehensive test solution for all Inter-AS options (A, B, and C), not only from control plane perspective, but also from the data plane. The control plane emulation offers full scalability in terms of emulated number PEs, VRFs, CEs; and the data plane auto resolve the needed MPLS labels, up to three labels. The traffic auto resolution without user intervention is the attractive feature of the test solution, which makes Inter-AS VPN testing extremely easy and scalable.

Introduction to Seamless MPLS

MPLS as an established and well known technology is widely deployed in today's core and aggregation/metro area networks. Many metro area networks are already based on MPLS delivering Ethernet services to residential and business customers. Until now, those deployments are usually done in different domains; for example, core and metro area networks are handled as separate MPLS domains.

Seamless MPLS extends the core domain and integrates aggregation and access domains into a **single** MPLS domain (Seamless MPLS). This enables a very flexible deployment of an **end to end** service delivery. In order to obtain a highly scalable architecture, Seamless MPLS takes into account that typical access devices (DSLAMs, MSAN) are lacking some advanced MPLS features, and may have more scalability limitations. Hence access devices are kept as simple as possible.

Below is a diagram that illustrates how an inter-regional VPLS is made possible with the labeled BGP (RFC 3107) session between Area Border Routers (ABR), and between ABR and PE routers in its own OSPF area.

The entire network is composed of three subnetworks each located in different geographic area/administrative zone. The ultimate goal is to bridge VPLS services in area 1 to the same VPLS services in area 2, across the core network which belongs to a total different area. The key to glue all these together is the labeled BGP, which sometimes is also known as infrastructure BGP as defined by RFC 3107.

If we denote an RFC 3107 BGP NLRI route to destination D with label L and next-hop N as [D, L, N], we can look at how the route, label, and next-hop are exchanged from Area 1 to Area 2 (Left to Right in below picture). PE1 advertises its own loopback with label 3 and next-hop self [PE1, 3, PE1] to ABR1 through the iBGP session within Area 1. ABR1 then advertises PE1 loopback with its own label L12’ and next-hop ABR1 [PE1, L12’, ABR1] to ABR2 through a separate iBGP session between ABR1 and ABR2, which are located in the same area (Area 0). ABR2 needs to further advertise the PE1 loopback with new label L11’ and next-hop ABR2 [PE1, L11’, ABR2] to PE2 in Area 2 through yet another BGP peer. In parallel, both PE1 and PE2 advertise VPLS instances with the Router Reflector sitting in Area 0 through a totally different BGP session (iBGP or eBGP). VPLS instances advertised by PE1 and PE2 carry PE1 and PE2 as its next-hop respectively. With that, PE2 has all the information needed to forward traffic source from VPLS instances served by itself and destined to the VPLS instances served by remote PE1. The label resolution process works as follows:

1. VPLS instances label is learned from RR with the next-hop as PE1
2. To reach PE1, PE 2 searches its learned database and finds an entry [PE1, L11’, ABR2]. This indicates that L11’ must be placed before VPLS label, and more importantly, it must continue searching for how to get to next-hop ABR2.

3. To reach ABR2, PE2 found an LDP label association with ABR2 [ABR2, L2'] advertised through basic LDP with transport address as ABR2. PE2 hits the very bottom of label resolution process as the next-hop is itself and there is no need to continue with the label resolution.

4. PE2 then encapsulates the VPLS traffic with [L2', L11', L0'] from outer to inner order.

5. Once traffic reaches ABR2, iASBR2 repeats the same label resolution process as done in PE2. The VPLS instance label is intact, but its next-hop PE1 must be re-looked up in ABR2's learned database. It found [PE1, L12', ABR1] entry for reaching PE1, therefore it puts L12' before L0' and continues to search how to get to ABR1. It then uses the learned LDP or RSVP-TE label to move packets from ABR2 to ABR1.

6. When ABR1 receives the traffic from ABR2, it also performs the same label resolution process: pop up both transport labels and keep the VPLS instance label; find out what is the label to reach next-hop PE1; and who is the next-hop to PE1.

7. When traffic finally reaches PE1, PE1 uses the VPLS instance label to distribute the traffic to the right CE router.

8. The same process is performed in parallel in the other direction from PE1 to PE2.

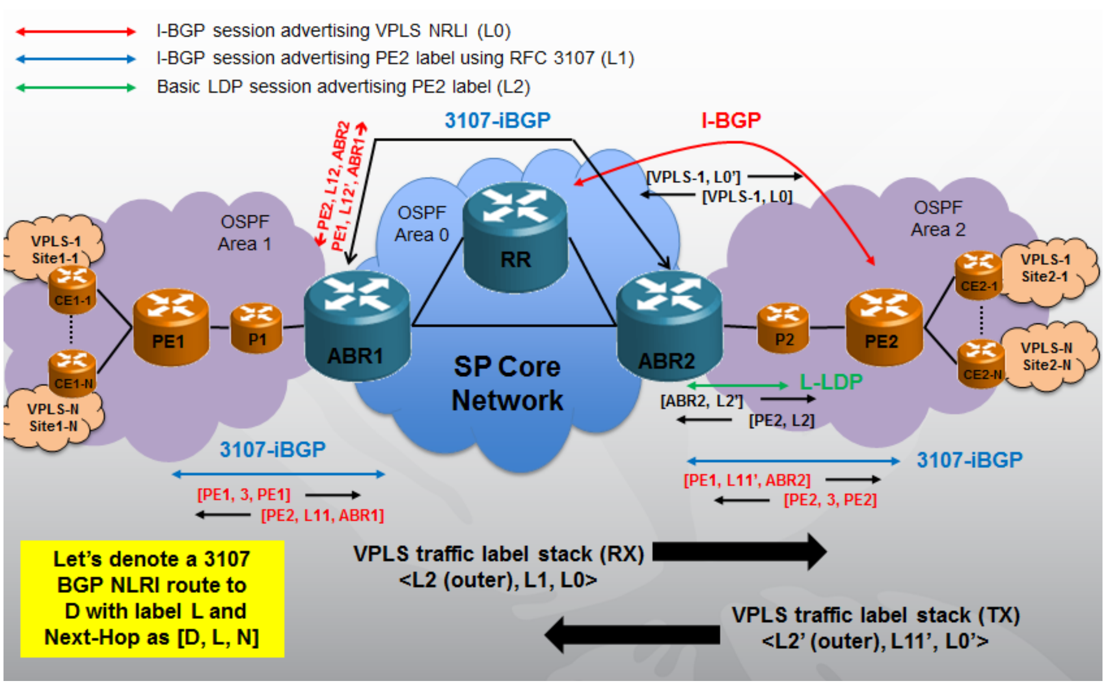


Figure 261. Seamless MPLS Topology – How Does It Work?

Relevant Standards

Seamless MPLS Architecture: draft-ietf-mpls-seamless-mpls-01

Carrying Label Information in BGP-4: RFC 3107

Test Case: Testing Seamless MPLS with Scalability

Overview

The labeled BGP based on RFC 3107 provides the fastening for end to end or seamless MPLS services. The introduction section has provided detailed description about the seamless MPLS, and how it works in a real setup. Here, we focus on how to configure the IxNetwork to perform the functional as well as scalability test. You can apply the same idea to other type of MPLS services in crossing different service provider domains.

Objective

The objective is to set up IxNetwork to perform seamless MPLS functionality and scalability test. An example is provided explaining the configuration.

Setup

Two or more Ixia test ports are required in order to test seamless MPLS with end to end traffic. Each test port emulates a number of P/PE routers (and all the CE routers and VPLS instances behind). The PE routers exchange VPLS info with the RR played by a real DUT. The RR can be in the same AS or different. The P router exchanges the 3107 labeled BGP routes with the DUT ABR. Bidirectional traffic is sent and verified.

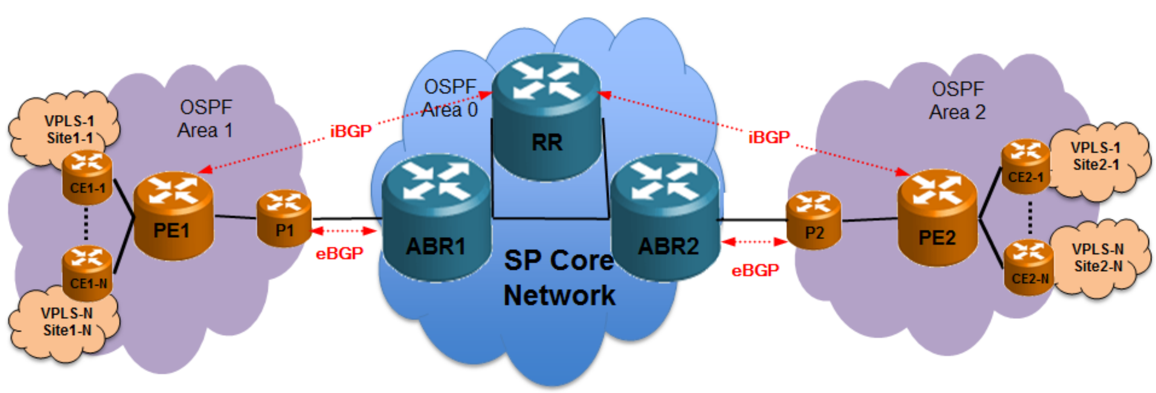


Figure 262. Seamless MPLS Test Setup

Step-by-Step Instructions

1. Launch the **L2VPN/VPLS** protocol wizard and perform the tasks as depicted in the following images as example configuration.

   Configure one test port at a time for flexibility

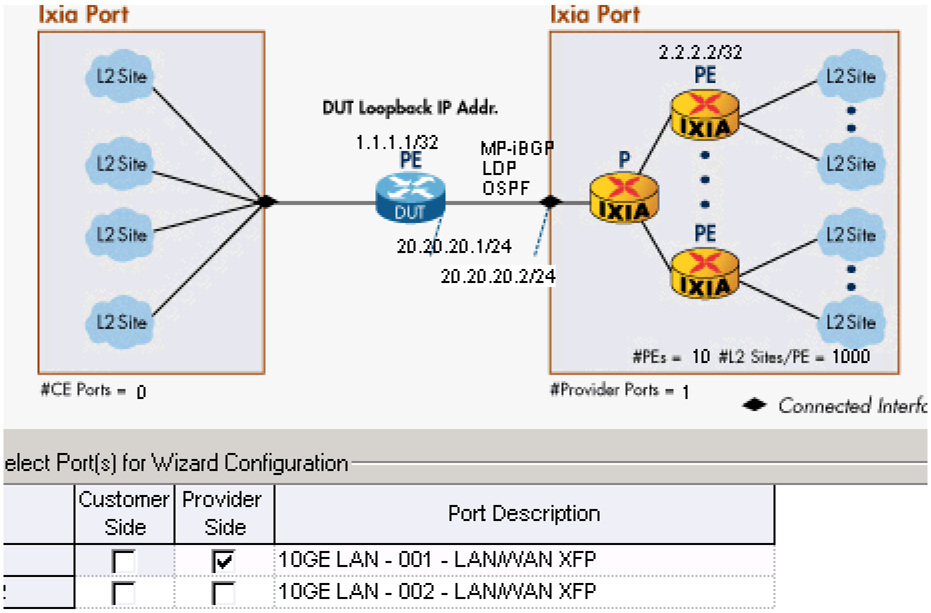


Figure 263. Select Test Port(s)

Select MP-iBPG as the L2VPN signaling protocol. This is the BGP based VPLS, also known as Kompella draft. Set the OSPF options accordingly.

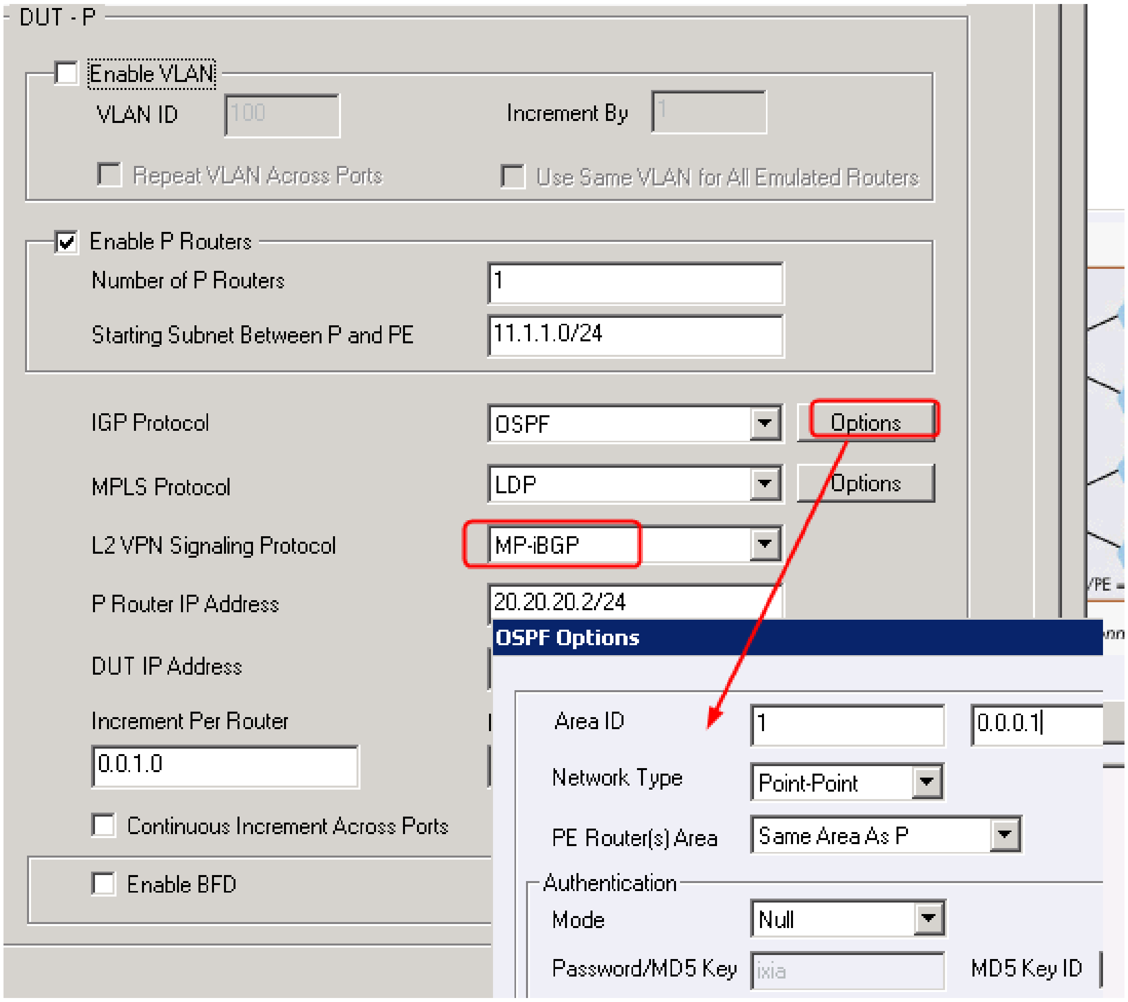


Figure 264. Configure P Router

For example, configure 10 PEs behind the single P router. These PE routers are the next-hop address for the VPLS instances advertised to the RR.

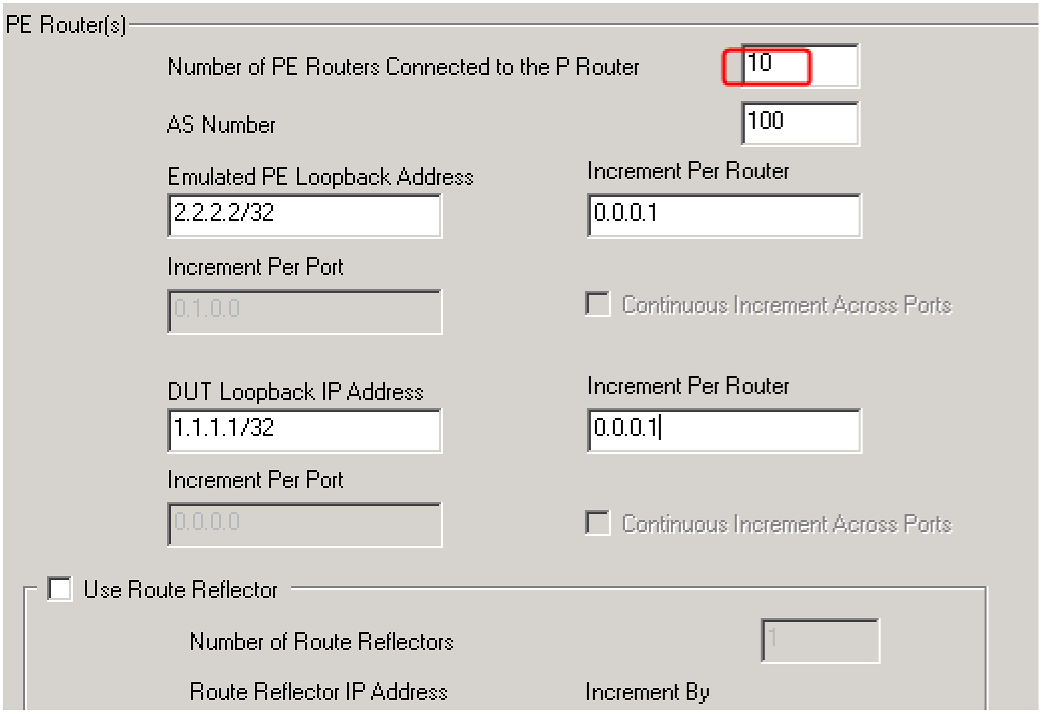


Figure 265. Configure PE Router

For example, configure 100 VPLS instances behind each PE. These VPLS instances repeat behind each of the 10 PEs creating 10 unique sites for each of the VPLS instances. Set the VE ID, as well as the label block size and offset according to your DUT setup.

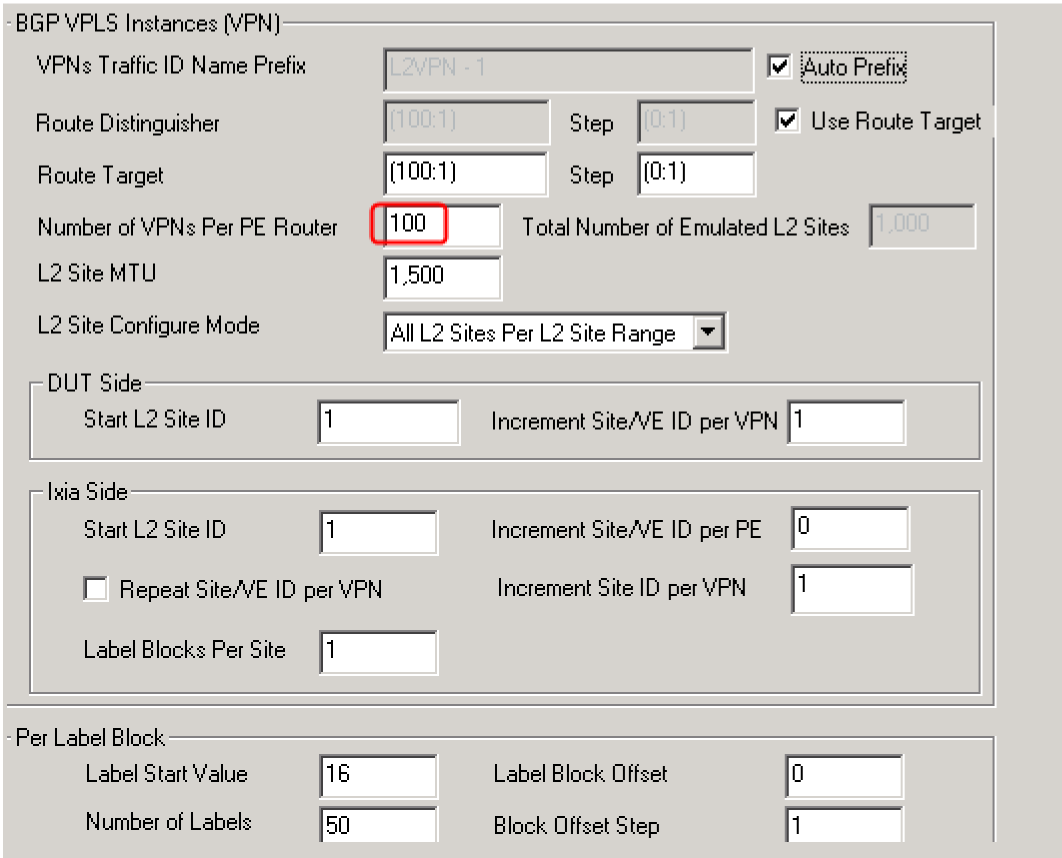


Figure 266. Configure VPLS Instances and Parameters

Set a few MAC addresses for traffic purpose

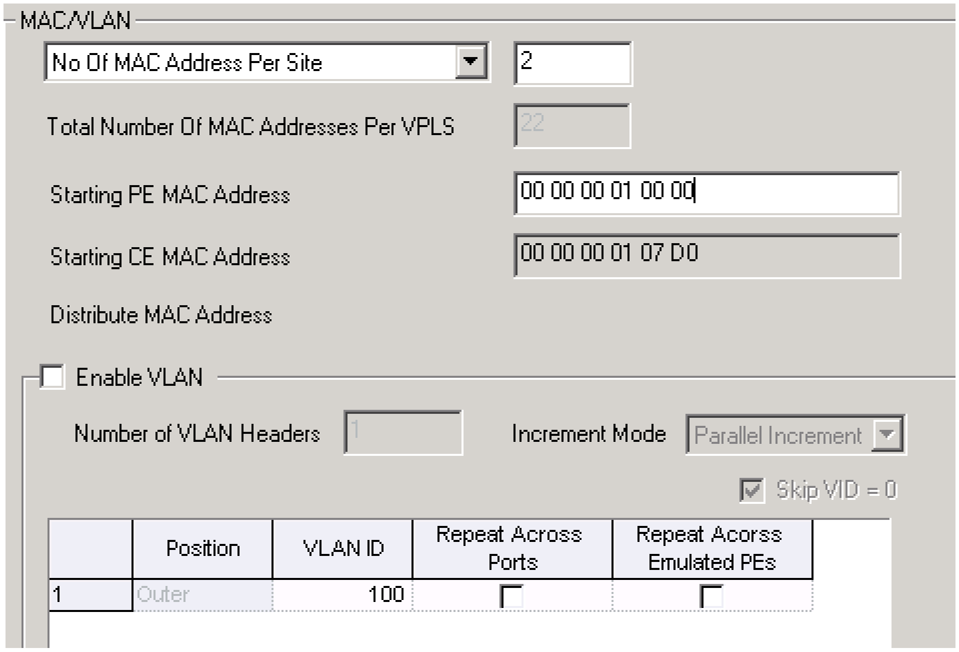


Figure 267. Configure MAC Address for VPLS Traffic

Give a name of the configuration and configure the test port

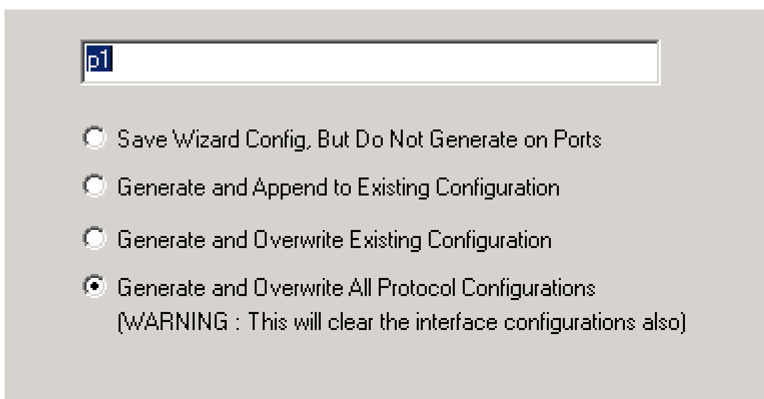


Figure 268. Save and Overwrite Config

2. Similarly, configure the test port2, with needed changes such as IP addresses, and OSPF area.

3. Customize the wizard generated configuration to suite seamless MPLS requirements. Refer to the following images for specific changes.

4. Clear the LDP check box, and, if necessary, the OSPF generated by the wizard.

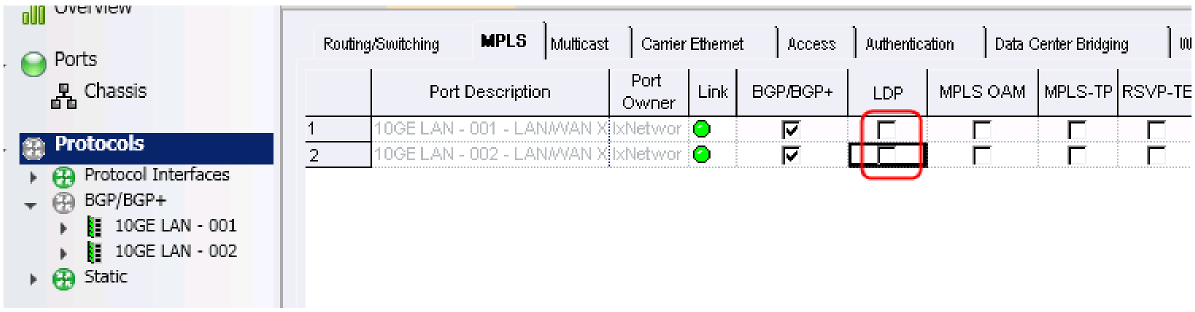


Figure 269. Disable Unwanted Protocols

5. Change the total number of BGP peers from 10 to 11, because of the RFC 3107 session.

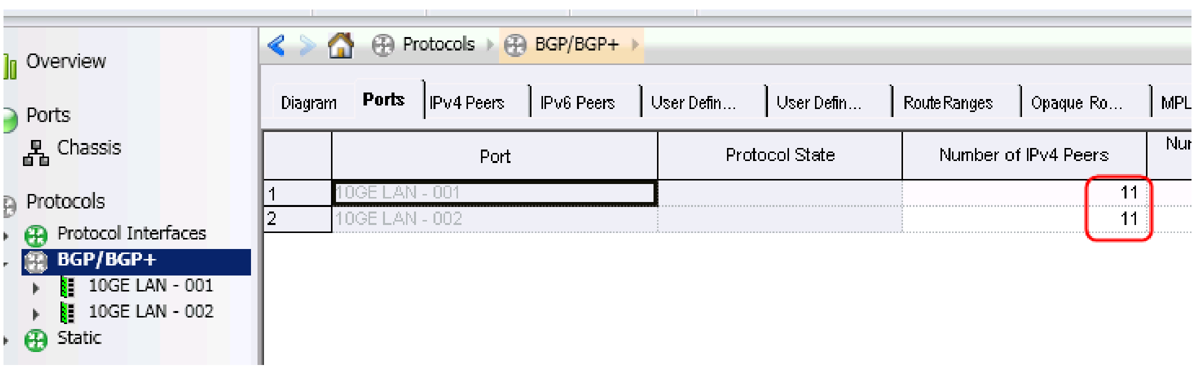


Figure 270. Change Totoal Number of BGP Peers

6. Change the RFC 3107 session to External and make sure you select **Is ASBR** check box.

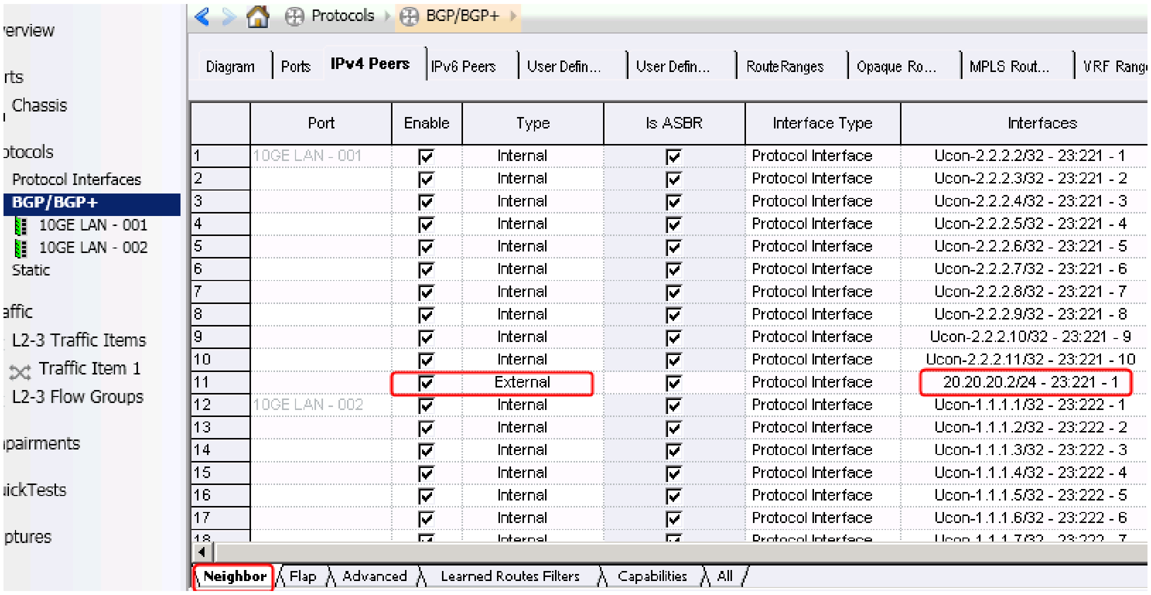


Figure 271. Change the Labeled BGP Peer to External and Enable Is ASBR Option

7. Change the peer IP address, and change **No. of MPLS RouteRanges** to 1 as depicted.

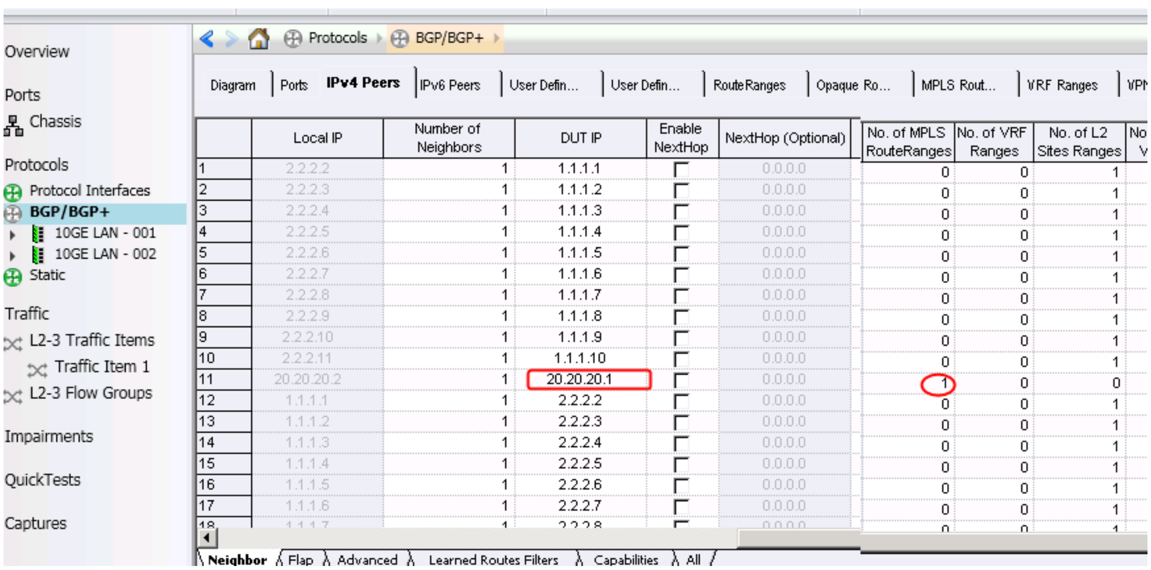


Figure 272. Change BGP Destination Addr and Add 1 MPLS Range

8. Select the **Filter IPv4 MPLS** check box to allow Learned Routes to be stored for traffic label binding.

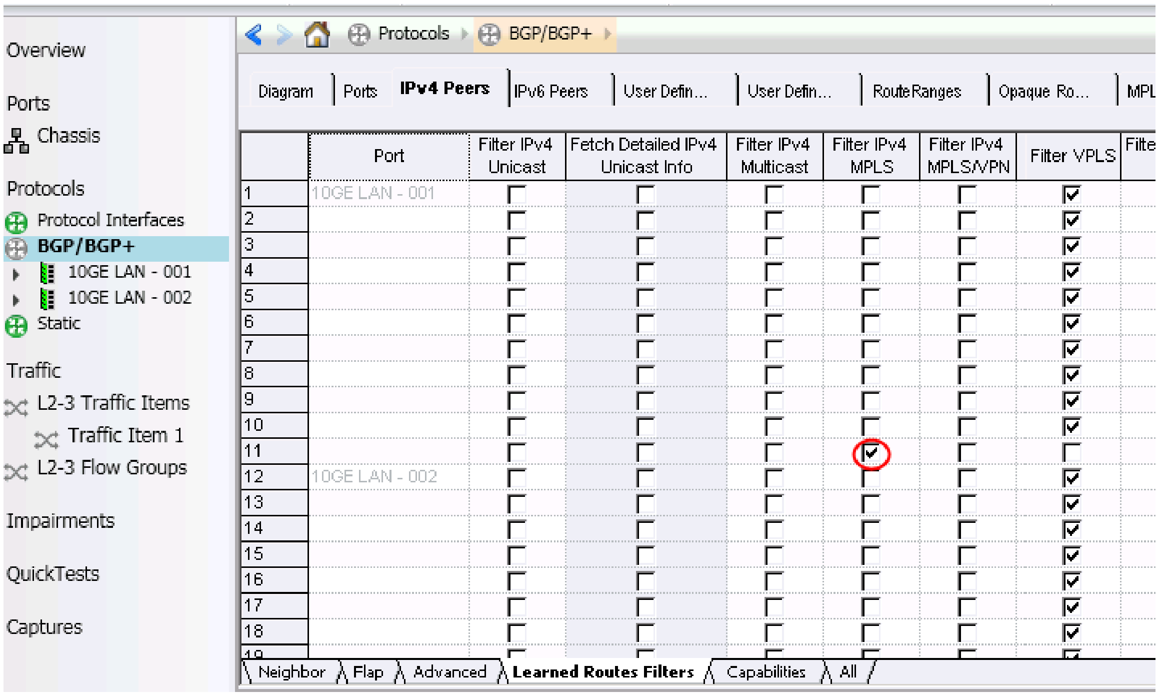


Figure 273. Enable MPLS Route Filter to Store Learned Labels

9. Modify the MPLS Route Ranges to advertise a total of 10 PE loopbacks. Optionally, modify the start MPLS label value.

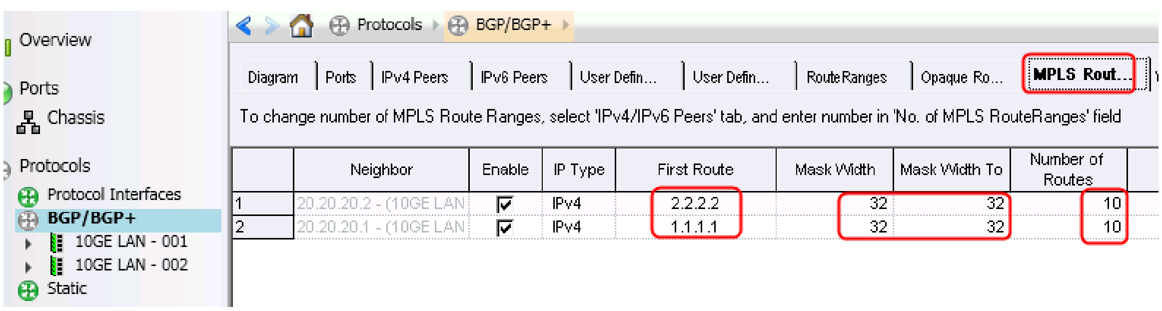


Figure 274. Configure Advertised Loopbacks

10. Select the **Expose Each L2Site as Traffic Endpoint** check box for traffic end point selection.

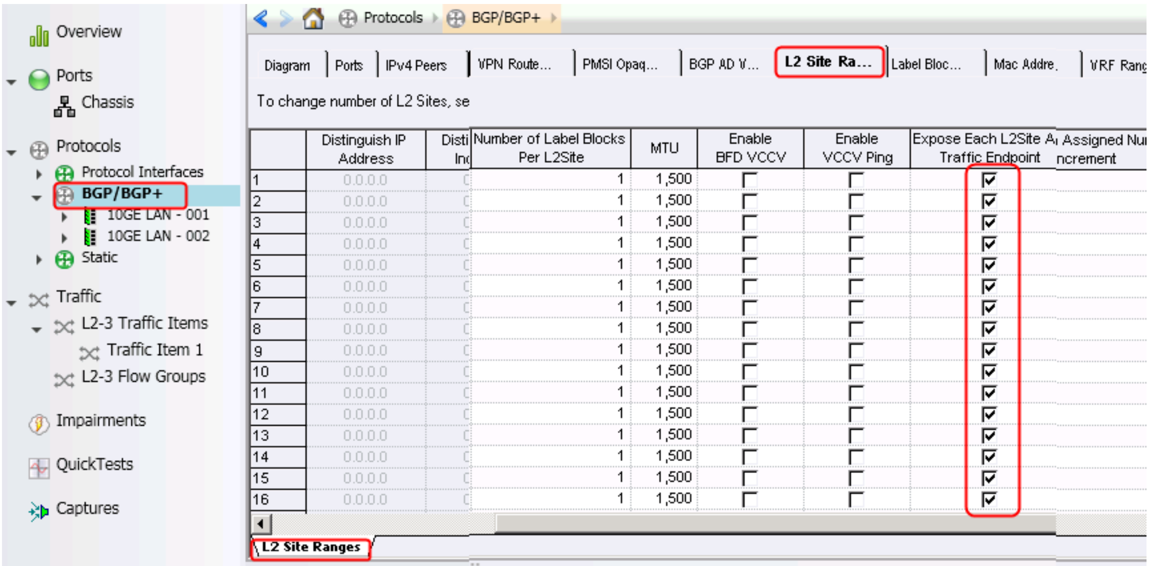


Figure 275. Expose Configured MAC to Traffic Endpoints

11. Start BGP protocols and make sure the Learned Info displays correct information.

BGP peers must be functioning.

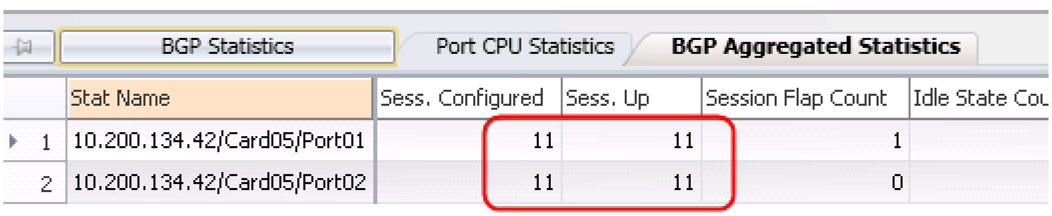


Figure 276. BGP Running Stats

The external peer (RFC 3107) shows learned far end PE loopback with MPLS labels.

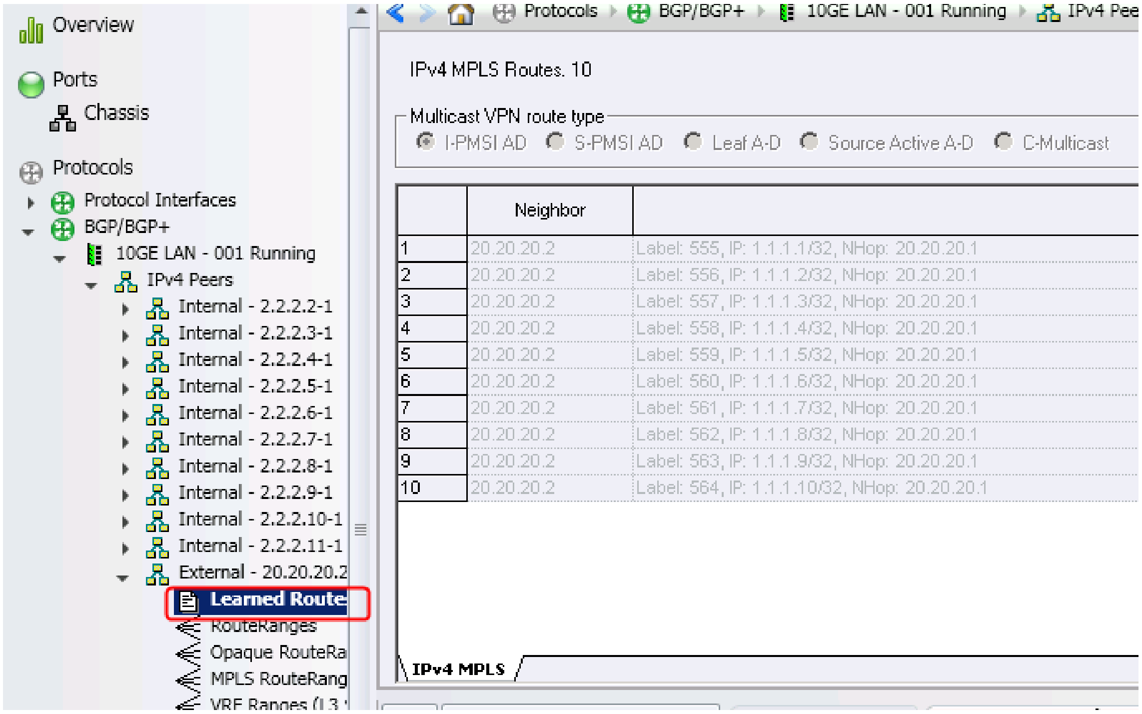


Figure 277. Labeled BGP Learned Loopbacks

Each of the internal BGP peers show the learned VPLS instance with label block information.

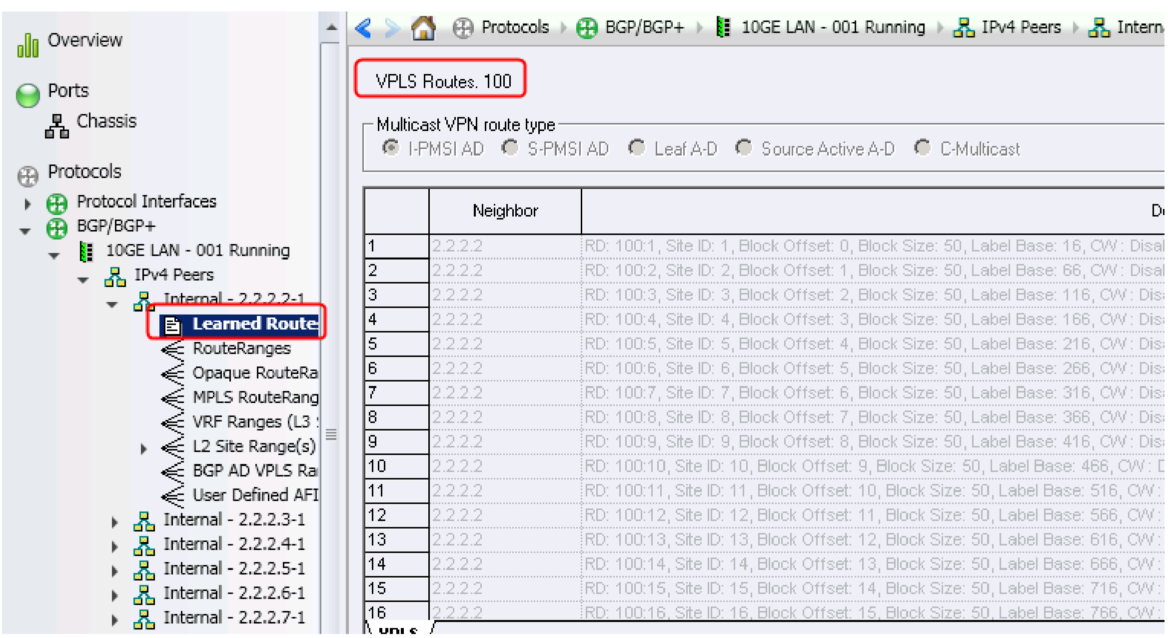


Figure 278. Learned VPLS Instances

12. Start traffic wizard.

13. Select **Etherent/VLAN** as **Type of Traffic** (we are dealing with VPLS), and then select BGP peers as both source and destiantion. You can expand to see the details of traffic end points that must correspond to the MAC address defined through VPLS wizard. Also make sure the **Max # of VPN Label Stack** is set as 2 (we are dealing with cross reginal VPN, so transport label is not needed).

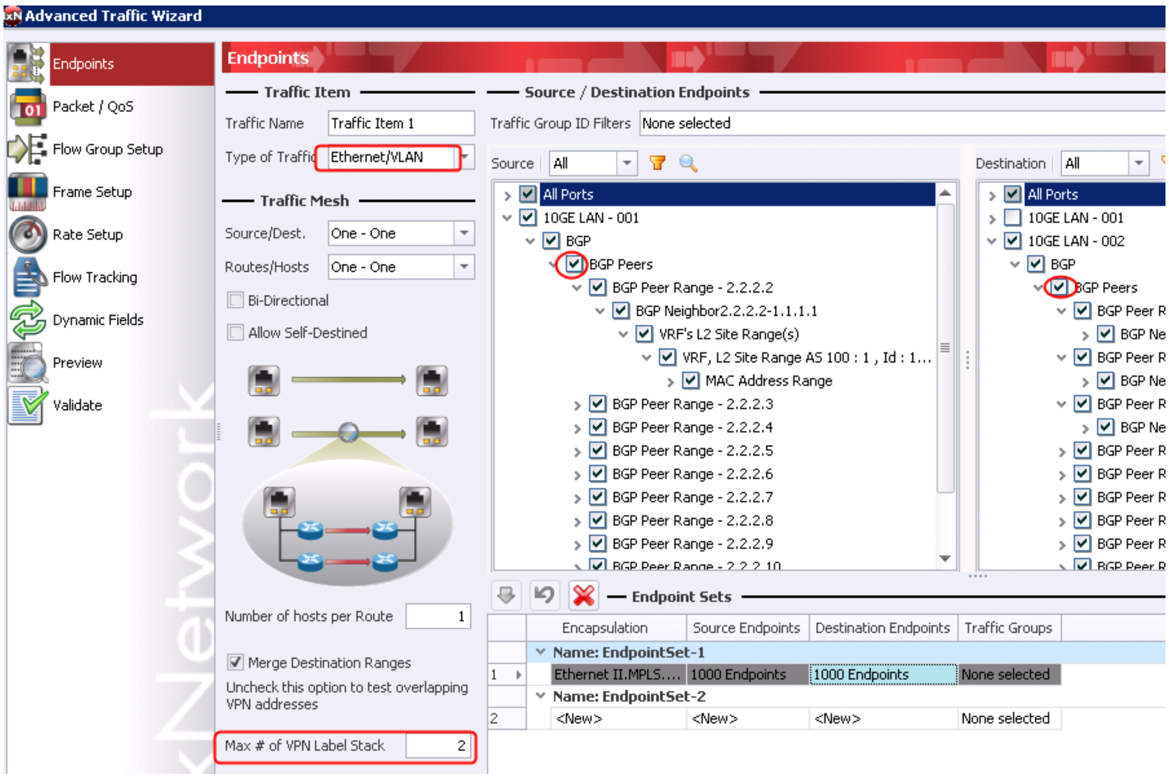


Figure 279. Select Traffic Endpoints

14. Select **MPLS Flow Description** as tracking option. It provides the most comprehensive description about an MPLS flow.

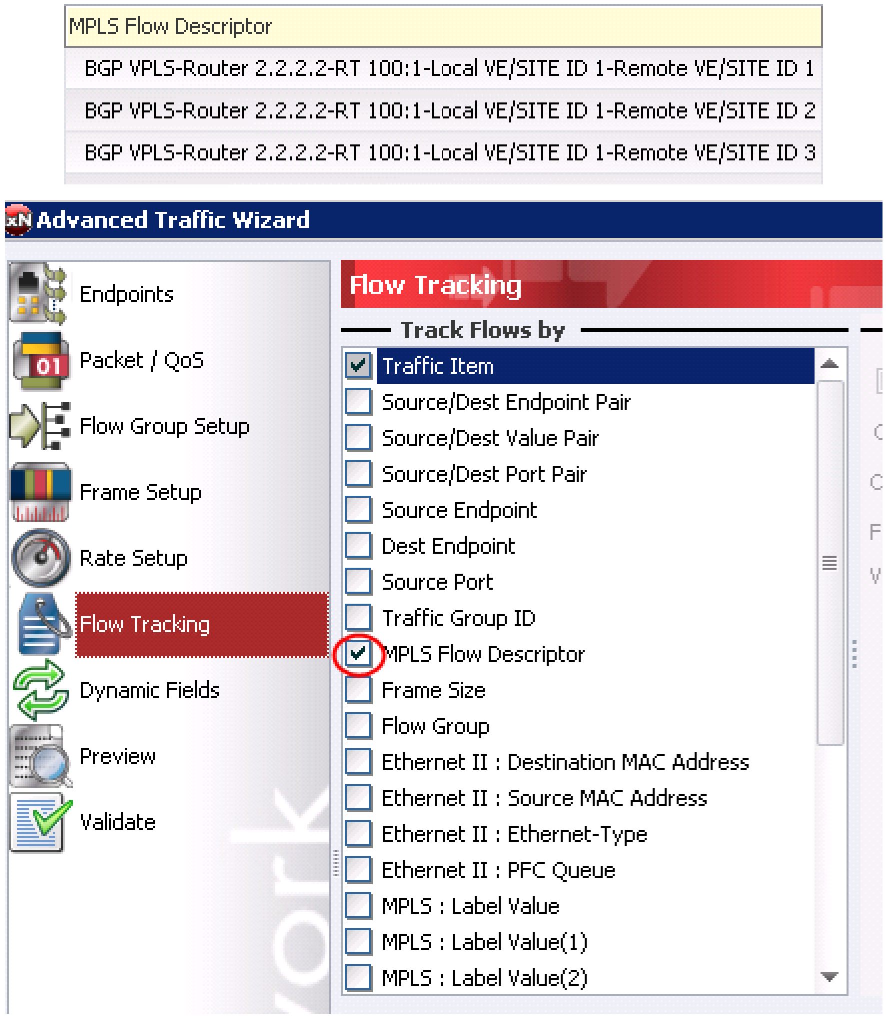


Figure 280. Select Tracking Option

15. Preserve the default value for **Inter-AS/Regional LSP Label Provider Preference**.

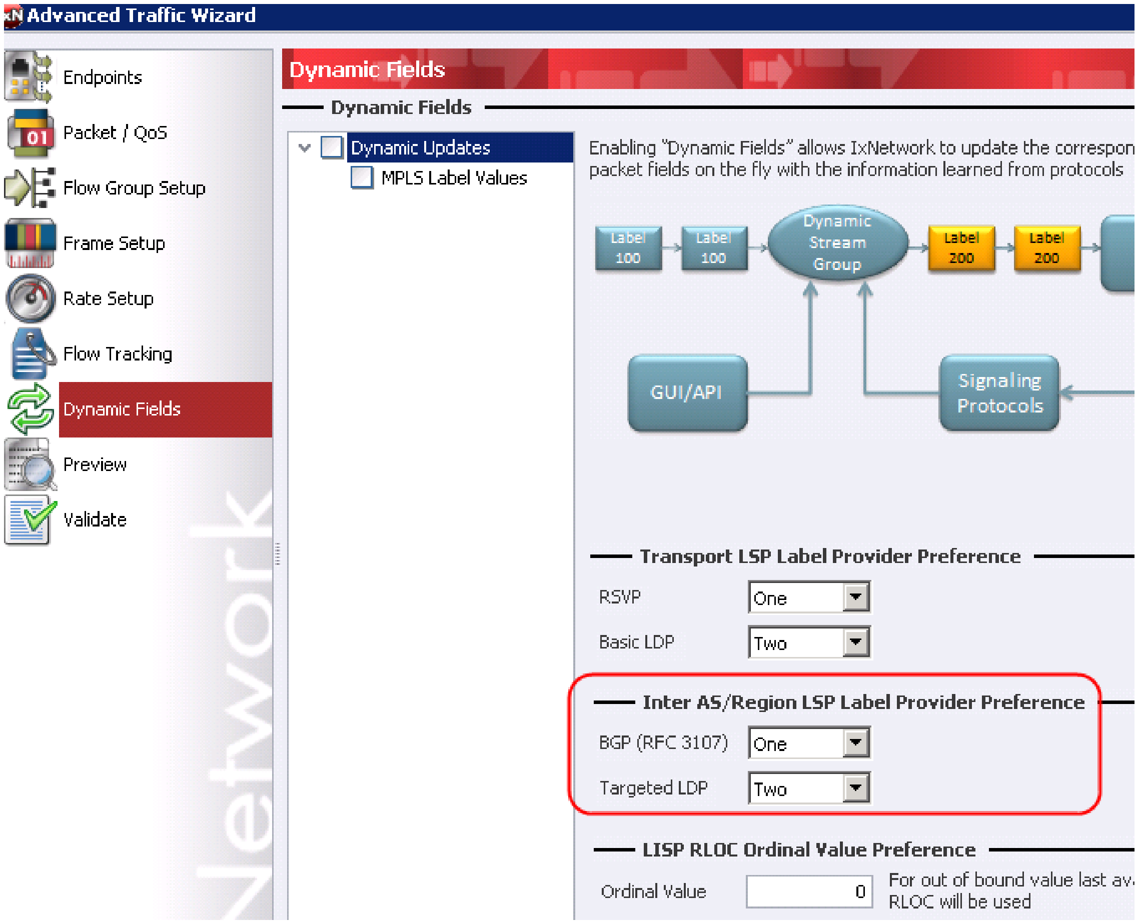


Figure 281. Default Label Preference List

16. When complete, verify the MPLS label binding using flow editor. It clearly indicates two MPLS labels being used, and they correspond to the RFC 3107 learned info as well as the VPLS learned info.

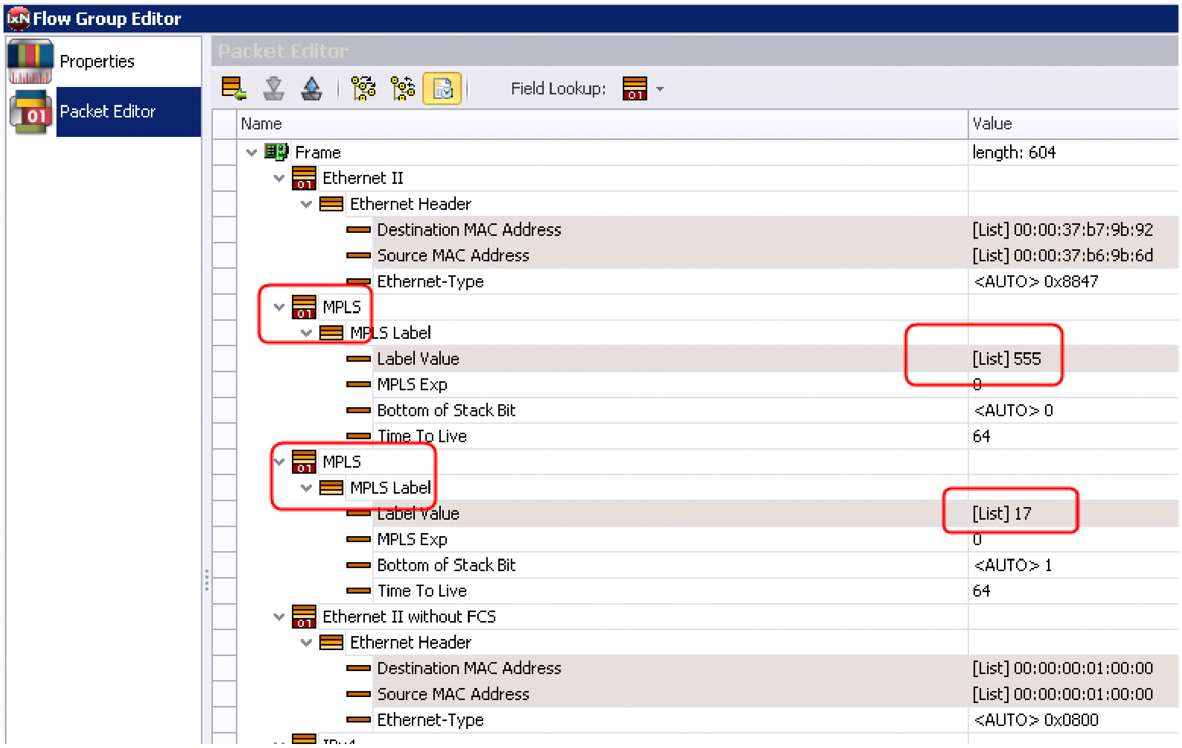


Figure 282. Packet Editor View of Generated Traffic

17. Send the traffic and adjust the rate and frame size as needed.

Result Analysis

- All BGP peer must result in correct learned RFC 3107 and VPLS information.
- Traffic contains two labels only. The outer label originates from labeled BGP peer, and the inner label originates from VPLS instances.
- Traffic is sent end to end without loss.

Test Variables

Consider the following of variables to add in the test to make the overall test plan better.

Performance Variable	Description
The number of PE routers and the number of VPLS instances in the two OSPF areas	Functionality and scalability are two different test types. It is common practice to ensure functionality working before expanding the test configuration for scalability test. Two most obvious dimensions one can scale the test into is the number of PE routers and the total number VPLS instances emulated by both Ixia test ports. This stretches not only the control plane, but also the data plane.
Bidirectional traffic with various frame size and rate; optionally running RFC 2544 methodology to cycle thru packet sizes and auto find the maximum throughput/latency	Traffic is also important to test seamless MPLS. Due to extra label encapsulation/de-capsulation, throughout and latency do matter to end to end MPLS applications, in addition to frame size and traffic rate.

Conclusions

IxNetowrk can handle seamless MPLS testing with relative ease. You can test both control plane and data plane with scalability. RFC 3107 labeled BGP peer provides the glue for bridging VPLS (and many other types of VPN) across different regions or ASes.

Introduction to H-L3VPN (t-LDP over RSVP-TE)

Today, an L3VPN MPLS network of reasonable size consists of around 500 Provider Edge (PE) routers at the access/aggregation, while about 60-70 Provider (P) Routers at the core. A full mesh of tunnels between all PE router pairs is required in order to achieve any-to-any L3VPN connectivity to serve VPN customers that connect to any of the PE routers. A flat network, if so designed, consisting of full mesh among all 500 PE routers creates almost 250K tunnels. This becomes prohibitive for network operation and management, and moreover it is tough to troubleshoot when application does not respond. Therefore, some level of hierarchy is strongly desired. Additionally, RSVP-TE is preferred in an MPLS network due to its ability for traffic engineering and its resiliency due to Fast Reroute in the presence of failure. It is difficult to establish and maintain 250K tunnels in a network, because, RSVP-TE is a resource intensive protocol. On the other hand, LDP is much simpler protocol and far less CPU intensive; however, it does not have any traffic engineering capability – traffic going through LDP tunnels are treated as best-effort.

To reduce the overall number of RSVP-TE tunnels and increase network scalability, it is common practice to run RSVP-TE only on selected routers, such as those core P routers that need strong traffic engineering features. In between those large numbers of PE routers at the edge and the P routers in the core, LDP is used. This approach will preserve the best of both worlds.

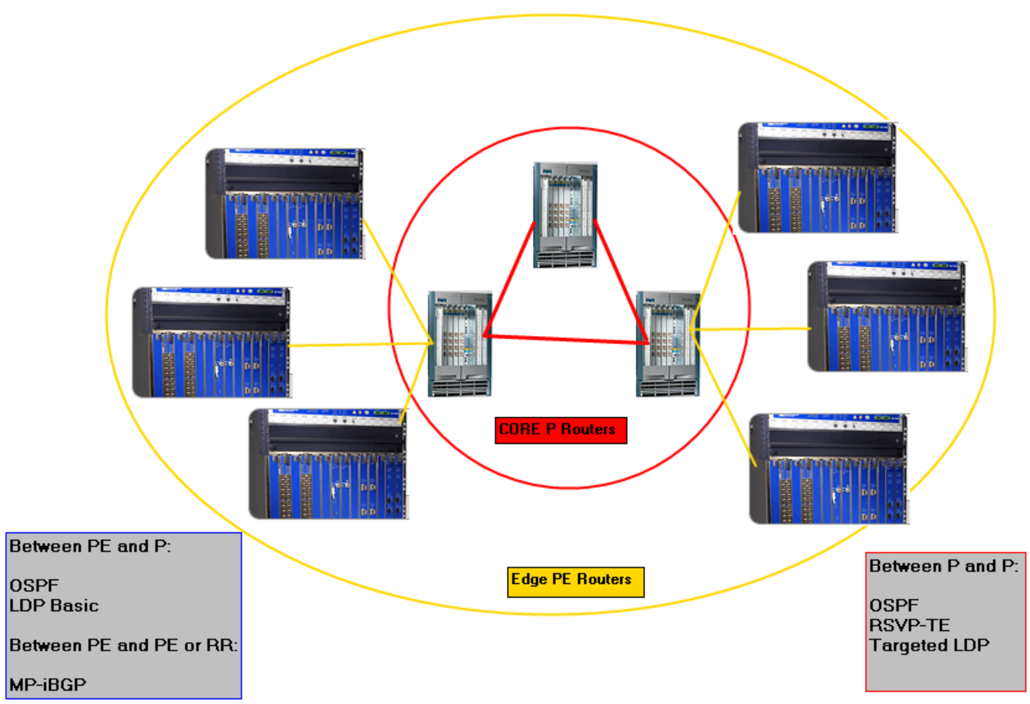


Figure 283. H-L3VPN Explained

The above diagram illustrates tiered network architecture. In the edge, there are many PE routers that speak OSPF/ISIS and basic LDP for MPLS tunnel. The VPN VRF is built and maintained through MP-iBPG typically between PE routers and a core P router that acts as Router Reflector (RR). In the core, all P routers speak OSPF/ISIS and RSVP-TE. There is a full mesh RSVP-TE tunnels between all P router pairs. To bridge the LDP sessions at the edge through the RSVP-TE at the core, there is a full mesh targeted LDP session between all ingress P router pairs just like the RSVP-TE mesh. These targeted LDP sessions run over the RSVP-TE tunnel instead of its native IP format to exchange the PE router loopbacks and their associated labels.

Traditional L3VPN deals with single MPLS signaling protocol, either LDP or RSVP-TE, across the entire MPLS core network. The data plane traffic consists only two labels; one for routing the traffic from ingress PE to egress PE and the other to identify or delineate which VRF it belongs to for a given PE. This is not scalable when the network size reaches certain level; as explained. In the new hierarchical L3VPN, it uses a combination of LDP and RSVP-TE in order to maximize the strength of each protocol and improve the scalability of L3VPN application. This brings new requirements on both the control plane and data plane; as shown in the diagram below.

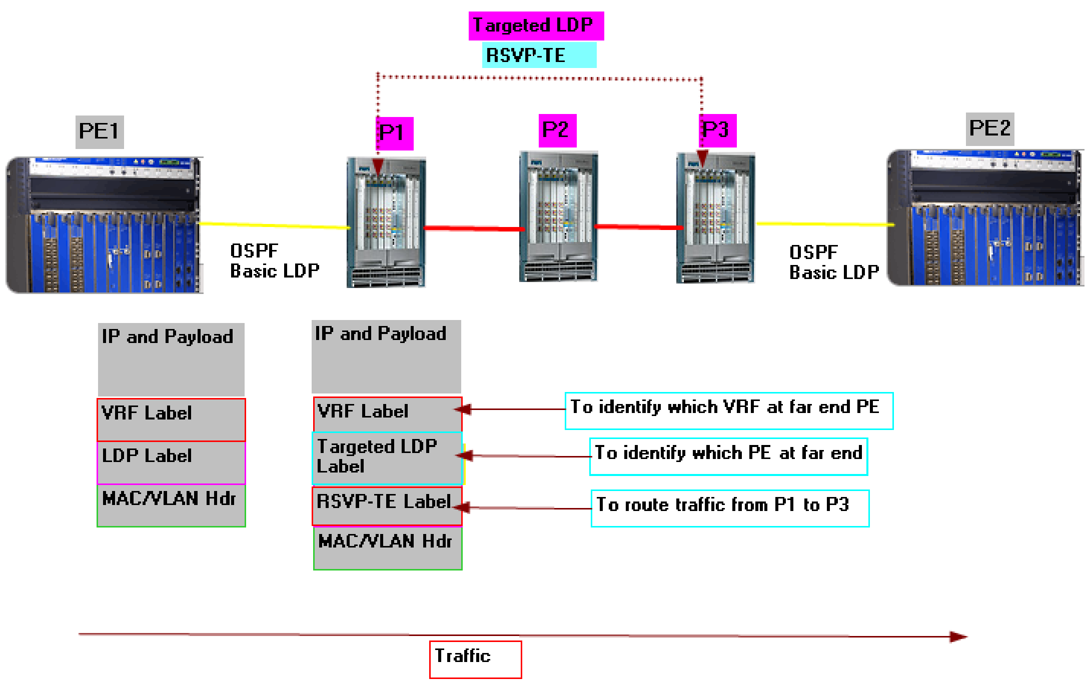


Figure 284. H-L3VPN Stack of Labels – Which Comes From What

Control plane wise, it requires extra targeted LDP session between every ingress/egress P router pair; in the same way RSVP-TE mesh was established. In fact, the targeted LDP session is running over the RSVP-TE tunnel. So there are same numbers of targeted LDP sessions as the number of RSVP-TE tunnels at the core. The targeted LDP is required to communicate to far end the PEs (PE2 in above example) to the ingress P router (P1). So when data plane traffic is delivered from ingress P (P1) to egress P (P3) there can be a way on the egress P router (P3) to identify which PE the traffic belongs to. Traditional L3VPN does not require this, because data plane is forwarded hop by hop using basic LDP tunnel. PE1 is talking to P1 and P1 is talking to P2 and P2 to P3, and so on; eventually traffic is delivered to far end PE2. In this new hierarchical L3VPN model, PE1 is dealing with P1 using LDP (like traditional), but P1 is dealing with P2 and P2 is dealing with P3 using RSVP-TE. The original LDP session lost its meaning from P1 to P2, therefore the egress P (P3) has no way identifying which PE the traffic should be delivered to. In order to do this, the egress P (P3) must communicate all PEs attached to P3 to the ingress P (P1) through targeted LDP FEC advertisement. On the ingress P (P1), this label is inserted in the middle of label stack. As long as the ingress P (P1) is responsible to deliver the traffic from P1 to P3 using the right RSVP-TE label, the egress P (P3) can identify which PE it belongs to. From that point, the PE can further identify which VPN it belongs to based on the last VRF label.

Data plane wise, the ingress PE (PE1) is doing encapsulation as usual. As soon as the data reaches ingress P router (P1), it is responsible to: 1) swap the LDP basic label with RSVP-TE label; 2) insert the middle LDP targeted label and ship it along the RSVP-TE path to reach egress P router (P3).

With both LDP and RSVP-TE working together, we can achieve a hierarchical MPLS network that can reach the scalability requirement, in the meantime fulfill the traffic engineering goals.

Relevant Standards

BGP/MPLS IP Virtual Private Networks (VPNs) – RFC 4364

RSVP-TE: Extensions to RSVP for LSP Tunnels – RFC 3209

LDP Specification – RFC 5036

Test Case: H-L3VPN Functional and Scalability Test

Overview

Hierarchical L3VPN (or simply H-L3VPN) refers to a tiered L3VPN network where RSVP-TE is employed by selected few core P routers, while LDP is employed by a majority of the edge PE routers. This is done to improve the scalability limit due to full mesh MPLS tunnel requirements among all PE routers. To bridge LDP VPN across RSVP-TE MPLS LSPs, extra target sessions are required between every core P router pair. Additionally, a three label stack is required to carry data plane traffic from one VRF to another VRF which is connected by core P routers running RSVP-TE.

Objective

The objective of this test is to show how to make IxNetwork to configure H-L3VPN to stress test the DUT either as Core Ingress/Egress P router or as Edge PE router. The test is generic and can be easily expanded for scalability and performance.

Setup

Two test ports are used to emulate H-L3VPN setup. One test port is to emulate core P routers as well as the edge PE routers. The other port is to emulate edge PE router. Traffic from coreP/edgePE side towards the DUT(s) contain three label stack with outer being the RSVP-TE tunnel, middle the t-LDP tunnel, and inner the VRF label.

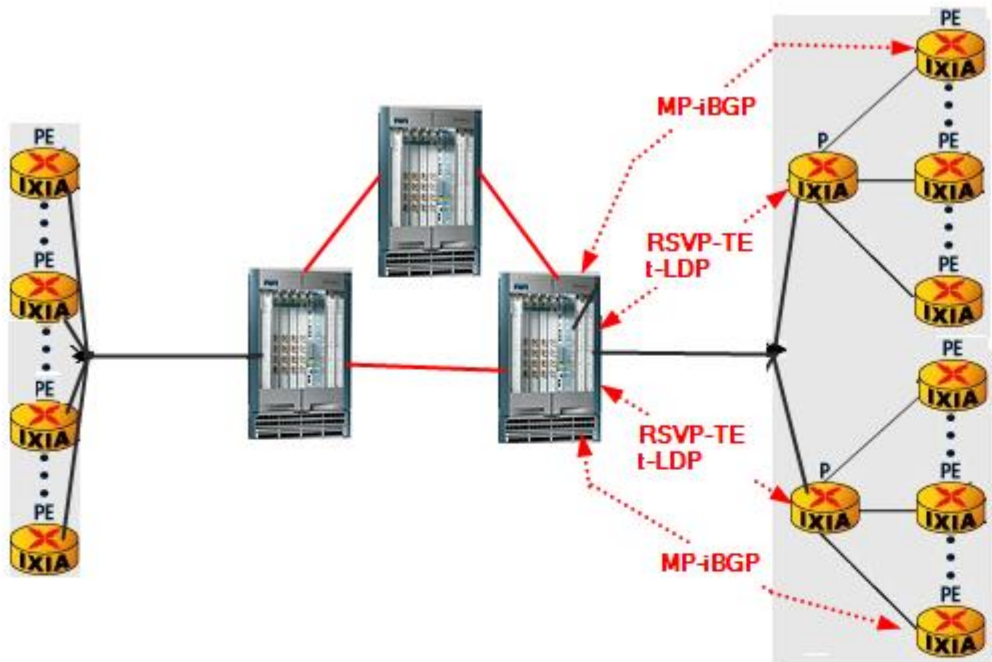


Figure 285. H-L3VPN Test Setup

Step-by-Step Instructions

1. Launch the **L3VPN/6VPE** protocol wizard to configure the MP-iBPG and VRF information
2. Select the port(s) to emulate the Core P and Edge PE routers.

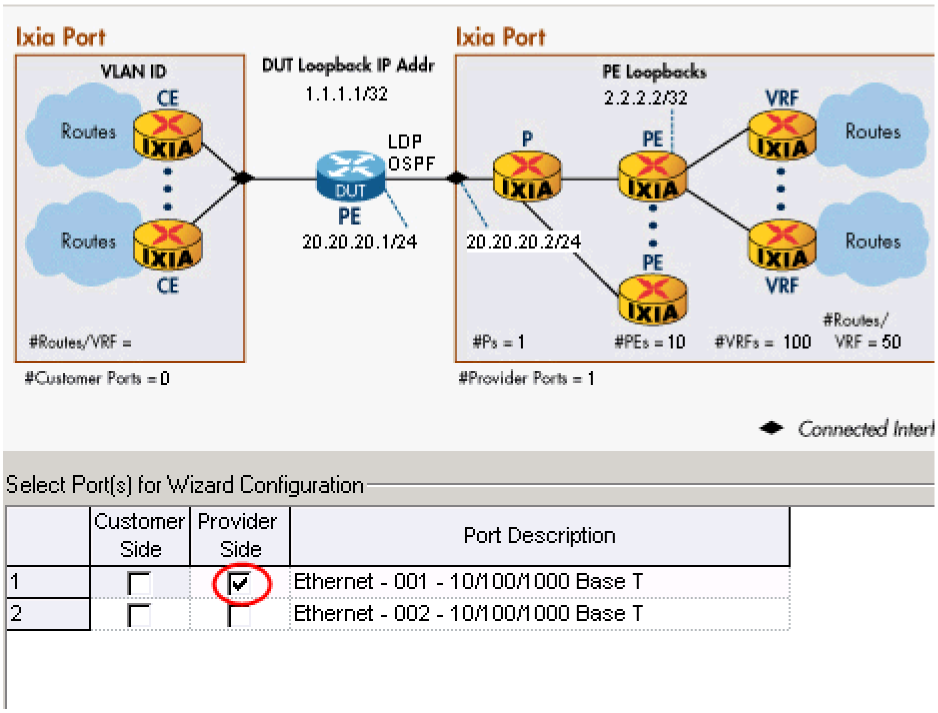


Figure 286. Select Test Port(s)

3. Configure the P router address and the protocols for the P router (LDP and OSPF)

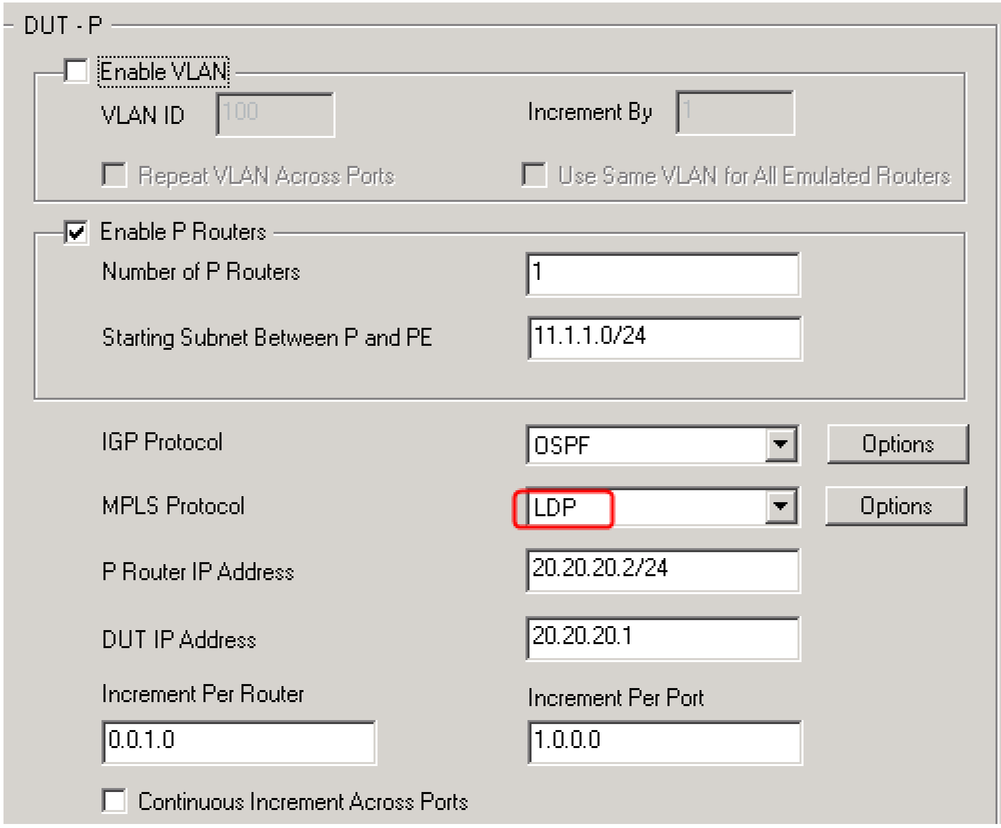


Figure 287. Configure the Core P Router

4. Configure the number of edge PE routers in the test topology.

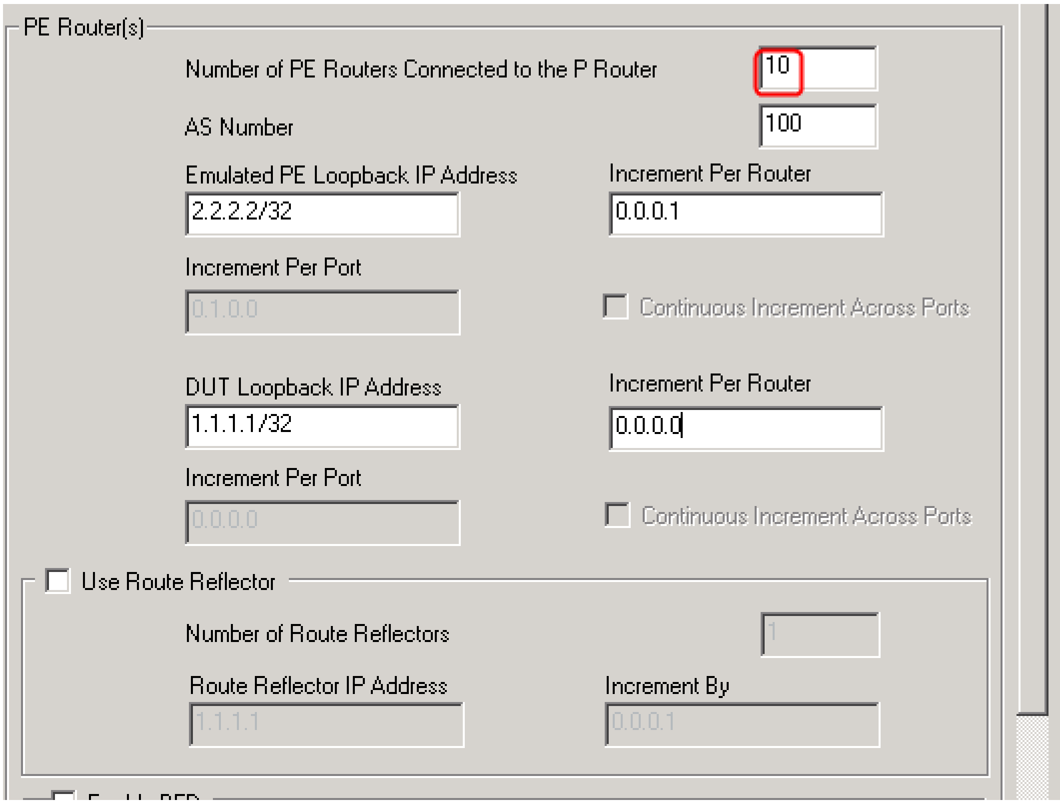


Figure 288. Configure the edge PE Router

5. Configure the number of VPNs per PE and VRF information.

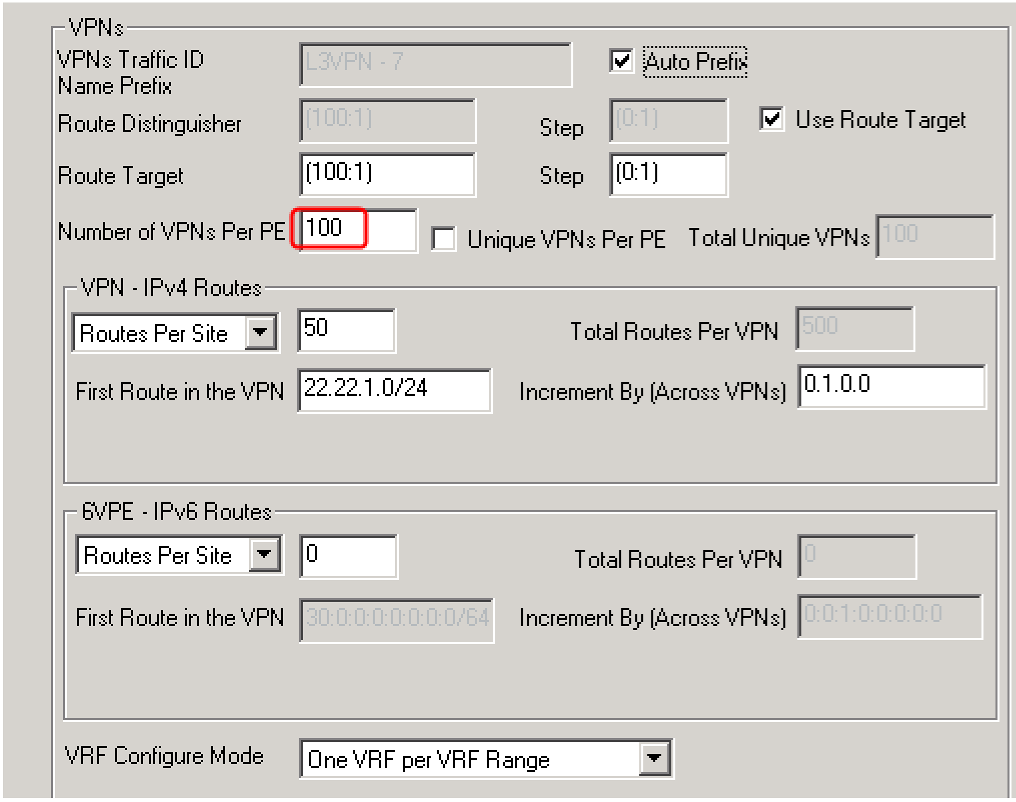


Figure 289. Configure L3VPN and Parameters

6. Give a name to the configuration and click **Generate and Overwrite All Protocol Configurations** to save and overwrite config.

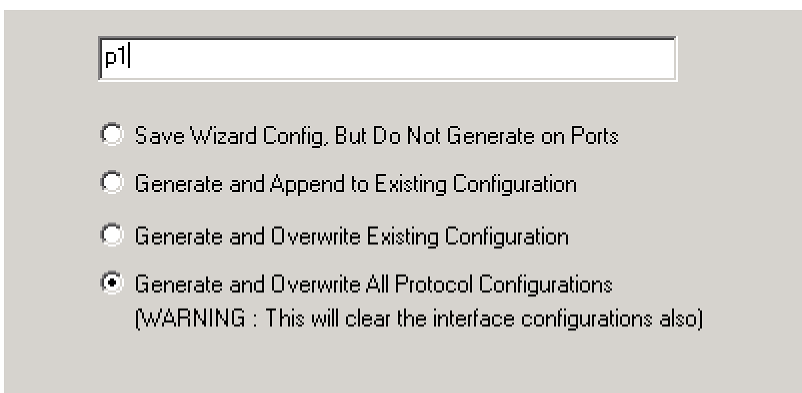


Figure 290. Save and Overwrite Config

7. Configure RSVP-TE between the Core P (ingress/egress) and the DUT P.
8. Start the RSVP-TE wizard and select the port to participate the RSVP-TE protocol.
9. Click both **SUT=Head** and **SUT=Tail** to select Ixia port as bidirectional tunnel, because the tunnel is going to be between DUT P and Ixia emulated core P.

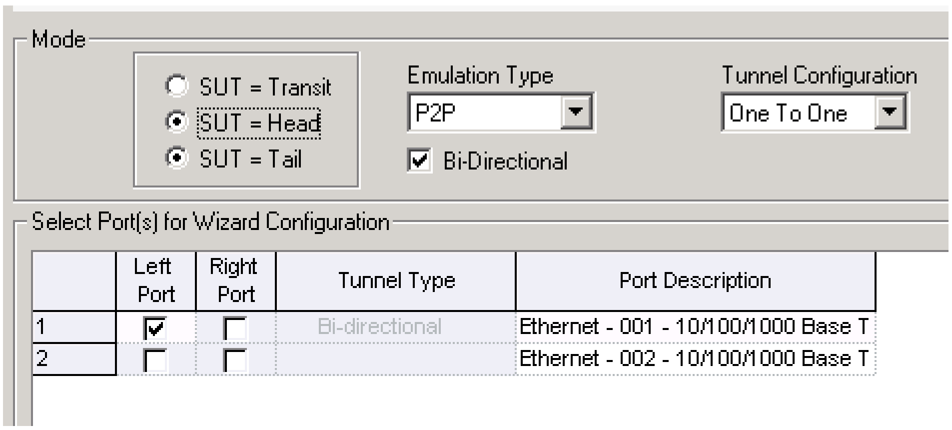


Figure 291. Configure the RSVP for the Core P Router

10. Configure the tunnel Head and Tail accordingly and use OSPF as the IGP protocol.

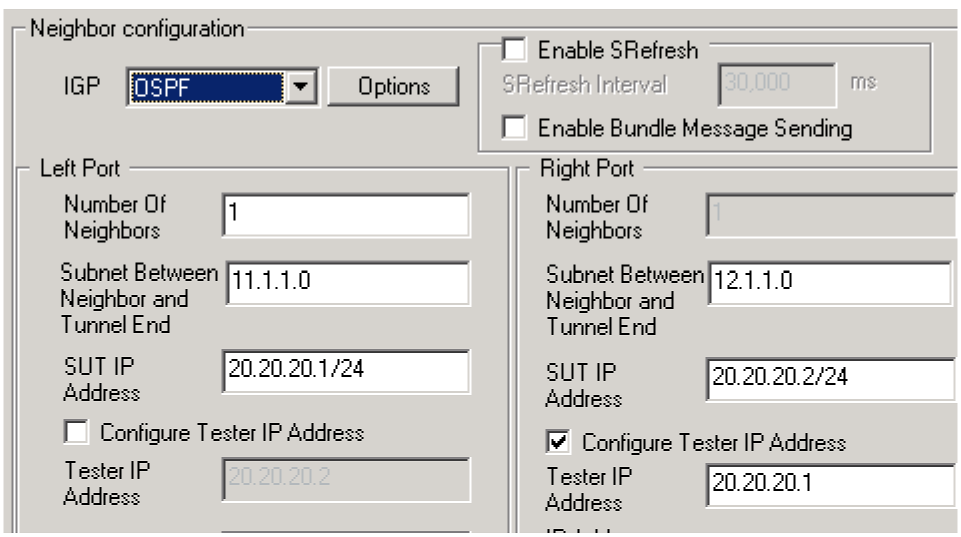


Figure 292. RSVP-TE LSR Parameters

11. Use the head port connected interface as the IP address, because the tunnel is between the emulated P and DUT,

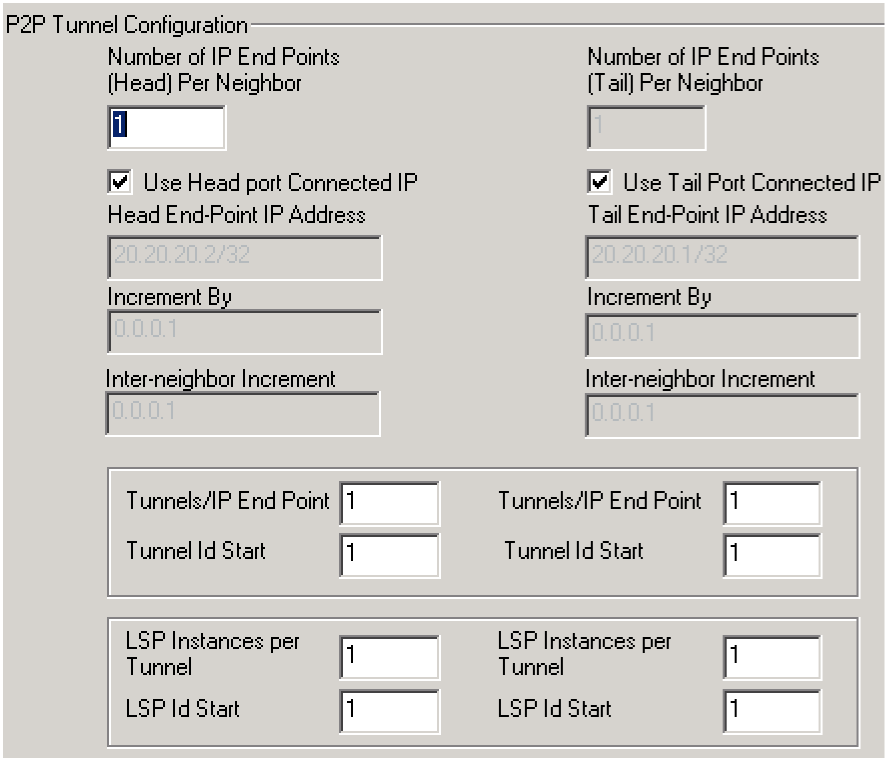


Figure 293. RSVP-TE Tunnel Endpoints

12. Provide a name to the configuration and click **Generate and Overwrite the existing configuration**. This action causes the OSPF configuration to contain only the RSVP-TE topology. The OSPF information configured through L3VPN wizard is overwritten.

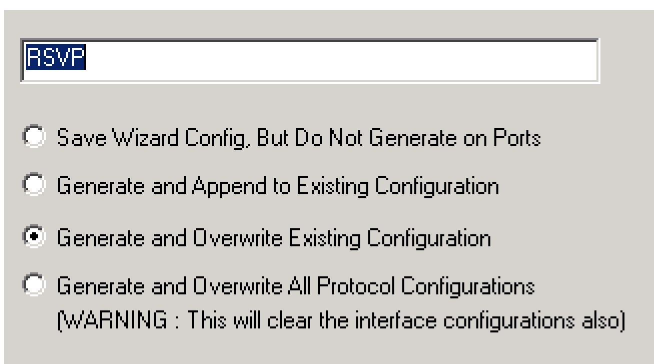


Figure 294. Overwrite the Config

13. Customize the generated configuration for the LDP configuration.

    The LDP configuration generated by L3VPN wizard uses the Basic LDP sessions. In the H-L3VPN setup, we need the t-LDP session. Click **Extended** to configure the LDP sessions as depicted in the following image. **Extended** is basically the mode to advertise the FEC using regular MPLS label. The **Extended Martini** is used for advertising PW (VC) which is different from **Extended** mode.

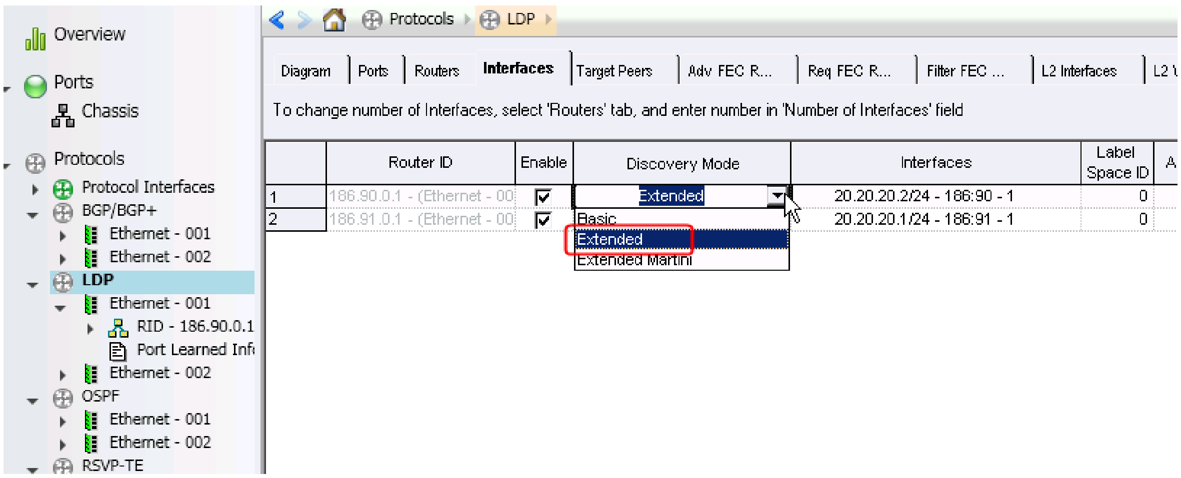


Figure 295. Change Wizard Generated LDP to t-LDP for LSP Label

14. Next, change the number of targeted peer to 1. If there are more Core Ingress/Egress P DUT in the test topology, set up a t-LDP session for each and every such DUT.

Discovery Mode	Interfaces	Label Space ID	Advertising Mode	Number of Target Peers
Extended	20.20.20.2/24 - 186:90 - 1	0	Unsolicited	1
Extended	20.20.20.1/24 - 186:91 - 1	0	Unsolicited	1

Figure 296. Configure One t-LDP

15. Set up the target LDP address per test topology.

Ports | Routers | Interfaces | **Target Peers** | Adv FEC R... | Req FEC R... | Filter FEC ...

e number of Targeted Peers, select 'Interfaces' tab, and enter number in 'Number of Target Peers' fie

Router ID	Enable	IP Address	Initiate Targeted Hello	Authentication
).20.20.2 - 186.90.0.1 - (	☑	20.20.20.1	☑	NULL
).20.20.1 - 186.91.0.1 - (	☑	20.20.20.2	☑	NULL

Figure 297. Set up t-LDP Peer Address

16. Customize Advertised FEC accordingly.

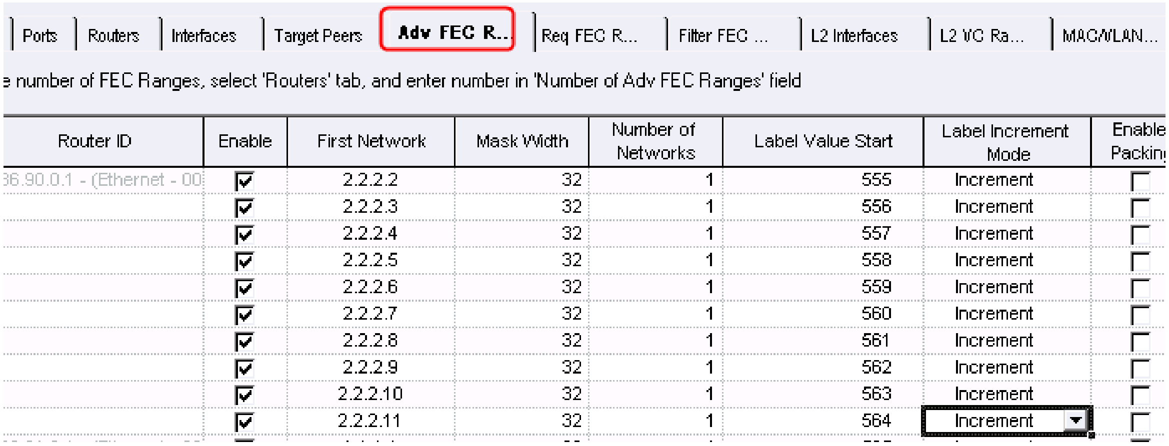


Figure 298. Verify Advertised Loopbacks

By default, the RSVP-TE is a label provider for other control sessions (t-LDP in this case) with the **Enable VPN Labels Exchange over LSP** check box selected. Make sure this check box is selected to allow t-LDP to run over RSVP-TE tunnel.

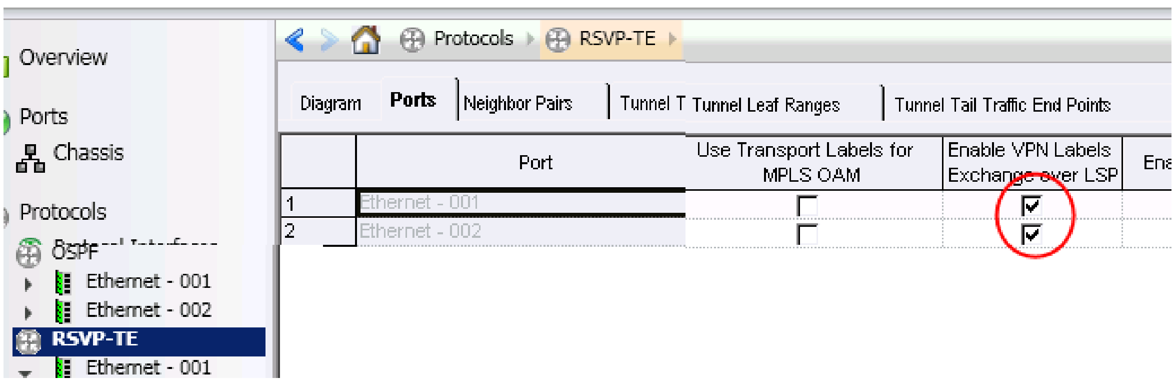


Figure 299. Set t-LDP to Run over RSVP-TE LSP

BGP on the other hand does not require to run over transport tunnels. Make sure the check box - **Request VPN Label Exchange over LSP** is cleared. This is because of the limitation that BGP can only run over a single label stack. In this setup, if BGP must run over LSP, it has to run over two label stacks (t-LDP and RSVP-TE), which currently is not supported. Running BGP in plain IP format is supported by all routers, hence we must clear this check box.

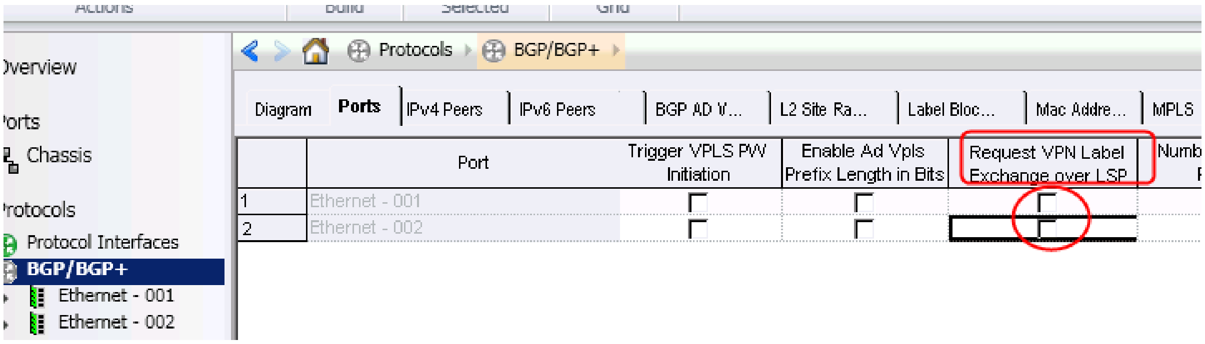


Figure 300. Set BGP to Run in Plain IP

17. Configure the other test ports as usual for L3VPN, skip the details. Refer to test case for L3VPN if you are not familiar with L3VPN.

18. Start to run all involved protocols and ensure that all sessions are functioning with correct learned info.

    All involved protocols in green status.

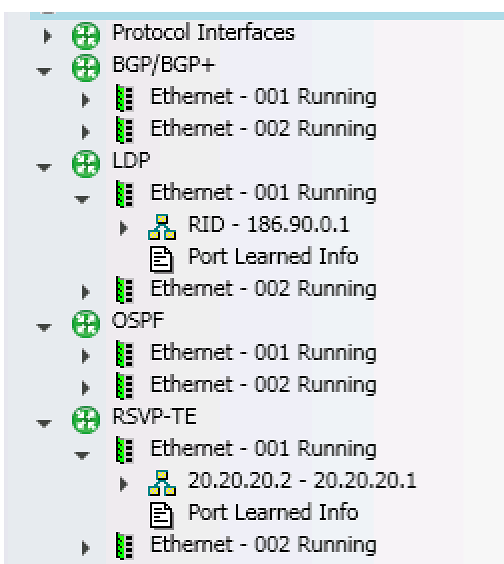


Figure 301. All Involved Protocols in Up State

RSVP-TE Learned Info shows the RSVP-TE tunnel with learned label.

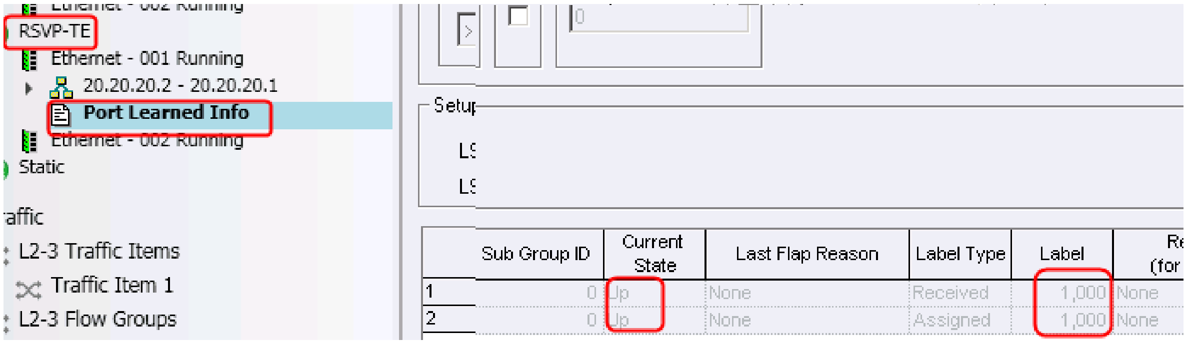


Figure 302. Learned RSVP-TE Info

The t-LDP shows the learned FEC and its labels.

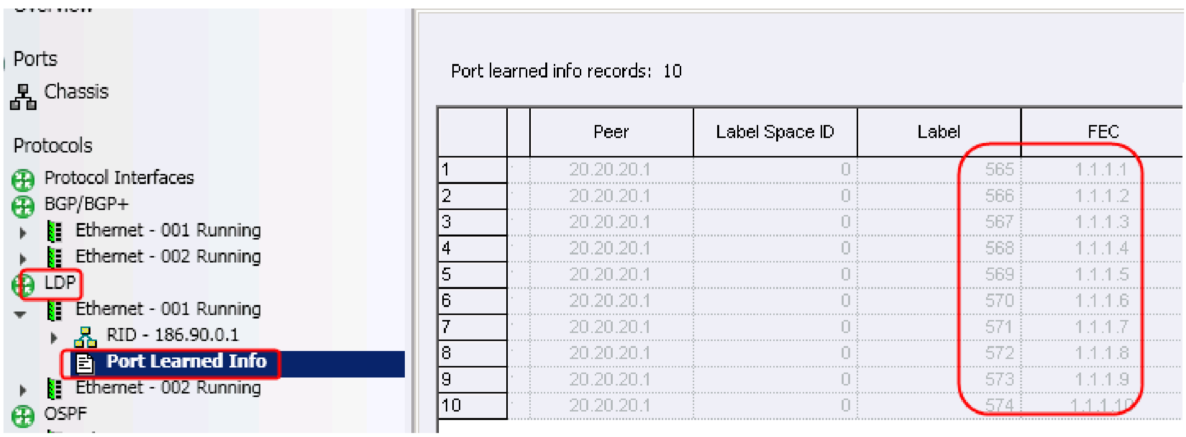


Figure 303. Learned t-LDP Info

The BGP peer shows the learned VRF routes and labels.

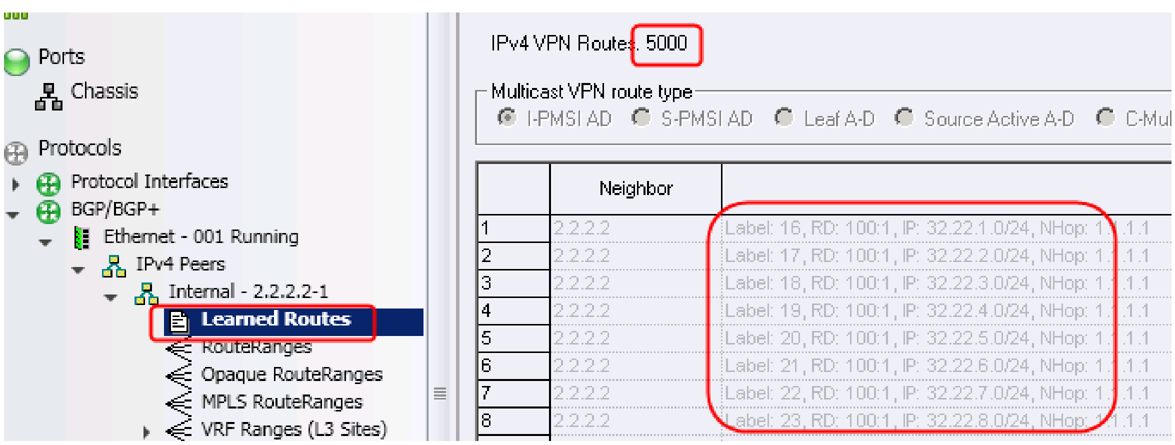


Figure 304. Learned BGP Info

19. Start the traffic wizard and configure the options as depicted in the following images.

20. Select the BGP VRF end points for both **Source** and **Destination**. Enter 3 for **Max # of VPN Label Stack**, because the number of labels to generate from core P (ingress) contains 3 labels.

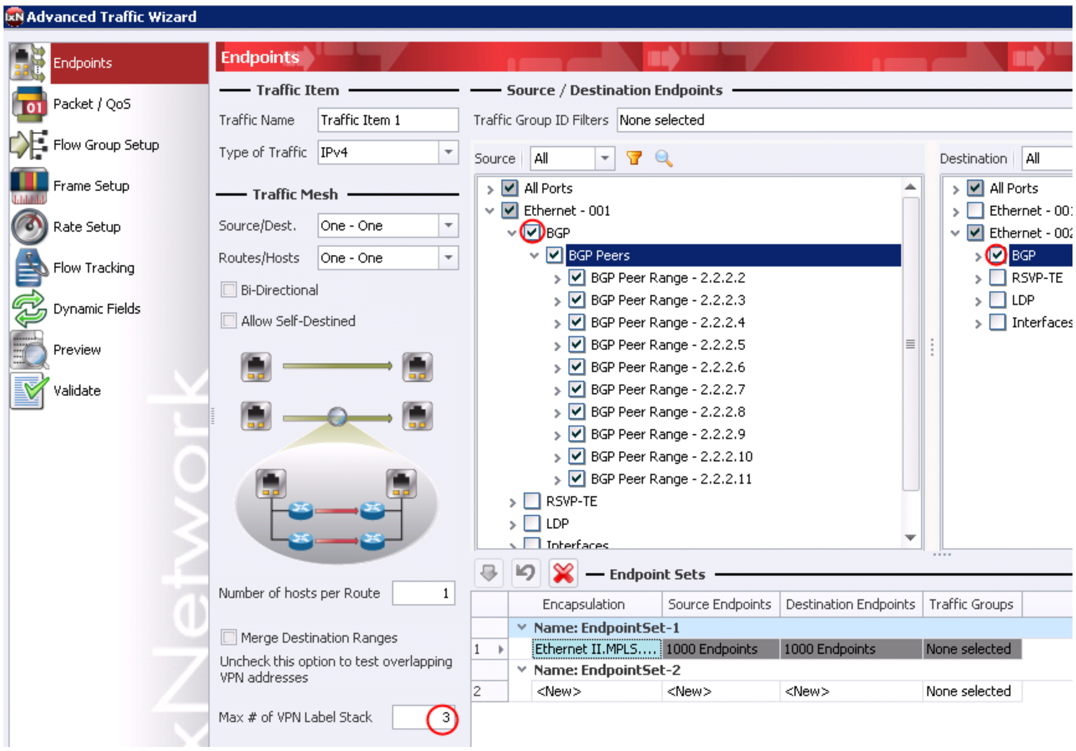


Figure 305. Select Traffic Endpoints

21. Next, you can select the **MPLS Flow Descriptor** check box for tracking. It provides the most comprehensive description about an MPLS flow; and more importantly gives you an option to display the MPLS labels. You can view from the flow stats what labels are used for traffic.

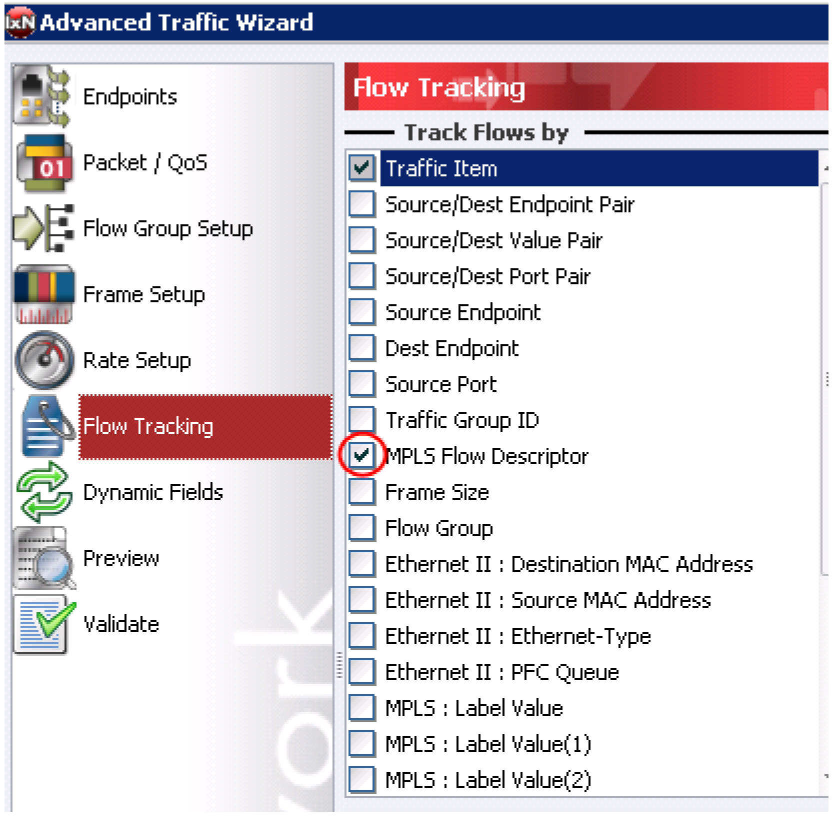


Figure 306. Select Tracking Option

22. All the other traffic options are direct and hence skipped here. The next page that one can tune is the preference of labels. You can choose RSVP-TE over LDP, and t-LDP over RFC 3107, in case the other option exists in your setup. IxNetwork automatically searches the labels per your preference list and in case, only one option exists, you do not have to set up the preference.

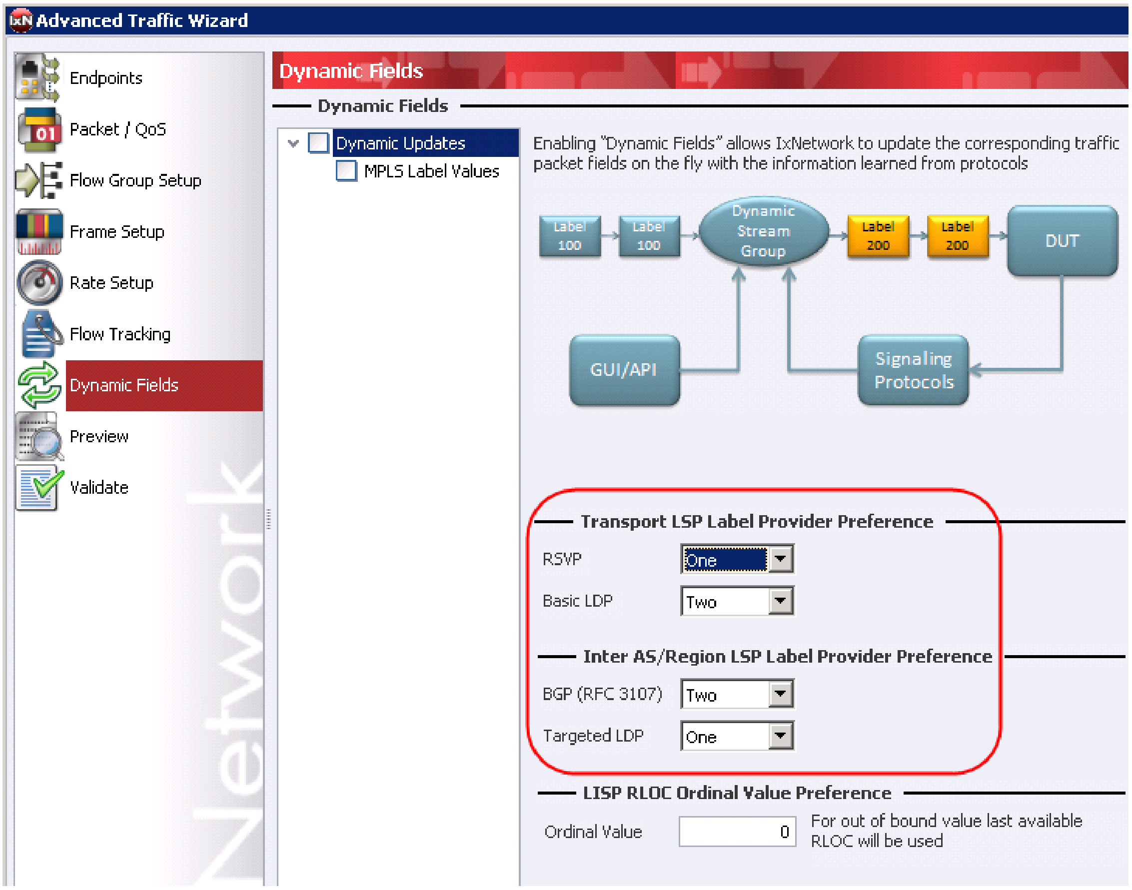


Figure 307. Set Label Preference List

23. On completion of traffic wizard, you can use the packet editor to ensure 3 MPLS label stack and each of the labels generated correspond to the right control plane protocols and their respective learned info.

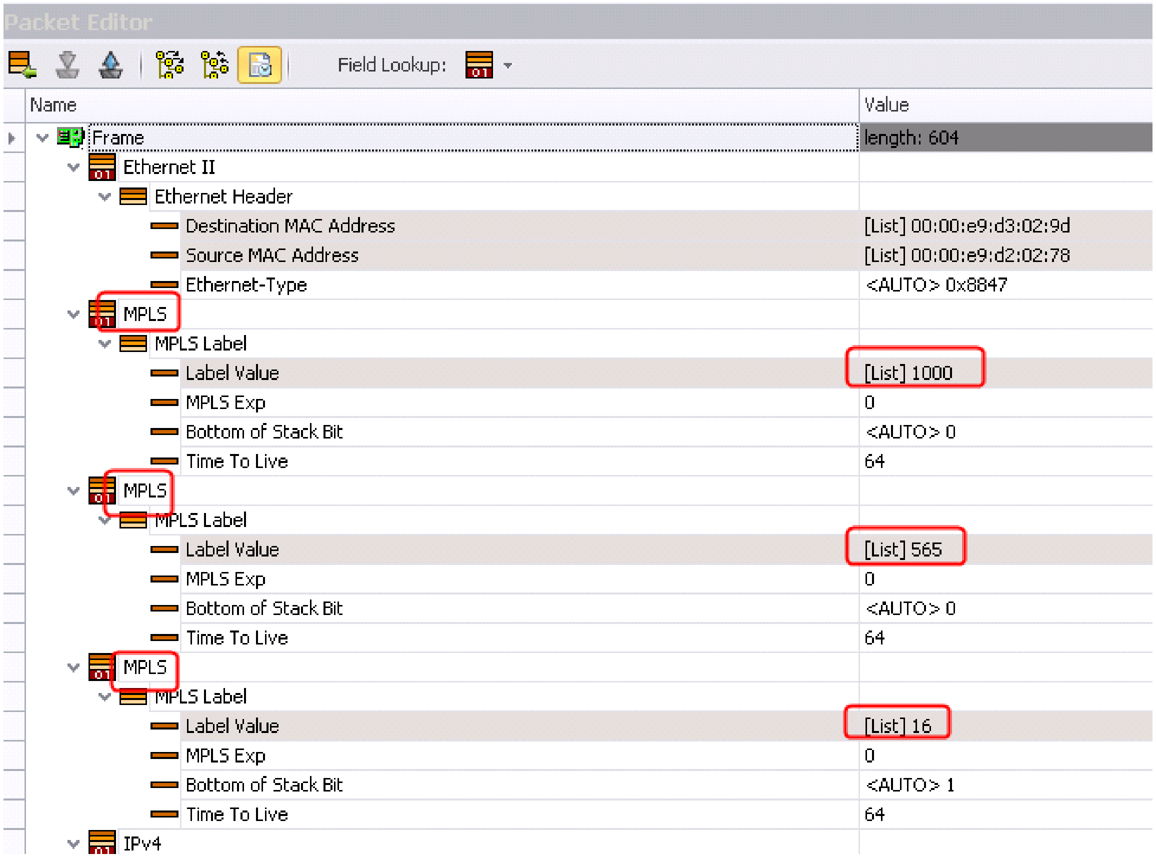


Figure 308. Verify Label Binding From Packet Editor

Result Analysis

1. All control plane are functioning and in green status.

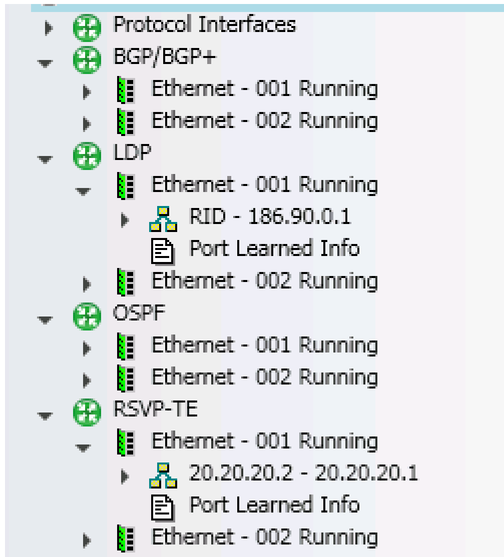


Figure 309. All Involved Protocols in UP State

2. Traffic is built successfully with correct number of labels and correct label values from the right protocol.

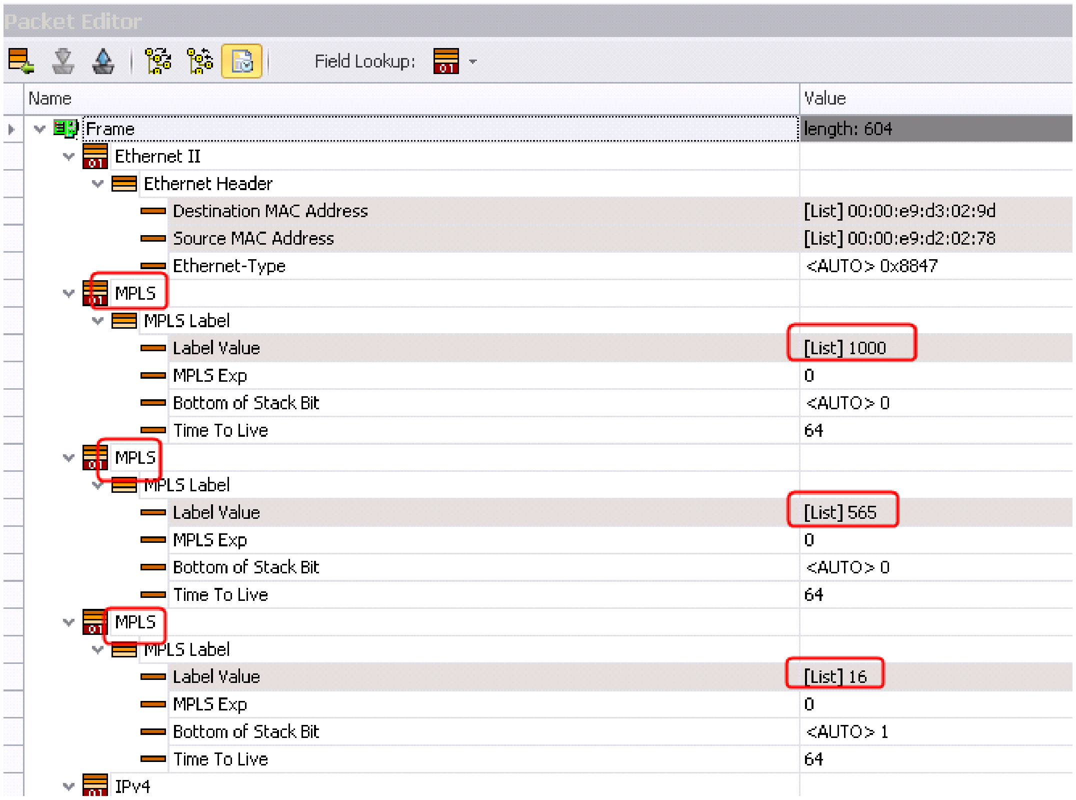
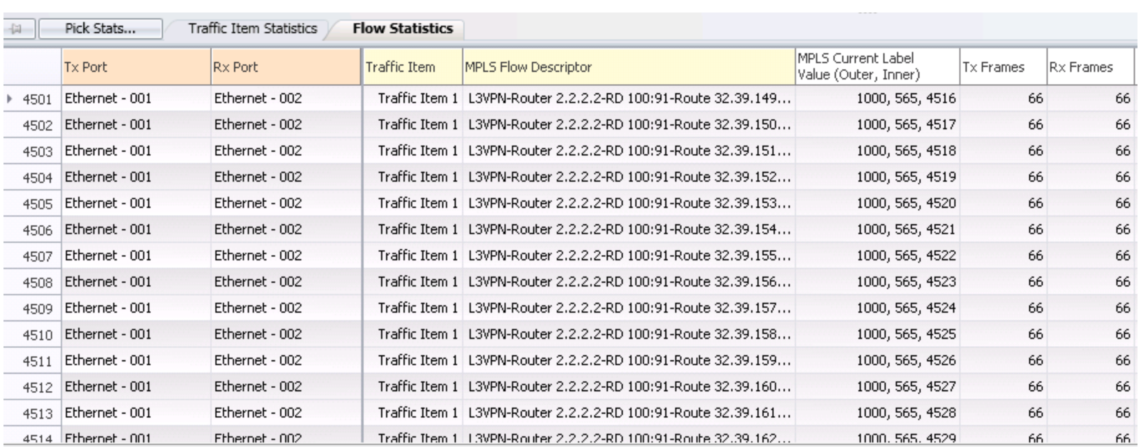


Figure 310. Correct Number of Labels and Label Values

3. Traffic is sent bidirectional with real labels.


Pick Stats... | Traffic Item Statistics | Flow Statistics

	Tx Port	Rx Port	Traffic Item	MPLS Flow Descriptor	MPLS Current Label Value (Outer, Inner)	Tx Frames	Rx Frames
4501	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.149...	1000, 565, 4516	66	66
4502	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.150...	1000, 565, 4517	66	66
4503	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.151...	1000, 565, 4518	66	66
4504	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.152...	1000, 565, 4519	66	66
4505	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.153...	1000, 565, 4520	66	66
4506	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.154...	1000, 565, 4521	66	66
4507	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.155...	1000, 565, 4522	66	66
4508	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.156...	1000, 565, 4523	66	66
4509	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.157...	1000, 565, 4524	66	66
4510	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.158...	1000, 565, 4525	66	66
4511	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.159...	1000, 565, 4526	66	66
4512	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.160...	1000, 565, 4527	66	66
4513	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.161...	1000, 565, 4528	66	66
4514	Ethernet - 001	Ethernet - 002	Traffic Item 1	L3VPN-Router 2.2.2.2-RD 100:91-Route 32.39.162...	1000, 565, 4529	66	66

Figure 311. Bidirectional Traffic with Real Labels

4. t-LDP is running over RSVP-TE tunnel and BGP is running in plain IP.

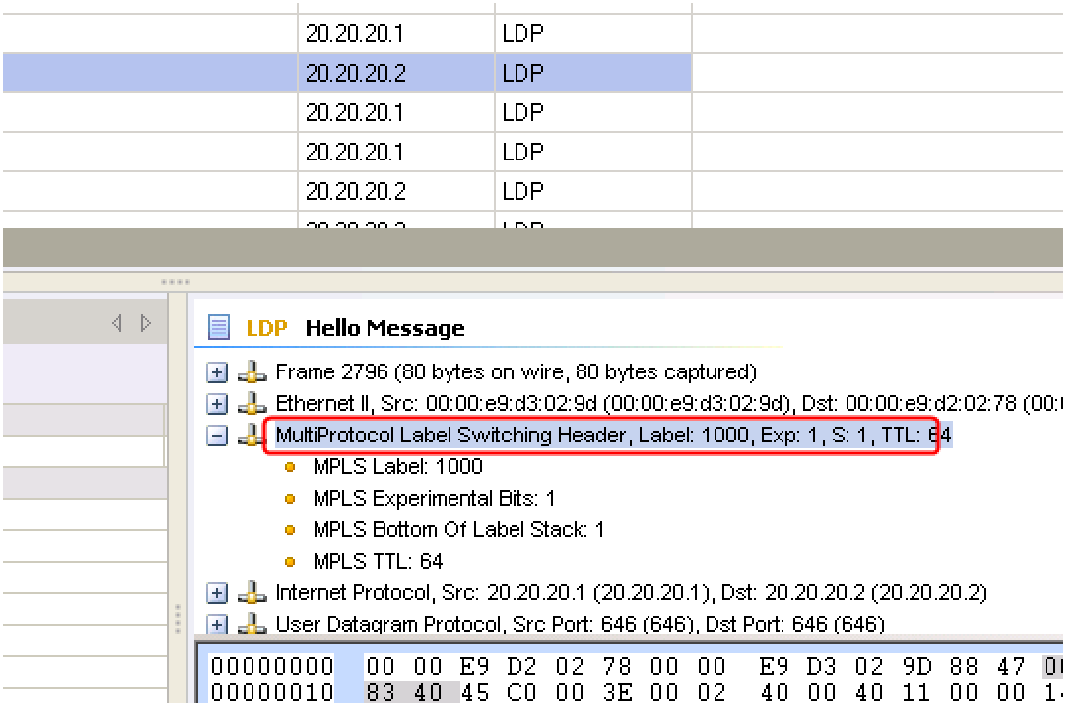


Figure 312. t-LDP over RSVP-TE LSP

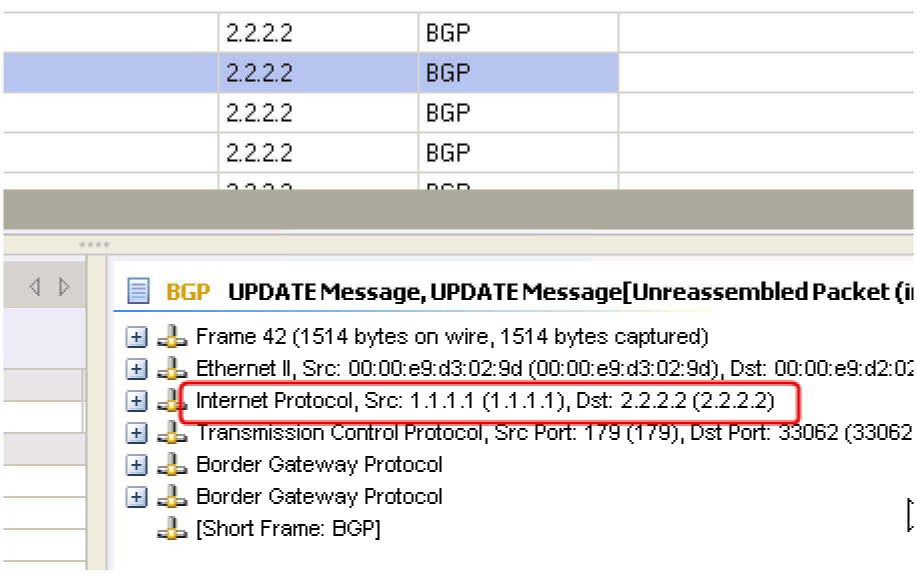


Figure 313. BGP Runs over Plain IP

Test Variables

Consider the following list of variables to add in the test to make the overall test plan better.

Performance Variable	Description
The number of core P, and edge PE routers and the number of VPN routes in each VPN	Functionality and scalability are two different test types. It is common practice to ensure functionality is working before expanding the test configuration for scalability test. The most obvious dimension the test can be scaled up to is the number of core P routers. In the example, we set up only one. This can be easily increased to meet the scalability of core P router requirements. The total number of edge PE routers as well as the number of VPN routes becomes the second dimension where you can scale the test. This will not only stress test the control plane, but also more importantly the data plane traffic.
Bidirectional traffic with various frame size and rate; optionally running RFC 2544 methodology to cycle thru packet sizes and auto find the maximum throughput/latency	Traffic is also important to test H-L3VPN. Due to extra label encapsulation/de-capsulation, throughout and latency do matter to end to end MPLS applications, in addition to frame size and traffic rate.

Conclusions

IxNetwork is fully capable of testing H-L3VPN either from functionality point of view or from scalability point of view, and with relative ease. Traffic labels are automatically bounded by the traffic wizard. The example test can be scaled up to many dimensions to meet the scalability requirements.

Introduction to Multicast VPN

Multicast is an efficient mechanism for transmitting data from a single source to many receivers in a network. Its major advantage over unicast is that only one copy of multicast data is forwarded on each link in the network. The multicast data is replicated at each router as needed. Thus, the bandwidth consumption is greatly reduced.

Over the past decade, multicast has become prevalent in financial application, software downloads, audio and video streaming application. The existing MPLS/BGP VPN users require that service provider support multicast traffic delivery transparently over the provider network as unicast traffic. Multicast VPN is introduced to address this demand.

Multicast VPN is a technology that deploys multicast service in an existing MPLS/BGP VPN infrastructure. It uses Multicast Domain (MD) concept, which is defined in Rosen draft. Each VPN with multicast enabled is a MD. A PE router that attaches to a particular multicast-enabled VPN is associated with that MD. This also requires that the service provider backbone support native IP multicast and is itself a MD.

Within the provider MD (P-network), a default Multicast Distribution Tree (MDT) is built through the backbone for each customer MD (C-network) to connect all PE routers that belong to that MD. A unique multicast group is associated with this default MDT. In this context, default means that this MDT is on as long as PE routers are on. It does not depend on the existence of multicast traffic in that MD. This is in contrast to another type of multicast distribution tree we will discuss later.

The default MDT in the P-network is signaled by P-multicast protocol, such as PIM-SM, PIM-SSM, and bi-directional PIM. All PE routers that belong to a particular C-network join the corresponding default MDT. The PE router maps the customer multicast flows for a specific VPN to the default MDT group allocated to that VPN. The customer multicast flow is encapsulated using GRE with outer source IP as PE router loopback address and outer destination IP as default MDT group for that VPN. The PE loopback address here is also used for BGP peering with Router Reflector (RR) or other PE routers. This flow is distributed natively across P-network. All PE routers of this VPN that join the tree will receive the multicast traffic. Each PE router then de-capsulate the packets and delivers them to local customer edge router, if there is receiver attached.

Figure Figure 314 shows an example of two multicast VPNs, VPN-Red and VPN-Blue.

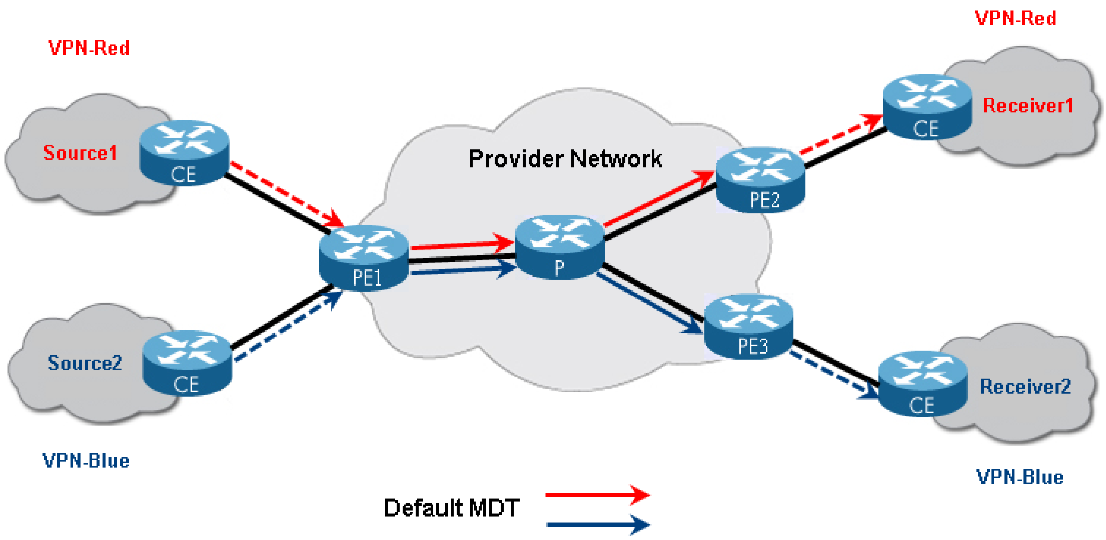


Figure 314. Multicast VPN default MDT

PE1 connects to both the VPN-Red and VPN-Blue customer site which have multicast sources. PE2 connects to the VPN-Red customer site which has a multicast receiver. PE3 connects to the VPN-Blue customer site which has a multicast receiver.

In the P-Network, two multicast distribution trees are built. One is for VPN-Red, which connects to PE1 and PE2. The other is for VPN-Blue which connects to PE1 and PE3. When Source1 in VPN-Red starts sending multicast traffic, it reaches PE1 first in native multicast format. PE1 then encapsulate the traffic with GRE and forwards it to the P-network. This traffic flows along the MDT tree for VPN-red and reaches PE2. PE2 removes the GRE encapsulation and delivers the original multicast packet from Source1 to the local attached CE in VPN-Red; the multicast traffic eventually reaches Receiver1. PE3 does not join the MDT for VPN-Red and therefore will not receive multicast traffic for VPN-Red. In a similar fashion, the multicast traffic from Source2 in VPN-Blue flows on the MDT for VPN-Blue and reaches to PE3 only. PE2 will not receive this traffic as it does not join the VPN-Blue tree.

The following image shows the packet format at various points in the network – before entering the P-network, inside the P-network, after exiting the P-network.

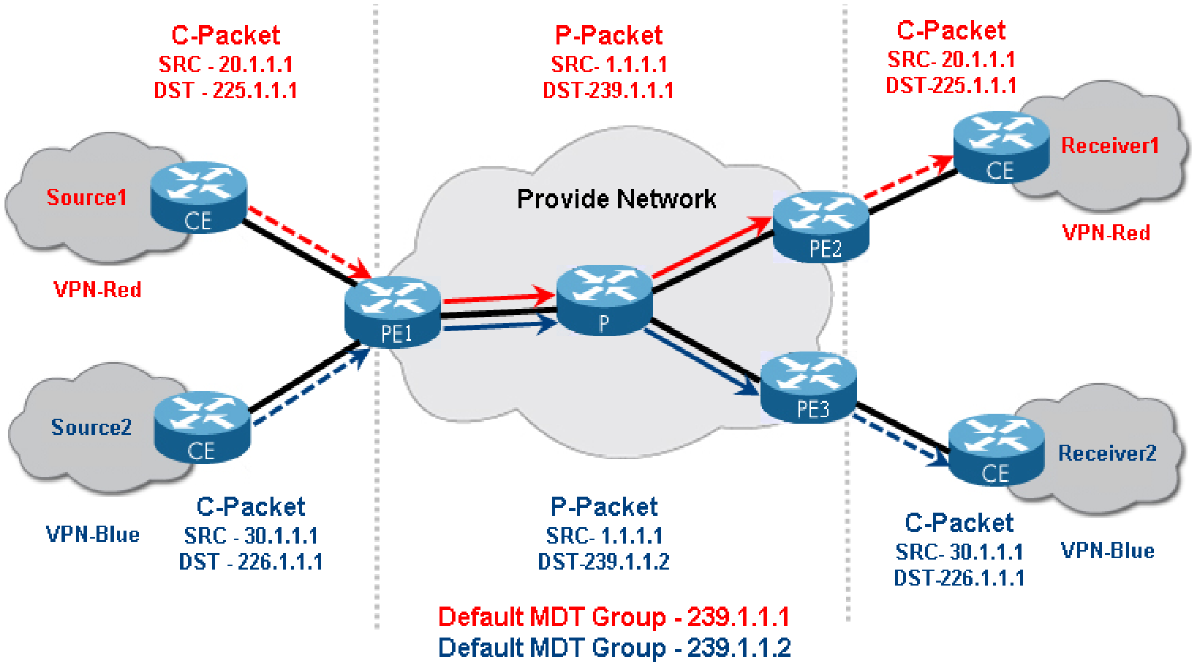


Figure 315. Multicast VPN default MDT packet encapsulation

The Multicast Domain solution does not require any change for P router except supporting native IP multicast. Each PE router needs to support separate multicast routing and forwarding instances (mVRF) for each VPN. This mVRF instance belongs to that customer multicast domain and contains all the multicast routing information for that VPN. Each mVRF maintains a separate multicast routing and forwarding table. When a PE router receives multicast data or control packets from a CE router, it identifies the mVRF that it belongs to based on the incoming interface and uses the multicast routing information for that VRF to conduce RPF check, and then forwards the packets.

Each PE router creates a single PIM instance for each VRF that has multicast routing enabled. This VRF-specific PIM instance forms two types of PIM adjacencies. The first one is a PIM adjacency with each PIM-enabled local CE router in that mVRF. The second one is a PIM adjacency with other PE routers that have mVRFs in the same MD. This PIM adjacency is accessible through the multicast tunnel interface (MTI) and is used to transport multicast information for a particular mVPN (through a MDT) across the backbone.

Each PE router also maintains global PIM adjacencies with each of its IGP neighbors, which are P routers or directly connected PE routers. The global PIM instance is used to create the multicast distribution trees (MDTs) that connect the mVRFs.

Multicast Domain solution has several key advantages:

- Provide multicast service to enterprise users over existing MPLS VPN infrastructures.

- Minimize the amount of state information that a P router must hold while providing optimal routing.
- Allows customer multicast network to choose their own multicast operations mode, multicast groups and source address for their private multicast data. Overlapping address space can be used among VPNs.

Data MDT

As discussed above, one of the advantages for the default MDT is that it does not require P routers to maintain any VPN-specific information to achieve scalability in the provider network. However, scalability is often traded off against optimal operation. While the default MDT maps all multicast control and data traffic for a customer multicast domain to a single MDT group, a multicast flow for that VPN will be delivered to all PE routers which are members of that VPN regardless whether it has interested receivers for that particular multicast flow or not. This results unnecessary flooding of multicast traffic throughout the provider network and consumes significant bandwidth, especially for high-bandwidth applications and sparsely located receivers. Each PE router also needs to process the encapsulated VPN traffic even if the multicast packets are then dropped. To overcome this problem, a mechanism is required to build a dynamic multicast distribution tree with only interested parties joined the tree. Data MDT is proposed for this purpose.

Data MDT requires the creation of new multicast distribution tree (MDT) to minimize flooding. It does this by sending data only to the PE routers that have active receiver for a specific multicast flow. In contrast with default MDT, data MDT is created dynamically when a particular multicast flow exceeds pre-configured bandwidth threshold. “Data”, is used here to indicate that it is created for Data traffic only. All multicast control traffic always flows on the default MDT to ensure that all PE routers receive control information.

The following image shows an example of data MDT.

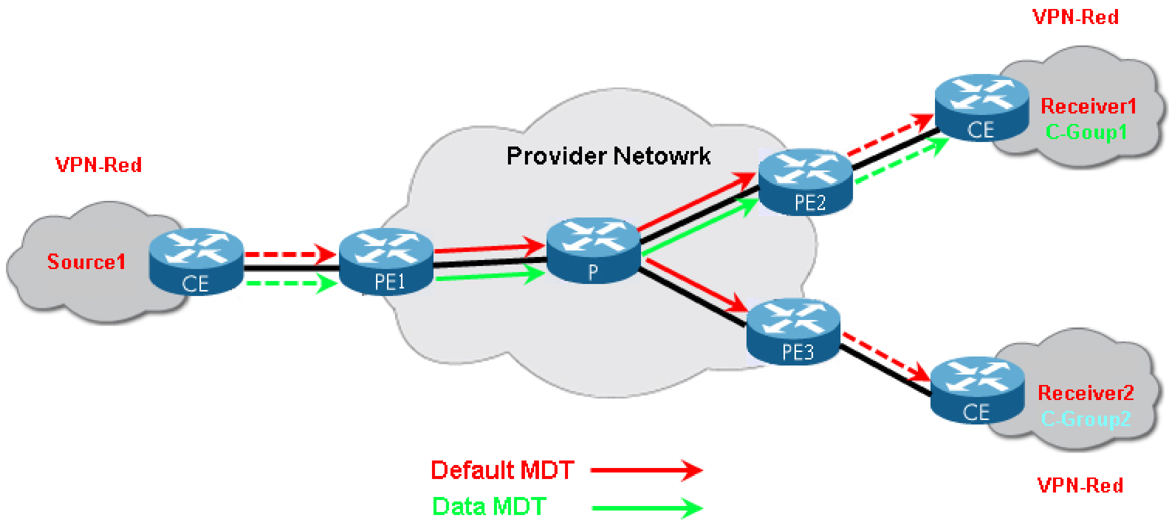


Figure 316. Multicast VPN data MDT

PE1, PE2 and PE3 are members of VPN-Red. Source1 is attached to PE1. Receiver1 and Receiver2 are attached to PE2 and PE3, respectively. Receiver1 is interested to C-Group1 and Receiver2 is interested to C-Group2. Source1 starts sending multicast traffic to C-Group1. With default MDT, both PE2 and PE3 receive the traffic. PE2 de-capsulates the multicast packets and delivers them to Receiver1. PE3 also de-capsulates the multicast packets and finds that there is no attached receiver interested in C-Group1, and therefore drops the packets. With data MDT, PE1 signals a new multicast distribution tree for this multicast flow. PE2 joins this tree since it has interested receiver. PE3 does not join the tree as it does not have interested receiver. After building the data MDT, PE1 switches over the multicast flow from default MDT to data MDT. Now only PE2 will receive the multicast flow.

Data MDT is signaled using a user datagram protocol (UDP) TLV called a data MDT join TLV. It describes the source and group pair for a C-multicast flow and a data MDT group used in provider network for this flow. The PE router monitors the multicast traffic it receives from locally attached CE routers. Once the multicast traffic exceeds a pre-configured rate threshold, the PE router signals a new MDT. The source PE periodically announces the MDT join TLV over the default MDT for that VRF instance, as long as the source is active. All PE routers receive the MDT join TLV over the default MDT. Only those PE routers with interested receivers for the multicast flow will join the new group, by sending a PIM join message for new group. The source PE router starts encapsulating the multicast traffic in new data MDT group after several seconds delay and stops encapsulation with the default MDT group. In this way traffic will only reach PE routers who join the new group.

The above discussed solution is widely deployed today. It has several disadvantages, however:

- It requires that the service provider network support IP multicast.
- It requires that the service provider network routes traffic based on destination address. It cannot utilize the MPLS LSP in the provider network to provide fast look up for delivery of multicast traffic.
- PE routers need to maintain PIM adjacencies with all other PE routers for each VPN. This is a significant burden on the PE router.

Draft l3VPN-2547bis-mcast introduces a BGP-based control plane that is modeled after its highly successful counterpart of the VPN unicast control plane. Multiple transport technologies are proposed for use in service provider networks. Besides PIM which is discussed above, RSVP-TE P2MP LSPs, mLDP P2MP or MP2MP LSP, and Ingress Replication have also been proposed as transport technologies for mVPN in service provider networks. Each transport technology has its own advantage and suitable deployment space. This draft also proposes several enhancements to existing Multicast Domain solution to reduce PIM adjacencies that needs to be maintained by PE routers. We will discuss the latest mVPN technology in subsequence addition of this book.

Relevant Standards

Multicast in MPLS/BGP IP VPNs – draft-rosen-vpn-mcast-08

Multicast in MPLS/BGP IP VPNs – draft-ietf-l3vpn-2547bis-mcast-08.txt

Protocol Independent Multicast – Sparse Mode – RFC 4601

BGP/MPLS VPNs – RFC2547

Multiprotocol Extensions for BGP4 – RFC2283)

Test Case: MVPN Scalability and Performance Test

Overview

With its increased popularity, the scalability of deploying mVPN has becoming of a great interest. The mVPN scalability, however, is a multi-dimensional metric. When measuring the mVPN control plane scalability of a PE device, the metrics typically include the number of mVPNs supported, the number of PE routers per mVPN, the number of (*,G)/(S,G) routes per mVPN, etc. This test section will focus on measuring the number of PIM adjacencies that a PE device can handle per line card or per system across all supported mVPNs. A PE establishes a PIM adjacency with each remote PE who belongs to same mVPN. Therefore the overall number of PIM sessions is (# of remote PEs) * (# of mVPNs).

There are two typical mVPN test topologies for use when testing using Ixia protocol emulation. These topologies are based on the location of the multicast sources and receivers.

- Topology 1 – The emulated customer multicast sources are located behind emulated PEs and the emulated multicast receivers are located behind emulated CEs.
- Topology 2 - The emulated multicast receivers are located behind emulated PEs and the emulated customer multicast sources are located behind emulated CEs.

For the purpose of this test, these two topologies are not different in significant way since the test is mainly focused on the number of PIM adjacencies. Therefore, topology 1 will be used to illustrate the work flow. After performing control plane measurements, traffic will be sent from source to receiver to validate data plane forwarding. Line rate traffic can be generated and verified for long duration tests. The system should sustain both control and data plane for the supported number of PIM adjacencies.

The mVPN data MDT switchover performance test will use the second topology. The differences in configuration between the two scenarios will be explained in the second test.

Objective

The object of this test is to determine the scalability of a PE device with respect to the number of mVPN instances that span the number of PE routers. We will assume that the PE device is designed to support a maximum of 200 mVPNs. This test is designed to find the maximum number of remote PEs that the device can handle. The number of multicast sources and groups per VPN are set to *2* for this test.

Setup

Six Ixia test ports are used in the setup. One Ixia port emulates a local CE connected to the DUT and five Ixia PE port emulate a total of 30 remote PEs, each of which supports 200 mVPNs. Assuming symmetry, each PE test port emulates six PE routers. You may vary the number of PE ports or emulated PE/mVPNs per PE port to match your requirements.

The IxNetwork mVPN protocol wizard is a great starting point. It walks you through, screen by screen from P/PE to CE configuration to help you quickly build a large mVPN configuration. With the wizard's append function, you can expand existing configuration so as to increase the number of PEs or the number of mVRFs per PE without interrupting your current test. Figure 317 shows you the topology we will emulate in this test.

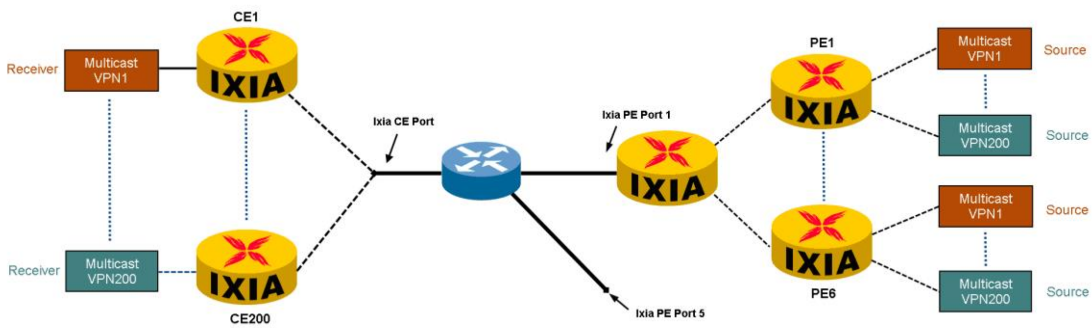


Figure 317. Multicast VPN scalability test topology

Step-by-Step Instructions

1. Launch the **Multicast VPN** protocol wizard.

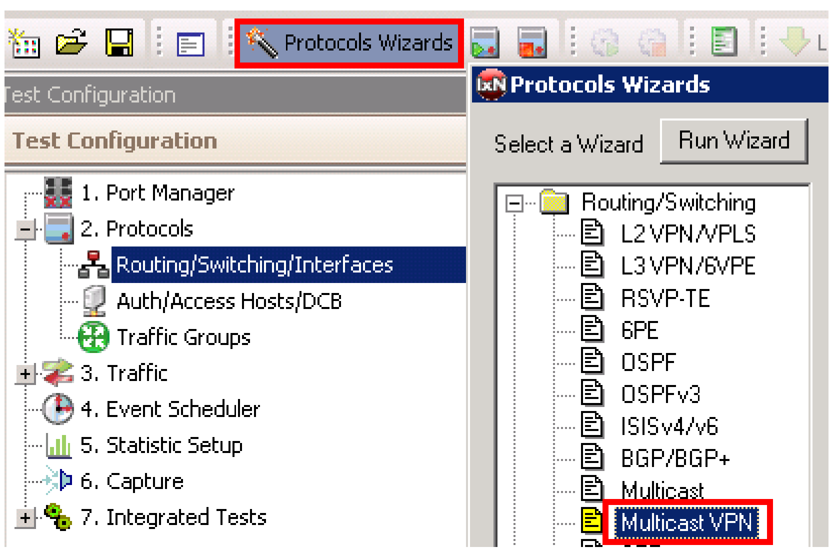


Figure 318. Launch mVPN wizard

2. Configure port **1** as a **CE Side** port and ports **2-6** as **PE Side** ports. Keep default **Source/Receiver** setting. The term **Source** means that emulated multicast sources are located behind the port and **Receiver** means that emulated receivers are located behind the port.

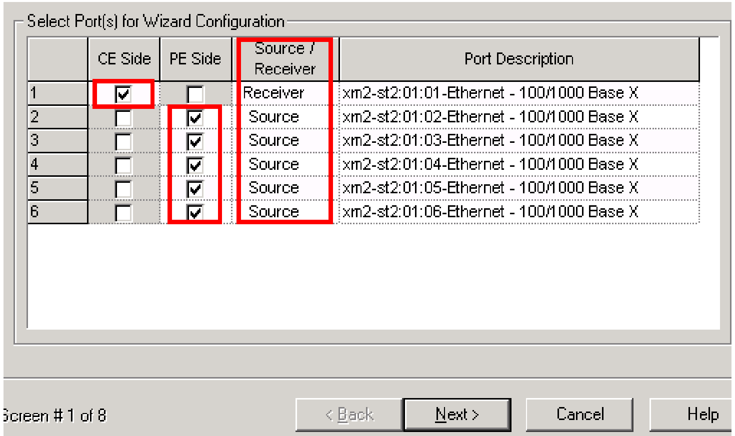


Figure 319. mVPN wizard screen #1

3. On Screen #2 of 7, perform the following configuration tasks:
   a. **P Router IP Address –** The emulated P router IP address that is connected to the DUT’s core-facing interface.
   b. **DUT IP Address** – The DUT core facing interface IP address . If the P Router IP Address is changed, the DUT IP Address will be auto-filled with the immediately preceding address within the subnet.
   c. **Increment Per Port** – This field controls the increment for the above 2 fields across ports.
   d. **Starting Subnet Between P and PE** – This is used for links between Ixia emulated Ps and PEs.
   e. **IGP Protocol** – The IGP protocol used in the core. The DUT will establish an IGP session with the Ixia emulated P router. Available selections are OSPF (default) and ISIS.
   f. **Provider Multicast Protocol** – Multicast protocol used in the provider multicast domain. Available selections are PIM-SM (default) and PIM-SSM.
   g. **Provider Network RP Address** – The RP address in the provider multicast domain when PIM-SM is used. It is grayed out if PIM-SSM is used. Please note that **Provider Network RP Address** should reside at the DUT or other P router outside the Ixia ports.
   h. **MPLS protocol –** The MPLS protocol used in the core. The DUT will establish an MPLS protocol session with the Ixia emulated P router and receive label mappings from the Ixia port for emulated PE loopback addresses.

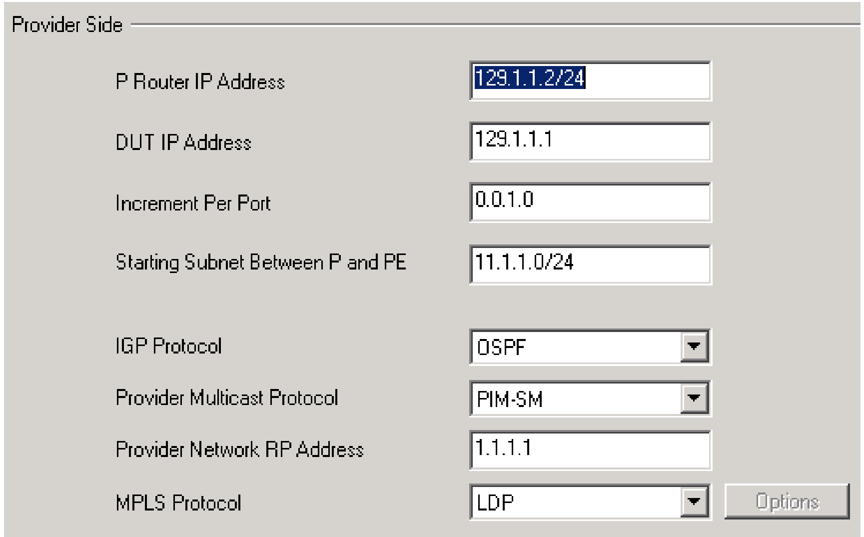


Figure 320. mVPN Wizard Screen #2 – Setup P router

4. On screen #3 of 7, perform the following configuration tasks:
   a. **Number of PE Routers Connected to the P router –** The number of emulated PE routers behind emulated P router.
   b. **AS number** – The AS number in which the emulated PE routers reside.
   c. **Emulated PE loopback IP Address** and increment options – The 1st emulated PE loopback address and increment option to determine the IP addresses of the rest of the PE loopback addresses. This will be used for BGP peering and PIM peering.
   d. **DUT Loopback IP Address** and increment options – The DUT loopback address which will be used for BGP peering and multicast tunnel source address.

   Be sure to enable **Ignore all Ixia Emulated PIM Neighbors** when you have more than one PE port and the emulated PEs support the same set of mVPNs. In this way the Ixia emulated PEs will only maintain PIM adjacencies over default MDT tunnels with the DUT and drop all other adjacencies among themselves, achieving better emulation performance.

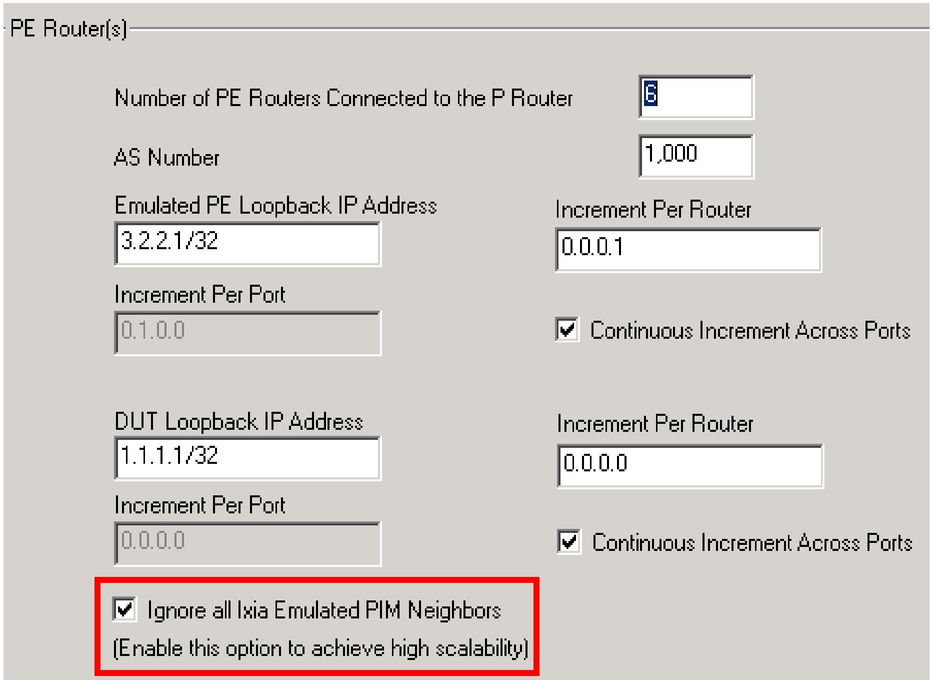


Figure 321. mVPN Wizard Screen #3 – Setup PE router

5. On screen #4 of 7, perform the following configuration tasks:
    a. Configure the **Route Target** (RT) value used for first mVPN and **Step** to increment the Route Target for the remaining mVPNs. In this example, the RT for the first mVRF is *(100:1)* and the step is *(0:1)*. Therefore RTs for the remaining mVPNs are 100:2, 100:3, 100:4 … 100:200.
    b. By default, the **Route Distinguisher** (RD) is configured to use the same value as the RT. If you want configure this separately, you can uncheck **Use Route Target** checkbox and configure the **Route Distinguisher** value and step separately from RT.
    c. Configure the **Number of VPNs per PE** as *200*.
    d. Configure **First Default MDT Group Address** as *239.1.1.1/32***.**

    For other parameters:
    a. **MVPNs Traffic ID Name Prefix** – This is used to attach a unique traffic group ID for each mVPN across the emulated PE and PE ports. The traffic group ID is used to filter traffic endpoint in the traffic wizard so that you only see the source/destination endpoints which you are interested in. This is auto-prefixed by default. If you want to define the traffic group ID differently, uncheck **Auto-Prefix**.
    b. **Unique VPNs per PE** – This is unchecked by default. This means that each emulated PE will support the same 200 mVPNs. If it is checked, then each PE will support a different set of 200 mVPNs which would result in 5 (# of PE ports) * 6 (# of PE/port) * 200 (# of mVPNs/PE) = 6000 mVPNs.
    c. **Total Unique VPNs** – The total number of unique VPNs across all emulated PEs and PE ports for the test configured through this wizard run. This is for information only. In this test, it is 200 since all emulated PEs support the same 200 mVPNs. If **Unique VPNs per PE** is unchecked, then each PE will support a different 200 mVPNs and this field will display 6000.

    Data MDT related configuration parameters will be discussed in next test.

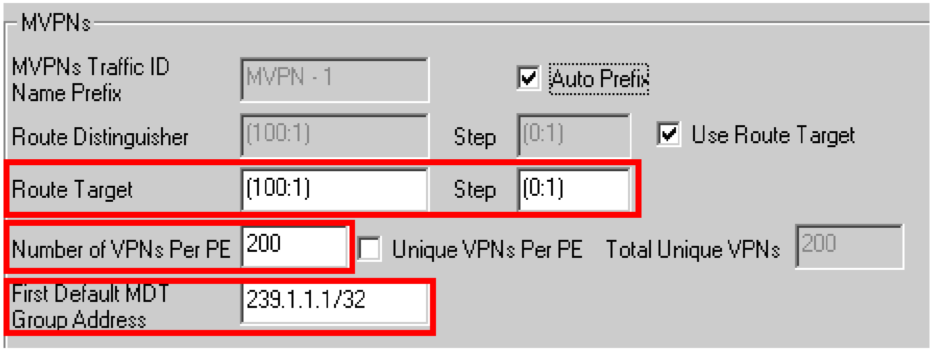


Figure 322. mVPN wizard screen #4 – setup mVPN

6. On screen # 5 of 7, perform the following configuration tasks:
   a. **Multicast Source Address:**
      - **Address per MVPN** - The number of C-multicast source addresses per mVPN per PE.
      - **Starting Source Address** - The first C-multicast source address used.
      - **Increment By** – The increment step used to configure the rest of the C-multicast source addresses.
   b. **Multicast Group Address:**
      - **Addresses per MVPN** - The number of C-multicast group addresses per mVPN per PE.
      - **Starting Group Address** – The first C-multicast group address used.
      - Increment By – The increment step used to configure the rest of the C-multicast group addresses.
      - **Group Address Distribution –** The default is Accumulated mode. This option applies when emulated receivers for the same mVPN are behind multiple emulated PEs or CEs. Emulate receivers for the same mVPN will join the same group addresses in Accumulated mode and different group address in Distributed mode.

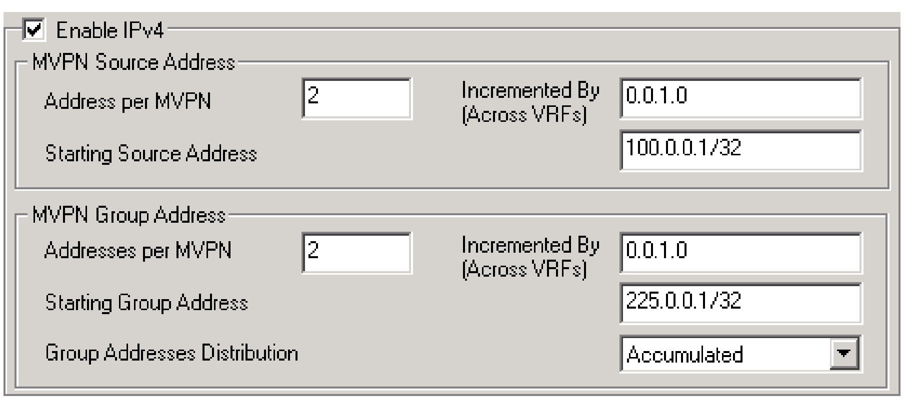


Figure 323. mVPN wizard screen #5 – setup IPv4 C-Multicast sources and groups

Similar configuration parameters are available for IPv6.

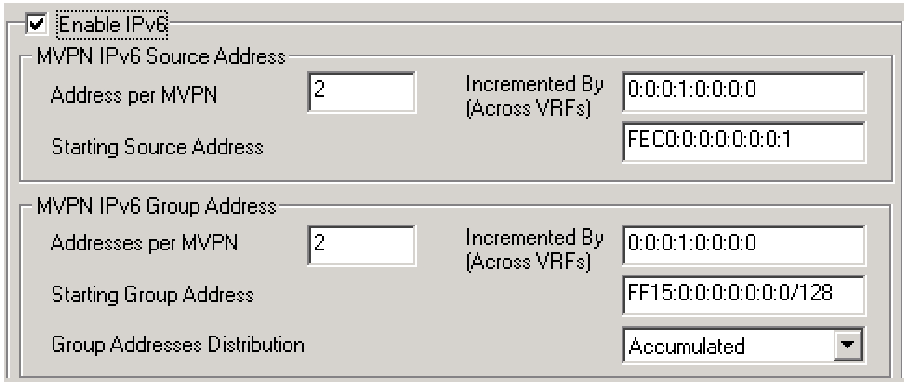


Figure 324. mVPN Wizard Screen #5 – Setup IPv6 C-Multicast Sources and Groups

7. On screen # 6 of 7, perform the following configuration tasks:

   a. **Enable VLAN**,**VLAN ID** and increment options – The VLAN ID of DUT CE facing interface and its increment option, if VLANs are enabled.
   b. **Mixed CE Protocol** and **IGP Protocol** – This is available when the emulated C-multicast sources are behind a CE port. It will be used to advertise C-multicast source addresses to the DUT PE. The DUT PE will install C-multicast source routes into its VPN routing table and use them for PIM RPF checks. If the CE port role is set to **Receiver** in wizard screen#1 (Figure 325), then this field will be grayed out.
   c. **Emulated CE IP Address –** The IP Address of Ixia emulated CE interface.
   d. **DUT IP Address –** The IP Address of DUT CE facing interface.
   e. **Increment Per Router** and **Increment Per Port** – Control the IP Address increment for multiple emulated Ixia CE interface and DUT CE facing interfaces.
   f. **Multicast Protocol** – The multicast protocol used in the customer's multicast domain. Available selections are PIM-SM (default) and PIM-SSM.
   g. **Source Group Mapping** – This is available when **Multicast Protocol** is set to **PIM-SSM**. It configures the C-multicast group and C-multicast source mapping. Available selections are **Fully Meshed** (default) and **One-to-One**.
   h. **Multicast Network RP Address** and **Increment By –** The RP address for the customer's multicast domain. Available when **Multicast Protocol** is set to **PIM-SM**. It is recommended that the RP address should reside at the DUT or other routers outside the Ixia ports.

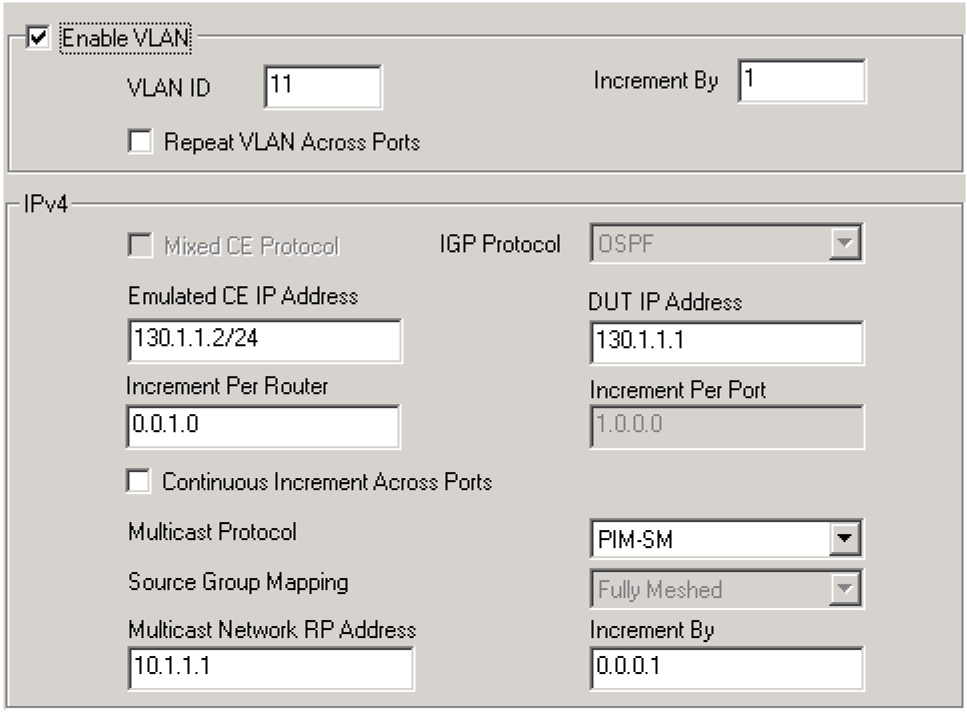


Figure 325. mVPN Wizard Screen #6 – Setup IPv4 CE Router

Similar options are available for IPv6 if the customer multicast domain is running with IPv6.

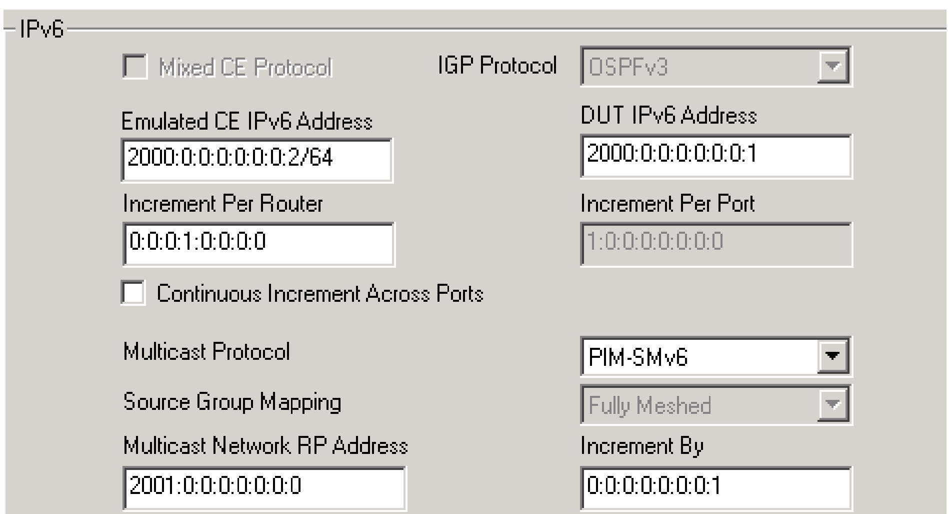


Figure 326. mVPN wizard screen #6 – setup IPv6 CE router

8. You have now finished the setup your mVPN emulation. On screen # 7 of 7, name your wizard configuration file and select **Generate and Overwrite Existing Configuration** to generate a configuration. The wizard will configure the ports with the required protocols.

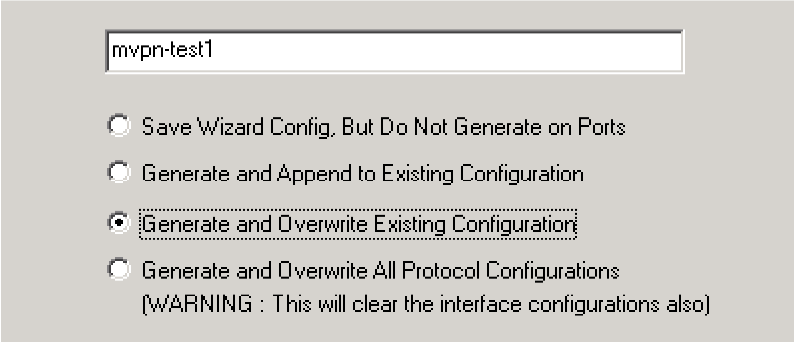


Figure 327. mVPN Wizard Screen #7

- **Save Wizard Config, But Do Not Generate on Ports** – This option saves the wizard configuration for this run, but will not configure the Ixia ports. The saved wizard configuration can be loaded later to configure the ports.
- **Generate and Append to Existing Configuration** – This option appends the configuration from this wizard run to the existing configuration. An append operation can be used to append additional emulated PEs and mVPNs to existing PEs, additional C-multicast sources and groups to existing mVPN of existing PEs, etc.
- **Generate and Overwrite Existing Configuration** – This option will overwrite the existing configuration with new configuration for protocols used in this wizard run.
- **Generate and Overwrite All Protocol Configurations** – This option will clean all the protocol configurations (include protocol interfaces) before write configuration from this wizard run.

9. Click on **Test Configuration → Protocols → Routing/Switching/Interfaces**. Inspect the configuration created by the wizard.

   One OSPF router is configured per PE port. These are emulated P routers which advertise emulated PE loopback addresses to DUT.

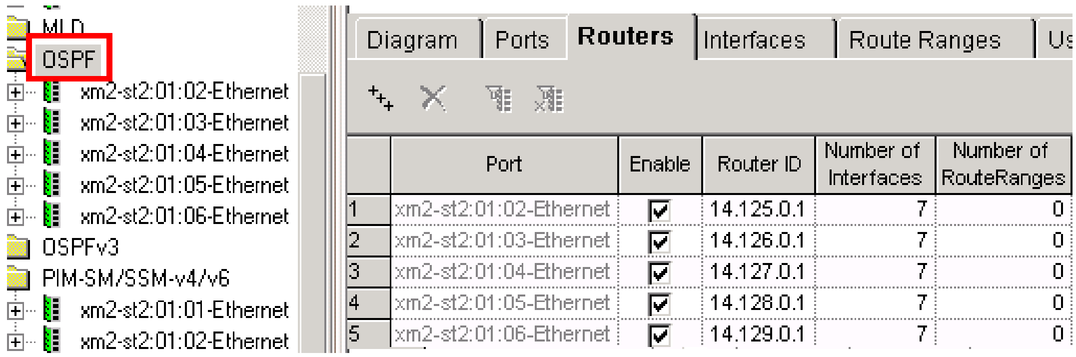


Figure 328. OSPF P emulation

   One LDP router is created per PE port. These are emulated P routers that advertise label mapping for emulated PE loopback addresses to DUT.

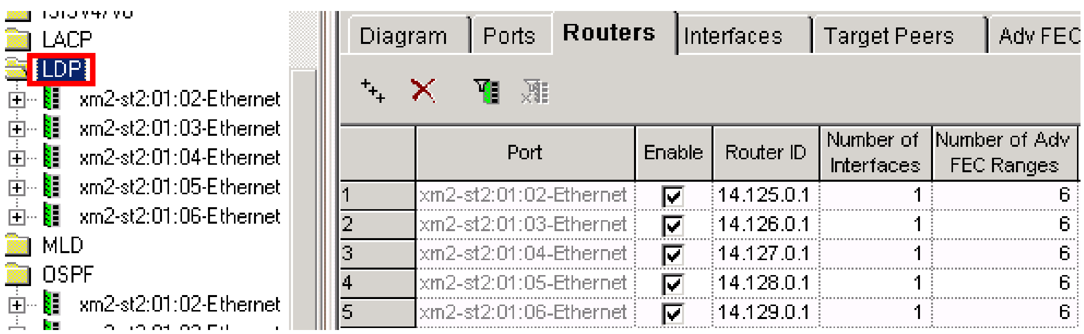


Figure 329. LDP P emulation

Six BGP routers are configured per PE port. These are emulated PE routers to establish BGP peering with DUT PE.

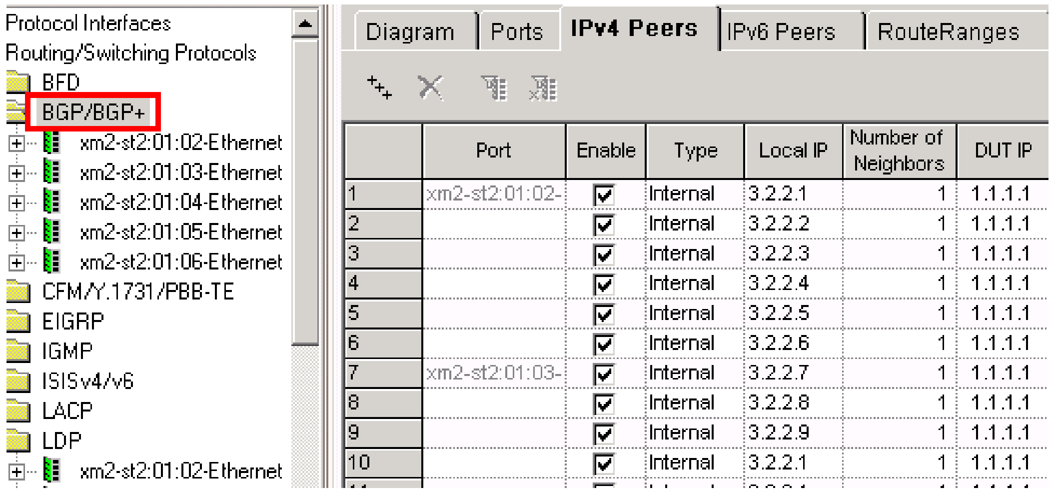


Figure 330. BGP PE emulation

C-multicast sources for each mVPN are advertised through BGP VPN Route Ranges.

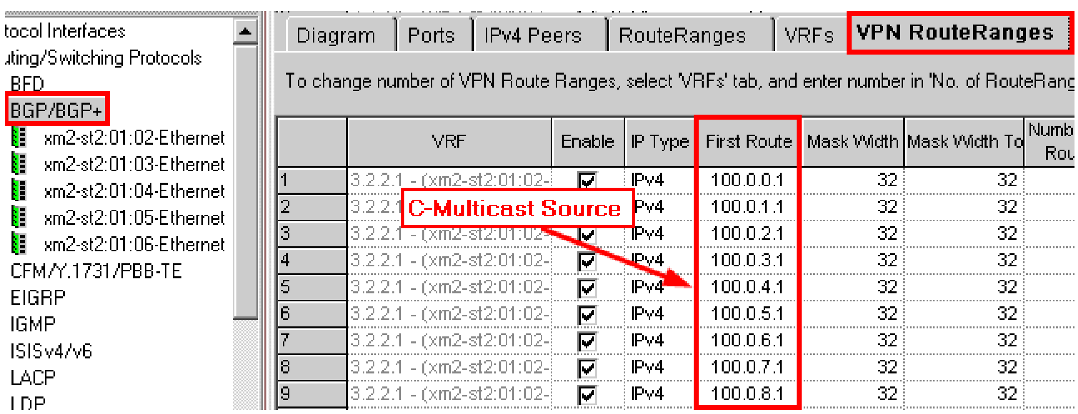


Figure 331. BGP PE Emulation VPN route range

Seven PIM routers are configured per PE port. The first six PIM routers are PE PIM routers. Each PIM router runs over 200 GRE interfaces for the 200 mVPNs supported. The last PIM router is the P PIM router which joins the default MDT groups for all mVPNs supported by the emulated PEs behind it and joins the multicast tree in the provider's multicast domain.

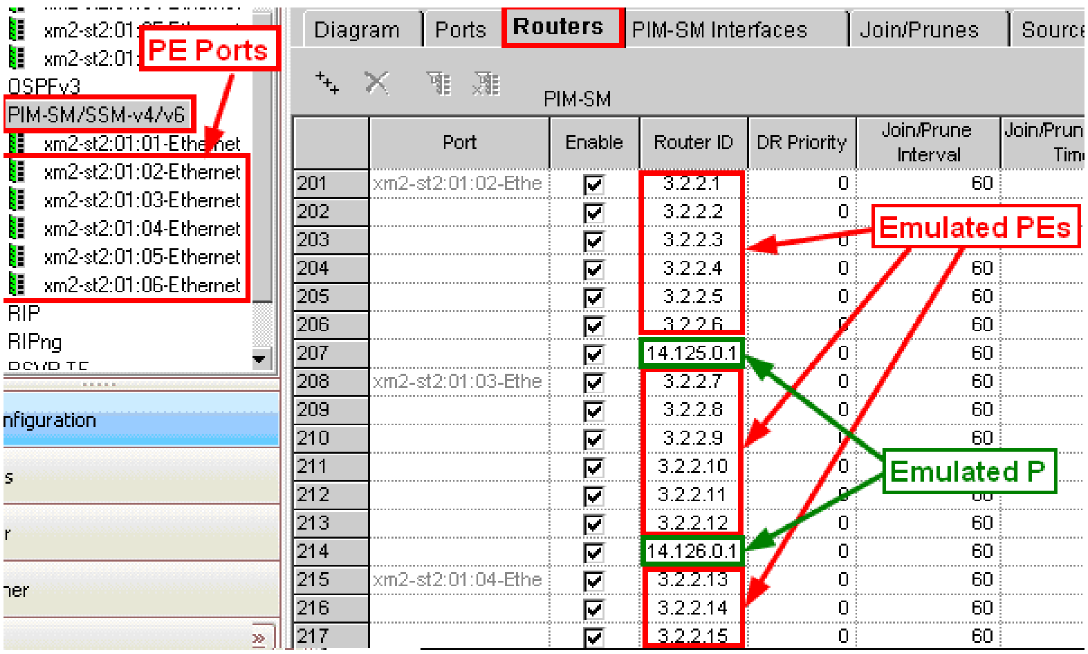


Figure 332. PIM PE emulation

Since C-Multicast sources are located behind the emulated PEs, the PE PIM routers are configured with a source range which will emulate the function of sources' DR and send Register to RP messages for each mVPN supported.

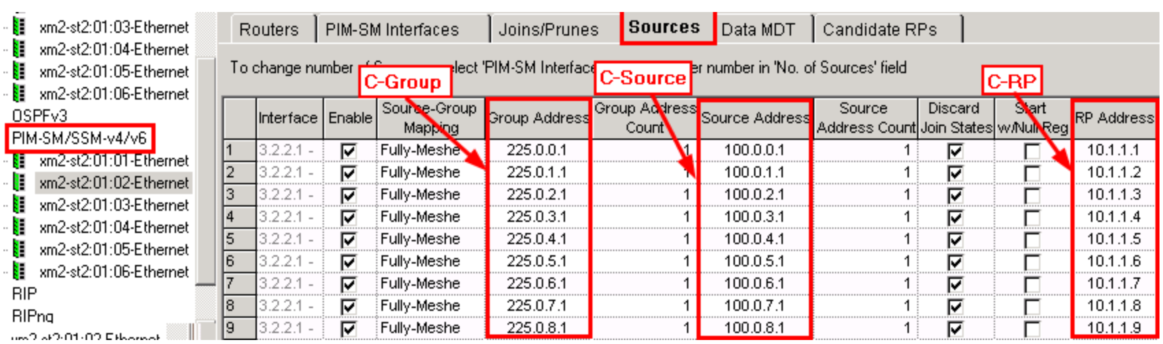


Figure 333. PIM PE emulation PIM source range

10. (Optional) This step is needed if the DUT uses Cisco IOS-XR:
   - Click on the CE port under **PIM-SM/SSMv4/6** in the protocol tree.
   - Go to the **Join/Prunes** tab in the right pane and click on the **Range Type** drop- down.
   - Select **(*,G)->(S,G)** from the drop-down list.
   - Highlight the entire **Range Type**, and then right click and select **Same**.

This is necessary due to an interoperability issue between the Ixia emulation and IOS-XR.

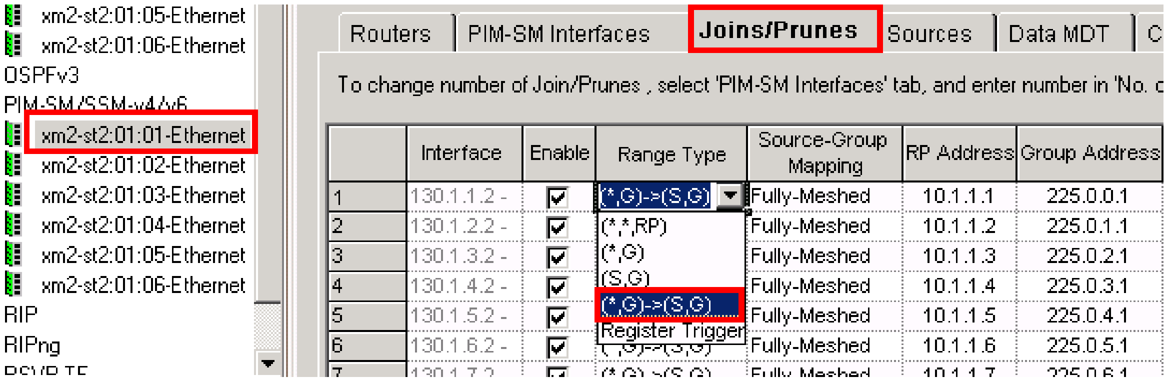


Figure 334. PIM CE émulation join/prune range

11. Start all protocols by clicking on the **Start Protocols** button in the top toolbar. This will start all configured protocols on all ports in this test session. You can also start protocols at the per-protocol or per-port level or on a per protocol and port level.

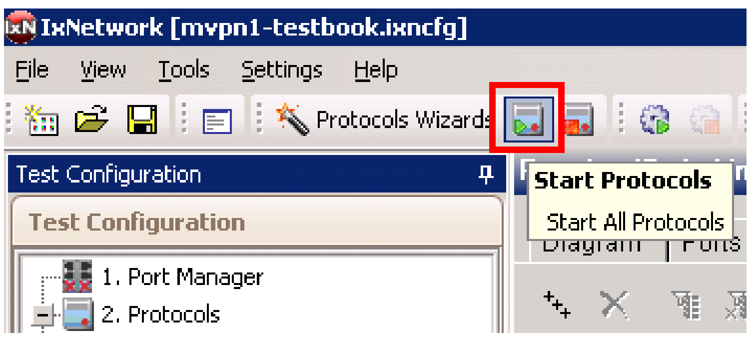


Figure 335. Start all protocols

Ensure that protocols are running at all ports.

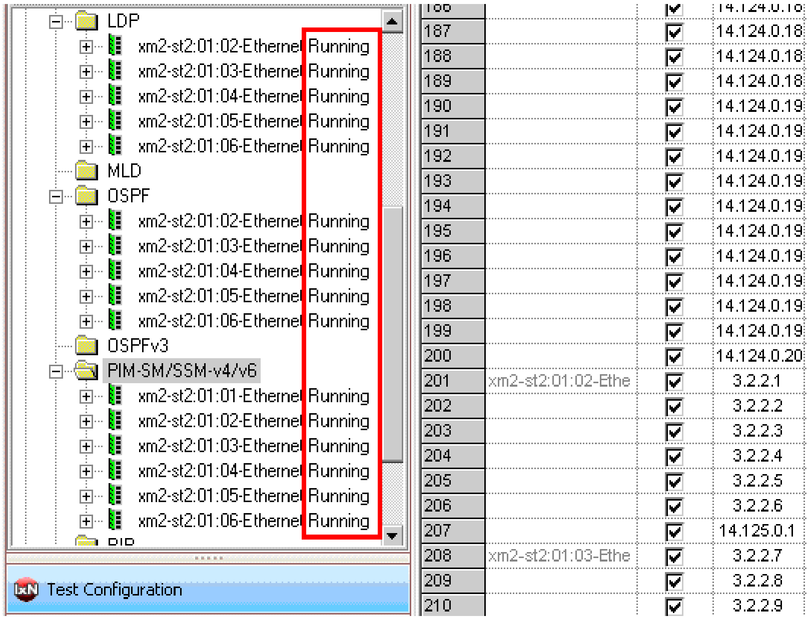
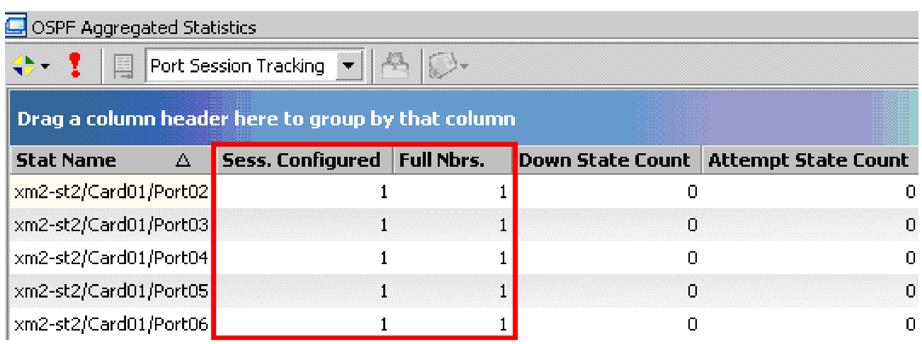


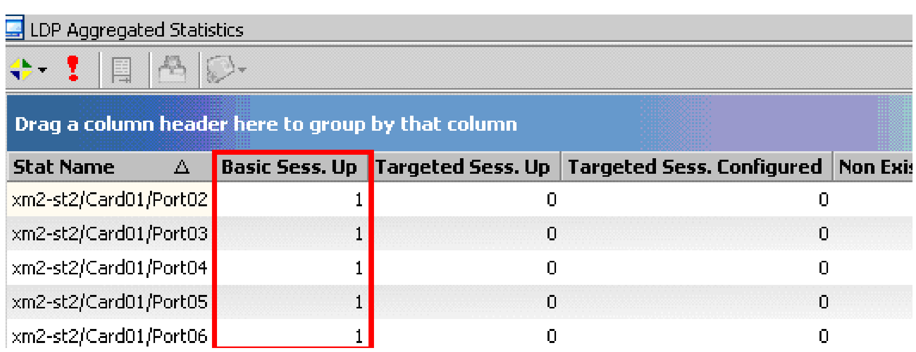
Figure 336. All protocols running

12. Switch to the **StatViewer** window and verify protocol statistics. Beside the general session statistics, each protocol statistics view will provide comprehensive statistics on protocol state machine operation for troubleshooting.



Stat Name	Sess. Configured	Full Nbrs.	Down State Count	Attempt State Count
xm2-st2/Card01/Port02	1	1	0	0
xm2-st2/Card01/Port03	1	1	0	0
xm2-st2/Card01/Port04	1	1	0	0
xm2-st2/Card01/Port05	1	1	0	0
xm2-st2/Card01/Port06	1	1	0	0

Figure 337. OSPF protocol statistics



Stat Name	Basic Sess. Up	Targeted Sess. Up	Targeted Sess. Configured	Non Exis
xm2-st2/Card01/Port02	1	0	0	
xm2-st2/Card01/Port03	1	0	0	
xm2-st2/Card01/Port04	1	0	0	
xm2-st2/Card01/Port05	1	0	0	
xm2-st2/Card01/Port06	1	0	0	

Figure 338. LDP protocol statistics

BGP Aggregated Statistics

Drag a column header here to group by that column

Stat Name	Sess. Configured	Sess. Up	Idle State Count	Connect State Count
xm2-st2/Card01/Port02	6	6	0	0
xm2-st2/Card01/Port03	6	6	0	0
xm2-st2/Card01/Port04	6	6	0	0
xm2-st2/Card01/Port05	6	6	0	0
xm2-st2/Card01/Port06	6	6	0	0

Figure 339. BGP protocol statistics

PIMSM Aggregated Statistics

Drag a column header here to group by that column

Stat Name	Rtrs. Configured	Rtrs. Running	Nbrs. Learnt	Hellos Tx	Hellos Rx
xm2-st2/Card01/Port01	200	200	200	7,600	2,622
xm2-st2/Card01/Port02	7	7	1,201	45,770	24,324
xm2-st2/Card01/Port03	7	7	1,201	45,698	24,308
xm2-st2/Card01/Port04	7	7	1,201	45,719	24,315
xm2-st2/Card01/Port05	7	7	1,201	46,672	24,955
xm2-st2/Card01/Port06	7	7	1,201	46,747	24,961

Figure 340. PIM-SM protocol statistics

Note: the number of PIM adjacencies=(# of emulated PEs) * (# of mVPN/PE) + 1.

13. After all the protocol sessions show as up in the Ixia protocol statistics, optionally verify the DUT's status for all protocol sessions. A Cisco DUT example is shown below.

```
RP/0/9/CPU0:ios#sh ospf neighbor
Mon Mar  9 09:32:48.027 UTC

* Indicates MADJ interface

Neighbors for OSPF 1000

Neighbor ID     Pri   State           Dead Time   Address     Interface
16.77.0.1       0     FULL/DROTHER    00:00:32    129.1.1.2   GigabitEthernet0/7/0/1
    Neighbor is up for 00:03:49
16.78.0.1       0     FULL/DROTHER    00:00:34    129.1.2.2   GigabitEthernet0/7/0/2
    Neighbor is up for 00:03:54
16.79.0.1       0     FULL/DROTHER    00:00:36    129.1.3.2   GigabitEthernet0/7/0/3
    Neighbor is up for 00:03:54
16.80.0.1       0     FULL/DROTHER    00:00:34    129.1.4.2   GigabitEthernet0/7/0/4
    Neighbor is up for 00:03:47
16.81.0.1       0     FULL/DROTHER    00:00:30    129.1.5.2   GigabitEthernet0/7/0/5
    Neighbor is up for 00:03:51

Total neighbor count: 5
```

Figure 341. Sample "show OSPF neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh bgp summary
Mon Mar  9 09:33:23.227 UTC
BGP router identifier 121.121.121.121, local AS number 1000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 1
BGP NSR converge version 1
BGP NSR converged
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker               1          1          1          1           1           1

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
3.2.2.1           0  1000   10016    9722        1    0    0 00:04:20          0
3.2.2.2           0  1000   10016    9722        1    0    0 00:04:22          0
3.2.2.3           0  1000   10016    9722        1    0    0 00:04:21          0
3.2.2.4           0  1000   10017    9722        1    0    0 00:04:22          0
3.2.2.5           0  1000   10016    9722        1    0    0 00:04:22          0
3.2.2.6           0  1000   10016    9722        1    0    0 00:04:24          0
3.2.2.7           0  1000    9801    9306        1    0    0 00:03:41          0
3.2.2.8           0  1000    9801    9306        1    0    0 00:03:38          0
3.2.2.9           0  1000    9801    9306        1    0    0 00:03:40          0
3.2.2.10          0  1000    9801    9306        1    0    0 00:03:41          0
```

Figure 342. Sample "show BGP summary" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh mpls ldp neighbor brief
Mon Mar  9 09:36:54.170 UTC

Peer              GR Up Time         Discovery Address
----------------- -- --------------- --------- -------
16.77.0.1:0       N  00:08:01                1       1
16.79.0.1:0       N  00:08:00                1       1
16.81.0.1:0       N  00:07:59                1       1
16.78.0.1:0       N  00:07:59                1       1
16.80.0.1:0       N  00:07:59                1       1
```

Figure 343. Sample "show MPLS LDP neighbor brief" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh pim neighbor
Mon Mar  9 09:39:56.718 UTC

PIM neighbors in VRF default

Neighbor Address  Interface              Uptime    Expires  DR pri   Flags

129.1.1.1*        GigabitEthernet0/7/0/1 2d20h     00:01:38 1 (DR) B A
129.1.1.2         GigabitEthernet0/7/0/1 00:10:57  00:01:17 0
129.1.2.1*        GigabitEthernet0/7/0/2 00:11:12  00:01:38 1 (DR) B A
129.1.2.2         GigabitEthernet0/7/0/2 00:10:58  00:01:17 0
129.1.3.1*        GigabitEthernet0/7/0/3 00:11:22  00:01:39 1 (DR) B A
129.1.3.2         GigabitEthernet0/7/0/3 00:10:57  00:01:17 0
129.1.4.1*        GigabitEthernet0/7/0/4 00:28:31  00:01:40 1 (DR) B A
129.1.4.2         GigabitEthernet0/7/0/4 00:10:57  00:01:17 0
129.1.5.1*        GigabitEthernet0/7/0/5 00:11:57  00:01:40 1 (DR) B A
129.1.5.2         GigabitEthernet0/7/0/5 00:10:58  00:01:17 0
```

Figure 344. Sample "show PIM neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh pim vrf mvpn1 neighbor
Mon Mar  9 09:41:40.723 UTC
PIM neighbors in VRF mvpn1

Neighbor Address    Interface              Uptime    Expires  DR pri   Flags

130.1.1.1*          GigabitEthernet0/7/0/0.1 00:30:09  00:01:19 1 (DR) B A
130.1.1.2           GigabitEthernet0/7/0/0.1 00:12:44  00:01:30 0
1.1.1.1*            mdtmvpn1               5d21h     00:01:26 1 (DR) B A
3.2.2.1             mdtmvpn1               00:11:44  00:01:30 0
3.2.2.2             mdtmvpn1               00:12:05  00:01:28 0
3.2.2.3             mdtmvpn1               00:11:44  00:01:30 0
3.2.2.4             mdtmvpn1               00:11:41  00:01:33 0
3.2.2.5             mdtmvpn1               00:11:44  00:01:30 0
3.2.2.6             mdtmvpn1               00:11:41  00:01:33 0
3.2.2.7             mdtmvpn1               00:11:44  00:01:30 0
3.2.2.8             mdtmvpn1               00:11:46  00:01:28 0
```

Figure 345. Sample "show PIM VRF mvpn1 neighbor" output for Cisco IOS-XR

14. When the control plane is up and running, you can build traffic from multicast sources to multicast receivers to validate data plane forwarding.

15. Go to **Test Configuration → Traffic** and click on  button to launch the Advanced Traffic wizard.

Figure 346. Add Traffic Item

16. At **Endpoint** page, perform the following configuration tasks:
    a. Name your traffic item and select Type of Traffic.
    b. Under Traffic Mesh, select One-One for Source/Dest. This is due to the nature of the VPN; sources and destinations that belong to different VPNs do not talk to each other.
    c. Under Traffic Mesh, select Fully Meshed for Routes/Hosts. In the mVPN case, this mesh should match with the Source-Group Mapping in the Register Ranges or Join/Prune range.
    d. In the Source window, select PIMSM Register Ranges under All Ports. This will select PIMSM Register Ranges under all PE ports.
    e. In the Destination window, click on the + button in front of the CE port to expand the tree by a level and select PIM-SM/SSM. This will select all PIM Join/Prune ranges under CE port.

    f. Click on button to add the source and destination endpoints. There are 6,000 source endpoints (30 PEs * 200 mVRFs/PE) and 200 destination endpoints (200 PIM Join range, one per mVRF).

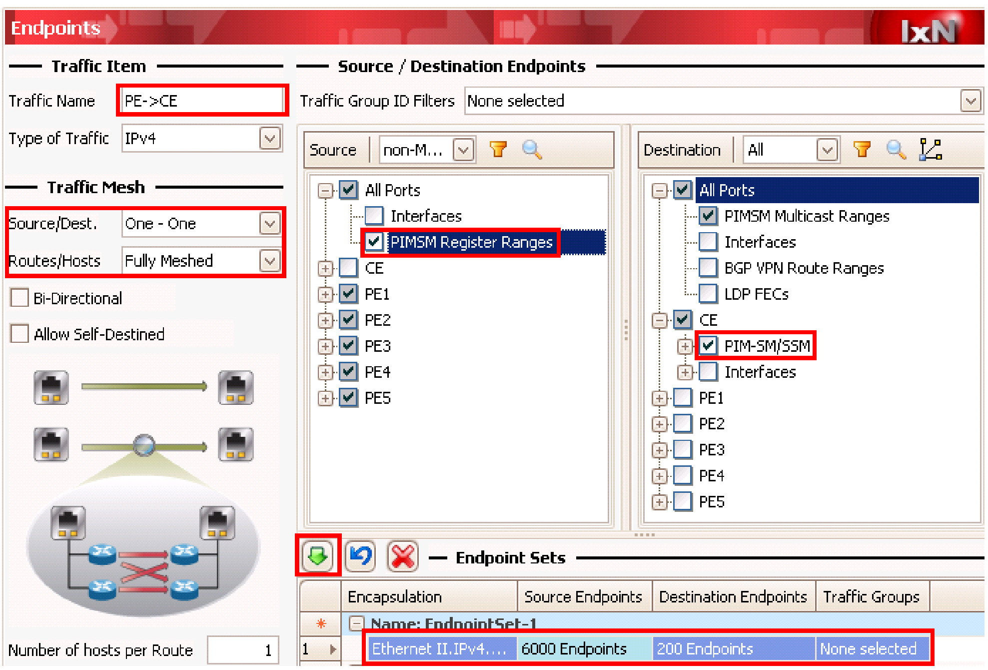


Figure 347. Traffic Wizard Endpoint Selection

Figure 348 expands the source and destination tree further to show the leaf endpoints.

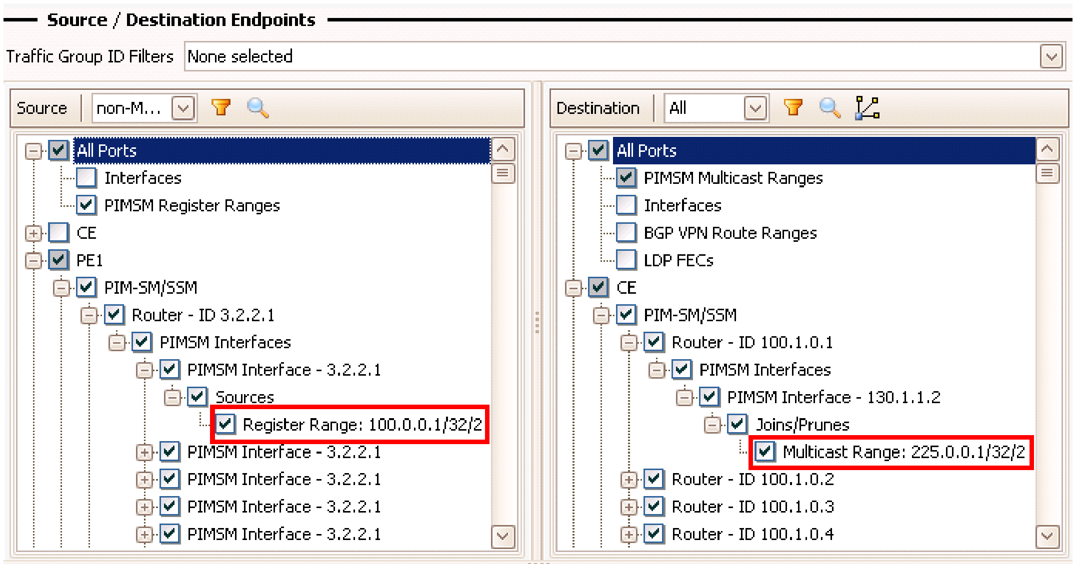


Figure 348. Traffic Wizard Endpoint Selection - Expanded Endpoints

Notes: The list below shows various options to filter the traffic endpoint tree and help you find a specific traffic endpoint quickly.

- Traffic Group ID Filters Traffic Group ID Filters
- Encapsulation
- Quick Selection
- Search
- Multicast Endpoint Selection

17. At the **Packet/QoS** page, available QoS fields are populated based on the traffic encapsulation. You can modify any available QoS field, e.g., IP Precedence. Skip this page if you do not want to modify QoS value.

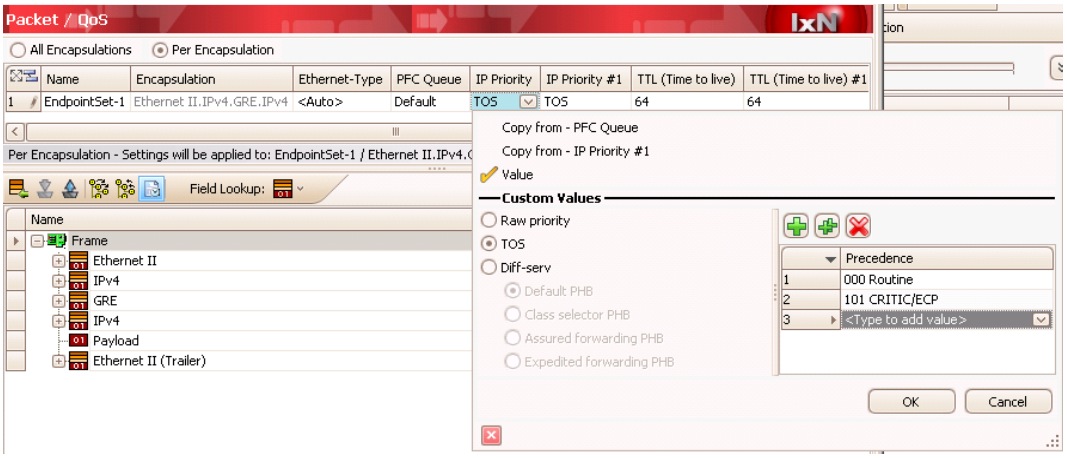


Figure 349. Traffic Wizard Option

18. At **Flow Group Setup** page, various options are populated based on packet content. These options are used to create various traffic profiles which allow you tune transmit parameters for each profile. Skip this page if you do not need create different traffic profiles.

19. At **Frame Setup** page, set desired frame size.

20. At **Rate Setup** page, select the **Transmit mode** which matches the transmit mode at port property and set desired rate. You can also use the **Rate Distribution** option to control how to apply the configured rate across flow groups and ports.

21. At the **Flow Tracking** page, select IPv4: **Destination Address** and IPv4: **Destination Address** (1). The **Traffic Item** is selected automatically as long as there is another tracking option selected. This will give you an aggregated view at the Traffic Item level, per-VPN level (**IPv4: Destination Address** is the default MDT group for multicast VPN and therefore gives per-VPN level aggregation), and per-flow statistics for each multicast group address.

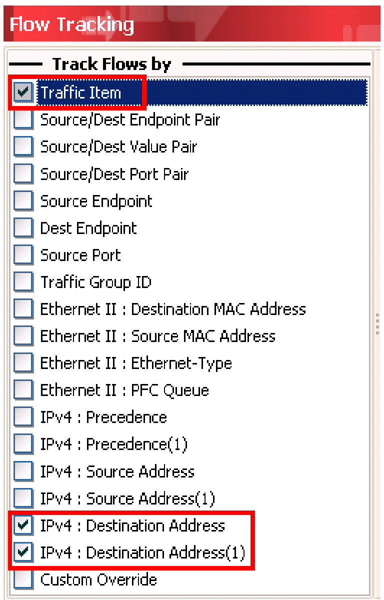


Figure 350. Traffic Wizard Tracking Option

22. At the **Preview** page, click on **View Flow Groups/Packets** to preview the packet content.

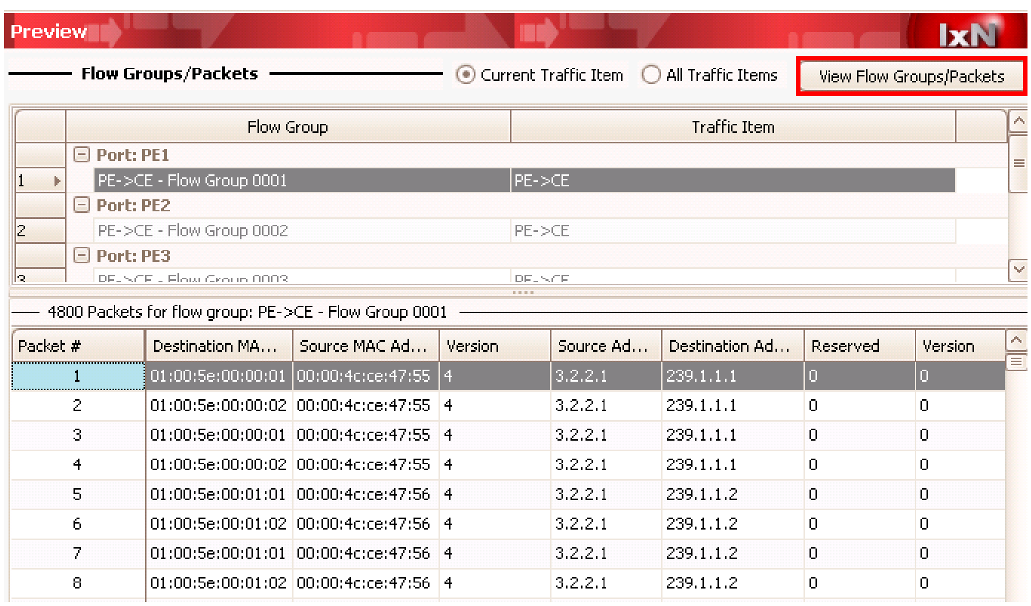


Figure 351. Traffic wizard – Preview

23. Upon clicking the **Finish** button, traffic will be built and a traffic item is created under the **All Traffic Items** tab in the left panel, and all flow groups for this traffic item will show in the traffic grid at the right panel.

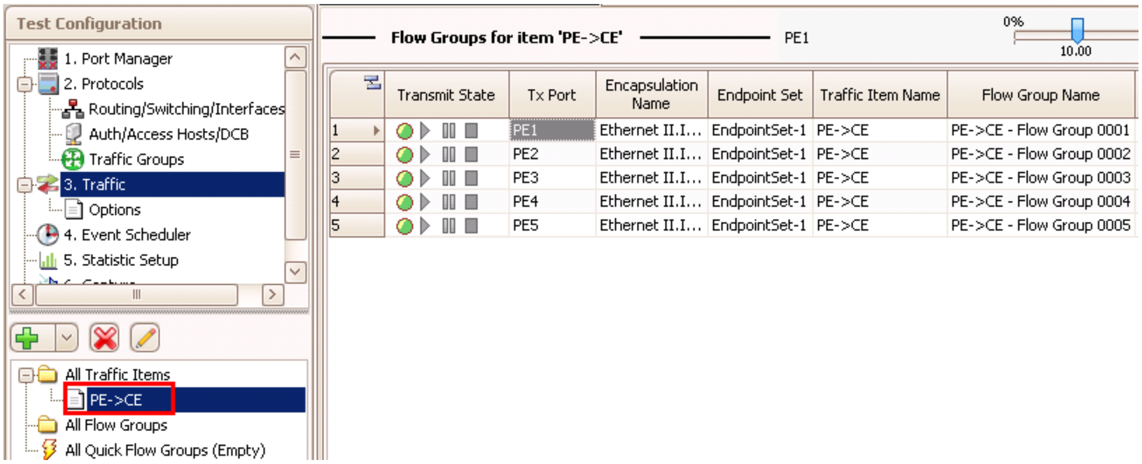


Figure 352. Traffic Item and Flow Groups

24. At the Traffic Grid, you can use grid options to customize Frame Size, Frame rate, etc. You can also control traffic start/stop/pause/resume at a per-flow group level.

25. To view the generated packet content in detail, right-click on any flow group to bring up the **Packet Editor** window. Figure 353 shows that the packets generated are GRE packets. The top part is a packet decoding. Click on **Hex View** on the lower left corner to bring up the binary encoding view. The total number of generated packets is also shown. You can click the **>>** button on the bottom to view the content of each packet.

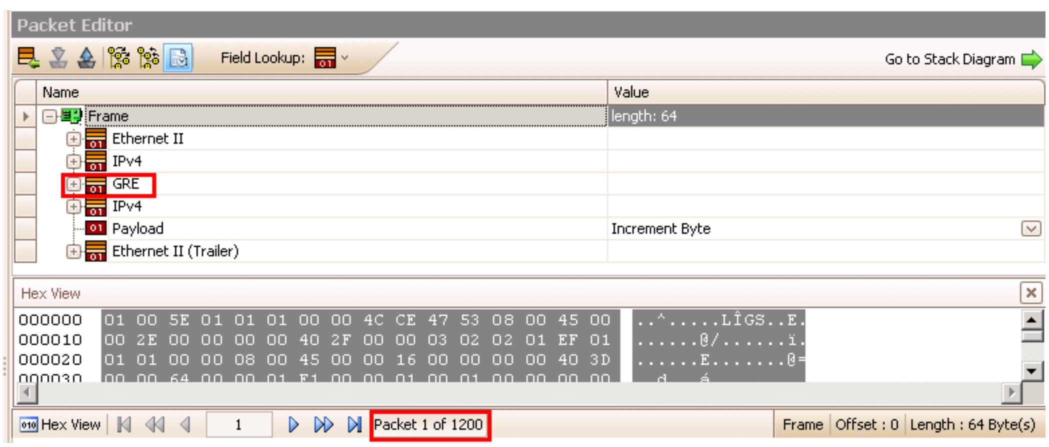


Figure 353. Packet Editor

26. Expand the outer IPv4 header to view the content. The source IP is from the emulated PE loopback address and the destination IP is the default MDT group for that mVPN.

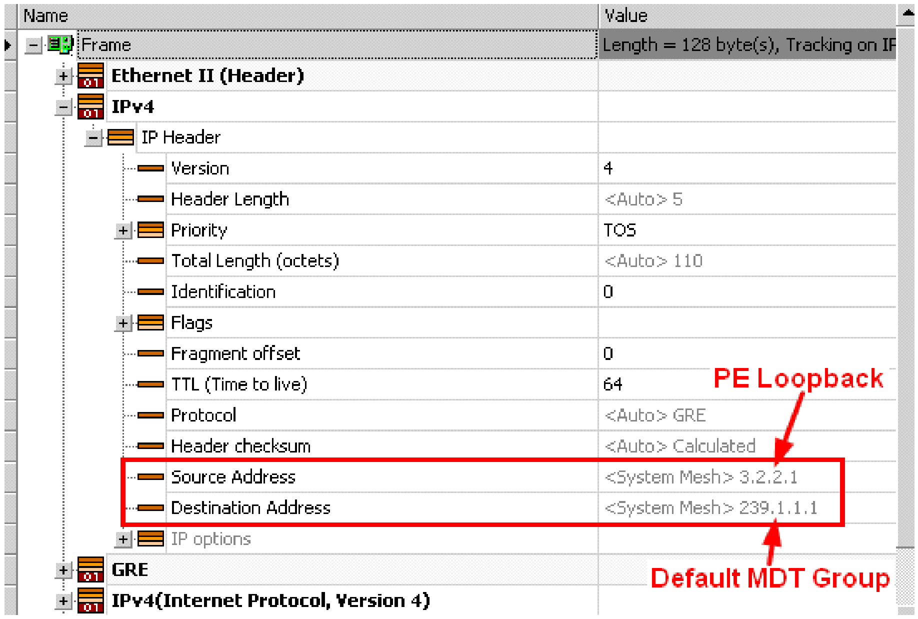


Figure 354. Packet Editor - outer IP expansion

Expand the inner IPv4 header to view the content. The source IP is the C-multicast source address and the destination IP is the C- multicast group address.

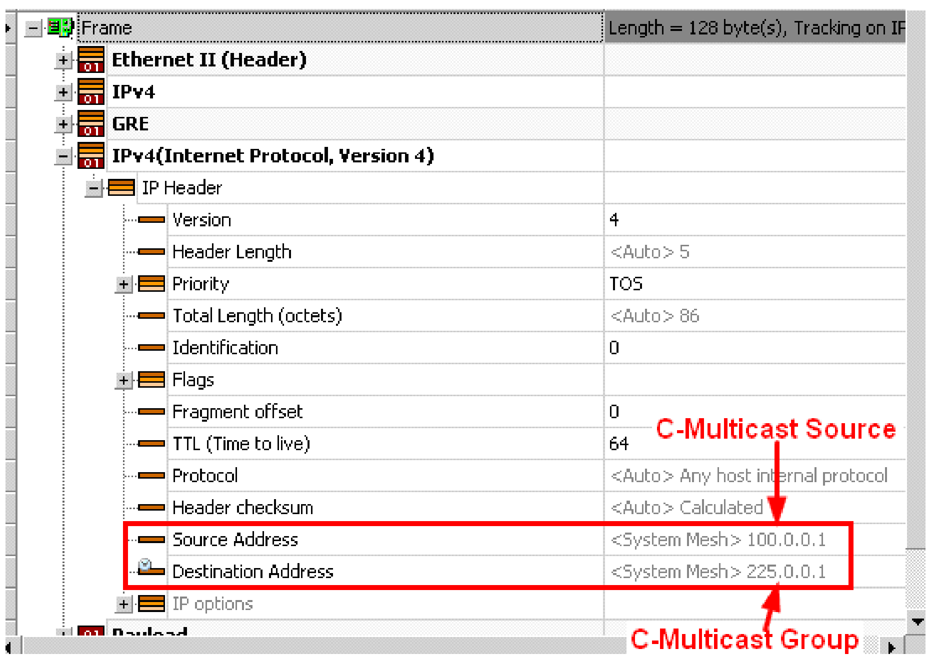


Figure 355. Packet Editor - inner IP expansion

27. **Apply** and **Start** the traffic.

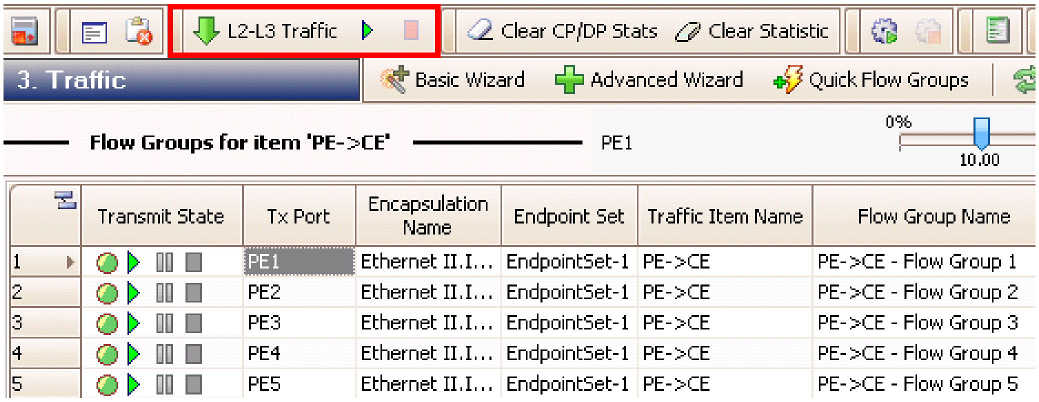


Figure 356. Apply and start traffic

28. Switch to the **StatViewer** window. Click on **Traffic Item Statistics** under the **Traffic** tab to bring up the aggregated traffic item statistics view at the right panel. This gives you aggregated statistics per traffic item.

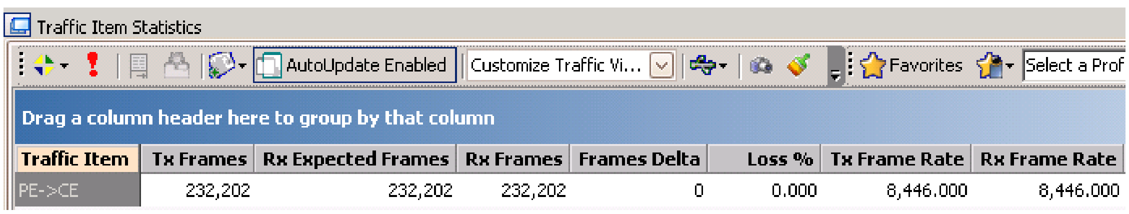
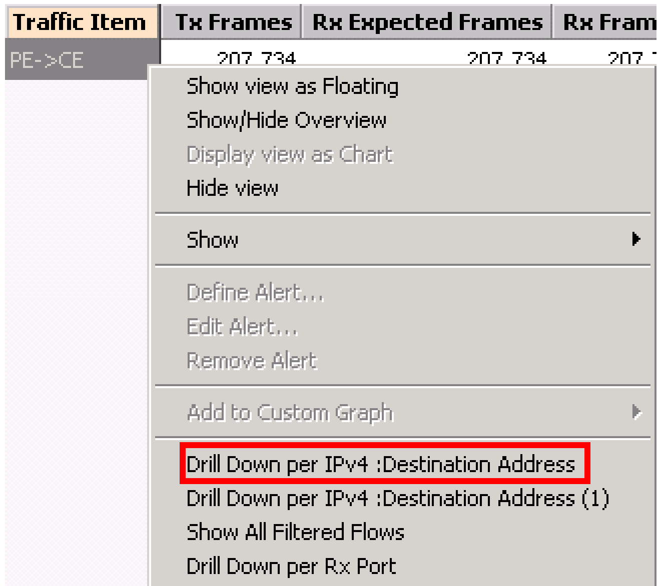


Figure 357. Traffic Item Statistics

29. Right click on the traffic item. Available drill-down options are populated based on tracking options selected. Select **Drill Down per IPv4 :Destination Address** to bring up an aggregated view per VPN.



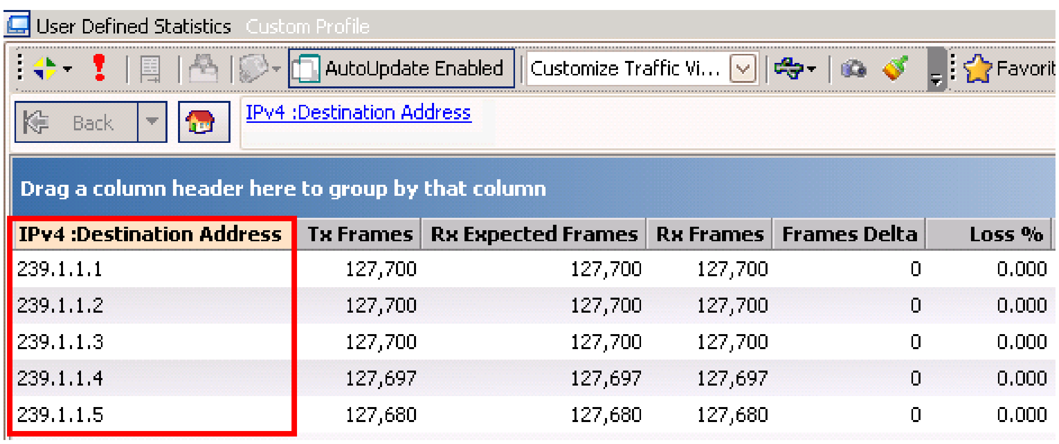


Figure 358. Drill down options and drill down view from Traffic Item Statistics

30. Right click on the **239.1.1.1** flow (default MDT group for mVPN1) and drill down further by selecting **Drill down per IPv4: Destination Address (1)** to bring up a per-destination address (C- multicast group) flow view for mVPN1.

    Notes: IPv4: Destination Address (1) means inner GRE IPv4 Destination Address.

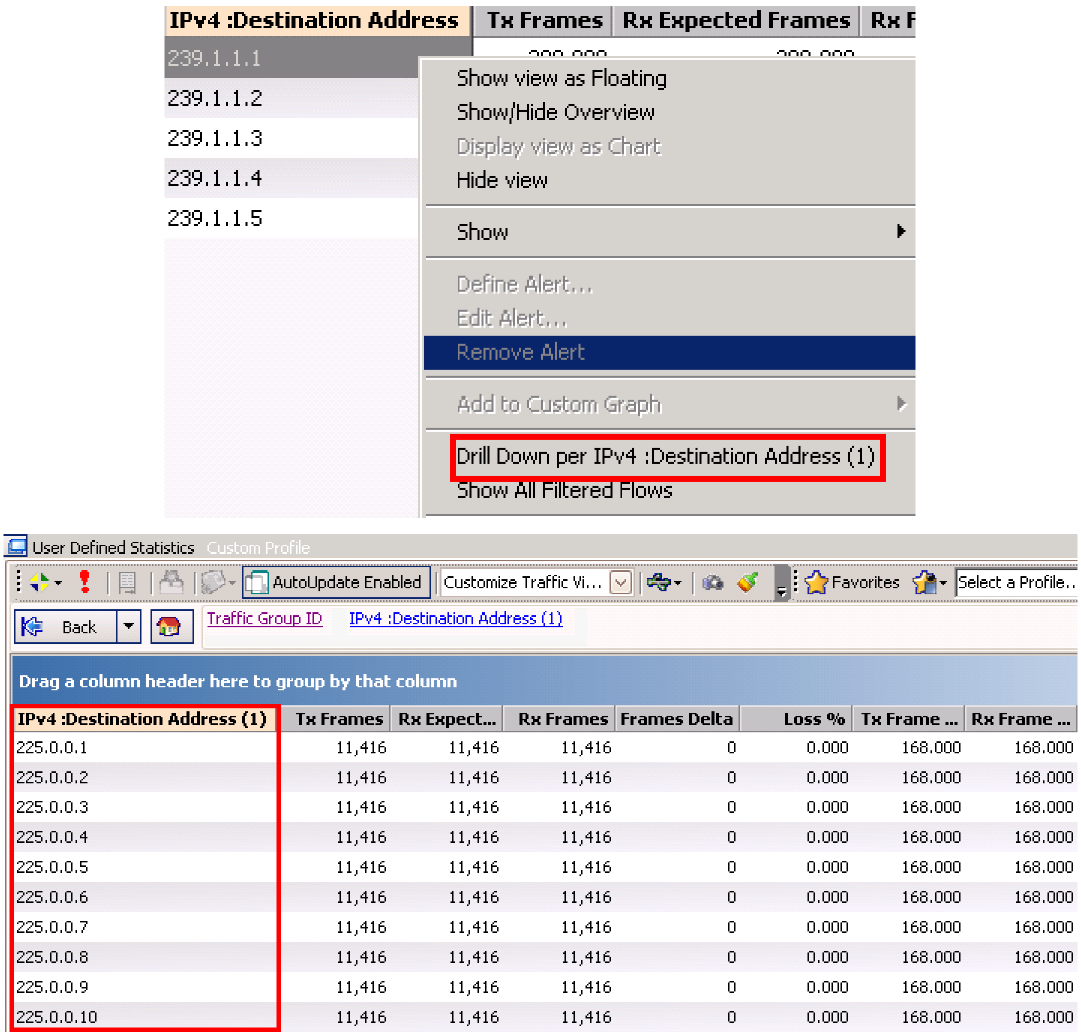
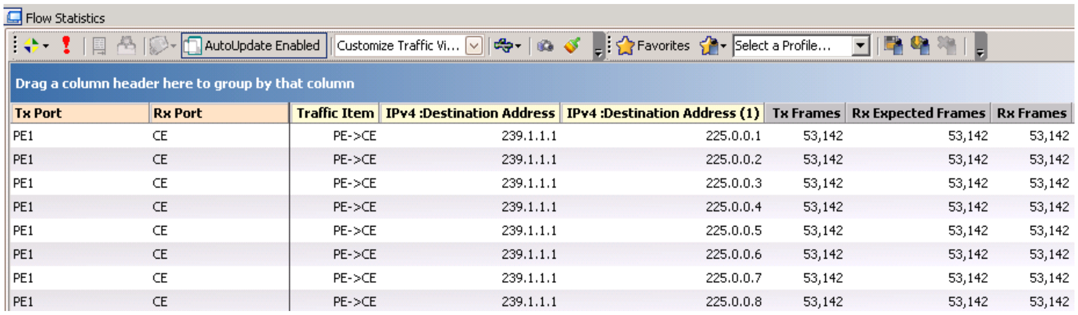


Figure 359. Drill down options and drill down view from per VPN level view

31. Click on **Flow Statistics** in the left panel to bring up the statistics view for all flows. This gives you a flat view for all flows of all traffic items.


Flow Statistics

AutoUpdate Enabled

Customize Traffic Vi...

Favorites

Select a Profile...

Drag a column header here to group by that column

Tx Port	Rx Port	Traffic Item	IPv4 :Destination Address	IPv4 :Destination Address (1)	Tx Frames	Rx Expected Frames	Rx Frames
PE1	CE	PE->CE	239.1.1.1	225.0.0.1	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.2	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.3	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.4	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.5	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.6	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.7	53,142	53,142	53,142
PE1	CE	PE->CE	239.1.1.1	225.0.0.8	53,142	53,142	53,142

Figure 360. Flow Statistics view

The aggregated, drill-down, and per-flow statistics impose a hierarchy on a typically huge amount of flow statistics. You can nail down the problem from top level down to look at only flows with problems. Both aggregated and detailed flow statistics views provide important statistics that allow you to monitor the data plane forwarding operation, including frame delta, loss %, Rx frame rate, various Rx rates (in Bps, bps, kbps and Mbps), various latencies (min, max and avg) and timestamps.

Result Analysis

Using Ixia protocol statistics, it can be seen that all expected protocol sessions are up and running. After starting traffic, continue to monitor protocol statistics to verify whether the control plan can sustain itself with data plane traffic.

In IxNetwork 5.40, Ixia introduced powerful aggregated and drill-down views at various user defined levels. This helps you to identify the problem quickly. You can start with the top level aggregated view for traffic items and monitor various Rx stats and latency/jitter. You can then drill down to various aggregated levels to narrow down the flows which have problems. This greatly reduces troubleshooting time.

The Snapshot CSV function can be used to record the statistics for one or more statistics views at any point of time. You can capture a particular view at any time for post analysis.

From the result we have so far, both control plane and data plane operation are sustained. Now we can add more Ixia ports to emulate additional PEs in order to scale up and verify both control plane and data plane operation. The test can be repeated with additional emulated PEs until the control plane and data plane fail.

Based on this test, we can determine the maximum number of remote PEs that the DUT can handle with 200 mVPN supported at the system level.

Troubleshooting and Diagnostics

Issue	Troubleshooting solution
Cannot Ping DUT	Check the **Protocol Interface** window to see whether there is a red exclamation mark (!) in front of any protocol interface. If there is, then there is a mismatch between the DUT IP and Ixia port's IP subnet, VLAN or link mode (copper versus fiber). Correct it and make sure red exclamation mark goes away.
OSPF session does not come up	Verify the OSPF area ID, link type and MTU on both the Ixia and DUT sides to make sure they match.
BGP sessions between emulated PEs and DUT PE do not come up or only partially not up	First verify the IGP session between the DUT and the emulated P router. If the session is up, verify that the DUT's routing table has routes to the emulated PE loopback address to avoid a possible connectivity issue. If this is not the case, then verify that the DUT and Ixia configuration have matching PE loopback address, BGP AS numbers, BGP capability, etc.
PIM sessions for VPNs do not come up	Make sure that PIM is enabled on the DUT loopback interface used for BGP peering. The PIM adjacencies for VPNs are setup using this address. Also verify that the RP address for the provider network on the DUT and Ixia port the same.
Traffic started from PE to CE or CE to PE, but no packet received on receiving port	Check the DUT's global and VPN multicast routing table to make sure that the multicast routes are correct. Also check the VPN unicast routing table to make sure that the C-multicast source is learned and is installed in the VRF routing table. If the DUT is a Cisco IOS-XR router, then make sure you performed Step 10 above.

Test Variables

Test Variable	Description
Port Role	An Ixia port can simulate either a multicast source or receiver behind it. You can choose this option on page 1 of the mVPN wizard.
# of PE ports	An Ixia port can emulate a provide edge router which will join an mVPN and peer with a DUT PE over a default MDT tunnel. You can increase the number of Ixia PE ports to satisfy your scalability requirement.
# of CE ports	An Ixia port will emulate a customer promise router connected to a DUT PE. You can increase the number of Ixia CE ports per your requirement.
IGP Protocol	The available options are OSPF and ISIS. The IPG protocol can be chosen based on your network.
MPLS Protocol	The available options are LDP and RSVP. The MPLS protocol can be chosen based on your network.
Provider Multicast Protocol	The available options are PIM-SM and PIM-SSM. The multicast protocol can be chosen based on your network.
# of Emulated PE Routers	An Ixia port can emulate a number of provider edge routers that support a number of mVPNs. This is one area that can grow quite large in a service provider's network. The DUT needs to maintain PIM adjacencies with remote PEs for each mVPN it supports. The BGP peering may or may not be a concern here as there will be router reflectors in a service provider network to reduce BGP peering for edge PEs.
# of Emulated mVPNs per PE router	This parameter should be considered in conjunction with **# of Emulated PE Routers**.
# of C-multicast sources per mVPN	With an increase of the number of C-multicast sources, the DUT multicast routing table entries and forward table entries will increase. With traffic, this will stress both the DUT control state and data forwarding state.
# of C-multicast groups	This parameter will also affect the DUT multicast routing table and forwarding table. It can also test a DUT's forwarding capability on replicated multicast packets.
CE IGP (unicast) Protocol	The unicast protocol running between CE and PE. This is used to advertise multicast sources behind the Ixia CE port. This option will be grayed out if the Ixia's CE port role is source.
IPv6 parameters	Ixia can emulate a customer IPv6 network. This is disabled by default.

The proposed test can be scaled up or down based on test variables described above.

Conclusions

Based on the Result Analysis, the maximum number of remote PEs per mVPN with 200 mVPNs per system will be determined. The DUT must sustain performance of both the control plane and the data plane to meet the specific scalability requirement.

Test Case: mVPN Data MDT Switchover Performance Test

Overview

mVPN data MDT was introduced to achieve optimal routing over default MDT. It connects PE routers with interested receivers for a particular multicast flow. The PE router monitors the multicast traffic rate on a per-flow basis and based on pre-configured bandwidth thresholds decides to signal data MDT that switches the traffic over from default MDT tree to data MDT tree. This test is designed to test a PE device's ability to source data MDT and measure its switchover latency at scale. The control plane data MDT signaling is setup first and is followed by data plane traffic to verify data MDT forwarding. The test can be scaled up until the switchover latency is beyond a specific tolerance.

The topology for this test is shown in Figure 361. The Ixia CE port will emulate C-multicast sources behind it and therefore the DUT PE will initiate data MDT tree and will perform data MDT signaling and switchover function.

Another data MDT switchover performance test measures a PE device's ability to join data MDT. The test procedure is similar to the test above; the difference in term of Ixia configuration will be explained in Appendix A.

Objective

The object of this test is to determine the DUT's ability to signal data MDT and perform data plane switchover from default MDT to data MDT. Traffic is first sent over default MDT. The traffic rate is then increased over a DUT configured threshold. Per-flow traffic packet loss statistics are measured during switchover.

Setup

Four Ixia test ports are used in this test. One port emulates a local CE connected to a DUT PE and the other three ports emulate P and remote PEs connected to the DUT's PE core-facing interfaces. C-multicast sources are emulated behind the CE port. C-multicast receivers are emulated behind the PE ports. Each PE port emulates 10 PEs with 20 mVPNs per PE. You can increase the number of C-multicast flows (C-multicast sources and/or C-multicast receivers), emulated PEs/mVPNs and PE ports to match your real network requirements.

The IxNetwork mVPN protocol wizard is a great starting point. It walks you through, screen by screen from P/PE to CE to help you quickly build a large mVPN configuration. With the wizard's append function, you can expand an existing configuration to increase the number of PEs or number of mVPNs per PE without interrupting your test. Figure 361 shows you the topology we will emulate in this test.

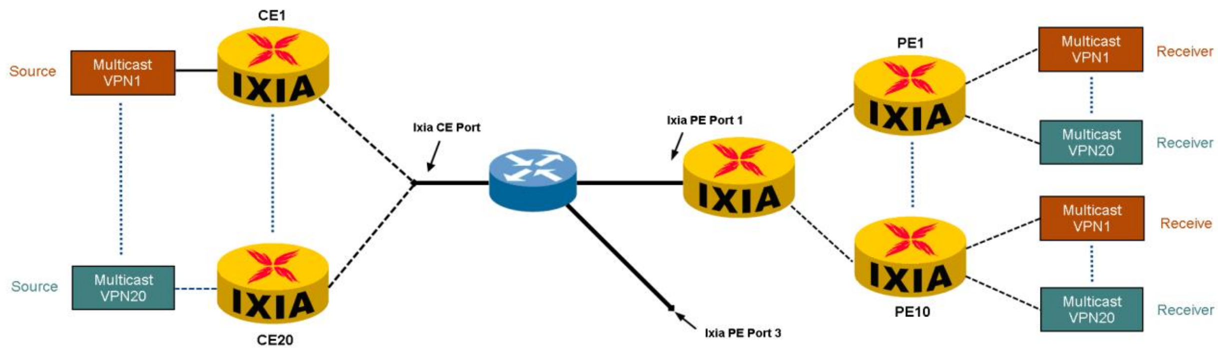


Figure 361. Multicast VPN data MDT switchover performance test topology

Step-by-Step Instructions

1. Launch the **Multicast VPN Wizard** and configure port 1 as a **CE Side** port and ports 2-4 as **PE Side** ports. Configure the CE port's role as **Source** and the PE ports' roles as **Receiver** (**Source** means that the emulated multicast sources are behind the port and **Receiver** means emulated receivers are behind the port).

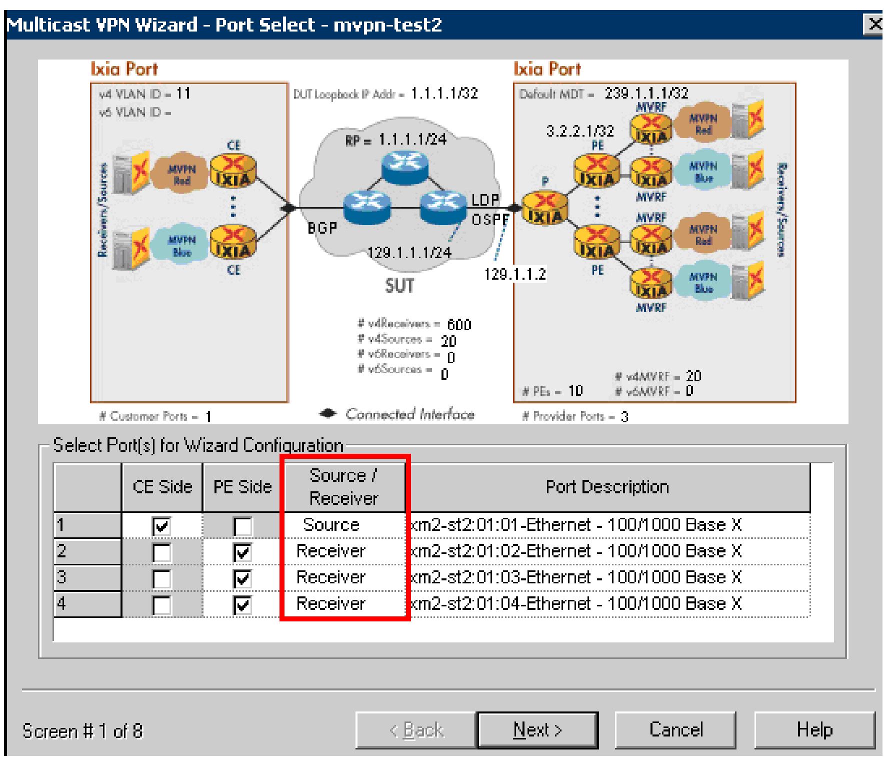


Figure 362. mVPN wizard screen #1

2. On Screen #2 of 7, perform the following configuration tasks:
   - **P Router IP Address** – The emulated P router IP address that is connected to the DUT's core facing interface.
   - **DUT IP Address** – The DUT interface IP address facing the core. If the P Router IP Address is changed, the DUT IP Address will be auto-filled with immediately preceding address within the subnet.
   - **Increment Per Port** – This field controls the increment across ports for the two fields above.
   - **Starting Subnet Between P and PE** – This is used for links between Ixia emulated Ps and PEs.
   - **IGP Protocol** – The IGP protocol used in the core. The DUT will establish IGP session with the Ixia emulated P router. Available selections are OSPF (default) and ISIS.
   - **Provider Multicast Protocol** – Multicast protocol used in the provider multicast domain. Available selections are PIM-SM (default) and PIM-SSM.
   - **Provider Network RP Address** – The RP address in the provider multicast domain when PIM-SM is used. It is grayed out if PIM-SSM is used. Please note that **Provider Network RP Address** should reside at the DUT or other P router outside the Ixia ports.
   - **MPLS protocol** – The MPLS protocol used in the core. The DUT will establish an MPLS protocol session with the Ixia emulated P router and receive label mappings from the Ixia port for emulated PE loopback addresses.

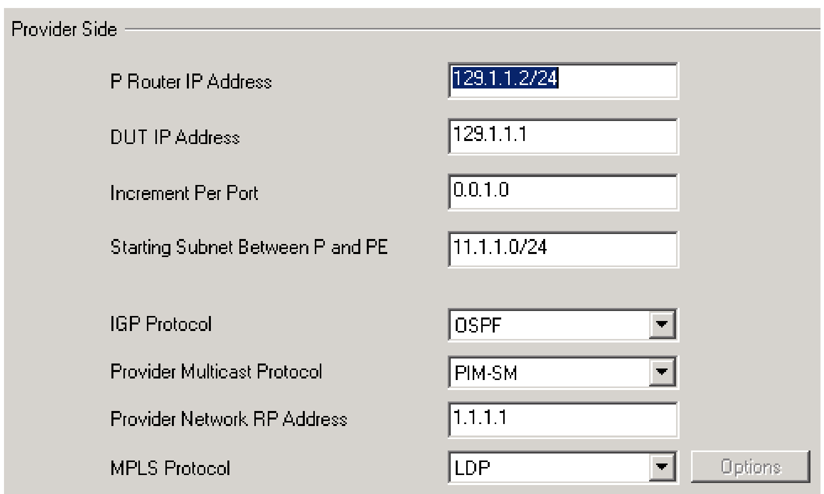


Figure 363. mVPN wizard screen #2 – setup P router

3. On Screen #3 of 7, perform the following configuration tasks.

   a. **Number of PE Routers Connected to the P router** – The number of emulated PE routers per P router.
   b. **AS number** – The AS number in which the emulated PE routers reside.
   c. **Emulated PE loopback IP Address** and increment options – The first emulated PE loopback address, and the increment option to determine the IP addresses of the rest of the PE loopback addresses. This will be used for BGP peering and PIM peering.
   d. **DUT Loopback IP Address** and increment options – The DUT loopback address which will be used for BGP peering and multicast tunnel source address.

Be sure to enable **Ignore all Ixia Emulated PIM Neighbors** when you have more than one PE port and the emulated PEs support the same set of mVPNs. In this way the Ixia PE port will only maintain PIM adjacencies over default MDT with the DUT and drop all other adjacencies among themselves in order to achieve better emulation performance.

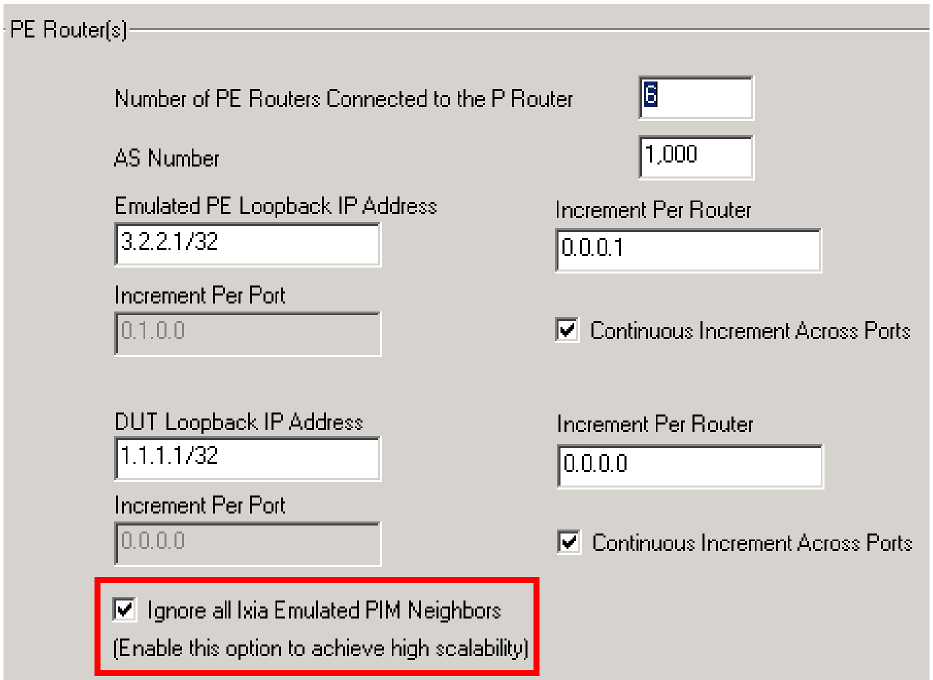


Figure 364. mVPN wizard screen #3 - setup PE router

4. On screen #4 of 7, perform the following configuration tasks:
   a. Configure the **Route Target** (RT) value used for first mVPN and **Step** to increment RT for the remaining mVPNs. In this example, the RT for the first mVPN is (100:1) and the step is (0:1). Therefore RTs for the remaining mVPNs will be 100:2, 100:3, 100:4 … 100:200.
   b. By default, **Route Distinguisher** (RD) is configured to be the same as RT. If you want to configure RD separately, you can uncheck **Use Route Target** and configure the RD value and step separately from RT.
   c. Configure **Number of VPNs per PE** to *200*.
   d. Configure **First Default MDT Group Address** to *239.1.1.1/32***.**
   e. Check **Enable DATA MDT (for IPv4 CE Ranges**). All data MDT related parameters will be available for editing.
   f. Keep the defaults for **Use SSM for DATA MDT** and **Increment DATA MDT Address per PE**.
   g. Configure **Starting Data MDT group address DUT side** to *232.1.1.1*. This address should match the data MDT group address configured at the DUT for each mVPN. The Ixia P router will be configured with a triggered join range to respond to DUT's data MDT join.
   h. Uncheck **Automatically calculate Data MDT Group Address for PE side** if you want to configure the Starting Data MDT group address at the Ixia side differently from the one calculated automatically.

i. Configure **Switchover Interval.** Default value is 60 sec. This is the time that the Ixia emulated PE router will send Data MDT join TLV messages after starting the PIM protocol in order to emulate the Data MDT switchover function.

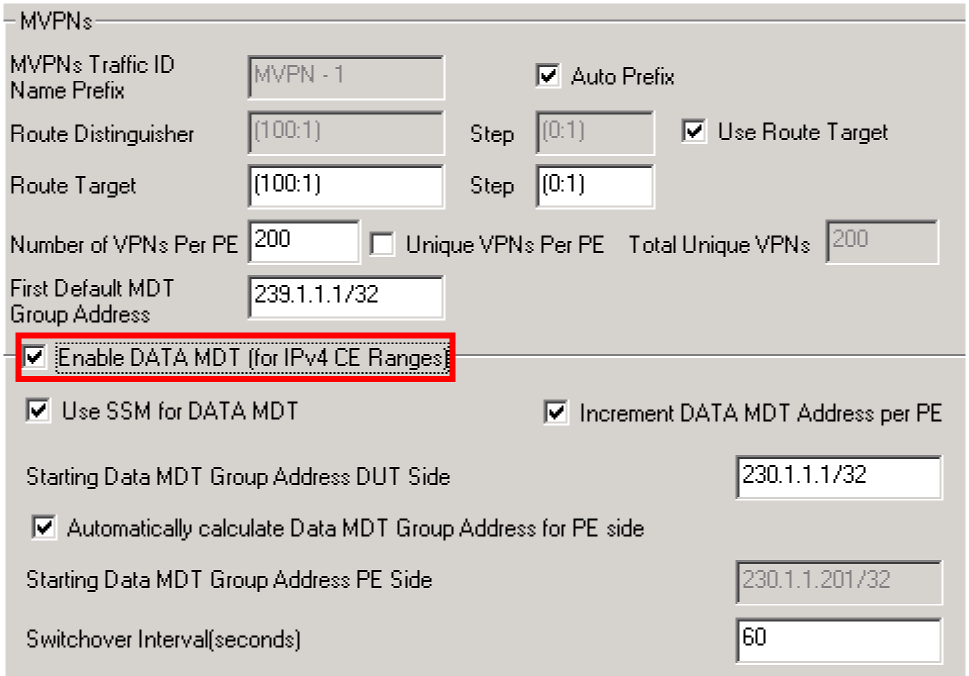


Figure 365. mVPN wizard screen #4 - setup mVPN and data MDT

5. On screen # 5 of 7, perform the following configuration tasks:
    a. **Multicast Source Address**
        - **Address per MVPN** – The number of emulated C-multicast source addresses per mVPN per PE.
        - **Starting Source Address –** The first C-multicast source address used.
        - **Incremented By –** The increment step for configuring the rest of the C-multicast source addresses.
    b. **Multicast Group Address**
        - **Address per MVPN –** The number of emulated C-multicast group addresses per mVPN per PE.
        - **Starting Group Address –** The first C-multicast group address used.
        - **Incremented By** - The increment step to use to configure the rest of the C-multicast group addresses.
        - **Group Address Distribution –** The default is **Accumulated** mode. This option applies when the emulated receivers for the same mVPN are behind multiple emulated PEs or CEs. Emulate receivers for the same mVPN will join the same group address in **Accumulated** mode and a different group address in **Distributed** mode.

To increase the number of C-multicast flows, you can increase either the C-multicast source addresses or C-multicast group addresses or both.

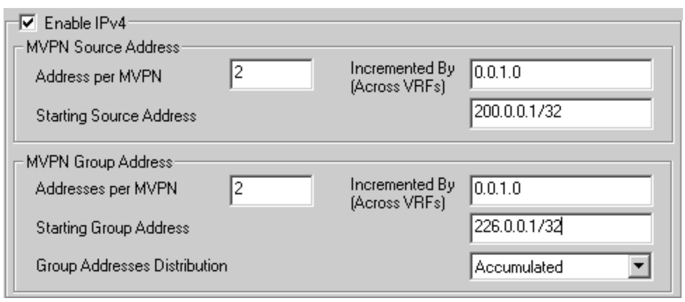


Figure 366. mVPN Wizard #5 - Setup IPv4 C-Multicast Sources and Groups

Similar configure parameters are available for IPv6 if the CE network is running IPv6 instead of IPv4.

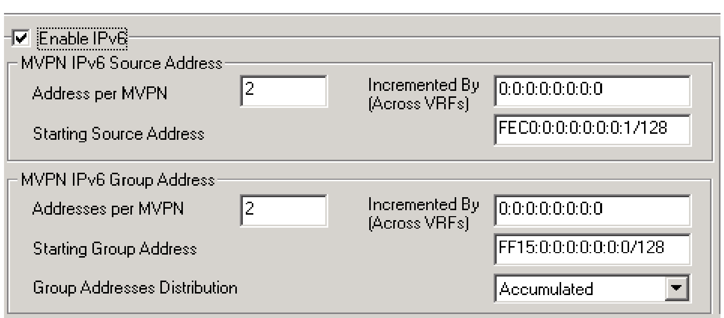


Figure 367. mVPN Wizard Screen#6 - Setup IPv6 C-Multicast Sources and Groups

6. On screen # 6 of 7, perform the following configuration tasks:

   a. **Enable VLAN**, **VLAN ID** and increment options – The VLAN ID of the DUT CE-facing interface and its increment option, if VLANs are enabled.
   b. **Mixed CE Protocol** and **IGP Protocol** – This is available when the emulated C-multicast sources are behind a CE port. It will be used to advertise C-multicast source addresses to the DUT PE. The DUT PE will install C-multicast source routes into its VPN routing table and use them for PIM RPF checks. If the CE port role is set to **Receiver** in wizard screen#1 (page 350), then this field will be grayed out.
   c. **Emulated CE IP Address –** The IP Address of the Ixia emulated CE interface.
   d. **DUT IP Address –** The IP Address of DUT CE facing interface.
   e. **Increment Per Router** and **Increment Per Port** – Control the IP Address increment for multiple emulated and DUT CE interfaces.
   f. **Multicast Protocol** – The multicast protocol used in the customer's multicast domain. Available selections are PIM-SM (default) and PIM-SSM.
   g. **Source Group Mapping** – This is available when **Multicast Protocol** is set to **PIM-SSM**. It configures the C-multicast group and C-multicast source mapping. Available selections are **Fully Meshed** (default) and **One-to-One**.
   h. **Multicast Network RP Address** and **Increment By** – The RP address for the customer's multicast domain. Available when **Multicast Protocol** is set to **PIM-SM**. It is recommended that the RP address should reside at the DUT or other routers outside the Ixia ports.

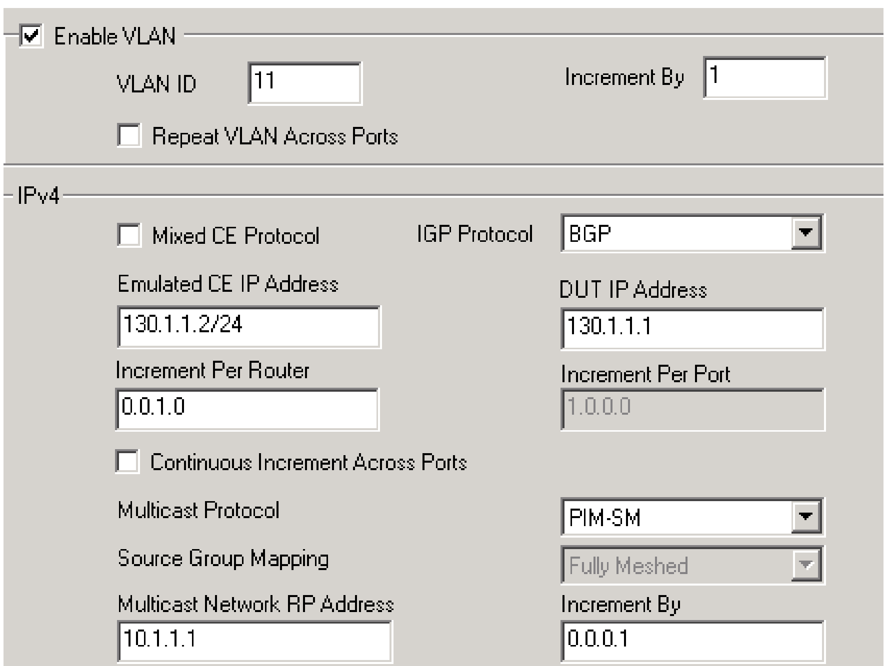


Figure 368. mVPN wizard screen #6 - setup IPv4 CE router

Similar options are available for IPv6 if the customer multicast domain is running with IPv6.

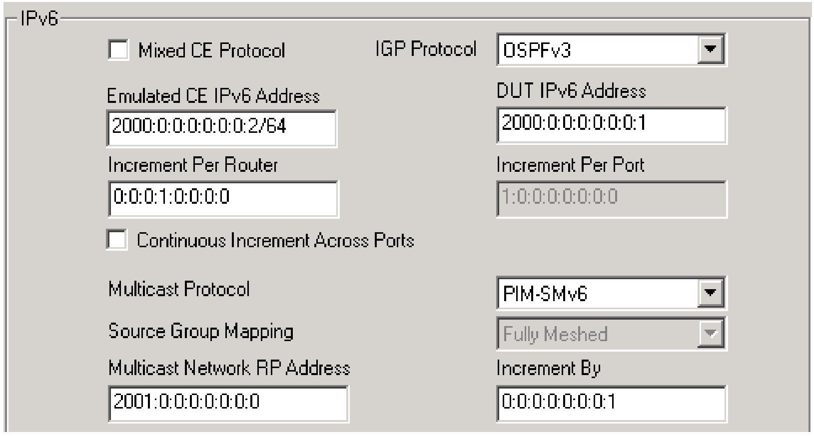


Figure 369. mVPN Wizard Screen #6 - Setup IPv6 CE Router

You have now finished the setup for your mVPN emulation. On screen # 7 of 7, name your wizard configuration file and select **Generate and Overwrite Existing Configuration** to generate the configuration. The wizard will configure the ports with the required protocols.

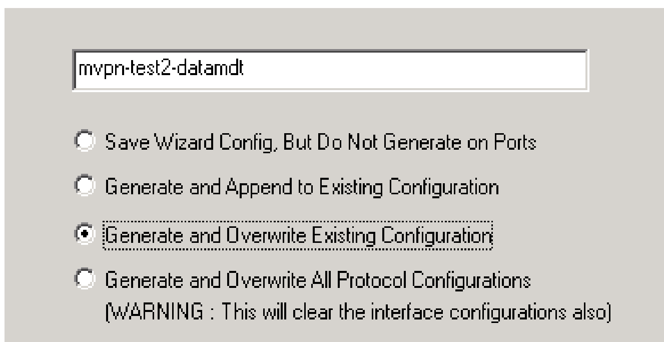
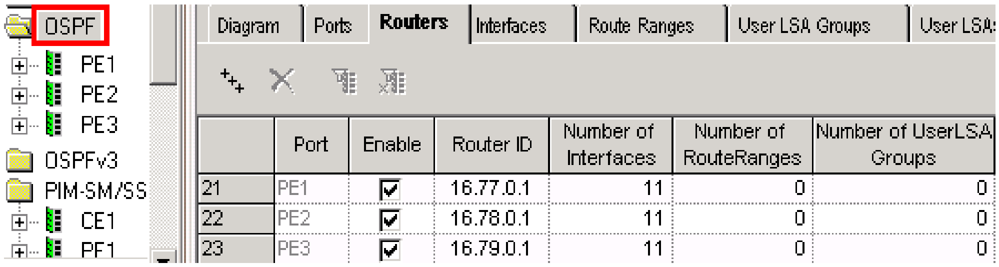


Figure 370. mVPN Wizard Screen #7

- **Save Wizard Config, But Do Not Generate on Ports** – This option saves the wizard configuration for this run, but will not configure the Ixia ports. The saved wizard configuration can be loaded later to configure the ports.
- **Generate and Append to Existing Configuration** – This option appends the configuration to the existing configuration on the port, merging the existing configuration and the new configuration. An append operation can be used to append additional emulated PEs and mVPNs to existing PEs, additional C-multicast sources and groups to existing mVPN of existing PEs, etc.
- **Generate and Overwrite Existing Configuration** – This option will overwrite the existing configuration with new configuration for protocols used in this run.
- **Generate and Overwrite All Protocol Configurations** – This option will clean all the protocol configurations (include protocol interfaces) before write configuration from this wizard run.

7. Click on **Test Configuration → Protocols → Routing/Switching/Interfaces**. Inspect the configuration created by the wizard.

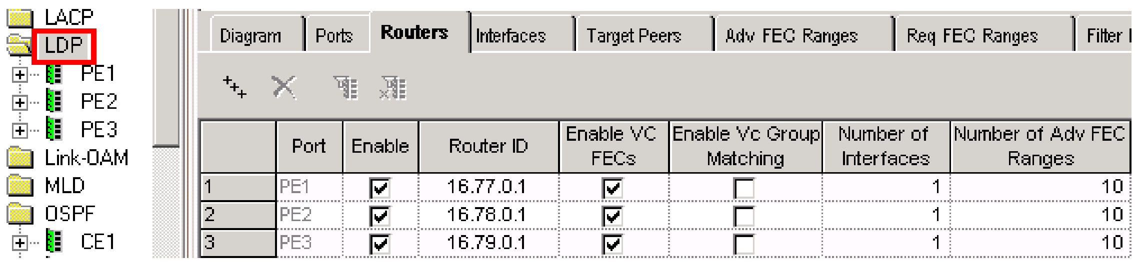
One OSPF is configured per PE port. This is an Ixia emulated P router that advertises the emulated PE loopback address to the DUT.



	Port	Enable	Router ID	Number of Interfaces	Number of RouteRanges	Number of UserLSA Groups
21	PE1	☑	16.77.0.1	11	0	0
22	PE2	☑	16.78.0.1	11	0	0
23	PE3	☑	16.79.0.1	11	0	0

Figure 371. OSPF P emulation

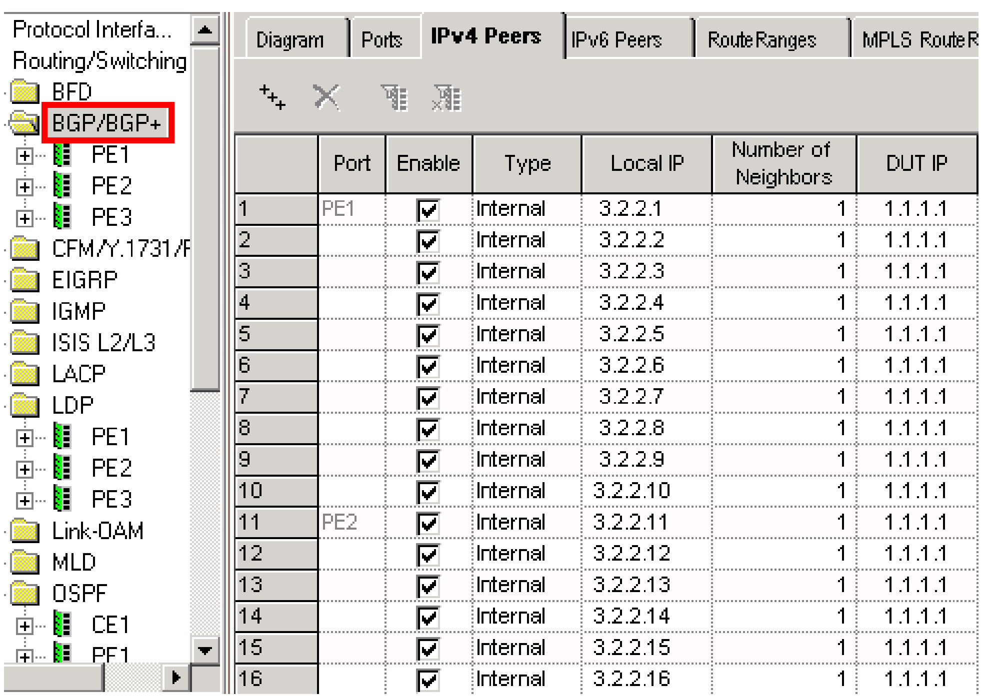
One LDP router is configured per PE port. This is an Ixia emulated P router that advertises label mapping for the emulated PE loopback address to the DUT.



	Port	Enable	Router ID	Enable VC FECs	Enable Vc Group Matching	Number of Interfaces	Number of Adv FEC Ranges
1	PE1	☑	16.77.0.1	☑	☐	1	10
2	PE2	☑	16.78.0.1	☑	☐	1	10
3	PE3	☑	16.79.0.1	☑	☐	1	10

Figure 372. LDP P Emulation

Ten BGP routers are configured per PE port. This is for BGP peering between the Ixia emulated PEs and the DUT PE.



	Port	Enable	Type	Local IP	Number of Neighbors	DUT IP
1	PE1	☑	Internal	3.2.2.1	1	1.1.1.1
2		☑	Internal	3.2.2.2	1	1.1.1.1
3		☑	Internal	3.2.2.3	1	1.1.1.1
4		☑	Internal	3.2.2.4	1	1.1.1.1
5		☑	Internal	3.2.2.5	1	1.1.1.1
6		☑	Internal	3.2.2.6	1	1.1.1.1
7		☑	Internal	3.2.2.7	1	1.1.1.1
8		☑	Internal	3.2.2.8	1	1.1.1.1
9		☑	Internal	3.2.2.9	1	1.1.1.1
10		☑	Internal	3.2.2.10	1	1.1.1.1
11	PE2	☑	Internal	3.2.2.11	1	1.1.1.1
12		☑	Internal	3.2.2.12	1	1.1.1.1
13		☑	Internal	3.2.2.13	1	1.1.1.1
14		☑	Internal	3.2.2.14	1	1.1.1.1
15		☑	Internal	3.2.2.15	1	1.1.1.1
16		☑	Internal	3.2.2.16	1	1.1.1.1

Figure 373. BGP PE emulation

The BGP routers for the emulated PEs do not have VPN routes configured and only MDT group is advertised. This is because there is no C-multicast source behind the emulated PEs. The BGP routers are created on the CE port and the C-multicast source is configured in the BGP **RouteRanges** tab.

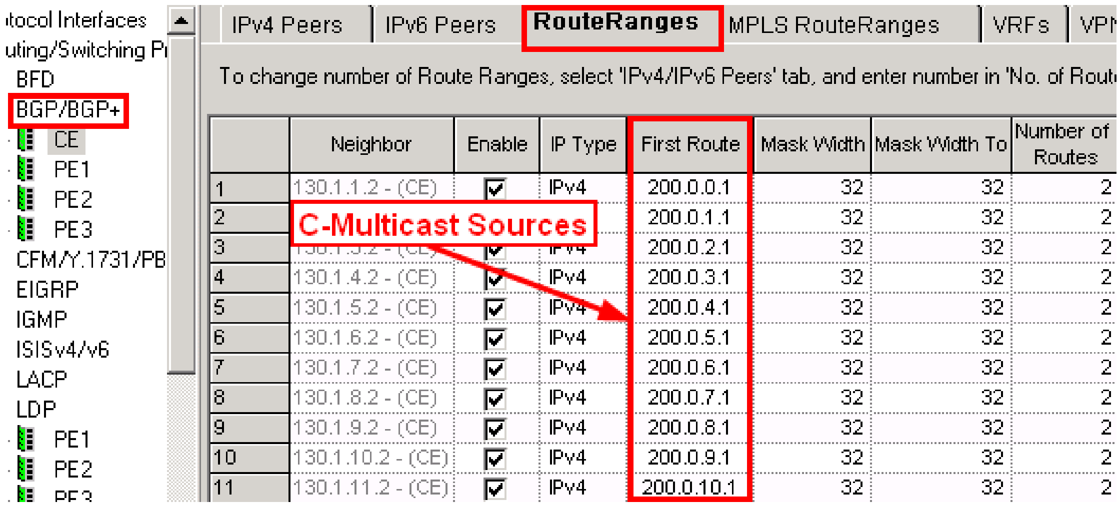


Figure 374. BGP PE émulation route range

There are eleven PIM routers configured per PE port. The first ten PIM routers are for the emulated PEs. Each PIM router runs over 20 GRE interfaces for the 20 mVPNs supported. The last PIM router is for the P router that joins the default MDT groups for all mVPNs supported by emulated a PE and building a multicast tree for the provider multicast domain.

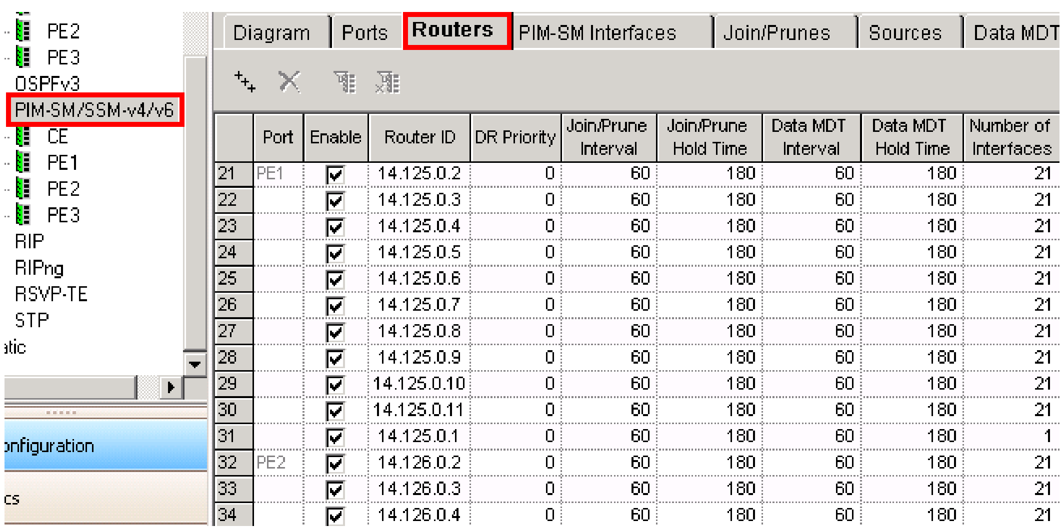
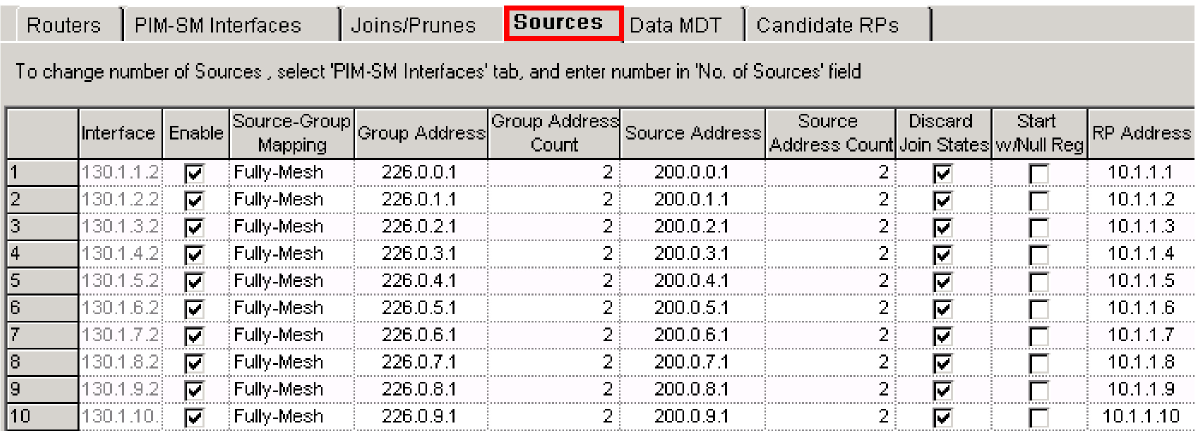


Figure 375. PIM PE emulation

Since the C-Multicast sources are behind the emulated CEs, the CE PIM routers are configured with a source range that will emulate the function of the sources' DR and send a Register to RP for each mVPN.

For the PIM configuration, the PE PIM router has a join/prune range configured to send (*,G) join for C-instance. The CE PIM router has a source range configured to send Register on behalf of the source's DR.



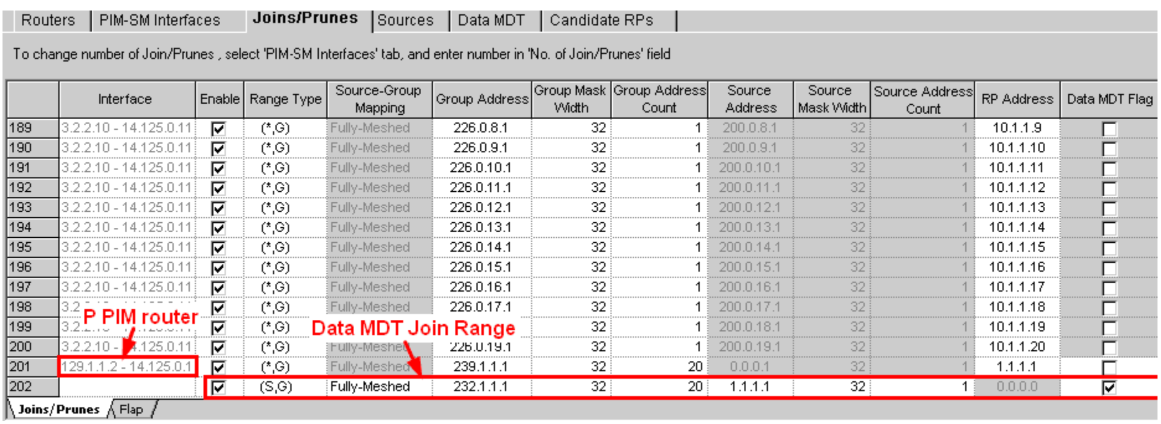
Routers | PIM-SM Interfaces | Joins/Prunes | Sources | Data MDT | Candidate RPs

To change number of Sources , select 'PIM-SM Interfaces' tab, and enter number in 'No. of Sources' field

	Interface	Enable	Source-Group Mapping	Group Address	Group Address Count	Source Address	Source Address Count	Discard Join States	Start w/Null Reg	RP Address
1	130.1.1.2	☑	Fully-Mesh	226.0.0.1	2	200.0.0.1	2	☑	☐	10.1.1.1
2	130.1.2.2	☑	Fully-Mesh	226.0.1.1	2	200.0.1.1	2	☑	☐	10.1.1.2
3	130.1.3.2	☑	Fully-Mesh	226.0.2.1	2	200.0.2.1	2	☑	☐	10.1.1.3
4	130.1.4.2	☑	Fully-Mesh	226.0.3.1	2	200.0.3.1	2	☑	☐	10.1.1.4
5	130.1.5.2	☑	Fully-Mesh	226.0.4.1	2	200.0.4.1	2	☑	☐	10.1.1.5
6	130.1.6.2	☑	Fully-Mesh	226.0.5.1	2	200.0.5.1	2	☑	☐	10.1.1.6
7	130.1.7.2	☑	Fully-Mesh	226.0.6.1	2	200.0.6.1	2	☑	☐	10.1.1.7
8	130.1.8.2	☑	Fully-Mesh	226.0.7.1	2	200.0.7.1	2	☑	☐	10.1.1.8
9	130.1.9.2	☑	Fully-Mesh	226.0.8.1	2	200.0.8.1	2	☑	☐	10.1.1.9
10	130.1.10.	☑	Fully-Mesh	226.0.9.1	2	200.0.9.1	2	☑	☐	10.1.1.10

Figure 376. PIM PE émulation source range

On the P PIM router, a special data MDT join range is configured. This range is different from other join ranges. It will not send a period join. This range is triggered by a join range and only sends a join when the receiver data MDT join comes from the initiated PE.



Routers | PIM-SM Interfaces | Joins/Prunes | Sources | Data MDT | Candidate RPs

To change number of Join/Prunes , select 'PIM-SM Interfaces' tab, and enter number in 'No. of Join/Prunes' field

	Interface	Enable	Range Type	Source-Group Mapping	Group Address	Group Mask Width	Group Address Count	Source Address	Source Mask Width	Source Address Count	RP Address	Data MDT Flag
189	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.8.1	32	1	200.0.8.1	32	1	10.1.1.9	☐
190	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.9.1	32	1	200.0.9.1	32	1	10.1.1.10	☐
191	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.10.1	32	1	200.0.10.1	32	1	10.1.1.11	☐
192	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.11.1	32	1	200.0.11.1	32	1	10.1.1.12	☐
193	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.12.1	32	1	200.0.12.1	32	1	10.1.1.13	☐
194	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.13.1	32	1	200.0.13.1	32	1	10.1.1.14	☐
195	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.14.1	32	1	200.0.14.1	32	1	10.1.1.15	☐
196	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.15.1	32	1	200.0.15.1	32	1	10.1.1.16	☐
197	3.2.2.10 - 14.125.0.11	☑	(*,G)	Fully-Meshed	226.0.16.1	32	1	200.0.16.1	32	1	10.1.1.17	☐
198	[illegible]	☑	(*,G)	Fully-Meshed	226.0.17.1	32	1	200.0.17.1	32	1	10.1.1.18	☐
199	[illegible]	☑	(*,G)	[illegible]	[illegible]	32	1	200.0.18.1	32	1	10.1.1.19	☐
200	3.2.2.10 - ...125.0.11	☑	(*,G)	Fully-Meshed	226.0.19.1	32	1	200.0.19.1	32	1	10.1.1.20	☐
201	129.1.1.2 - 14.125.0.1	☑	(*,G)	Fully-Meshed	239.1.1.1	32	20	0.0.0.1	32	1	1.1.1.1	☐
202		☑	(S,G)	Fully-Meshed	232.1.1.1	32	20	1.1.1.1	32	1	0.0.0.0	☑

Joins/Prunes | Flap

Figure 377. PIM P emulation data MDT join range

8. Start all protocols by clicking on the **Start Protocols** button in the top toolbar. This will start all configured protocols on all ports. You can also start protocols at the per-protocol level or per-port level or per-protocol and port level.

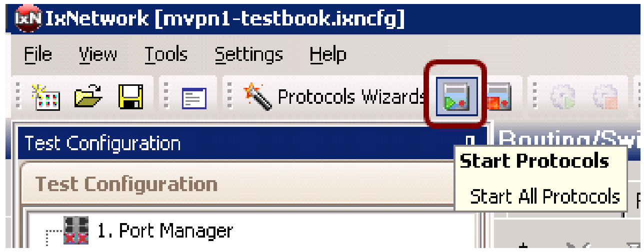


Figure 378. Start all protocols

Ensure all protocols are running on the ports.

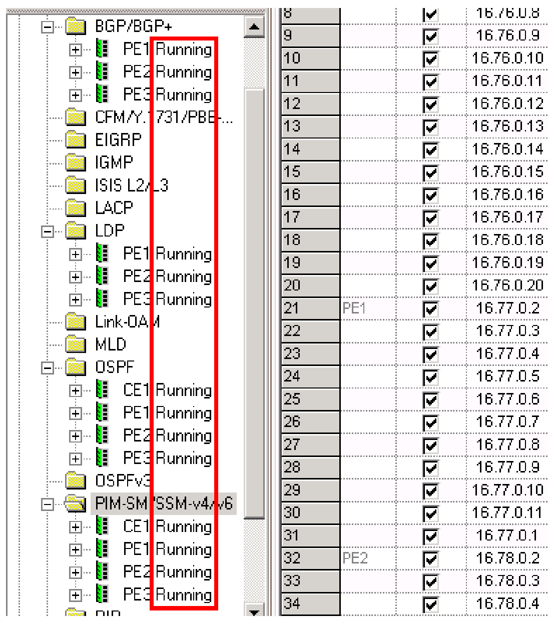
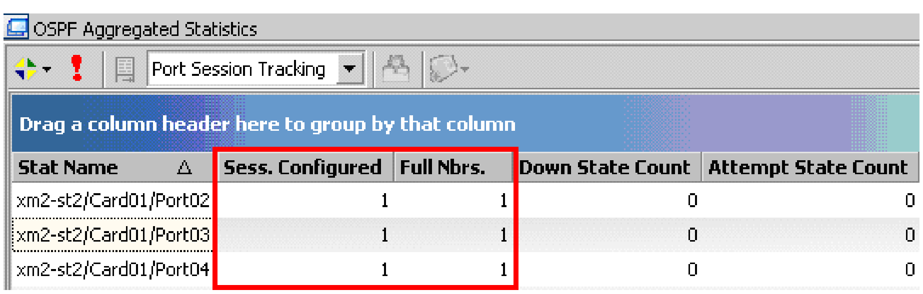


Figure 379. All protocols running

9. Switch to the **StatViewer** window and verify protocol statistics. Besides the general session statistics, each protocol's statistics view also provides comprehensive statistics on protocol state machine operation. This is very helpful for troubleshooting.



Stat Name	Sess. Configured	Full Nbrs.	Down State Count	Attempt State Count
xm2-st2/Card01/Port02	1	1	0	0
xm2-st2/Card01/Port03	1	1	0	0
xm2-st2/Card01/Port04	1	1	0	0

Figure 380. OSPF protocol statistics

LDP Aggregated Statistics

Drag a column header here to group by that column

Stat Name	Basic Sess. Up	Targeted Sess. Up	Targeted Sess. Configured	Non Existe
xm2-st2/Card01/Port02	1	0	0	
xm2-st2/Card01/Port03	1	0	0	
xm2-st2/Card01/Port04	1	0	0	

Figure 381. LDP protocol statistics

BGP Aggregated Statistics

Drag a column header here to group by that column

Stat Name	Sess. Configured	Sess. Up	Idle State Count	Connect State Count
xm2-st2/Card01/Port01	20	20	0	0
xm2-st2/Card01/Port02	10	10	0	0
xm2-st2/Card01/Port03	10	10	0	0
xm2-st2/Card01/Port04	10	10	0	0

Figure 382. BGP protocol statistics

PIMSM Aggregated Statistics

Drag a column header here to group by that column

Stat Name	Rtrs. Configured	Rtrs. Running	Nbrs. Learnt	Hellos Tx	Hellos Rx
xm2-st2/Card01/Port01	20	20	20	56,473	57,126
xm2-st2/Card01/Port02	11	11	201	567,423	575,060
xm2-st2/Card01/Port03	11	11	201	567,423	575,062
xm2-st2/Card01/Port04	11	11	201	567,423	575,061

Figure 383. PIM-SM protocol statistics

Notes: The # of PIM adjacencies = (# of emulated PEs) * (# of mVPN/PE + 1).

10. After verifying the protocol statistics on the Ixia side, you can also optionally verify the protocol session on the DUT (a Cisco DUT is used as example).

```
RP/0/9/CPU0:ios#sh ospf neighbor
Sat Mar 14 23:08:44.046 UTC

* Indicates MADJ interface

Neighbors for OSPF 1000

Neighbor ID     Pri   State           Dead Time   Address         Interface
14.125.0.1      0     FULL/DROTHER    00:00:32    129.1.1.2       GigabitEthernet0/7/0/1
    Neighbor is up for 23:37:09
14.126.0.1      0     FULL/DROTHER    00:00:37    129.1.2.2       GigabitEthernet0/7/0/2
    Neighbor is up for 23:37:04
14.127.0.1      0     FULL/DROTHER    00:00:39    129.1.3.2       GigabitEthernet0/7/0/3
    Neighbor is up for 23:37:09

Total neighbor count: 3
```

Figure 384. Sample "show OSPF neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh mpls ldp neighbor brief
Sat Mar 14 23:08:47.920 UTC

Peer               GR Up Time          Discovery Address
-----------------  -- ---------------  --------- -------
14.126.0.1:0       N  23:37:16                 1       1
14.125.0.1:0       N  23:37:14                 1       1
14.127.0.1:0       N  23:37:13                 1       1
```

Figure 385. Sample "show MPLS LDP neighbor brief" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh bgp summary
Sat Mar 14 23:12:26.328 UTC
BGP router identifier 1.1.1.1, local AS number 1000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 1
BGP NSR converge version 1
BGP NSR converged
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker               1          1          1          1           1           1

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
3.2.2.1           0  1000   17926   17404        1    0    0 23:40:49          0
3.2.2.2           0  1000   17925   17352        1    0    0 23:40:50          0
3.2.2.3           0  1000   17925   17404        1    0    0 23:40:49          0
3.2.2.4           0  1000   17926   17352        1    0    0 23:40:49          0
3.2.2.5           0  1000   17924   17352        1    0    0 23:40:50          0
3.2.2.6           0  1000   17924   17352        1    0    0 23:40:47          0
3.2.2.7           0  1000   17710   16936        1    0    0 23:40:47          0
3.2.2.8           0  1000   17708   16937        1    0    0 23:40:47          0
3.2.2.9           0  1000   17707   16936        1    0    0 23:40:49          0
3.2.2.10          0  1000   17710   16935        1    0    0 23:40:49          0
```

Figure 386. Sample "show BGP neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh pim neighbor
Sat Mar 14 23:14:32.586 UTC

PIM neighbors in VRF default

Neighbor Address     Interface              Uptime    Expires  DR pri   Flags

129.1.1.1*           GigabitEthernet0/7/0/1 1d00h     00:01:34 1 (DR) B A
129.1.1.2            GigabitEthernet0/7/0/1 23:42:56  00:01:28 0
129.1.2.1*           GigabitEthernet0/7/0/2 1d00h     00:01:39 1 (DR) B A
129.1.2.2            GigabitEthernet0/7/0/2 23:42:57  00:01:28 0
129.1.3.1*           GigabitEthernet0/7/0/3 1d00h     00:01:42 1 (DR) B A
129.1.3.2            GigabitEthernet0/7/0/3 23:42:56  00:01:28 0
129.1.4.1*           GigabitEthernet0/7/0/4 1d00h     00:01:36 1 (DR) B A
129.1.5.1*           GigabitEthernet0/7/0/5 1d00h     00:01:29 1 (DR) B A
129.1.6.1*           GigabitEthernet0/7/0/6 4d09h     00:01:16 1 (DR) B A
129.1.7.1*           GigabitEthernet0/7/0/7 4d09h     00:01:34 1 (DR) B A
1.1.1.1*             Loopback0              4d09h     00:01:34 1 (DR) B A
```

Figure 387. Sample "show PIM neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh pim vrf mvpn1 neighbor
Sat Mar 14 23:17:14.272 UTC

PIM neighbors in VRF mvpn1

Neighbor Address     Interface              Uptime    Expires  DR pri   Flags

130.1.1.1*           GigabitEthernet0/7/0/0.1 1d00h     00:01:16 1 (DR) B A
130.1.1.2            GigabitEthernet0/7/0/0.1 23:45:42  00:01:15 0
1.1.1.1*             mdtmvpn1               4d09h     00:01:37 1 (DR) B A
3.2.2.1              mdtmvpn1               23:45:38  00:01:15 0
3.2.2.2              mdtmvpn1               23:45:38  00:01:15 0
3.2.2.3              mdtmvpn1               23:45:38  00:01:15 0
3.2.2.4              mdtmvpn1               23:45:38  00:01:15 0
3.2.2.5              mdtmvpn1               23:45:38  00:01:16 0
3.2.2.6              mdtmvpn1               23:45:38  00:01:18 0
```

Figure 388. Sample "show PIM VRF mvpn1 neighbor" output for Cisco IOS-XR

```
RP/0/9/CPU0:ios#sh mrib vrf mvpn1 route
Sat Mar 14 23:21:28.016 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, MA - MDT Address, ME - MDT Encap,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, MF - MPLS Encap, EX - Extranet
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet

(*,226.0.0.1) RPF nbr: 10.1.1.1 Flags: C
  Up: 1d00h
  Incoming Interface List
    Decapstunnel200 Flags: A, Up: 1d00h
  Outgoing Interface List
    mdtmvpn1 Flags: F NS MI, Up: 1d00h

(200.0.0.1,226.0.0.1) RPF nbr: 130.1.1.2 Flags: L MA MT
  MDT Address: 232.1.1.1
  MT Slot: 0/7/CPU0
  Up: 1d00h
  Incoming Interface List
    GigabitEthernet0/7/0/0.1 Flags: A, Up: 23:49:53
  Outgoing Interface List
    mdtmvpn1 Flags: F NS MI, Up: 1d00h
```

Figure 389. Sample "show mrib vrf mvpn1 route" output for Cisco IOS-XR

11. Now you can to build traffic from C-multicast source to C-multicast receiver to validate data plane forwarding.

Go to **Test Configuration → Traffic** and click to launch the Traffic wizard.

12. At the **Endpoint** page, perform the following configuration tasks:
    a. Name your traffic item and select **Type of Traffic**.
    b. Under **Traffic Mesh,** select **One-One** for **Source/Dest**. This is due to the nature of the VPN; sources and destinations that belong to different VPN do not talk to each other.
    c. Under **Traffic Mesh**, select **Fully Meshed** for **Routes/Hosts**. In mVPN case, this mesh should match with the Source-GroupMapping in the Register Ranges.
    d. In the **Traffic Group ID filters**, select the traffic group for all 20 VPNs and apply the filter. The **Source**/**Destination Endpoints** windows will only show endpoints which are attached to these traffic groups.
    e. In the **Source** window, select **PIMSM Register Ranges** under **All Ports**. This will select **PIMSM Register Ranges** under CE port.
    f. In the **Destination** window, select **PIMSM Multicast Ranges** under **All Ports**. This will select all PIM join ranges under PE ports.
    g. Click the button below to add **Source Endpoints** and **Destination Endpoints**. As you can see that there are 20 source endpoints (one per mVPN) and 600 destination endpoints (30 PEs * 20 mVPNs = 600).

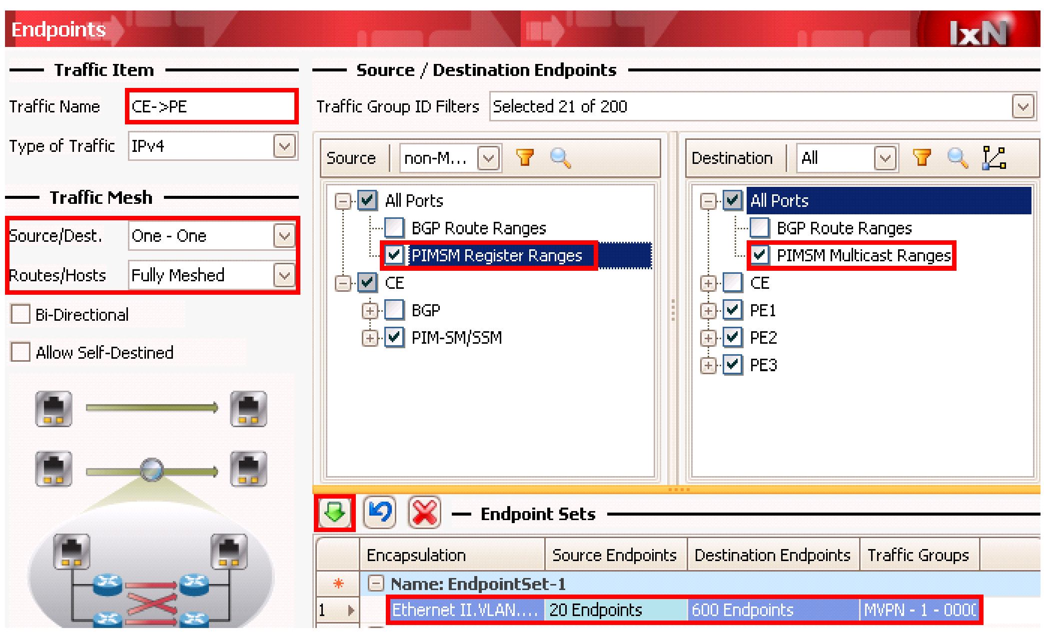


Figure 390. Traffic wizard - Endpoints

Figure 391 expands the source and destination tree further to show the leaf endpoints.

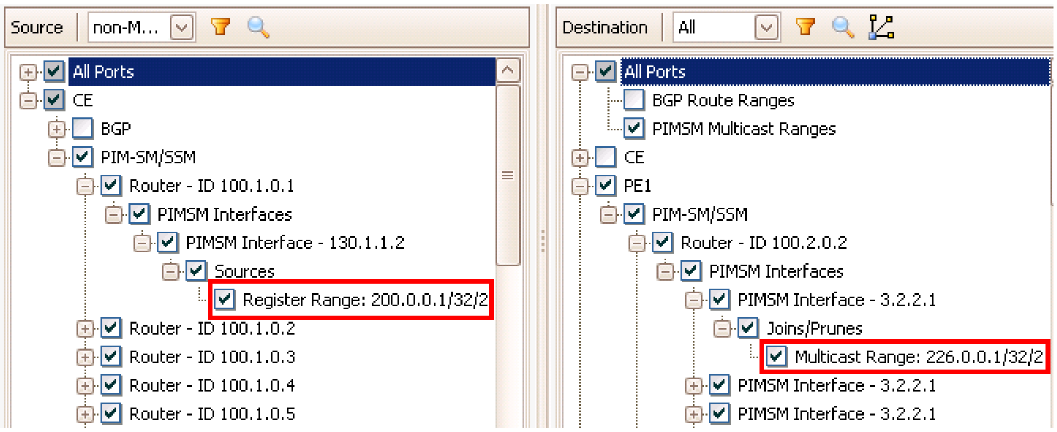


Figure 391. Traffic wizard endpoints selection – Expanded endpoints

Notes: The list below shows various options to filter the traffic endpoint tree and help you find a specific traffic endpoint quickly.

- Traffic Group ID Filters Traffic Group ID Filters
- Encapsulation
- Quick Selection
- Search
- Multicast Endpoint Selection

13. On the **Packet/QoS** page, available QoS fields are populated based on the traffic encapsulation. You can select a QoS field you want to modify, e.g., IP Precedence. Skip this page if you do not want to tune QoS values.

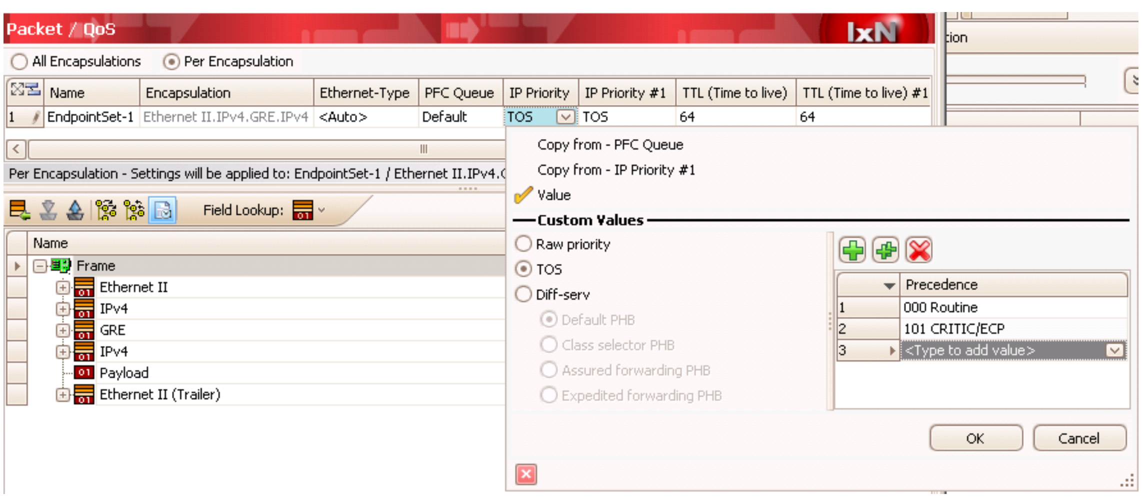


Figure 392. Traffic Wizard Packet/QoS

14. On the **Flow Group Setup** page, various options are populated based on traffic content. These options are used to create various traffic profiles which allow you tune transmit parameters for each profile. Skip this page if you do not need multiple traffic profiles.

15. On the **Frame Setup** page, set the desired frame size.

16. On the **Rate Setup** page, select the **Transmit mode** which matches the transmit mode at the port, and set the desired rate. You can also use the **Rate Distribution** option to control how to apply the configured rate across flow groups and ports.

17. On the **Flow Tracking** page, select Traffic Group ID and IPv4: **Destination Address**. The **Traffic Item** is checked as long as there is another traffic option checked. This will give you an aggregated view at the Traffic Item level and VPN level, plus per-flow statistics for each C-multicast group address.

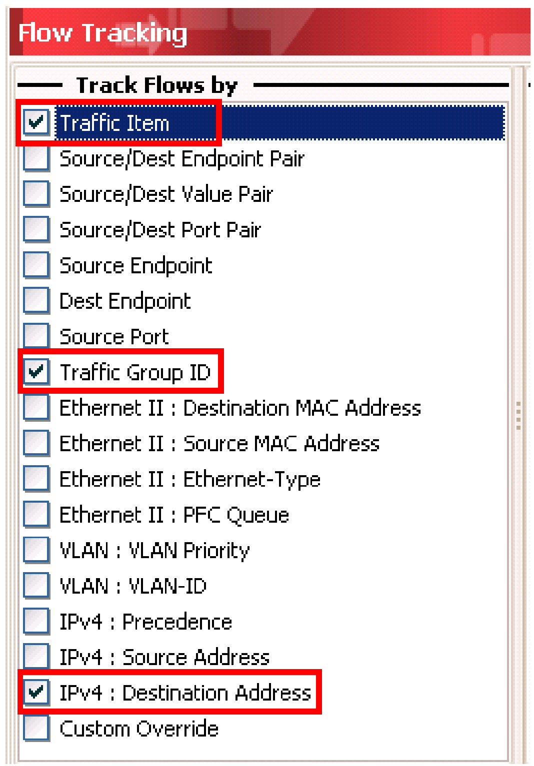


Figure 393. Traffic wizard Flow Tracking

18. On the **Preview** page, click **View Flow Groups/Packets** to preview the packet content.

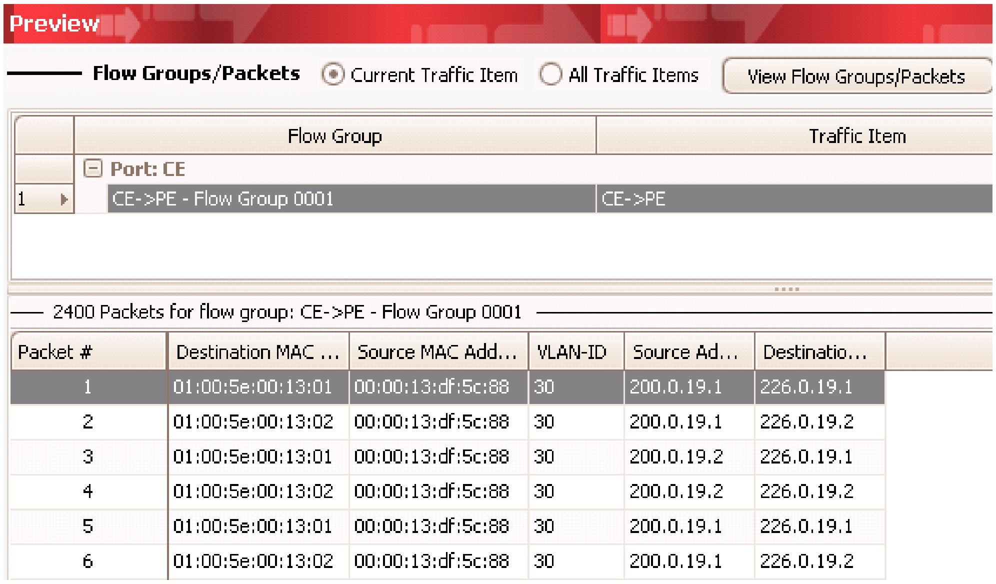


Figure 394. Traffic wizard Preview

19. On the **Validate** page, click the **Validate** button to validate the current traffic item. This will report any error or warning for configuration and packets. It will also verify whether there are enough hardware resources to support this traffic item.

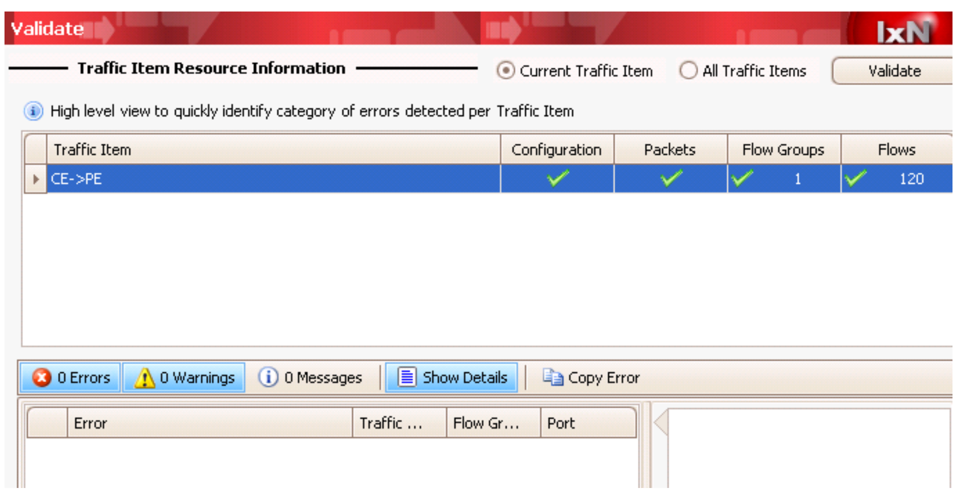


Figure 395. Traffic wizard - Validate

20. Click the **Finish** button to build traffic. A traffic item is created under **All Traffic Items** and all flow groups for this traffic item will show up at the **Traffic** grid on the right panel.

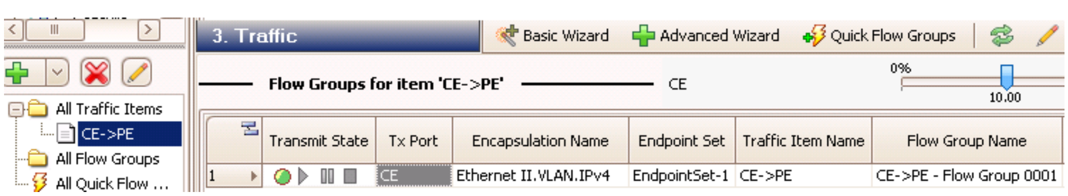


Figure 396. Traffic item and Flow Groups

21. In the **Traffic** grid, you can use grid options to customize frame size, frame rate, etc. You can also control traffic start/stop/pause/resume at a per flow group level.

22. If you want to view the generated packets in detail, you can right click on any flow group to bring up the Packet Editor window. Figure 397 shows that the packets generated are IPv4 packets. The top part shows the packet decoding. Click **Hex View** at the lower left corner to bring up a binary encoding view. It also shows the total number of generated packets. You can click the **>>** button on the bottom to view the contents of each packet.

    Expand the IPv4 header to view the content. As you can see, the source address is a C-multicast source address and the destination address is C-multicast group address.

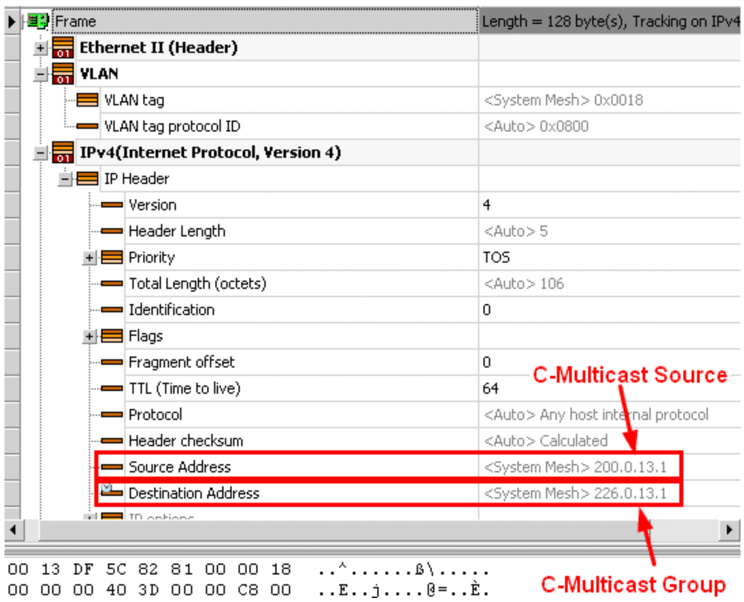


Figure 397. Packet Editor

23. **Apply** and **Start** the traffic.

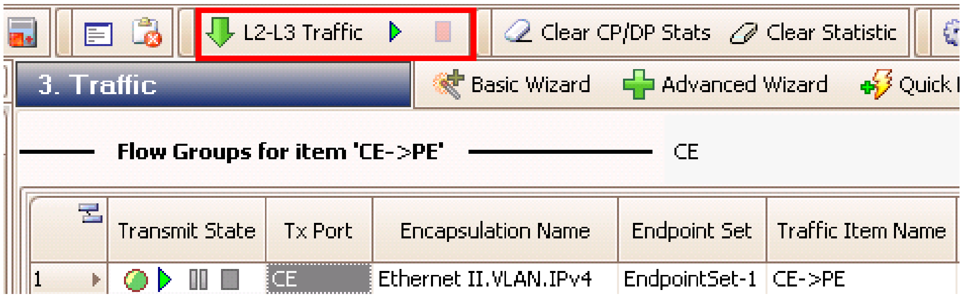


Figure 398. Apply and start traffic

24. Switch to the **StatViewer** window. Click on **Traffic Item Statistics** view to bring up the aggregated traffic item statistics view at the right panel.

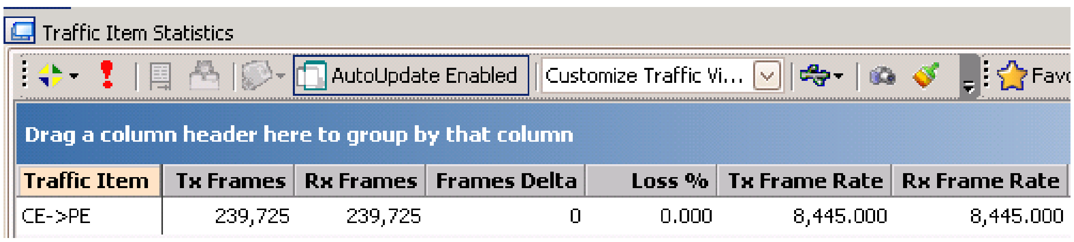


Figure 399. Traffic Item Statistics

25. Right click on the traffic item. The available drill-down options are populated based on the Track options selected. Select **Drill Down per Traffic Group ID** to bring up a view that is aggregated per VPN level.

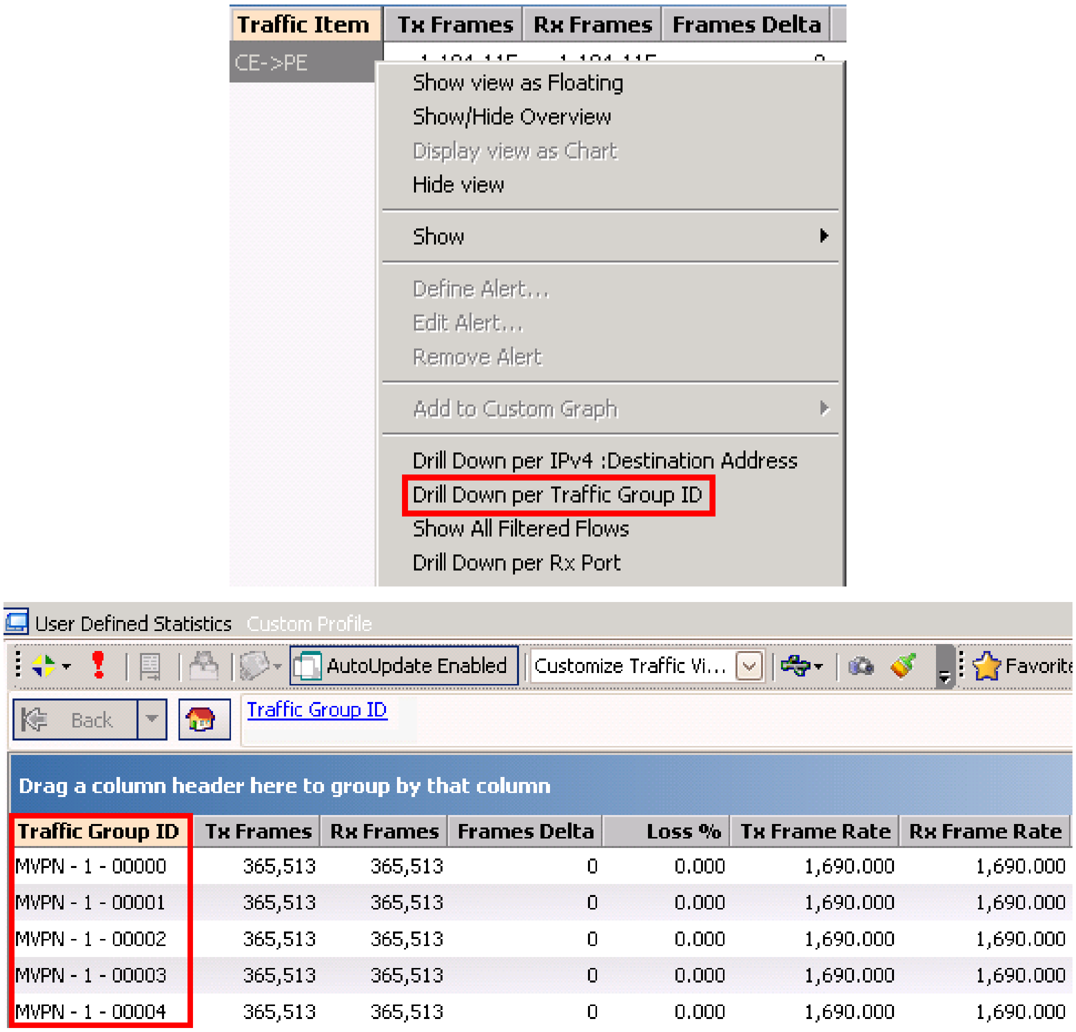


Figure 400. Drill down options and drill down view from Traffic Item Statistics

26. Right click **MVPN-1-0000** flows and drill down further by selecting **Drill down per IPv4: Destination Address** to bring up a per-destination address (destination group) flow view for **MVPN-1-0000**.

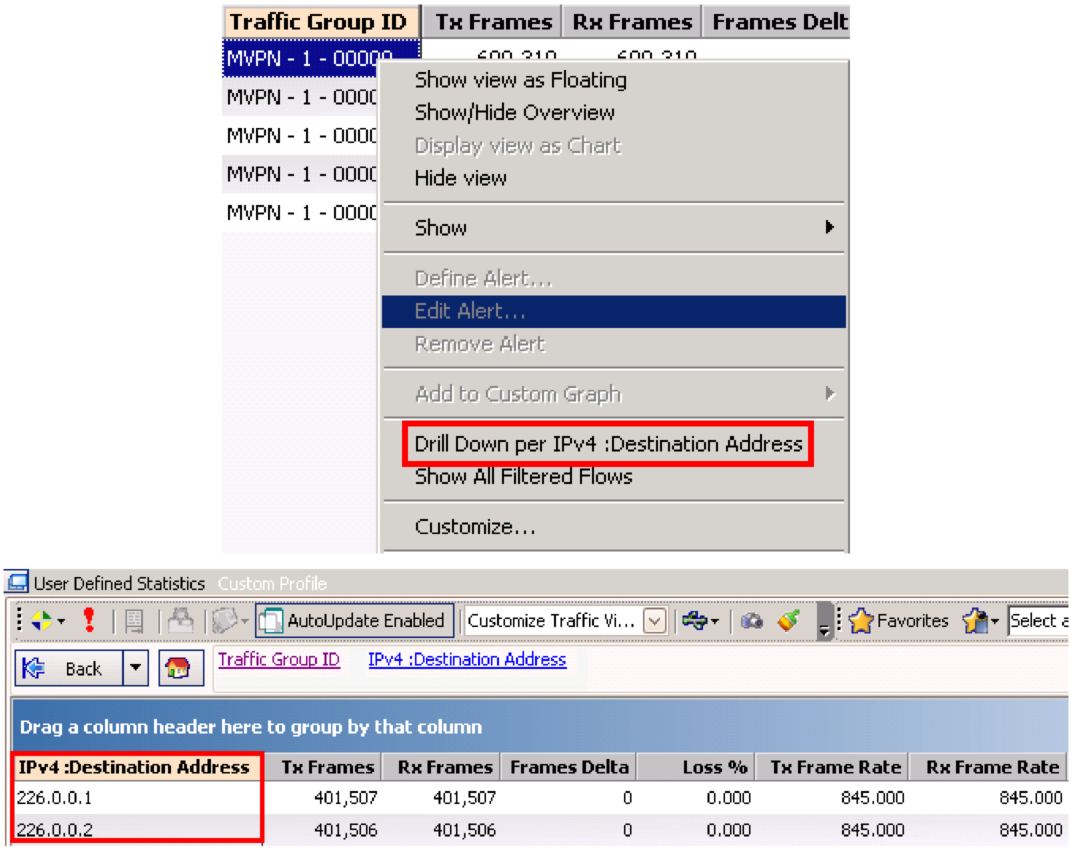


Figure 401. Drill down options and drill down view from VPN level view

27. Click the **Flow Statistics** view at the left panel to bring up a statistics view for all flows.

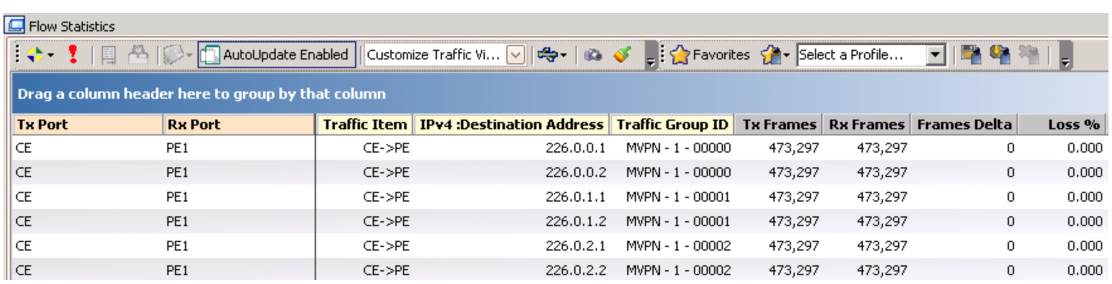


Figure 402. Flow Statistics

The aggregated, drill-down, and per-flow statistics impose a hierarchy on a typically huge amount of flow statistics. You can nail down the problem from top level down to look at only flows with problems. Both aggregated and detailed flow statistics views provide important statistics that allow you to monitor the data plane forwarding operation, including frame delta, loss %, Rx frame rate, various Rx rates (in Bps, bps, kbps and Mbps), various latencies (min, max and avg) and timestamps.

28. Now stop traffic and go back to the **Traffic** window. Increase the traffic line rate by dragging the sliding bar from 1 % to 10 %. With this rate, multicast flow will exceed the configured data MDT thresholds and the DUT PE will perform a switchover.

    Note: Use the pre-configured data MDT threshold on the DUT for the proper traffic rate setting.

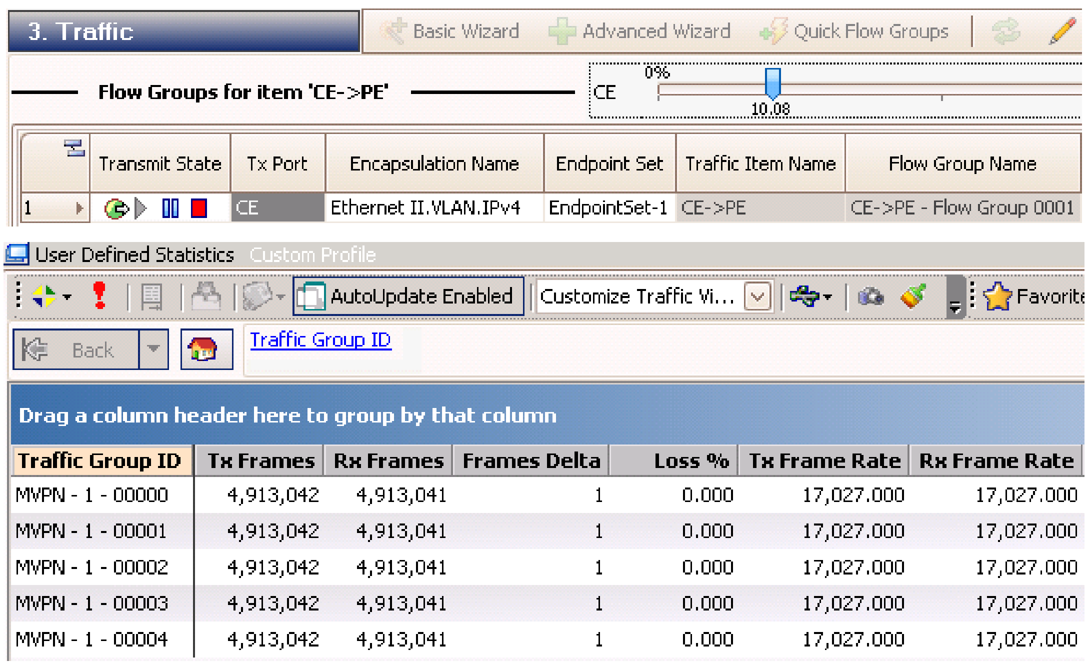


Figure 403. Dynamic rate change and aggregated VPN level statistics

The per-VPN level statistics shown above are based on the C-multicast group address. Therefore, they may not provide a straightforward indication of whether the data MDT switchover occurred. To confirm this, you can use the following methods.

- Verify DUT stats.
- Use egress tracking to track part of outer IP address which is the MDT group address
- Use the Ixia Analyzer to capture a data packet and verify the outer IP destination address.

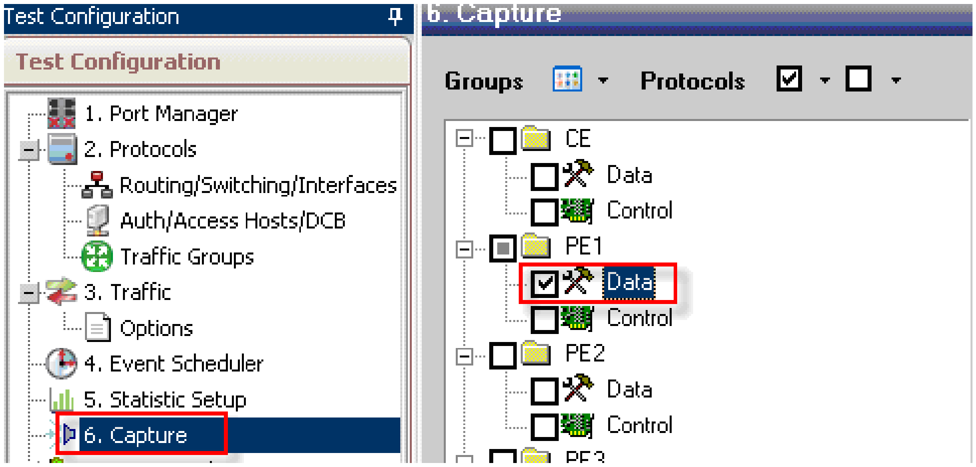


Figure 404. Enable data capture

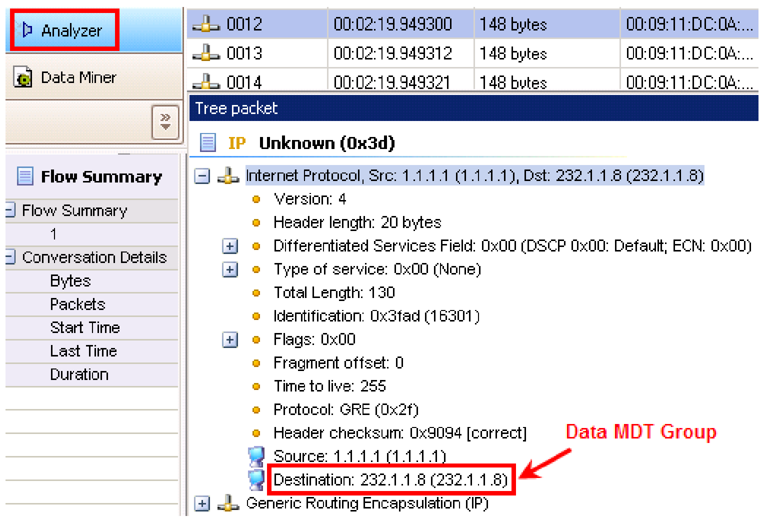


Figure 405. Analyzer decoding of data traffic from DUT

Result Analysis

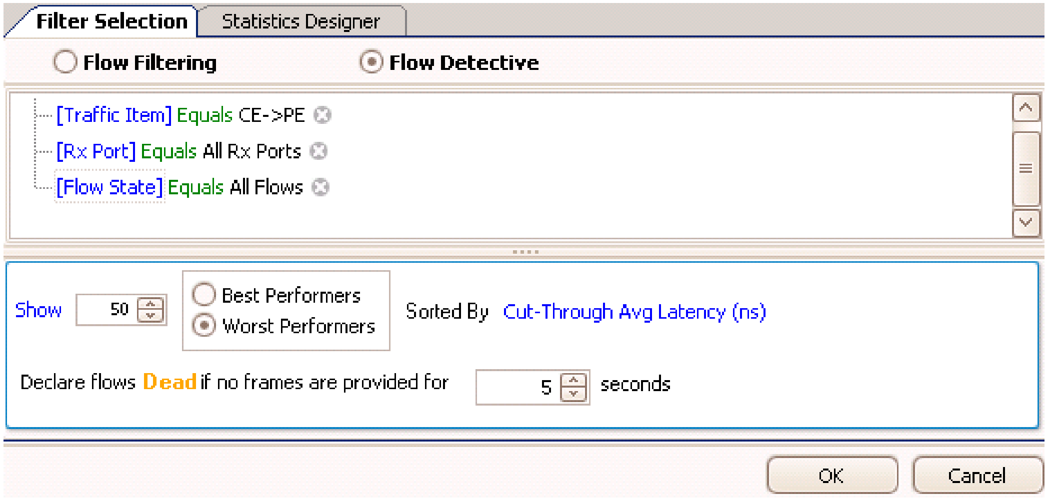
Using the Ixia protocol statistics, it can be seen that all expected protocol sessions are up and running. After starting traffic, continue to monitor protocol statistics to verify whether the control plan can sustain itself with data plane traffic.

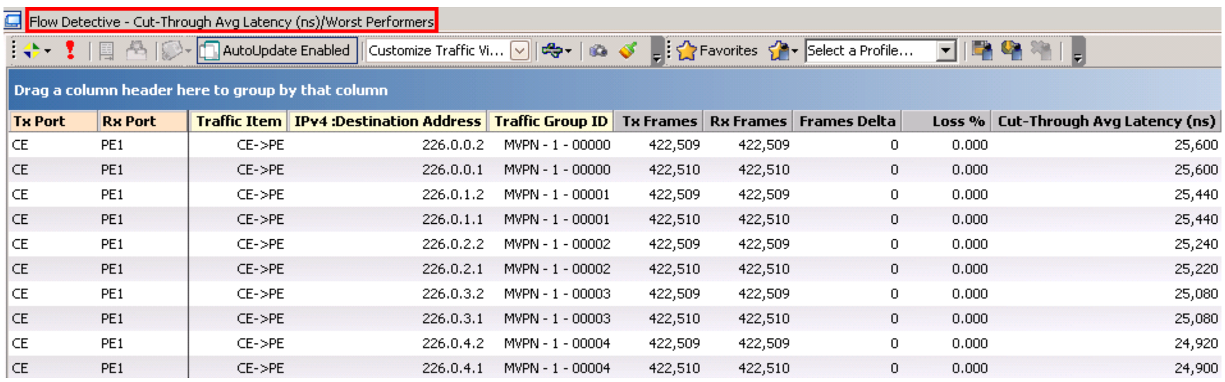
In IxNetwork 5.40, Ixia introduced powerful aggregated and drill-down views at various user defined levels. This helps to identify the problem quickly. You may start with the highest level aggregated view for traffic items and monitor various Rx stats and latency/jitter. You can then drill down to various aggregated levels to narrow down the flows which have problems. This greatly reduces troubleshooting time.

The Snapshot CSV function can be used to record the statistics for one or more statistics views at any point of the time. You can store a view that is of interest at any time for post analysis.

Use Traffic item statistics to verify that the loss % and latency are within tolerance. If not, identify the flow with the most loss or worst latency by drilling down at the VPN level to find out which VPN has a problem. Drill down further to the destination group level as needed. This can help troubleshoot which flow has the highest loss or worst latency/jitter.

Flow Detective is another way to quickly identify problematic flows which have a higher loss %, higher latency/jitter, and so on.





Tx Port	Rx Port	Traffic Item	IPv4 :Destination Address	Traffic Group ID	Tx Frames	Rx Frames	Frames Delta	Loss %	Cut-Through Avg Latency (ns)
CE	PE1	CE->PE	226.0.0.2	MVPN - 1 - 00000	422,509	422,509	0	0.000	25,600
CE	PE1	CE->PE	226.0.0.1	MVPN - 1 - 00000	422,510	422,510	0	0.000	25,600
CE	PE1	CE->PE	226.0.1.2	MVPN - 1 - 00001	422,509	422,509	0	0.000	25,440
CE	PE1	CE->PE	226.0.1.1	MVPN - 1 - 00001	422,510	422,510	0	0.000	25,440
CE	PE1	CE->PE	226.0.2.2	MVPN - 1 - 00002	422,509	422,509	0	0.000	25,240
CE	PE1	CE->PE	226.0.2.1	MVPN - 1 - 00002	422,510	422,510	0	0.000	25,220
CE	PE1	CE->PE	226.0.3.2	MVPN - 1 - 00003	422,509	422,509	0	0.000	25,080
CE	PE1	CE->PE	226.0.3.1	MVPN - 1 - 00003	422,510	422,510	0	0.000	25,080
CE	PE1	CE->PE	226.0.4.2	MVPN - 1 - 00004	422,509	422,509	0	0.000	24,920
CE	PE1	CE->PE	226.0.4.1	MVPN - 1 - 00004	422,510	422,510	0	0.000	24,900

Figure 406. Flow Detective

If there is no frame loss or the loss % is within tolerance, additional multicast flows should be added to the test. This can be done by increasing the number of C-multicast sources and the number of C-multicast groups emulated by Ixia ports. You can also add additional PEs or/and mVPNs to the test. The test can be repeated until the loss % and latency are beyond tolerances. The DUT data MDT switchover performance numbers can be determined and the switchover latency can be quantified.

Troubleshooting and Diagnostics

Issue	Troubleshooting solution
Cannot Ping DUT	Check the **Protocol Interface** window to see whether there is a red exclamation mark (!) in front of any protocol interface. If there is, then there is a mismatch between the DUT IP and Ixia port's IP subnet, VLAN or link mode (copper versus fiber). Correct it and make sure red exclamation mark goes away.
OSPF session does not come up.	Verify the OSPF area ID, link type and MTU on both the Ixia and DUT sides to make sure they match. You can also use the Analyzer control capture in order to view the control packet exchange between the DUT and Ixia port to determine root cause.
BGP sessions between emulated PEs and DUT PE do not come up or partially not up.	First verify the IGP session between the DUT and the emulated P router. If the session is up, verify that the DUT's routing table has routes to the emulated PE loopback address to avoid a possible connectivity issue. If this is not the case, then verify that the DUT and Ixia configuration have matching PE loopback address, BGP AS numbers, BGP capability, etc.
PIM sessions for VPNs do not come up	Make sure that PIM is enabled on the DUT loopback interface used for BGP peering. The PIM adjacencies for VPNs are setup using this address. Also verify that the RP address for the provider network on the DUT and Ixia port are the same.
PIM session for VPN is up, but no PIM join is received from the receiver	If you turn on DUT debugging, you might see a message such as this "Receive Join. Upstream neighbor is not us. Discard…". This might be because that the Ixia port sent a PIM join for the C-instance without the DUT as upstream neighbor. To fix this problem, go to PE port **PIM protocol → PIM-SM** interfaces tab, uncheck **Auto Pick Neighbor** and configure the DUT loopback address used for BGP peering as the neighbor for all GRE interfaces. Then restart the PIM protocol. The Ixia PE will send a C-PIM join with the DUT as the upstream neighbor. With **Auto Pick Neighbor** enabled, the Ixia PE will pick a neighbor that it hears a Hello from first as an upstream neighbor. If there are multicast Ixia PE ports that have emulated receivers behind them, there is a chance that an Ixia port will hear a Hello from another Ixia port first and therefore use it as upstream neighbor for C-PIM Join.
Traffic started from PE to CE or CE to PE, but no packet received on receiving port	Check the DUT's global and VPN multicast routing table to make sure that the multicast routes are correct. Also check the VPN unicast routing table to make sure that the C-multicast source is learned and is installed in the VRF routing table.

Test Variables

Test Variable	Description
Port Role	An Ixia port can simulate either a multicast source or receiver behind it. You can choose this option on page 1 of the mVPN wizard.
# of PE ports	An Ixia port can emulate a provide edge router which will join an mVPN and peer with a DUT PE over a default MDT tunnel. You can increase the number of Ixia PE ports to satisfy your scalability requirement.
# of CE ports	An Ixia port will emulate a customer promise router connected to a DUT PE. You can increase the number of Ixia CE ports per your requirement.
IGP Protocol	The available options are OSPF and ISIS. The IPG protocol can be chosen based on your network.
MPLS Protocol	The available options are LDP and RSVP. The MPLS protocol can be chosen based on your network.
Provider Multicast Protocol	The available options are PIM-SM and PIM-SSM. The multicast protocol can be chosen based on your network.
# of Emulated PE Routers	An Ixia port can emulate a number of provider edge routers that support a number of mVPNs. This is one area that can grow quite large in a service provider's network. The DUT needs to maintain PIM adjacencies with remote PEs for each mVPN it supports. The BGP peering may or may not be a concern here as there will be router reflectors in a service provider network to reduce BGP peering for edge PEs.
# of Emulated mVPNs per PE router	This parameter should be considered in conjunction with **# of Emulated PE Routers**.
# of C-multicast sources per mVPN	With an increase of the number of C-multicast sources, the DUT multicast routing table entries and forward table entries will increase. With traffic, this will stress both the DUT control state and data forwarding state.
# of C-multicast groups	This parameter will also affect the DUT multicast routing table and forwarding table. It can also test a DUT's forwarding capability on replicated multicast packets.
CE IGP (unicast) Protocol	The unicast protocol running between CE and PE. This is used to advertise multicast sources behind the Ixia CE port. This option will be grayed out if the Ixia's CE port role is source.
IPv6 parameters	Ixia can emulate a customer IPv6 network. This is disabled by default.
Data MDT PIM protocol	The PIM protocol used for data MDT. It can be either SSM or SM. PIM-SSM is recommended as it will use the same data MDT group.

The proposed test can be scaled up or down based on the test variables above.

Conclusions

Based on result analysis, the DUT can source the required Data MDT tree and switchover the traffic on it with tolerable loss % and latencies. The DUT can sustain performance at both the control plane and the data plane to meet the specific scalability requirement.

Introduction to NextGen mVPN (NG mVPN)

The previous section talks in detail about GRE based mVPN. This section will touch on NextGen mVPN. Compared to mVPN, the NG mVPN improves on the following:

1) Instead of using PIM in the core to build and maintain the multicast tree across the provider core, it utilizes the MP-iBGP with new extensions to bridge the PIM domain from different VPNs connected via CE devices. This removal of PIM from the core network makes the solution much more scalable and easier to maintain.

2) In mVPN, data plane packets are encapsulated using GRE tunnel. In NG mVPN, data plane are MPLS label encapsulated. To distinguish the multicast traffic from the unicast counterpart, P2MP (as opposed to P2P for unicast) is established across the core. The P2MP tunnel is much effective in delivering multicast traffic as the same source can reach many receivers. Both mLDP and RSVP-TE P2MP are defined. Many vendors, including Ixia, support both. One added benefit of using RSVP-TE P2MP, the multicast traffic can now enjoy traffic engineering properties including FRR which usually provides sub 50 ms recovery time.

3) Both I-PMSI and S-PMSI and switchover procedures are defined which replaces the Default MDT and Data MDT in the GRE based mVPN. To further increase scalability of the solution, aggregation of both I-PMSI and S-PMSI are supported. That means many VPNs can share the same I-PMSI or S-PMSI with another top label as delineator of different VPNs. This can reduce the number of I-PMSI/S-PMSI (i.e., P2MP tunnels) in the core and will increase the scalability of the solution and reduce the complexity of maintaining and troubleshooting too many tunnels.

4) New SAFI (5) is defined for MCAST-VPN NLRI. 7 Types of C-multicast routes are defined as summarized below:

- **Type 1: Intra-AS I-PMSI A-D route**
  - Used by PE to announce mVPN membership (within an AS)
- **Type 2: Inter-AS I-PMSI A-D route**
  - Used by PE to announce mVPN membership (across AS boundaries)
- **Type 3: S-PMSI A-D route**
  - Used by Ingress PE to announce C-flows bound specific P-Tunnels
- **Type 4: Leaf A-D route**
  - Used to provide explicit tracking (enables a PE to announce itself as a receiver of a particular flow)

– **Type 5: Source Active A-D route**

  • Sent by PE to announce active sources within the sites connected to it

– **Type 6: Shared Tree Join route**

  • Equivalent to PIM (*,G) Join

– **Type 7: Source Tree Join route**

  • Equivalent to PIM (S,G) Join

5) Additionally, new attributes and new extended communities are defined

- New BGP Path Attributes:
  - PMSI Tunnel Attribute
  - PE Distinguisher Labels Attribute
- New BGP Extended Communities:
  - Source AS Extended Community
  - VRF Route Import Extended Community

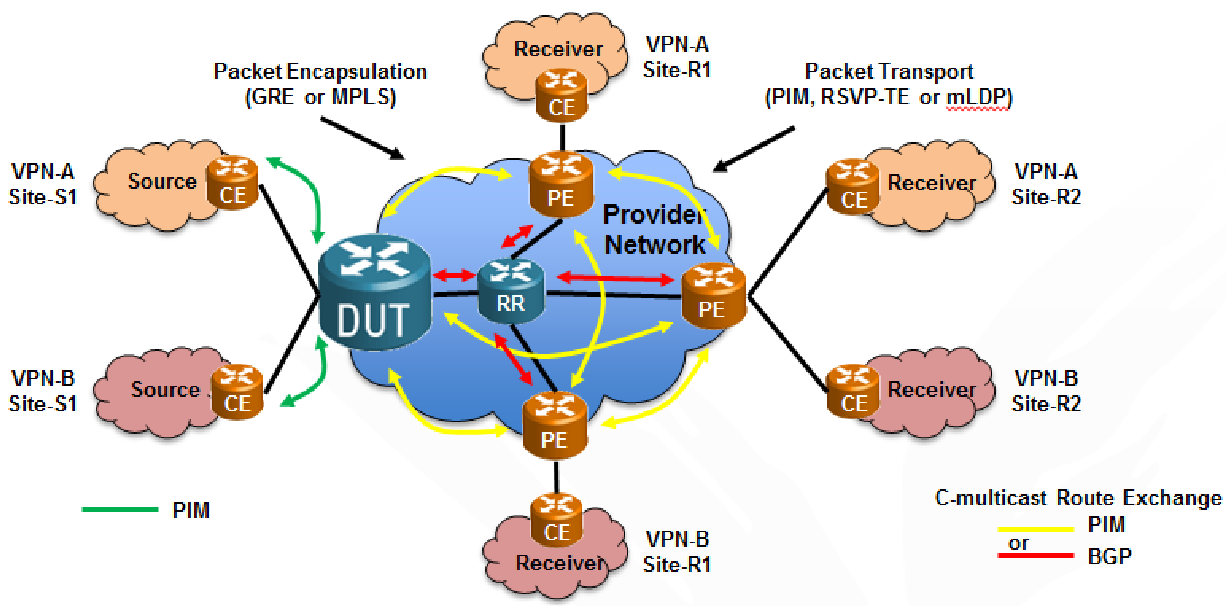


Figure 407. mVPN and NG mVPN in Comparison

Above diagram shows the comparison between mVPN and NG mVPN – they differ only in the core with one using PIM for control plane, and GRE for the data plane, while the other using

BGP (with new extensions) for control plane and MPLS P2MP for the data plane. Customer VPNs connected the core thru CE devise remain the same.

Here is how it works in a high level.

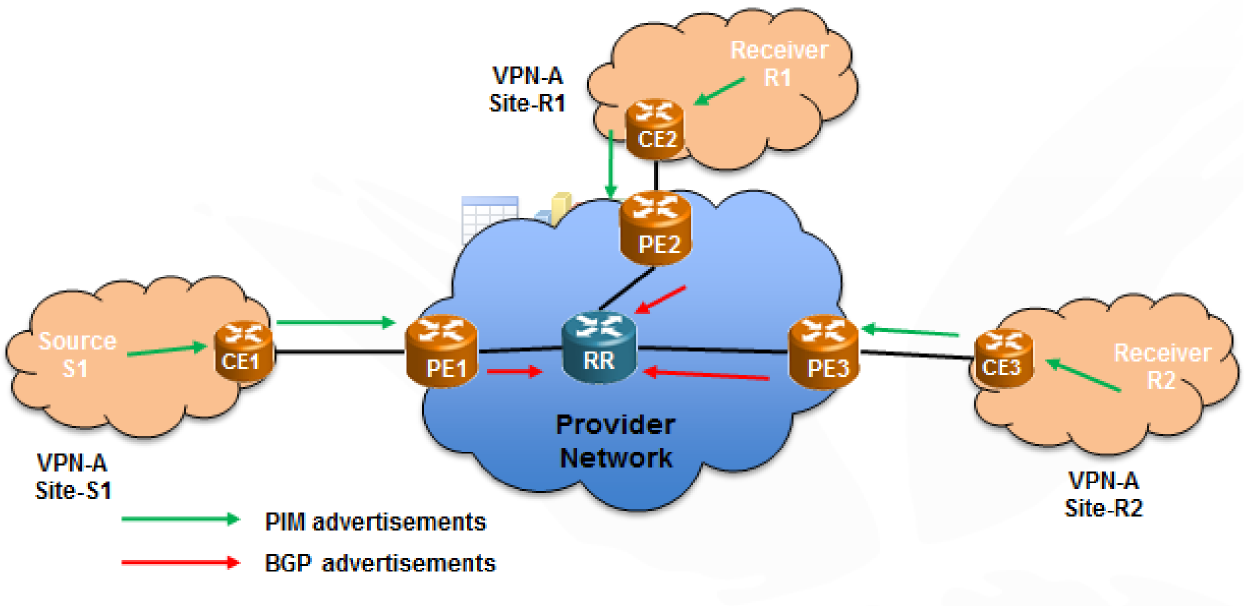


Figure 408. C-Multciast Route Exchange using BGP to Support PIM-SM in NGmVPN

Logic flow for PIM-SM SSM (S,G) in NG mVPN:

1. PE2 receives PIM Join from R1 for (S1,G)
2. PE2 constructs C-multicast route (Type7 - PIM Source tree route)
    a. Finds unicast VPN-IPv4 route for S1 in VRF-VPN-A and extracts RD and VRF Route Import extended community
    b. Builds route using:
        i. (S1,G) information from PIM Join
        ii. RD (using VPN-IPv4 route)
        iii. RT (using VRF Route Import)
3. PE2 sends C-multicast route (to all other PEs)
4. PE1 accepts C-multicast route into VRF-VPN-A because Import RT matches RT attached to route
5. PE1 propagates (S1,G) towards CE1 using PIM Join

Logic flow for PIM-SM ASM (*,G) in NG mVPN:

1. All PEs act as collocated Candidate Rendezvous Point (C-RP)
2. PE1 notified of S1 via PIM Register message from DR connected to S1
3. PE1 advertises this information (S1,G) to other PEs using a BGP Source Active (SA) auto-discovery route (Type 5), including
    a. RD and RT
4. PE2 receives PIM Join (*,G) from R1
5. PE2 constructs C-multicast route (Type 6) - one for each received SA AD route that has G
    a. Based on receipt of SA routes PE2 and PE3 know which PEs to send C-multicast routes
6. When Receiver switches from RPT (shared tree) to SPT (source tree), the switch is localized (R1 switches to SPT by sending a PIM Join (S1,G) to CE2, then PE2.

Relevant Standards

- RFC 4364 – BGP/MPLS IP Virtual Private Networks (VPNs)
- draft-ietf-l3vpn-2547bis-mcast-bgp-08 (RFC 6514) – BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

Test Case: NG mVPN Functional Verification with I-PMSI and S-PMSI, and Switchover Test

Overview

NG mVPN is a complex technology and it's critical to understand the fundamental elements in this technology. I-PMSI and S-PMSI are the two basic constructs of the technology, and their switchover by the ingress PE that is connected to the multicast source can be triggered either on the fly by configuring bandwidth threshold, or by administrative means. It's important to understand what processes are involved, and how to verify if the switchover indeed took place. Other key constructs in the NG mVPN includes all the other types of C-Multicast Routes. The most important part is to understand where to look for them, and how to verify them and be assured everything's works as expected. Additionally, MPLS P2MP tunnel is the underline transport. It must work seamlessly with MP-BGP to encapsulate the data plane traffic over the right tunnel.

Objective

This test is designed to illustrate the key steps to configure a basic NG mVPN test, and how to verify if it is working correctly. We will use two test ports to simulate both PEs with multicast source, as well as PEs with multicast receivers behind the simulated CE and hosts cloud. This test is not so much concerned in testing scalability with many PEs, or many MVRFs, rather focused on the key configuration and verification steps to get thorough understanding of the technology. Once this is accomplished, scale to multiple PEs or multiple MVRF is fairly straightforward. Next test case will also discuss in detail how to scale the test even further with aggregation enabled.

The transport P2MP tunnel will need to be verified and the traffic over I-PMSI, or S-PMSI after switchover needs to be encapsulated over correct tunnel. We will show you the steps how to verify if they all worked correctly according to the standard.

Setup

Two Ixia test ports are required for the test as depicted below. In the real setup, most likely one of the test ports will be used to emulate a CE that is connected to the DUT as PE. We will walk you step-by-step to configure test ports either as the Ingress PE that is connected to the multicast source, or the egress PE that is connected to multicast receiver. You're covered in the real setup, as you can choose either step to follow: If DUT is the ingress PE, and set Ixia to emulated the egress PE. Likewise, if DUT is the egress PE, then set Ixia as the ingress PE.

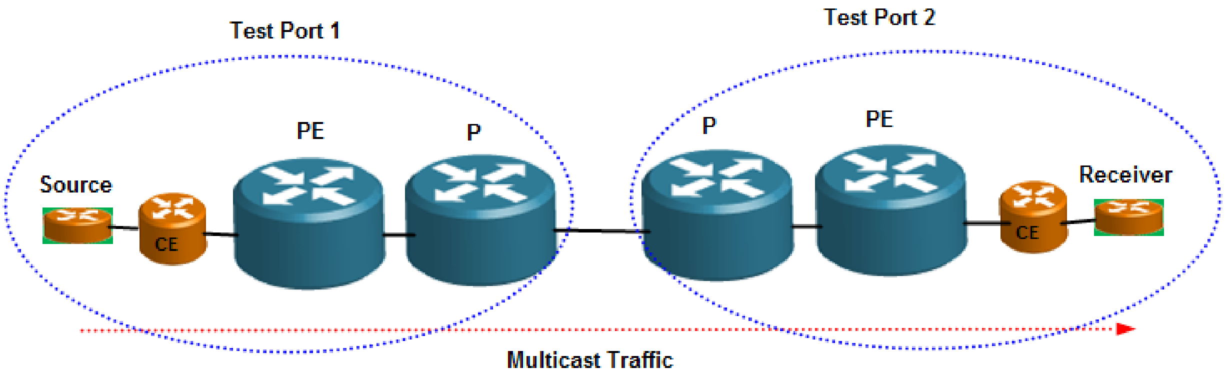


Figure 409. NG mVPN Functional Verification Test Setup

Step-by-Step Instructions

1. Launch the IxNetwork “Multicast VPN” wizard, and go to the first page to select port role. We will configure the first test port that emulated P and PE with multicast source behind. Leave the second port idle for the moment, and will configure that port with multicast receiver later. In the meantime, use a dummy (offline) port as the CE with receiver. This is needed because wizard would need some receivers in order to move to next pages.

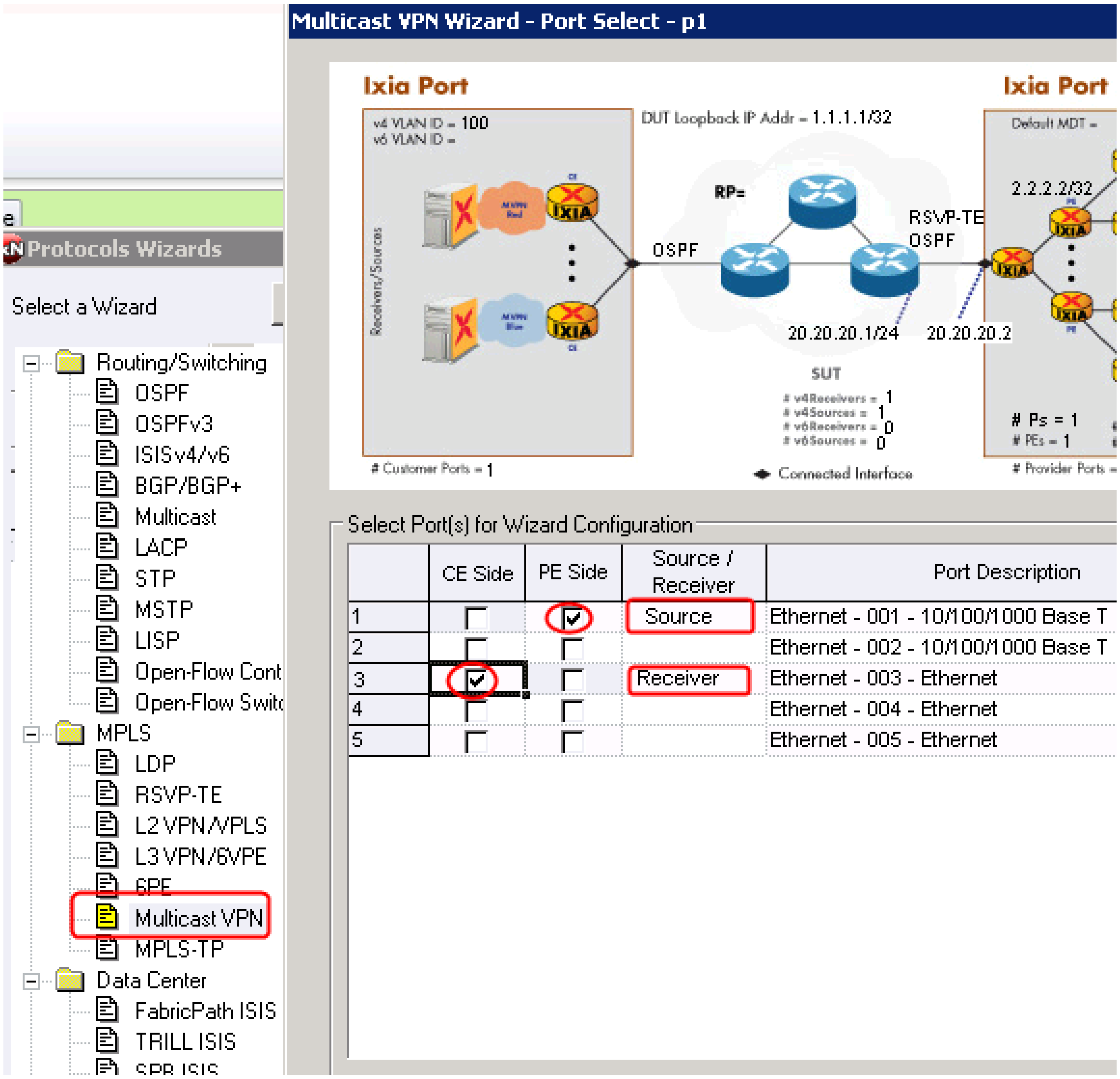


Figure 410. Seletc port role in the mVPN wizard

2. In the next page of the wizard, select the correct P-Tunnel Protocol that fits your needs. PIM-SM and PIM-SSM are for the drafter-Rosen GRE based mVPN. RSVP-TE P2MP is using RSVP-TE protocol to establish a P2MP tree from the ingress PE (multicast source behind) to all the egress PE with multicast receivers behind. mLDP is to use the LDP with the multicast extension to accomplish the same. While protocol may differ, the procedures to configure the NG mVPN and troubleshooting are more or less the same. In steps to come, we will use RSVP-TE P2MP as examples. mLDP is very much the same. Note that the rest of parameters are similar to other wizard such as the L3VPN. If you're not familiar with those, you are encouraged to review the L3VPN test cases detailed in previous sections of this book.

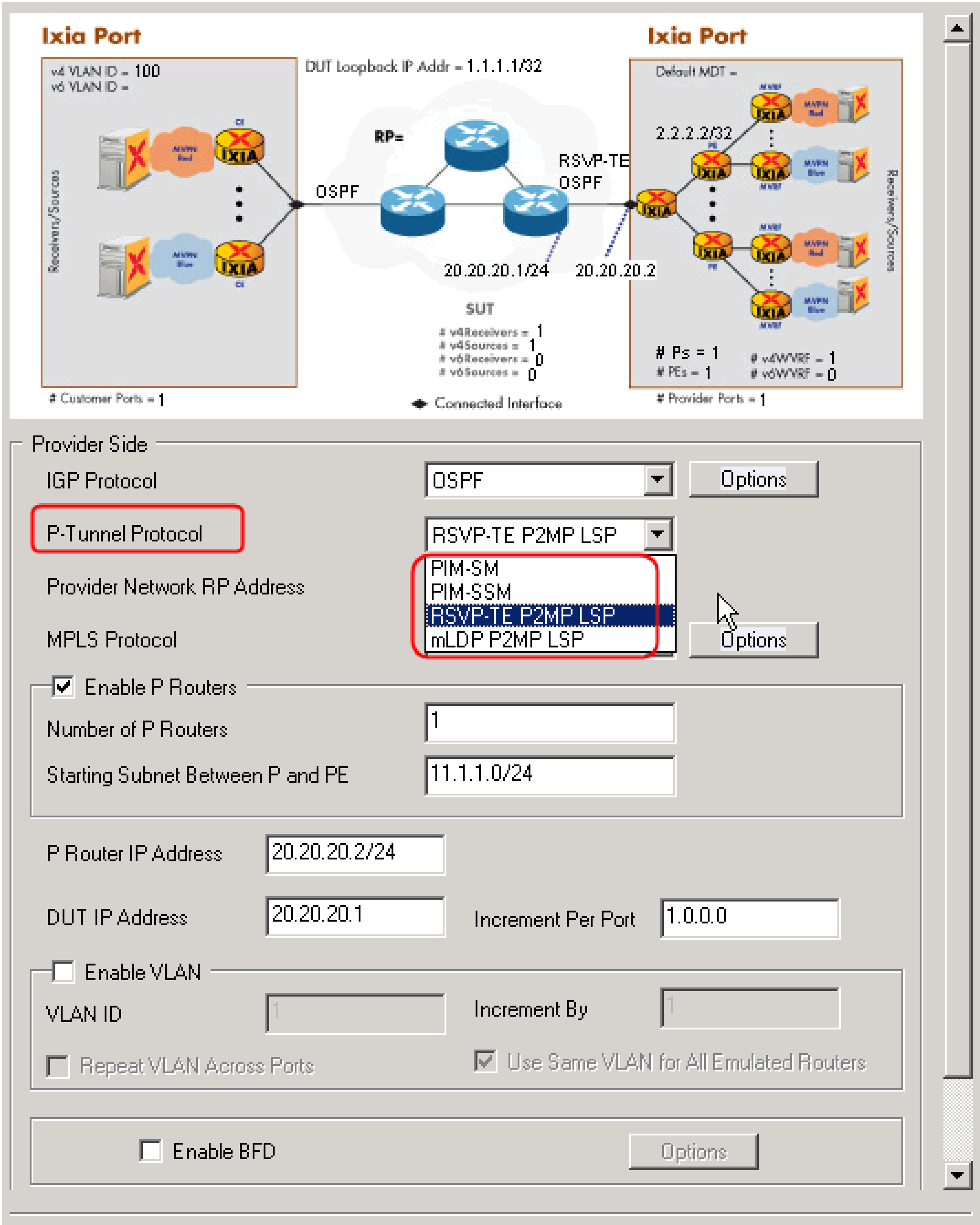


Figure 411. Select the right P-Tunnel for NG mVPN

3. The next page of the wizard is the same as the L3VPN wizard. After all, the NG mVPN is built on top of the L3VPN to deliver the multicast traffic. They go side by side.

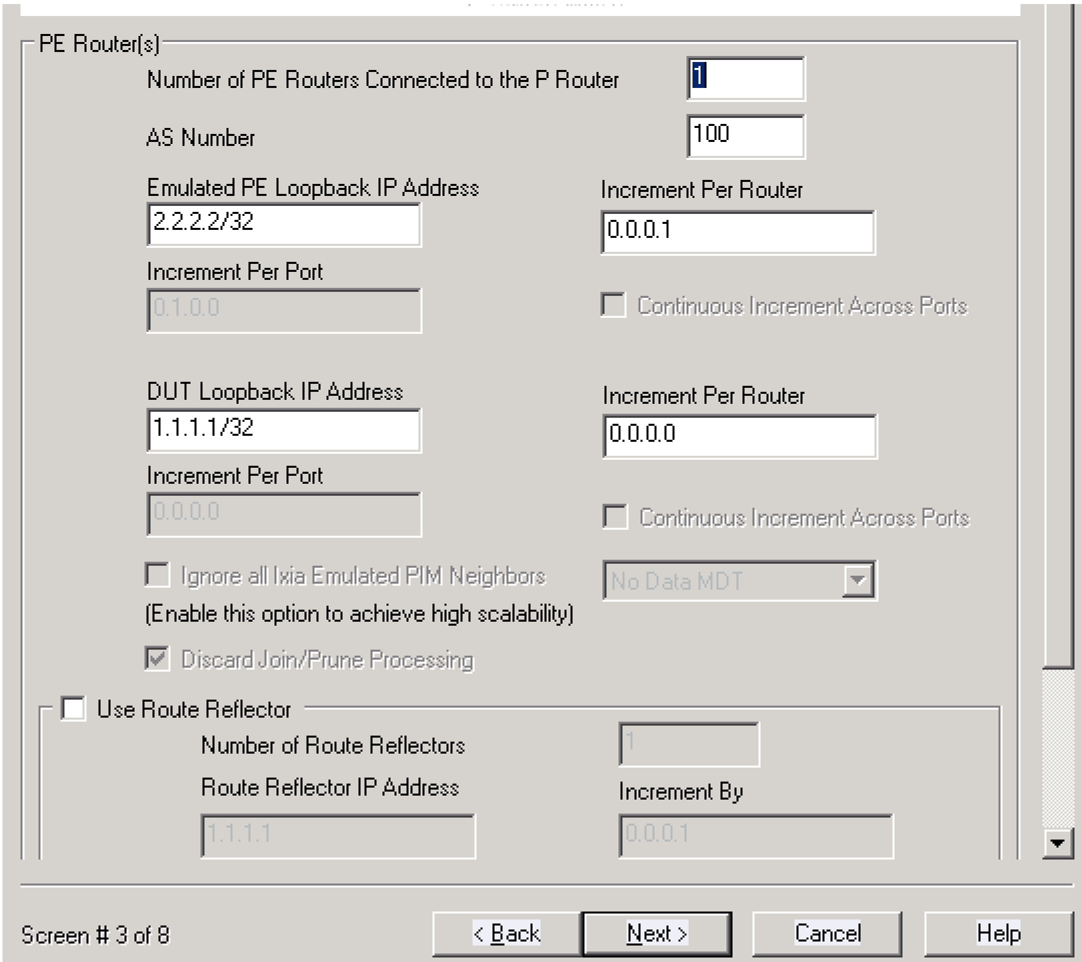


Figure 412. Configure P and PE routers

4. In the next page of the wizard, the Route Distinguisher, Route Target, The number of VPNs per PE, whether or not they are unique – are the same as L3VPN. Again, if you're not familiar with them, you're encouraged to browse the L3VPN configuration detailed in previous sections of this book. Here we only focus on the NG mVPN specific configuration parameters.

   Don't enable the "Aggregation" and "Use I-PMSI Upstream Label" options yet. We will discuss them in next test case.

   The P-Tunnel configuration parameters are related to the protocol you had chosen in the "P-Tunnel Protocol" option in the second page of the wizard. Since we chose the "RSVP-TE P2MP LSP", these parameters are related to RSVP-TE P2MP protocol. If you're not familiar with the RSVP-TE P2MP protocol, you should go back to the section of this book where RSVP-TE P2MP is introduced and detailed. Here we assume you have the technical knowledge of that protocol.

The only option that needs to be enabled is the "Enable S-PMSI" which basically configures the PE router with multicast source to prepare itself with not only the I-PMSI, but also the S-PMSI. The user then can trigger the I-PMSI to S-PMSI switchover on demand. Usually, a real DUT, as the ingress router, will also support the dynamic on-the-fly switchover, by allowing the user to configure a bandwidth threshold for example. As a tester, we don't support this feature. However, to test the switchover functions, user on-demand switchover is more than enough.

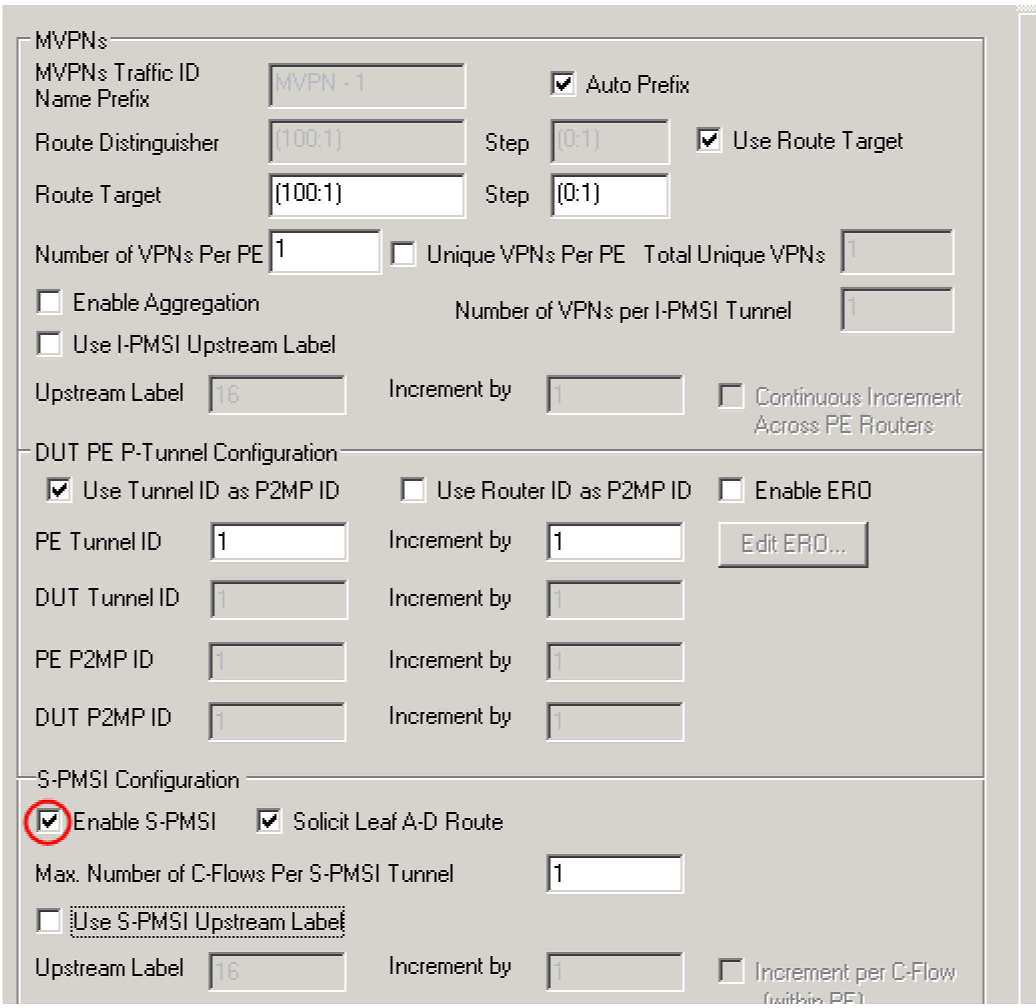


Figure 413. I-PMSI and S-PMSI selection for functional test

5. Next page of the wizard lets the user configure the multicast source and receiver. They are fairly straightforward. One extra option called "Use UMH Selection Routes" can be optionally enabled. What this option is to allow the emulated PE to advertise the "source" using SAFI=129 instead of SAFI=128 to the far end PE. UMH stands for Upstream Multicast Hop. If this is not enabled, the ingress PE will advertise the multicast source as standard L3VPN VRF route. This route will be used by the egress PE to identify which VPN, and where the source is behind so the egress PE can signal to the right PE if they have (S,G) or (*,G)

interest associated with this multicast source. The logic of how (S,G) and (*,G) from egress PE perspective is described in detail in the introduction section. The need for a new SAFI (129) for these multicast routes are two folds: 1) if advertised with SAFI 129, the egress PE will maintain a separate VRF table for these routes to make them distinct from regular VRF routes which are used for data forwarding. These multicast routes are NOT for forwarding rather for PE identification of where the source is located. 2) Some applications require fast convergence during failover and by use of new SAFI, the ingress PE will do special procedure on these routes for quicker convergence.

All the other parameters are obvious. Note that IxNetwork also supports IPv6.

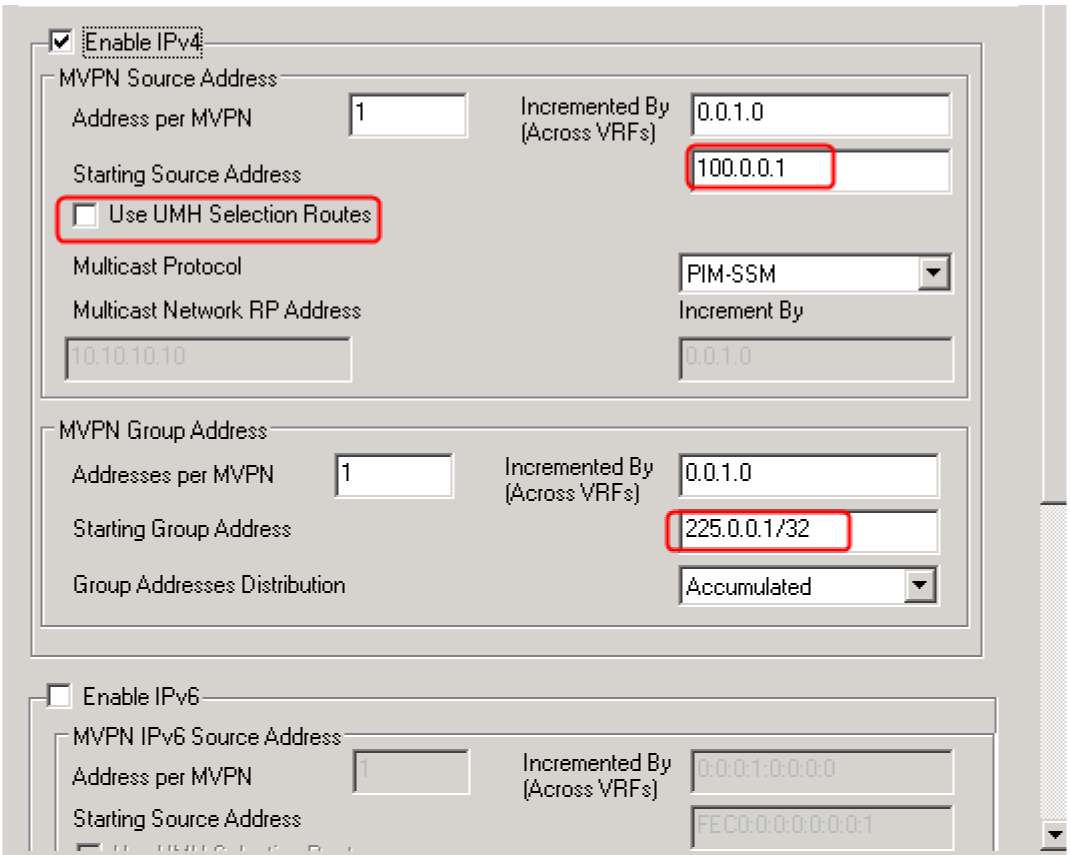


Figure 414. Customer Multicat settings behind the emulated P/PE core

6. Next page is on the CE configuration. It’s not used in our test setup but will be in real test setup. Their configuration is similar to L3VPN and won’t be explained further here.

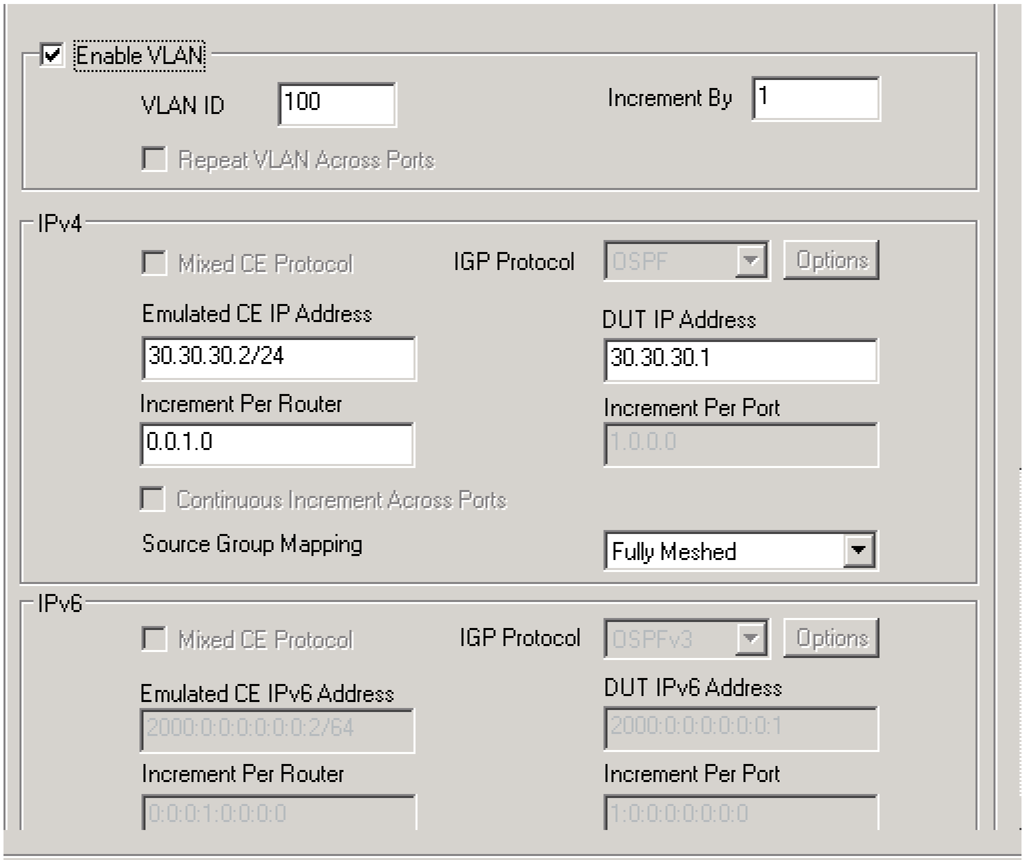


Figure 415. CE port setup

7. Give a name and save and overwrite the config.

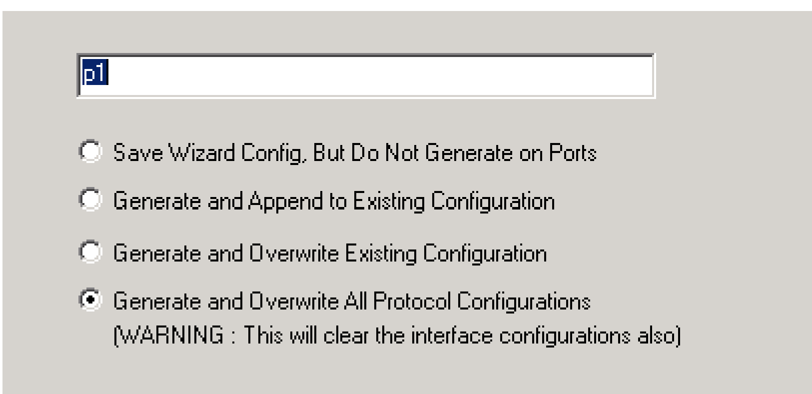


Figure 416. Last page of configuration wizard

8. Now that we have finished configuring of the first port which simulated PE and multicast source. Let's proceed to configure the second test port with PE and multicast receivers

behind. The quickest way is to double click on the saved wizard configure (p1) and that will inherit configuration parameters from the first run. Simply select the second port and put it into “receiver” mode. Again, use the dummy port as “source” to facilitate the rest of configuration.

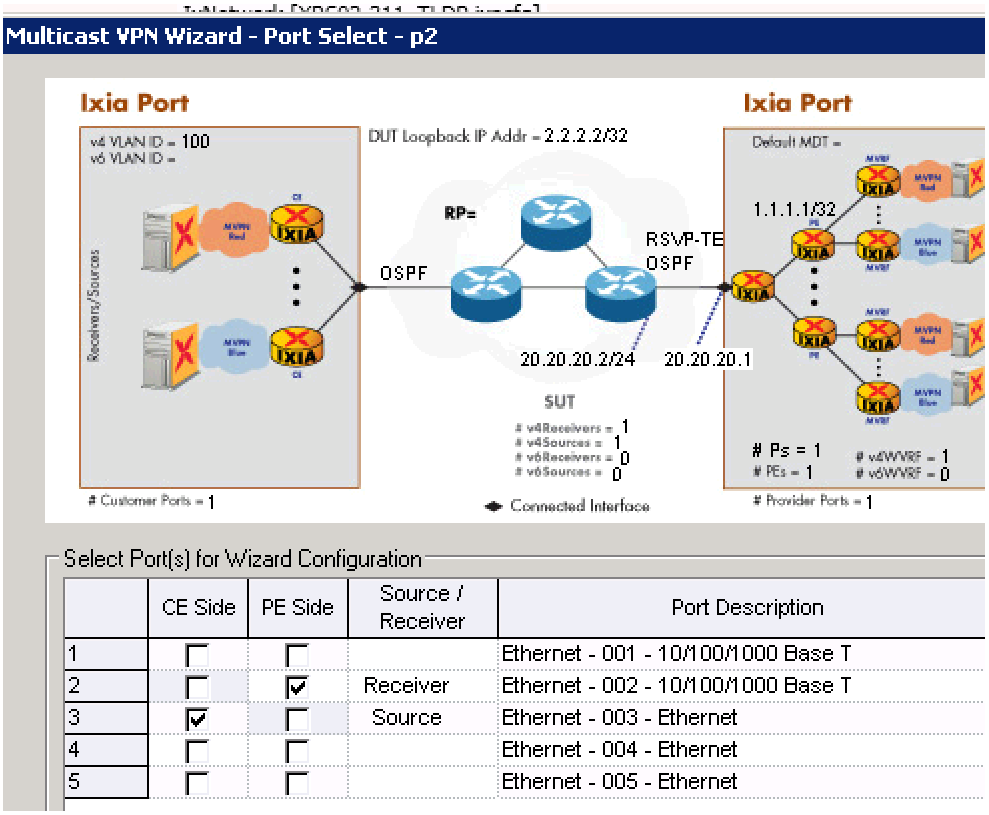


Figure 417. Configuration of multicast receiver port

9. Next page is to configure the P-Tunnel Protocol. Keep it the same as previous wizard run. Configure the IP address accordingly.

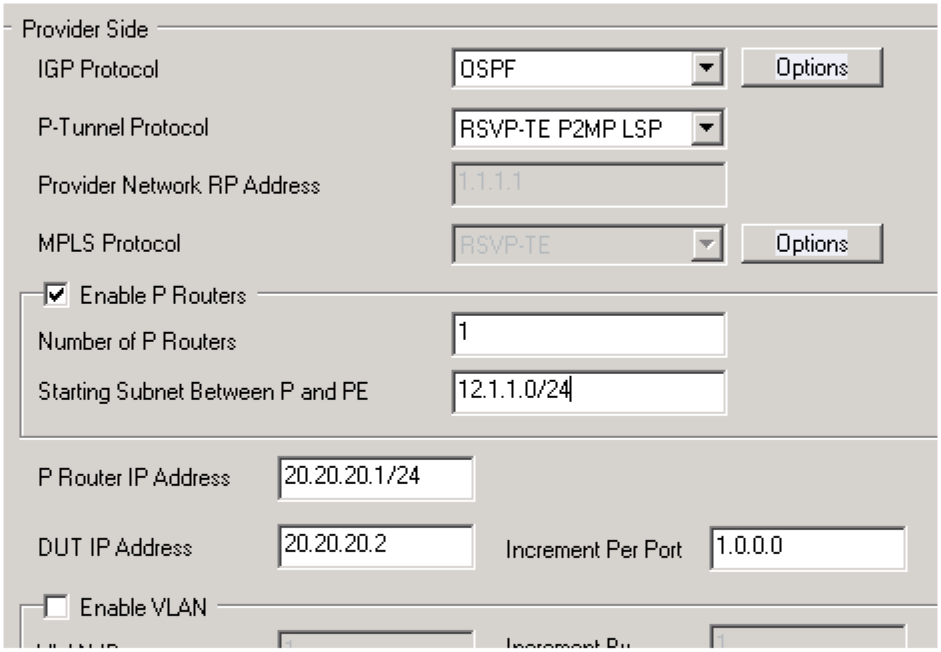


Figure 418. Seletc the right P-tunnel protoocol

10. The rest of pages are similar to the first test port and they won't be repeated here.

11. Now we have completed most of the configuration work for the setup depicted in the setup diagram. Before we start running the config and examine the learned info in order to determine what should be seen and whether or not they are working. But before that, we need to do some tweak on the RSVP-TE P2MP configuration.

12. Because we configured the port 1 with multicast source only (no PE with receivers in the wizard run), the RSVP-TE P2MP tunnel will need to be manually tweaked so the head (RSVP-TE P2MP tunnel head) knows what the leaf nodes are. Below screen capture shows how to make the change: change the "**No of Tunnel Leaf Ranges**" from default 0 to 1, and then change the **Tunnel Leaf Ranges** and enable it. The RSVP-TE for the first port shows two P2P tunnels (bidirectional), and two RSVP-TE P2MP tunnel – one for I-PMSI, and the other for S-PMSI.

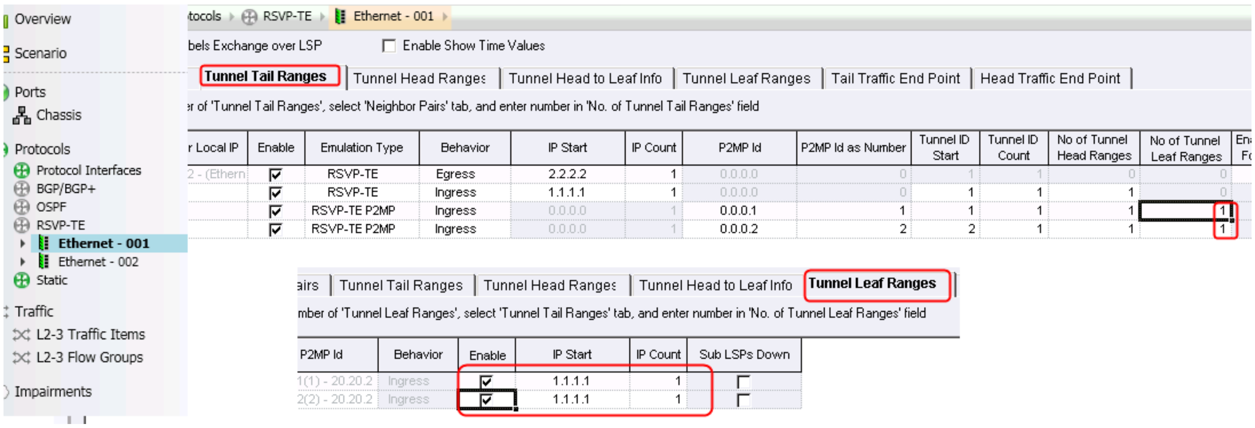


Figure 419. Manual changes for RSVP-TE on the Source port

13. Optionally you can also change the label value on the second port to avoid identical labels for RSVP-TE and BGP due to common default (16). This will aid in troubleshooting if things don't work as expected.

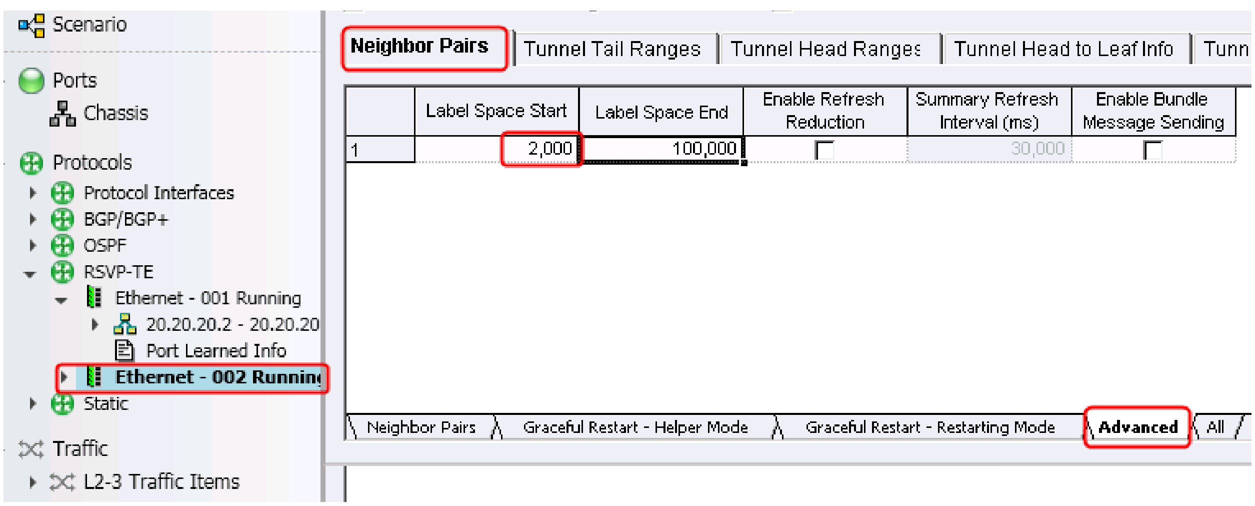


Figure 420. Configuring RSVP-TE label space

14. Start all protocols and examine learned info one by one to understand and determine if everything works as expected. Start with RSVP-TE tunnel. Check from the test port for learned info. Clearly it shows two P2P tunnels (one ingress and one egress), and two P2MP tunnels with label values we just assigned. The P2P tunnel will be used for unicast while the P2MP tunnels are for multicast. Traffic riding on the I-PMSI will be encapsulated using the first RSVP-TE P2MP tunnel (label = 2001) and should I-PMSI to S-PMSI switchover takes place, the same multicast traffic will need to ride on the second P2MP tunnel (label=2002). These will need to be clearly understood in order to tell if the DUT is behaving as expected.

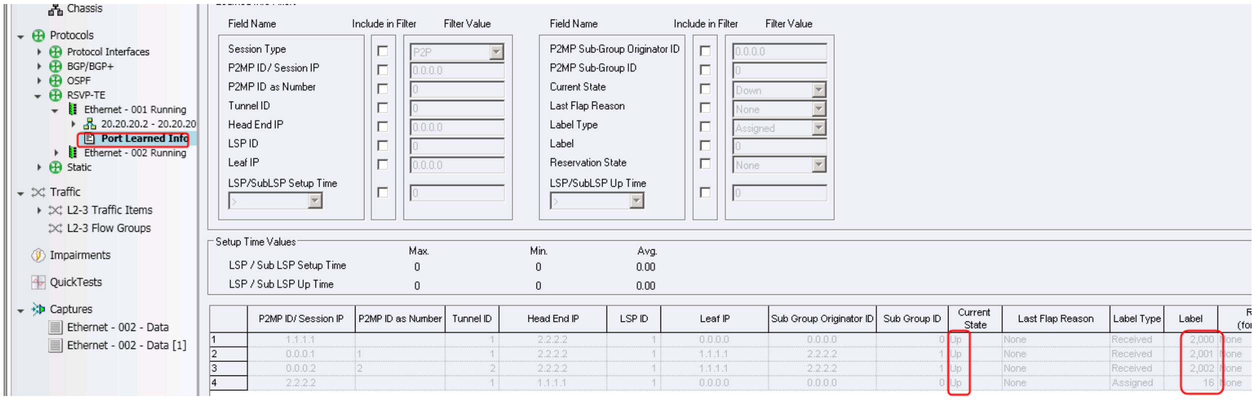


Figure 421. RSVP-TE learned info for both P2P and P2MP tunnels

15. Next, we will examine BGP learned info. On the ingress PE that is connected to the multicast source (test port 1), we can see I-PMSI AD and C-Multicast AD routes. I-PMSI indicate VPN membership advertisement from egress PE, and C-Multicast AD route indicate (S,G) request form the egress PE that is connected to the multicast receiver. We don’t see the other types because: 1) No I-PMSI to S-PMSI switchover taking plane yet 2) There is no Inter-AS scenario configured so there is no Leaf-AD; and there is switchover taking place so there is no proactive solicitation of Leaf-AD 3) The ingress PE will advertise Source Active AD, not receiving it.

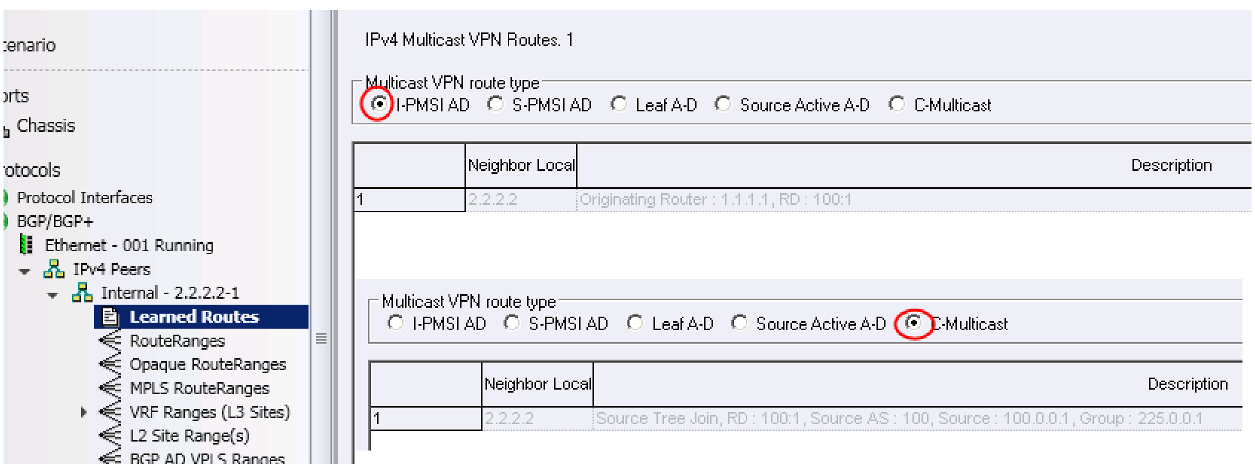


Figure 422. Verifying learned C-Multicast routes on the source port

16. Let’s look at the learned info from egress PE point of view. It displays both I-PMSI AD as well as the Source Active AD. I-PMSI AD indicates VPN membership from the Ingress PE, as well as the P2MP tunnel it’s going to use for traffic encapsulation. Note that it includes a second label value of zero which means there is not second label in the traffic. This is because we did not enable the aggregation using upstream assigned label. Each (S,G) or (*,G) will have its own I-PMSI to ride on and a single label is good enough for the egress PE

to delineate the multicast traffic. We didn't see the other types of AD routes because 1) no I-PMSI to S-PMSI switchover taking plane yet 2) no Leaf AD from the ingress PE, and it's not about Inter-AS use case 3) no C-multicast AD routes from the multicast source.

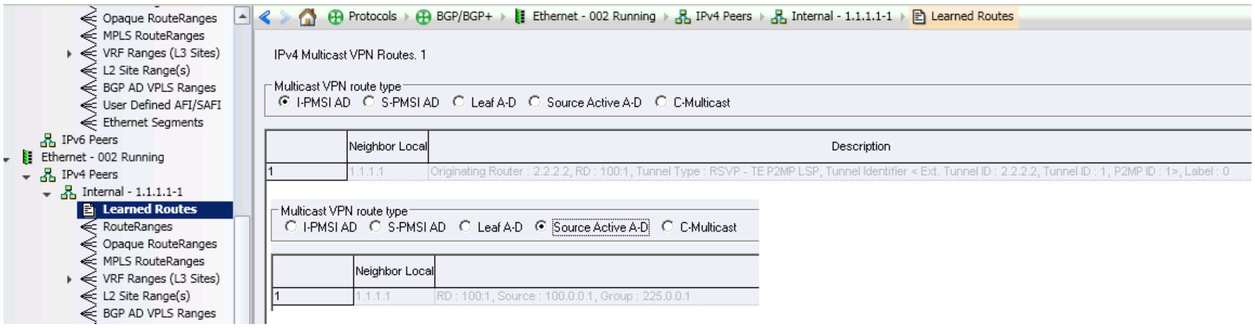


Figure 423. Verifying the learned C-Multicast routes from receiver port

17. Now let's activate the on-demand I-PMSI to S-PMSI switchover from the ingress PE. The way to do it is by going to the **Multicast Sender Sites** tab and click and highlight the S-PMSI tunnel to switchover to, and click on **Switch to S-PMSI** icon in the ribbon area.

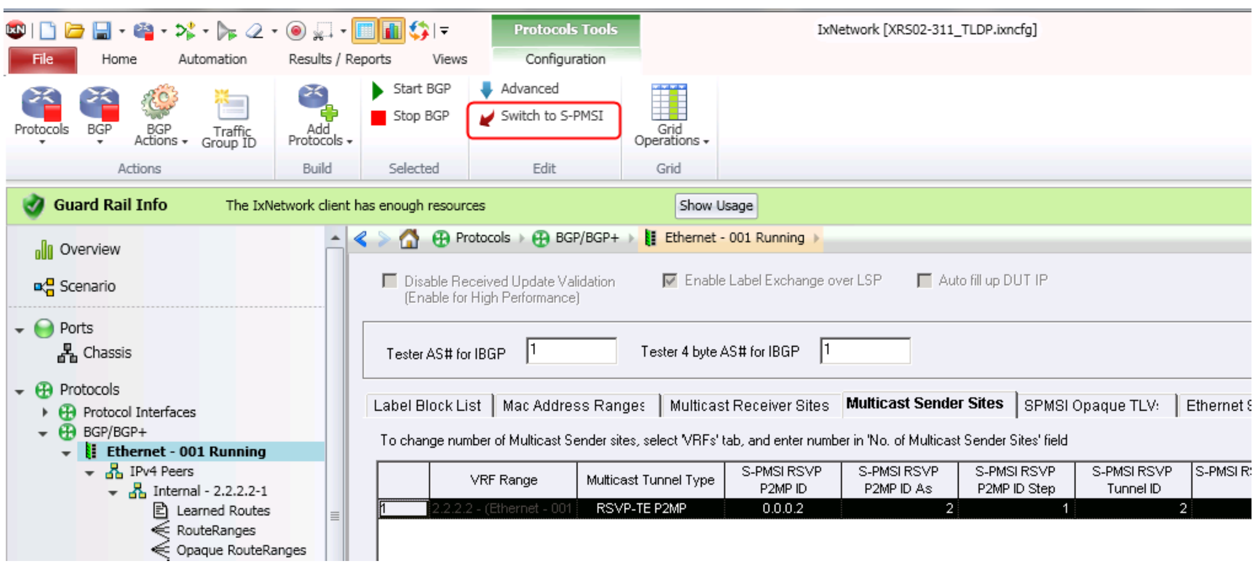


Figure 424. I-PMIS to S-PMSI switchover

18. After the on-demand switchover taking place, let's examine the learned info again on both the ingress PE as well as the egress PE.

19. On the ingress PE (connected to multicast source), the only new thing we see is the Leaf-AD route compared to before the switchover.

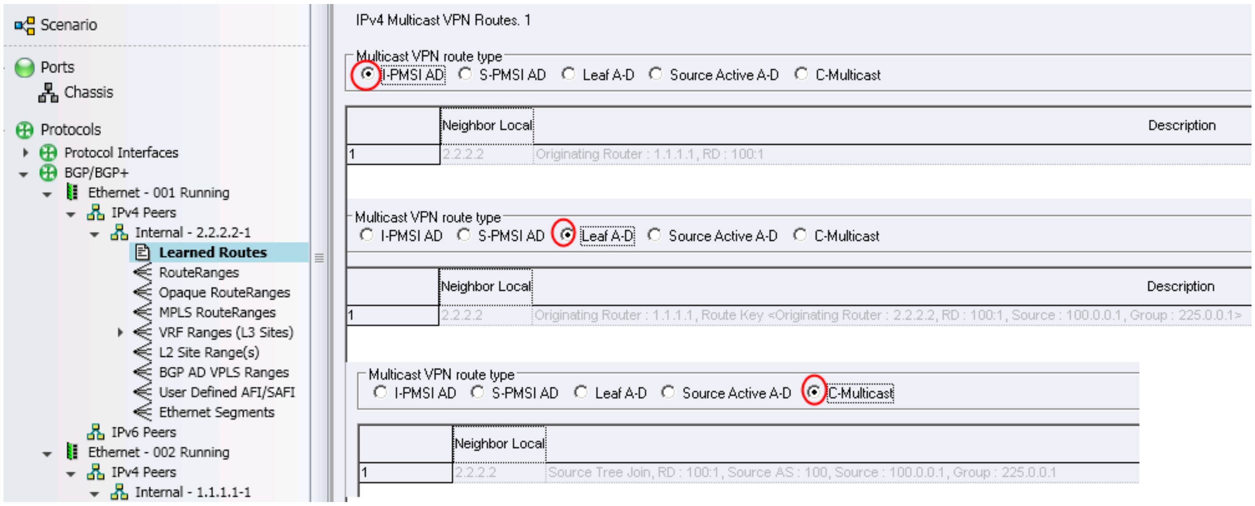


Figure 425. Learned AD routes from soruce port after switchover

20. The reason we see an extra Leaf-AD route is because we have toggled on the “Solicit Leaf A-D Route” option when configuring the S-PMSI on the wizard, the corresponding GUI bit is also shown in the screen capture.

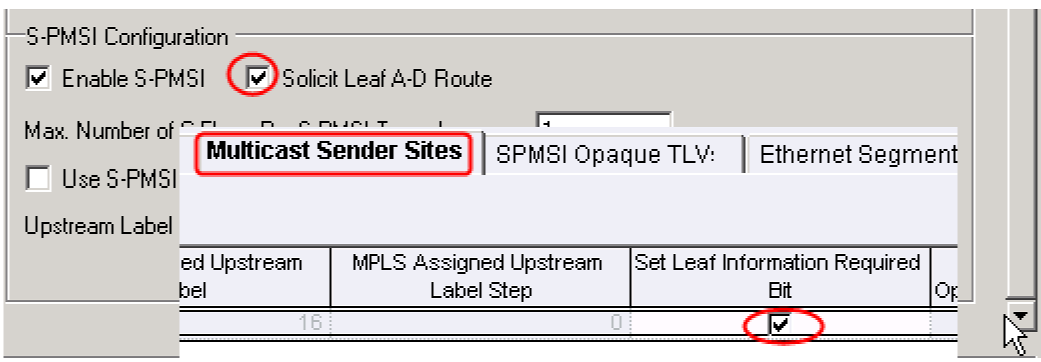


Figure 426. Leaf AD route settings

21. On the egress PE, we also see an extra S-PMSI AD routes with lable value of zero which means no aggregation labels available. The S-PMSI AD route is to tell the receiver that the ingress PE has switched the traffic from the original I-PMSI to the new S-PMSI tree.

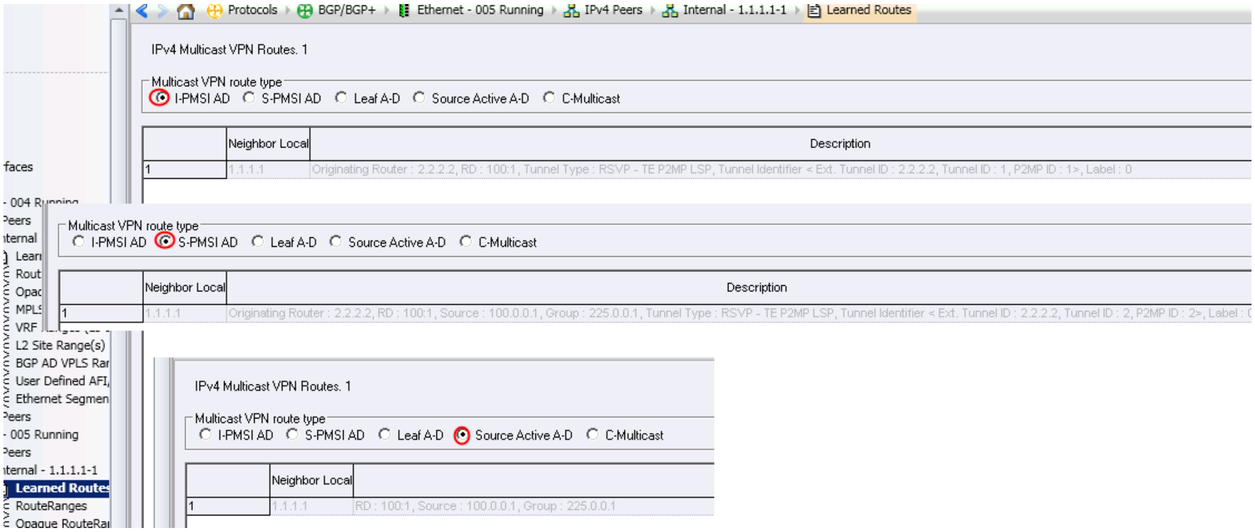


Figure 427. Learned AD routes from receiver port after switchover

22. Now all control plane activities before and after I-PMSI to S-PMSI switchover can be clearly explained and verified, let's see how to set up the traffic and verfify the label encapsulation.

23. Launch the traffic wizard and let's start with I-PMSI traffic. Since Ixia is not a real router, it doesn't have the logic to automatically switch the data plane traffic from I-PMSI to S-PMSI based on for example a pre-configured bandwidth threshold. Instead, it listed the multicast source under both the I-PMSI and S-PMSI category so the user knows exactly which one is currently sending. Since we're building traffic to go over the I-PMSI tree, make sure you select the source under **Multicase I-PMSI Sender Ranges**. The traffic wizard will knows which label to use for the traffic to build.

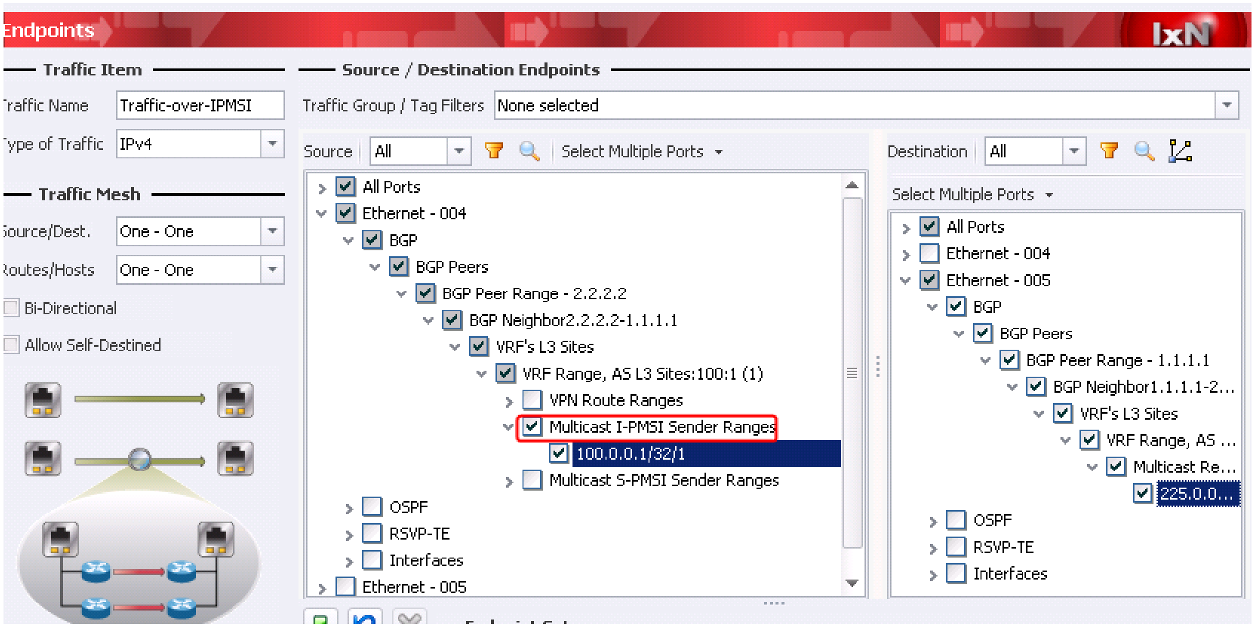


Figure 428. Traffic end points selection for NG mVPN traffic

24. All the rest of traffic wizard steps are straightforward, and exactly the same as any other VPN technologies under test. You can examine the generated traffic by use of flow group editor to view the MPLS labels used for the traffic, and verify if it's consistent with the RSVP P2MP label learned at the ingress PE. In our case, they match well as expected.

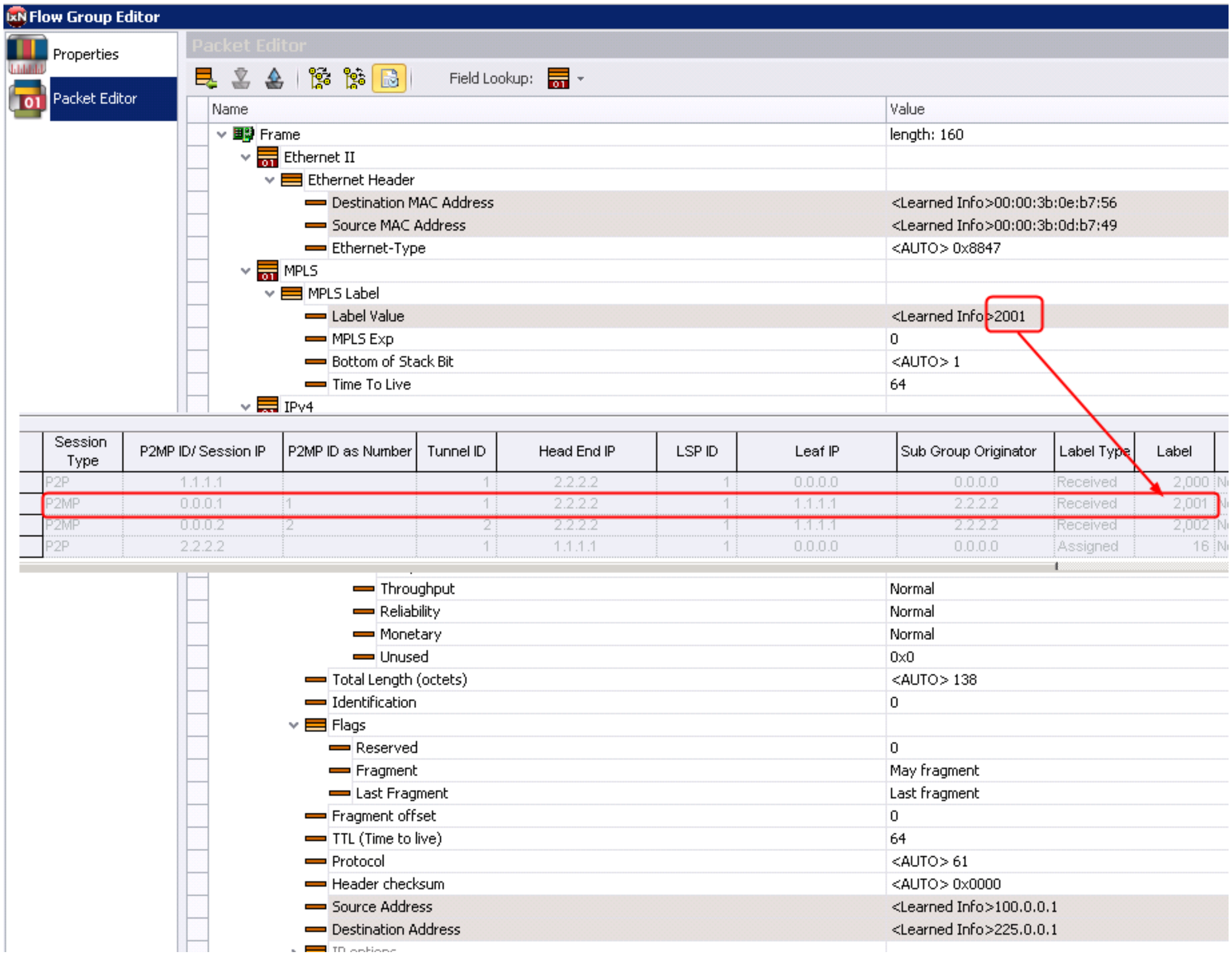


Figure 429. Traffic verification to ensure correct encapsulation

25. Next, we will build the traffic to go over the I-PMSI tunnel. Launch the traffic wizard in a similar fashion, and this time the only difference is to select the **Multicast S-PMSI Sender Ranges** as the traffic source. This will trigger the traffic wizard to look for S-PMSI labels to build the traffic.

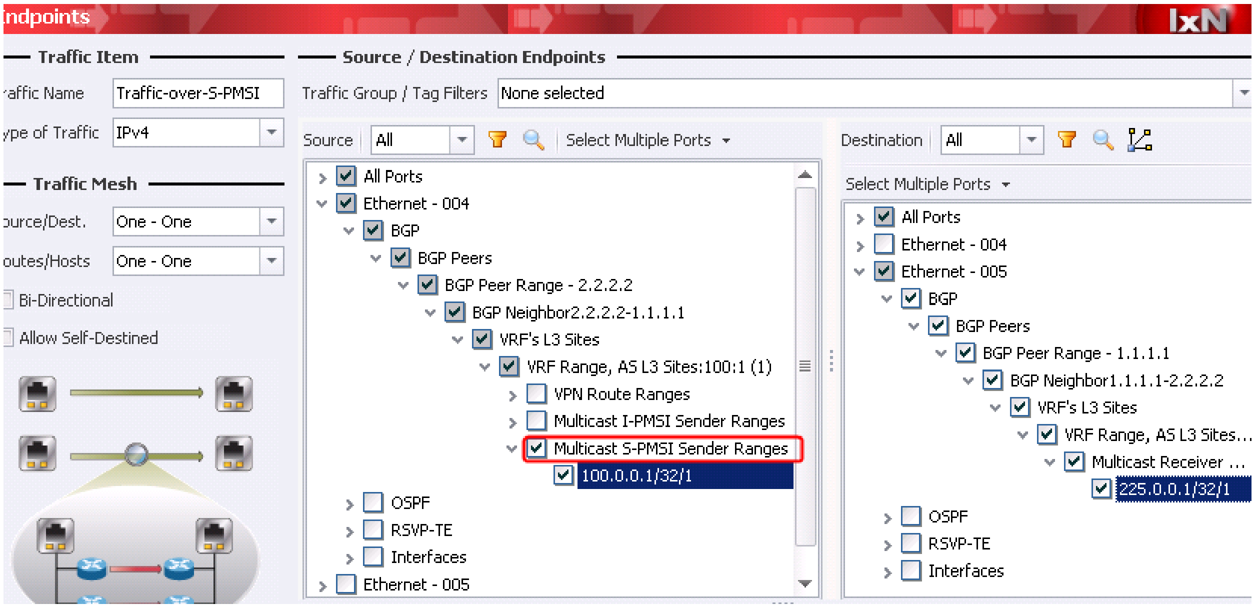


Figure 430. Separate traffic item for traffic going into S-PMSI tunnel

26. Of course, you need to verify the labels after finishing the traffic wizard generation. In our case, label 2002 which corresponds to the S-PMSI label at the RSVP P2MP head end (ingress PE).

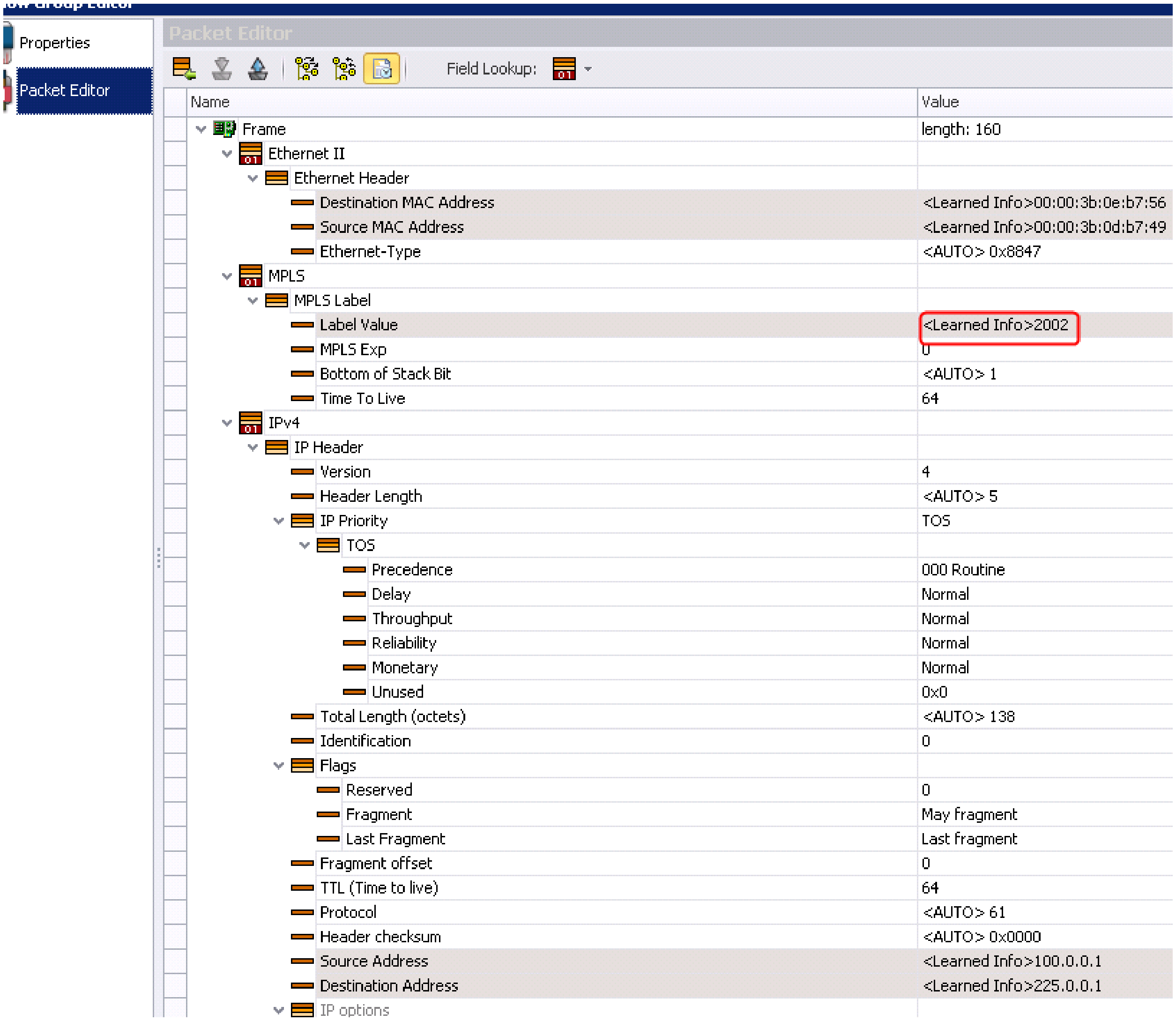


Figure 431. Traffic verification to ensure correct encapsulation

27. We have successfully completed testing procedures to conduct basic functional test for NG mVPN using RSVP-TE P2MP as the P-Tunnel technology. If you prefer using mLDP instead, the configuration and verification steps are very much the same with the exception in selction of P-Tunnel protocol in the wizard configuration as shown below.

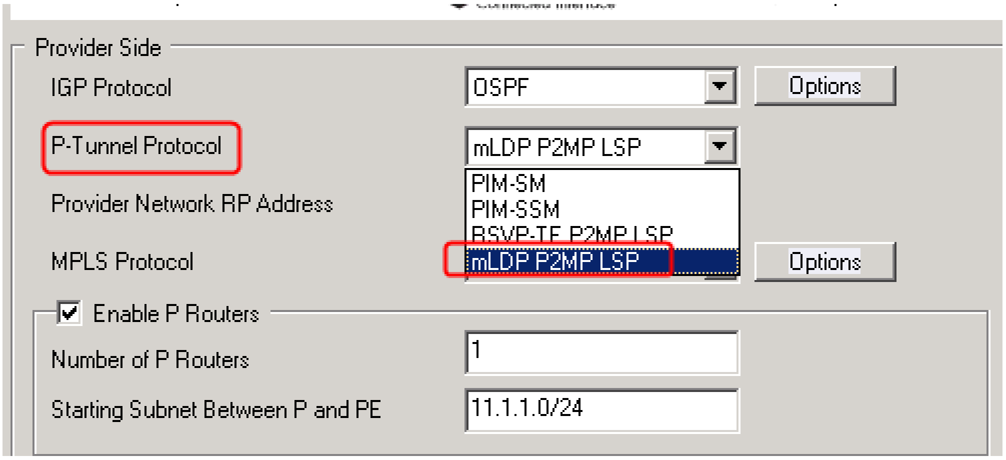


Figure 432. How to enabled mLDP instead of RSVP P2MP as the P-Tunnel

28. The ingress PE port will show the learned info reflecting mLDP P2MP label assignment for both the I-PMSI and S-PMSI tree, and the egress PE will show the BGP learned I-PMSI AD indicating mLDP P2MP as the tunnel type.

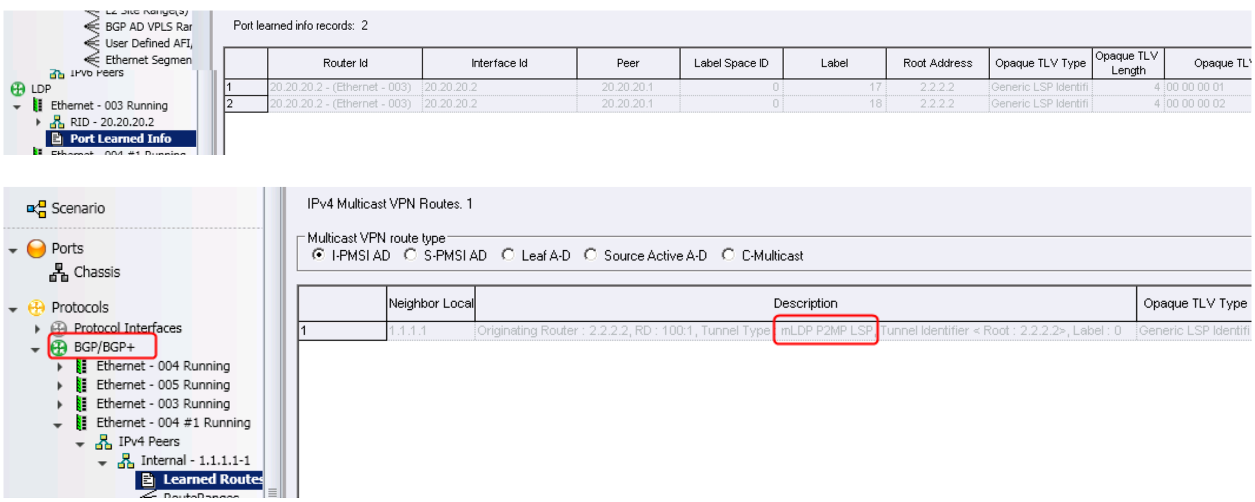


Figure 433. mLDP learned info

29. The key to both test cases is to have a full understading about the various AD routes, and where they should appear. When building traffic, make sure to pick the end points from the right category and be able to verify the labels before sending the traffic. Of course, you can write a Test Composer script to simulate the true DUT behavior where once the I-PMSI to S-PMSI switchover is triggered, stop sending traffic over the I-PMSI tunnel, and start sending the same traffic over the S-PMSI tunnel. This is important to test realsm especially with large number of VPNs, or large number of Source/Groups.

Test Variables

Consider the following list of variables to add in the test in order to make the overall test plan better.

Functional/Performance Variable	Description
Increase the number VPNs per emulated PE, and optionally the number of PEs, and the number of Source and Multicast Group in each VPN. This will increase the number of I-PMSI and S-PMSI and will help stress test the DUT.	While funcational verification is one thing, scale test is another. Many DUT will behave strangly, or sluggishly when facing with large number of C-multicast AD routes and many I-PMSI to S-PMSI switchover policies. This will further validate the need for aggregation that we will examine in detail in next test case.
Test mix of P-Tunnel techlogies with both RSVP P2MP and mLDP	The RSVP P2MP P-Tunnel is as popular as the mLDP and many commertial DUT support both flavors. It's important to verify they can coexist.
Upper Multicast Hop (UMH) selection test	UMH routes are advertised via a different SAFI value and they are sometimes used for specific purpose. In our example, we didn't show the steps to configure and verify correction of UMH. If UMH is actively used by your DUT, you will need to test both the function and scale when this feature is enabled.

Test Case: NG mVPN Stress and Scale Test with I-PMSI and S-PMSI Aggregation

Overview

While functional test is an important starting point, it's the stress and scale test that usually reveals the true strength or weakness of a given DUT. In previous test, we have stayed away on purpose to not include the aggregation labels and leave stress and scale test to this section.

Scalability of NG mVPN can be achieved from many dimensions. The simplest is to increase the number of P and PEs in the simulated network. The next is to increase the number of VPNs per simulated PE. The last one is to increase the number of (S,G) or (*,G) across the VPN. This will effectively populate DUT with many C-Multicast AD routes, and increase the total number of P-Tunnels across the core network. As the number of P-Tunnel increases, further scalability of the solution become more difficult. Fortunately, the technology has built-in mechanism to increase the scalability to much further via the use of aggregation labels. The aggregation label is applicable to both I-PMSI and S-PMSI tunnels. The idea is to bundle multiple VPNs into a single P2MP tunnel to create sharing so to keep the total number of P-tunnels in the core to a comfortable level. Imagine that if we have to test a DUT with 8K mVPN, without aggregation it will require 8K I-PMSI, and 8K S-PMSI - a total of 16K P2MP tunnels in the core. This is hard to manage and/or troubleshoot. If we enable aggregation for example to use 10:1 ratio – meaning 10 VPN to share single I-PMSI P2MP tunnel, that will reduce the total number of I-PMSI to just 800 (instead of 8K) which is much easy to create and manage. On the other hand, if a particular mVRF has many (S,G) customer flows and a single S-PMSI is too coarse to tailor the needs of specific VIP customers, the technology also defined aggregation on customer flows so that a few VIP customer flows can enjoy their own S-PMSI. Because of the aggregation for both I-PMSI and S-PMSI, we will have to use a second label to delineate the traffic at the egress PE. This is the focal point of this test.

Objective

This test is to test DUT aggregation capability in order to achieve high scalability. Both control plane and data plane configuration and verification are provided in detail.

Setup

The setup is very similar to previous functional test with two Ixia test port simulating both ingress PE with multicast sources behind, and egress PE with multicast receivers behind. The difference in this case is that we will introduce multiple VPNs to share the same I-PMSI and S-PMSI while introducing aggregation labels to distinguish between different VPNs.

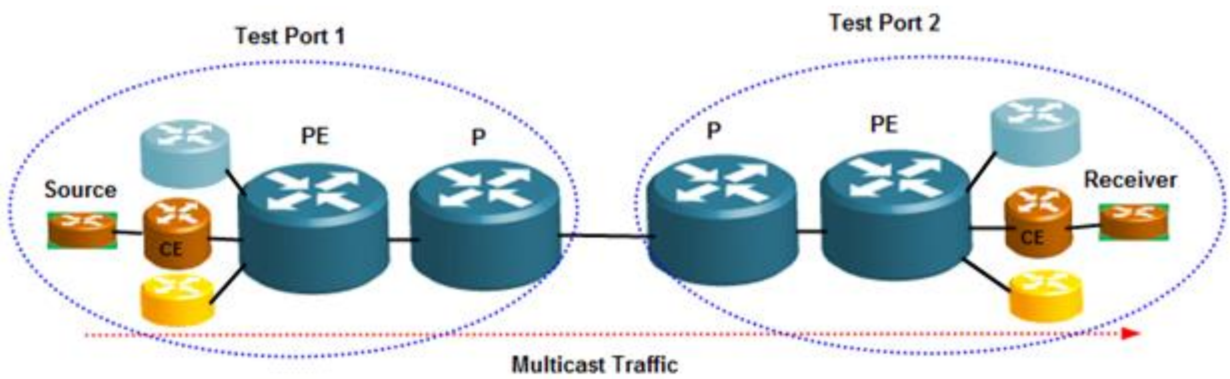


Figure 434. Test Setup for NG mVPN Stress and Scale Test

Step-by-Step Instructions

Note I: If you haven't gone thru previous test which details the functional test, you're encouraged to review that test first. Lots of details in this test will be omitted for simplicity.

Note II: we will focus on the I-PMSI aggregation in the procedures described below. The S-PMSI aggregation can be configured via wizard however; currently there is a bug that keeps it from generating the correct BGP info. The generated contents can still be manually tweaked however in the interest of being short and concise; we will not describe the steps in detail. When due, the wizard parameters for the S-PMSI will be explained in full.

1. Just like in previous test case, launch the NG mVPN protocol wizard and setup the source port and destination port in a separate wizard run. Using a dummy port (offline port) as the CE port as the wizard requires at least one receiver port.

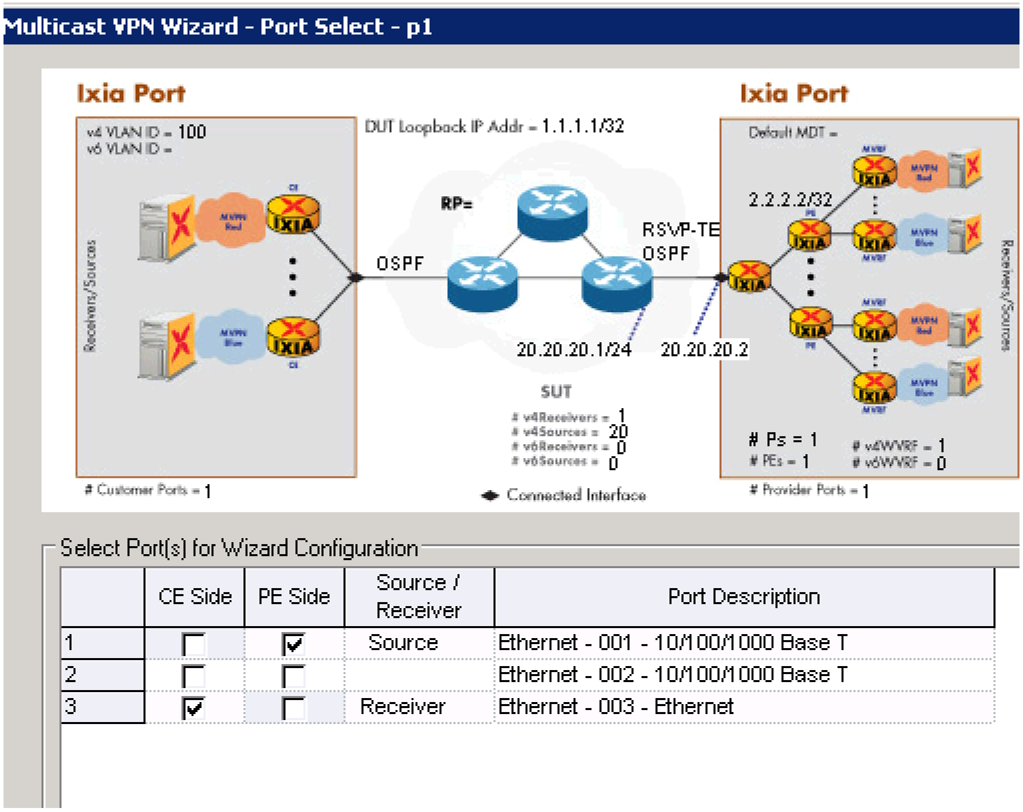


Figure 435. NG mVPN wizard port selection page

2. In the second page of the wizard, select RSVP-TE P2MP as the P-Tunnel protocol. Select the mLDP if needed.

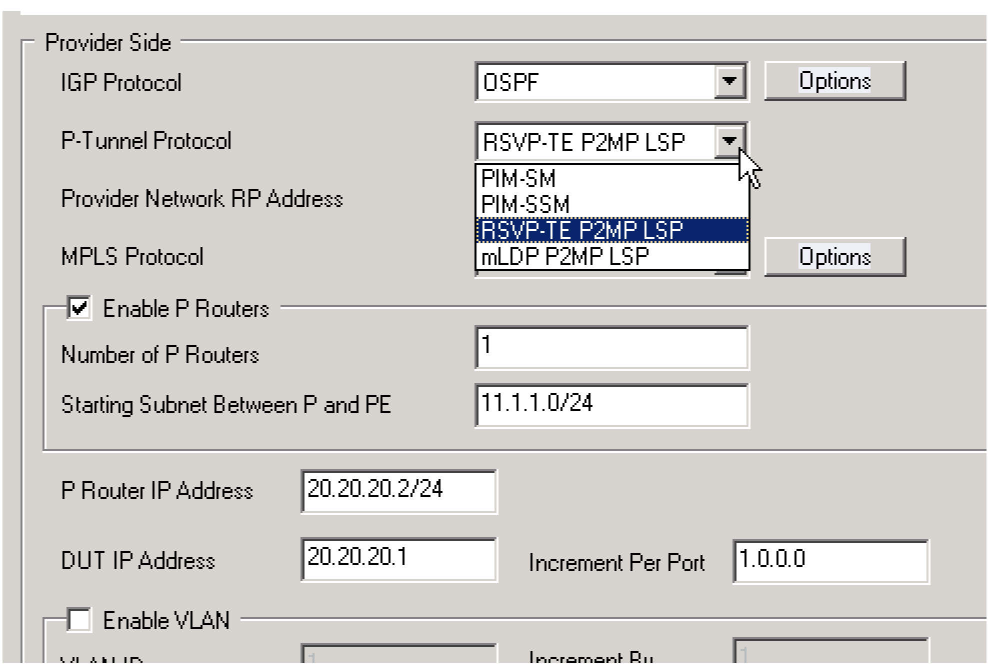


Figure 436. P-Tunnel selection page

3. The next page is about configuring the emulated PE routers. No difference from configuring a regular MPLS VPN network.

4. In the next page of the wizard, we need to understand how I-PMSI aggregation works. Suppose we want to emulate 20 VPNs, and we want to bundle 5 VPNs into a single I-PMSI. Below is how to achieve this. Enter "**Number of VPNs Per PE**" as 20. Check to enable "**Enable Aggregation**". Enter "**Number of VPNs per I-PMSI Tunnel**" as 5. Check to enable "**Use I-PMSI Upstream Label**". Enter a proper "**Upstream Label**" value. The data packet will carry two labels, the outer from RSVP-TE P2MP LSP for I-PMSI, and the inner for the "Upstream Label". The second label is needed because of the aggregation.

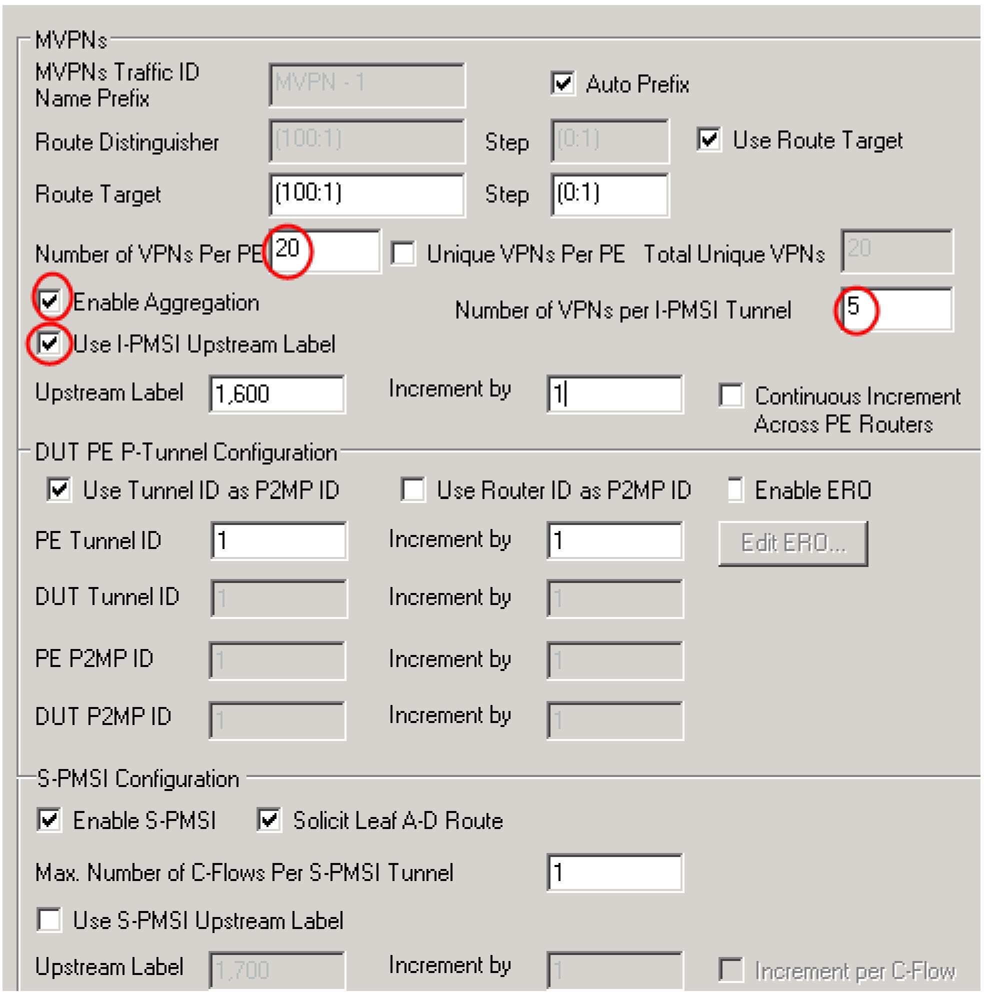


Figure 437. mVRF configuration with I-PMSI aggregation

5. We will not configure the S-PMSI aggregation in this test. However, make sure that you understand what it is used for. Unlike the I-PMSI aggregation where the VPN is the aggregated object, the S-PMSI aggregation applies to the customer flows that constitute the unique (S,G) state in the customer facing interface of a PE router. The next page of the wizard is asking for how many S and G in a given VPN. If you have 10 Sources, and 5 Groups per VPN, when configured in a full-mesh mode, it will yield 10x5=50 customer flows.

By default without S-PMSI aggregation, all 50 C-Flows will ride on the same S-PMSI. If you want more granular control of C-Flows, you can spread them out into multiple S-PMSIs. In this sense, the “aggregation” is more a de-aggregation.

6. The rest of wizard pages are apparent and we won’t repeat the configuration steps here. In a very similar fashion, configure the Receiver port. The only attention needed is the I-PMSI aggregation – make sure you configure identical info as in the Source port configuration: 20 VPNs, Aggregation enabled, 5 VPNs per I-PMSI tunnel.

7. Let’s examine the generated configuration to see if they make sense. First, let’s look at RSVP configuration. A total of 26 tunnels created – 2 for P2P, and 24 for P2MP. Among the 24 tunnels, 4 are for I-PMSI and 20 for S-PMSI. The reason is that we have enabled the aggregation on the I-PMSI with 5 VPNs to share one I-PMSI on a total of 20 VPNs, so only 4 I-PMSI tunnels are needed. On the other hand, we didn’t enable S-PMSI aggregation therefore it will need one S-PMSI tunnel for each of the 20 VPNs hence a total of 20 S-PMSI tunnels are needed.

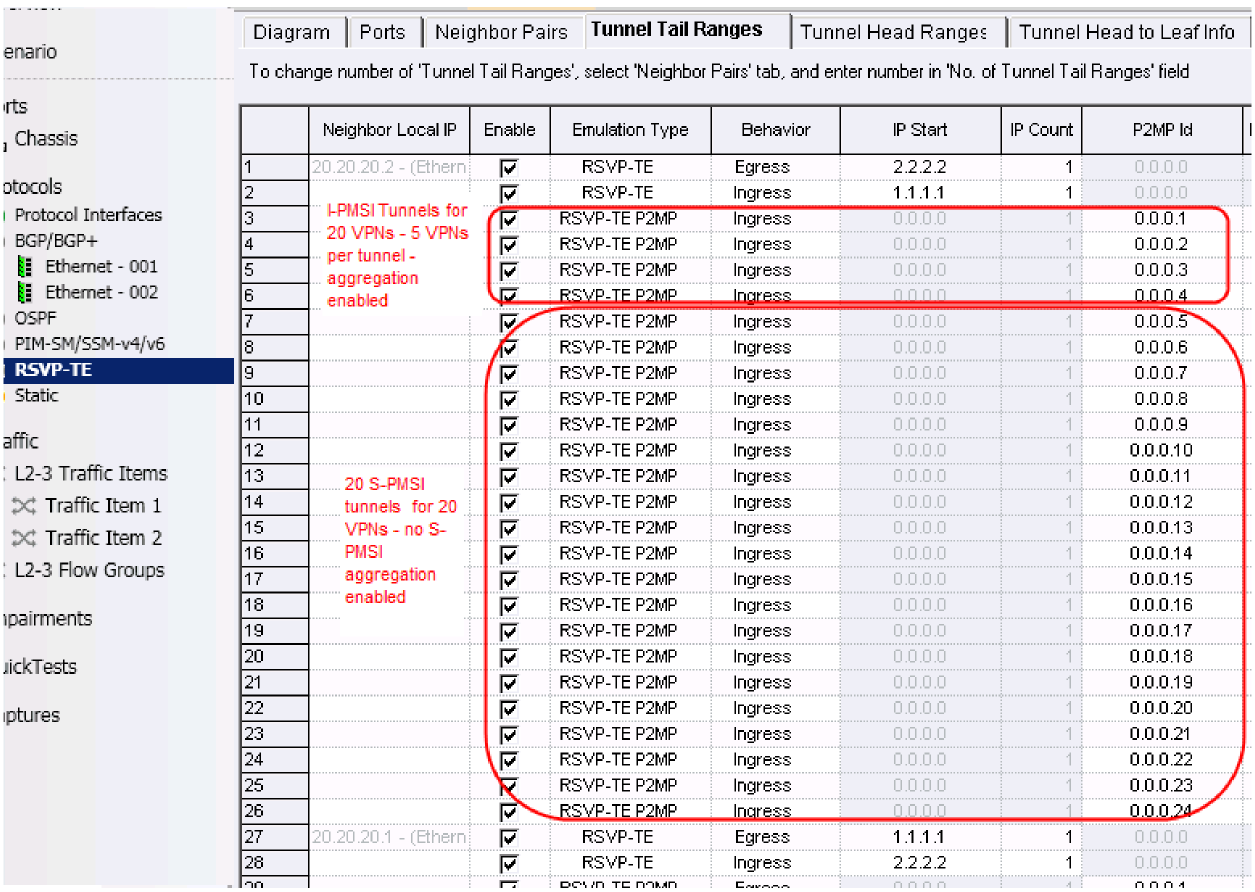


Figure 438. RSVP-TE P2MP config generated by the wizard

8. You can further confirm the I-PMSI configuration by looking at the BGP configuration on the source port. Below clearly shows tunnel 1,2,3,4 are used for I-PMSI.

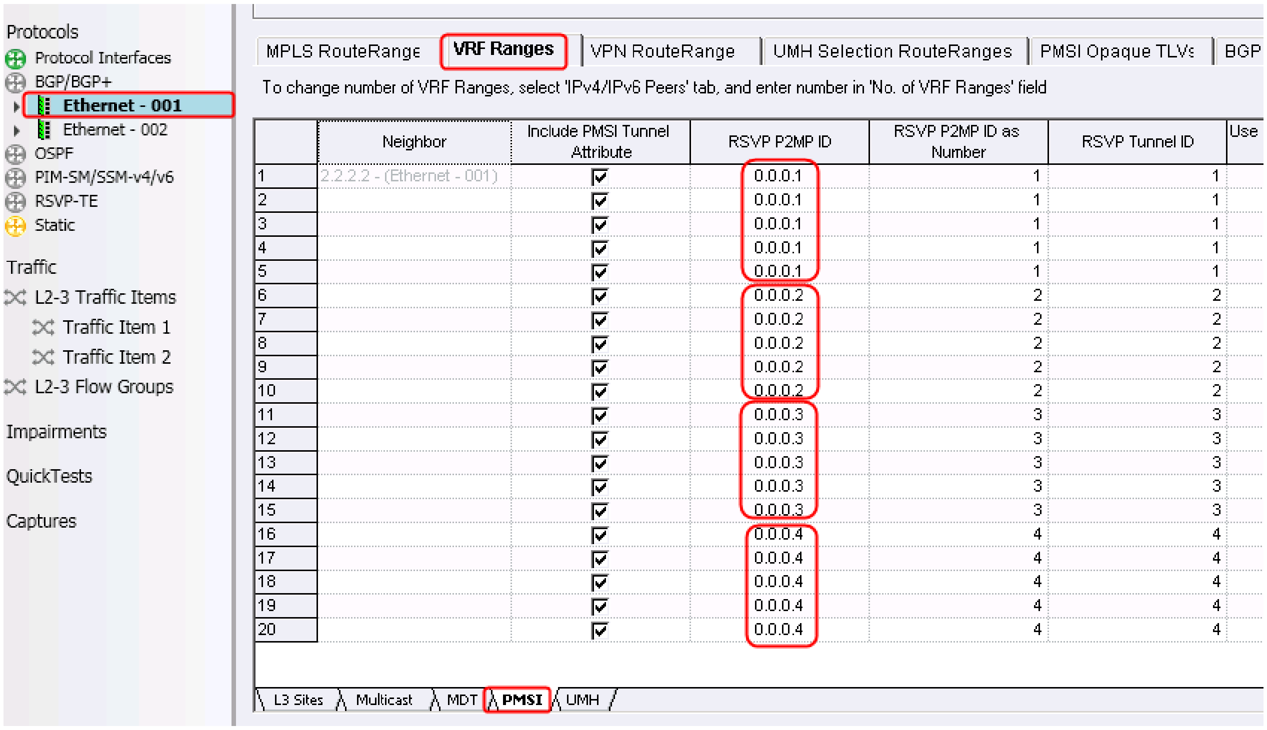


Figure 439. BGP configuration for I-PMSI at the source port, with aggregation enabled

9. The S-PMSI tunnels can be confirmed by looking at the "**Multicast Sender Sites**" tab

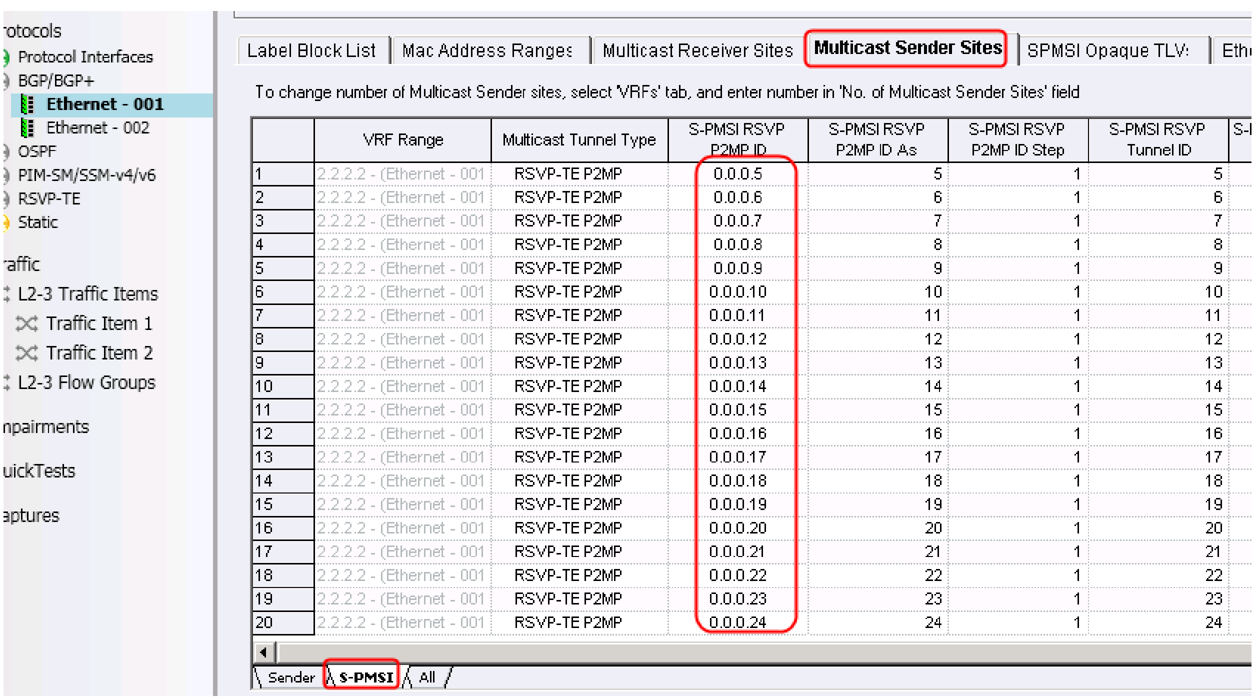


Figure 440. BGP configuration for the S-PMSI at source port, with no aggregation

10. Start the protocols and examine the learned info to confirm they match what are expected. First, the RSVP-TE leaned info on the source port shows a total of 26 tunnels which corresponds to 2 P2P, 4 I-PMSI, and 20 S-PMSI, tunnels respectively.

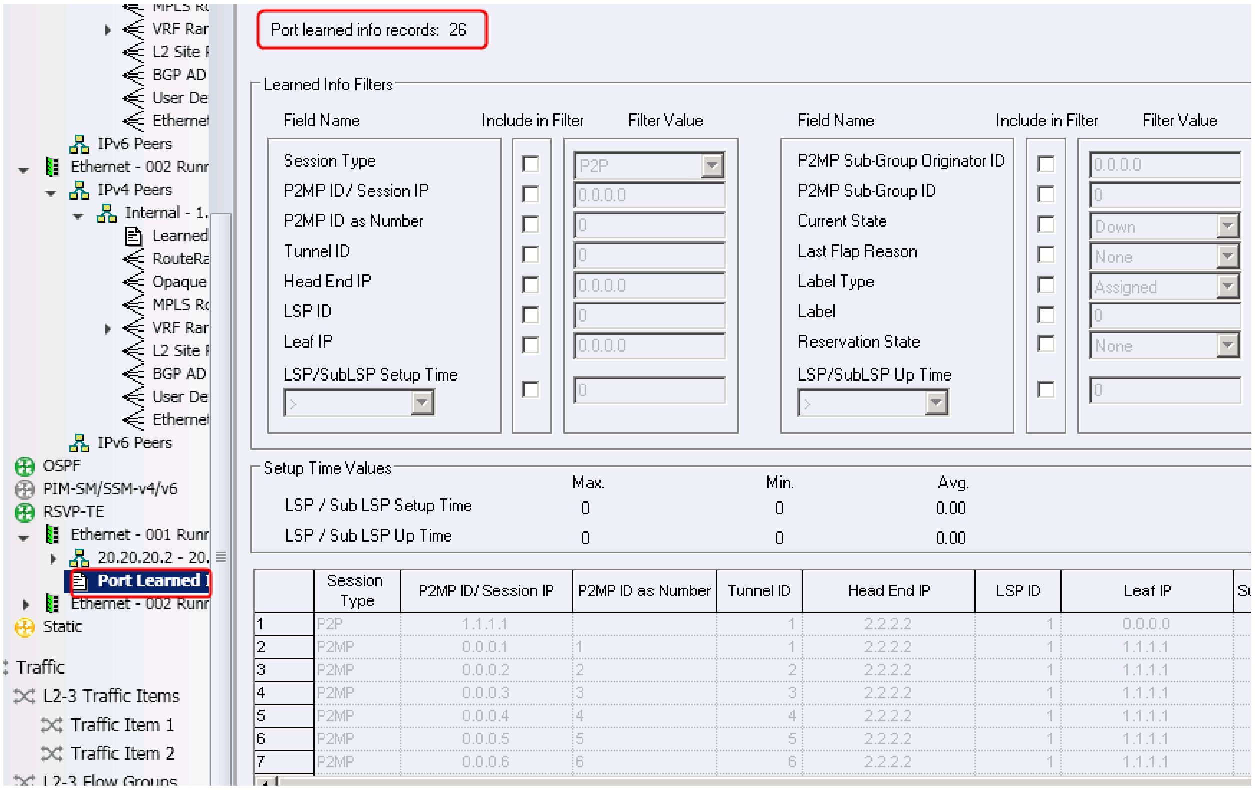


Figure 441. RSVP-TE Learned Info verification

11. Next look at the receiver port BGP learned info. Four distinct P2MP tunnels are repeated five times each for the 5 VPNs to share.

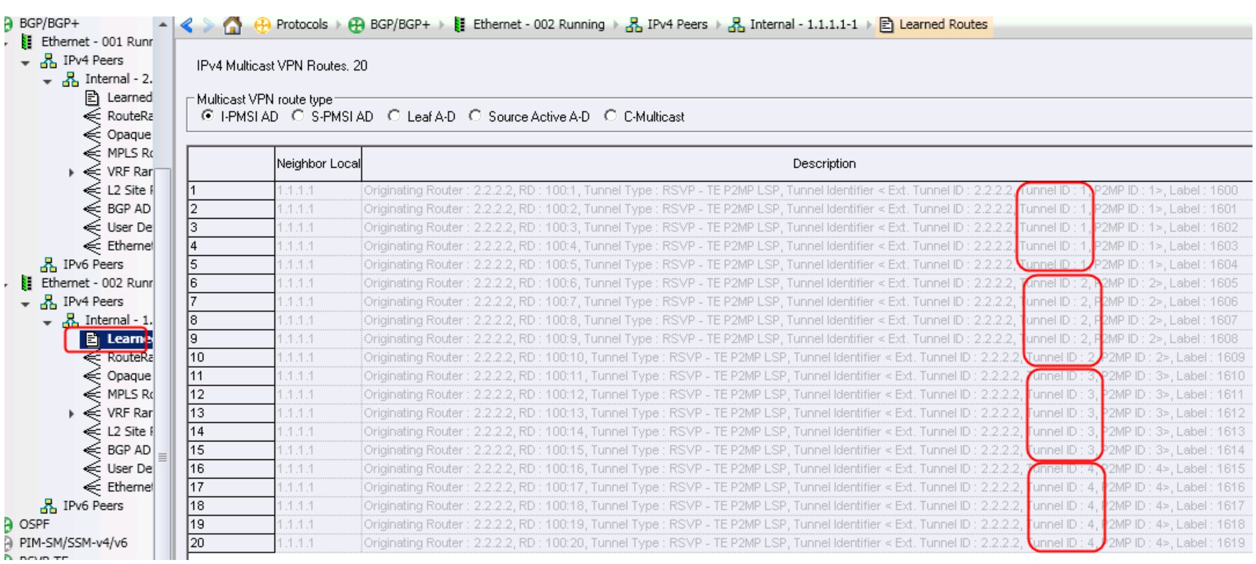


Figure 442. The receiver side BGP learned info verification

12. Now, let's build traffic to see how the labels are encapsulated. Launch the traffic wizard and select the "**BGP Multicast IPMSI Sender Ranges**" as the source, and "**BGP Multicast Receiver Ranges**" as the destination. This is to quickly select all sources and receivers for all 20 VPNs. Use "**One-One**" mapping.

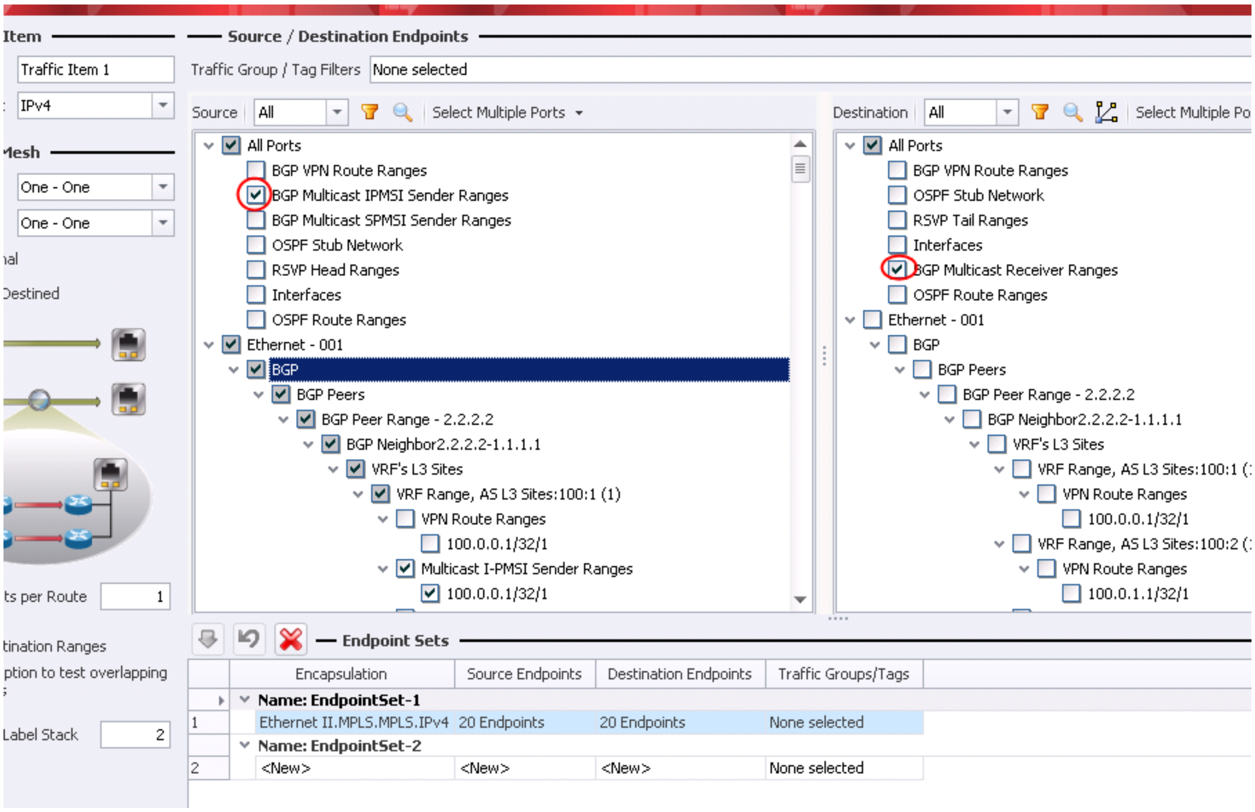


Figure 443. Traffic Source and Destination endpoints selection

13. The rest of traffic wizard is easy to follow. Once finished, you can use the flow group editor to view the generated packets. Examine how the labels are listed. For the RSVP P2MP tunnel, 4 distinct label values each repeated 5 times which means there will be 4 I-PMSI tunnels each will be shared by 5 VPNs. This is exactly what is expected. Pay also attention to the second label which corresponds to our input for the "**Use I-PMSI Upstream Label**" configured in step 4 of this test case.

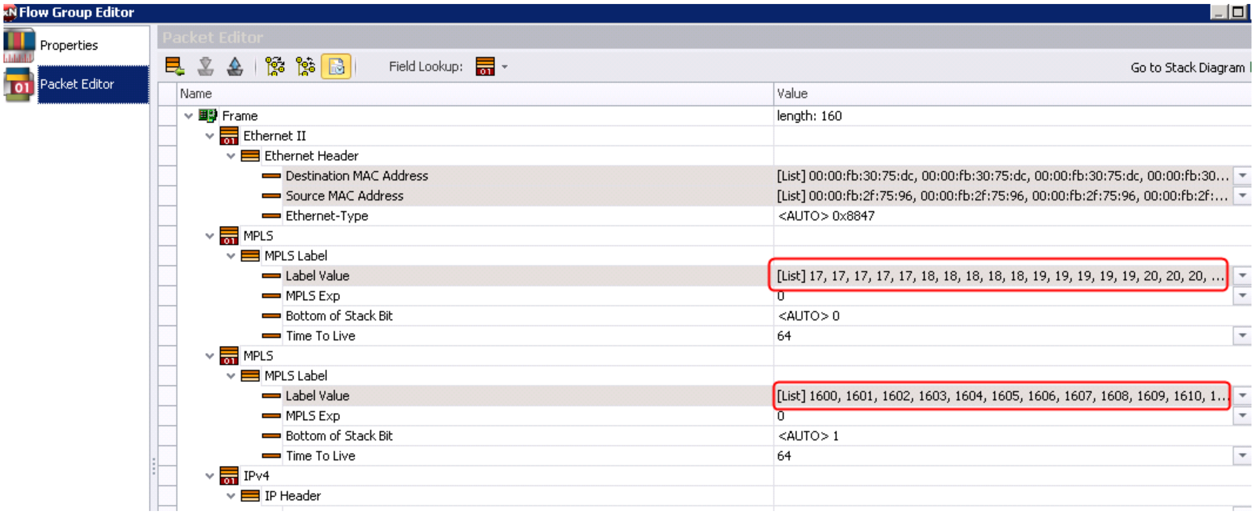


Figure 444. NG mVPN traffic encapsulation vericiation with I-PMSI aggregation enabled

14. Introduce more VPNs or PEs in the test topology to scale the test even further.

Test Variables

Consider the following list of variables to add in the test in order to make the overall test plan better.

Functional/Performance Variable	Description
Change the RSPV-TE P2MP to mLDP and verify all functions detailed in this test	mLDP works very similar to RSVP P2MP. The key difference is the way labels are assigned. With RSVP P2MP, I-PMSI and S-PMSI labels are requested by the Root and assigned by the Leaf nodes; while with mLDP, the labels are automatically assigned by the Leaf nodes. The aggregation mechanisms, as well as the label resolution principle are the same.
Increase the number of P, PE, and the number of VPNs to experience how the aggregation improve the scalability	Aggregation is a great way to scale the test to huge number of P, PE, and VPNs. The DUT typically has some system limit and it’s essential to test those limit
Increase the number of sources, and the number of multicast groups per VPN to test DUT’s system limit	The number of (S,G) or (*,G) that can be supported by DUT per VPN is another key measure that usually the system under test will have a limit for. It’s essential to test not only the control plane scalability and stability, but also the data plane traffic forwarding, and with possible I-PMSI to S-PMSI switchover for key multicast applications.
Testing NG mVPN simultaneously with unicast L3VPN, and 6VPE	This is the ultimate goal to prove DUT (as PE) can handle MPLS VPN traffic for both unicast, and multicast, with scalability.

Introduction to EVPN and PBB-EVPN

L2VPN based PW and VPLS transport is an important MPLS technology that has found applications in access, mobile backhaul, core transport, and new areas such as Carrier Ethernet and Data Center Interconnect (DCI).

Widespread adoption of L2VPN and VPLS has caused new set of issues such as multi-homing, which requires load balancing on all active links under normal condition and yet provides failover protection when failures occur in the network. Existing active/standby resiliency model is good for redundancy and service protection, but not suitable for load sharing, because standby links cannot carry traffic under normal condition. Furthermore, Data Center Interconnect and Virtualization are fuelling the increase of MAC addresses. There is a strong need to contain frame forwarding for Broadcast, Unknown, and Multicast (BUM) traffic to avoid flooding at all cost. The architecture also requires network re-convergence upon failure to be independent of the number of MAC addresses learned and stored in the forwarding table

EVPN and PBB-EVPN are next generation L2VPN solutions based on a BGP control-plane for MAC distribution and learning over the core MPLS network. EVPN and PBB-EVPN were designed to address the following requirements:

- All-active redundancy and load balancing
- Simplified Provisioning and operation
- Optimal Forwarding
- Fast convergence

In addition, PBB-EVPN and its inherent MAC-in-MAC hierarchy provides:

- Scale to millions of C-MAC (Virtual Machine) addressed
- MAC summarization co-existence with C-MAC (VM) mobility

MP-BGP has been successfully used in the NG mVPN to bridge C-Multicast domains through the core without the need for PIM. It advertises many Auto-Discovery (AD) routes and P-Tunnel types such as RSVP-TE P2MP, mLDP, Ingress Replication for traffic encapsulation. Based on the same concept of AD routes and P-Tunnel delivery mechanism, a new set of AFI/SAFI is defined for EVPN and PBB-EVPN, new BGP NLRI types, as well as new extended communities are defined, as summarized below:

New NLRI Types for EVPN and PBB-EVPN:

- 0x1 – Ethernet Auto-Discovery Route
- 0x2 – Mac Advertisement Route
- 0x3 – Inclusive Multicast Route
- 0x4 – Ethernet Segment Route

New Extended Communities

- ESI MPLS Label
- ES-Import
- MAC Mobility
- Default Gateway

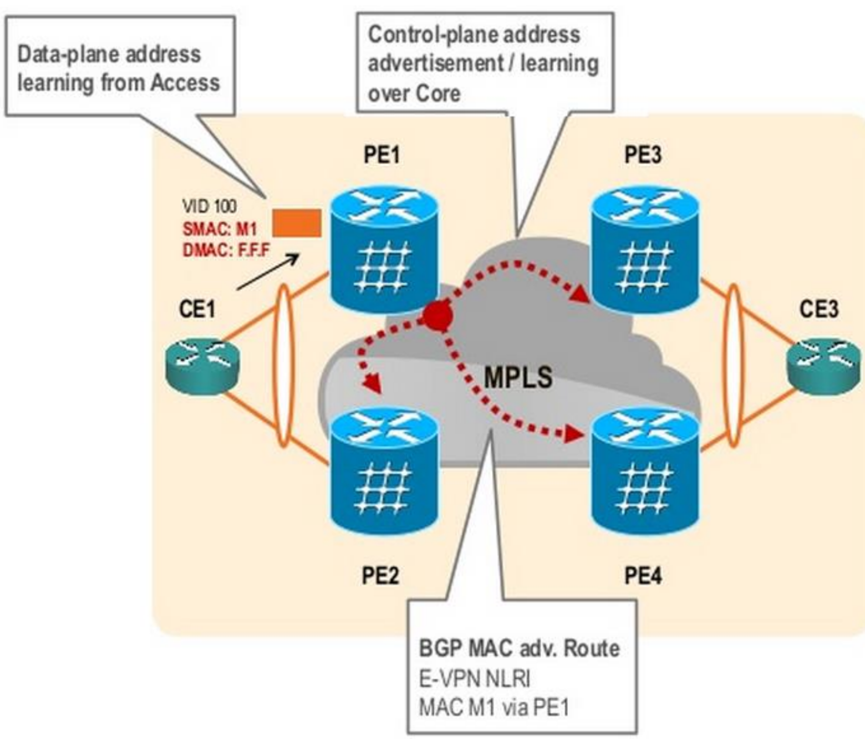


Figure 445. How EVPN works in a high level

The above diagram displays a high level view of how EPVN works. PE routers learn the MAC from CE based on data plane forwarding, then advertise the MAC in the core through MP-BGP new NLRI types (MAC Advertisement Routes), so the rest of PEs are aware of the new MACs. Unlike the traditional L2VPN PW emulation, P2P PWs across the core are no longer needed. Instead, known unicast traffic (Dest MAC is advertised by peer PE) is encapsulated over the usual two labels stack – the bottom being the transport tunnel (LDP or RSVP-TE), and the top is the label associated with the MAC advertisement route by the remote PE. The unknown unicast is part of the BUM (broadcast, unknown, multicast) traffic and it follows:

- Through a pre-negotiated label path through Ingress Replication or
- P2MP tunnels negotiated through mLDP or RSVP-TEP2MP.

There are many procedures, such as load balancing, Split Horizon, Designated Forwarder election, fast convergence that are introduced due to challenges of multi-homing. Forturnately, Ixia's IxNetwork offers feature rich EVPN and PBB-EVPN emulation. Coupled with some of the industry unique Hardware features, IxNetwork truly represents the best tool to test nextGen protocols.

Relevant Standards

- draft-ietf-l2vpn-evpn-req-02
- draft-ietf-l2vpn-evpn-03
- draft-ietf-l2vpn-pbb-evpn-04

Test Case: EVPN and PBB-EVPN Single Home Test Scenario

Overview

Single home test scenario is the simplest form of EVPN and PBB-EVPN. Two Ixia test ports are required to verify the basic functions of both EVPN and PBB-EVPN. One test port is emulating CE routers connecting to DUT as PE, and the other test port emulating PE routers as well as CE routers behind the emulated PE routers. In both cases, the CE routers are connected only to one PE router hence the term ‘single home’. DUT and Ixia emulated PE will exchange MAC Advertisement Routes, Inclusive Multicast Routes, and Ethernet Segment Routes. DUT is responsible for traffic encapsulation from Ixia CE to PE direction, while Ixia emulated PE is responsible for encapsulating two label stack traffic sent by the simulated CE to DUT for decapsulation and forwarding.

Objective

The test is to perform basic functional verfication for single homed EVPN and PBB-EVPN. The example config will emulate a single Ethernet Segment with 3 EVIs but can be easily expanded to test many Ethernet Segments each with many EVIs. Different types of NLRI are exchanged between DUT and Ixia emulated PE routers and can be verified via the Learned Info. Traffic will be created for both Known Unicast, as well as the Broadcast, Unknow, and Multicast (BUM). Two labels stack should be verified to ensure DUT and tester are both encapsulating the traffic with correct labels.

Setup

Two Ixia test ports are required for the test as depicted below. One test port emulates CE and one test port emulates both PE and CE. Both CE routers are single homed to their respective PE routers.

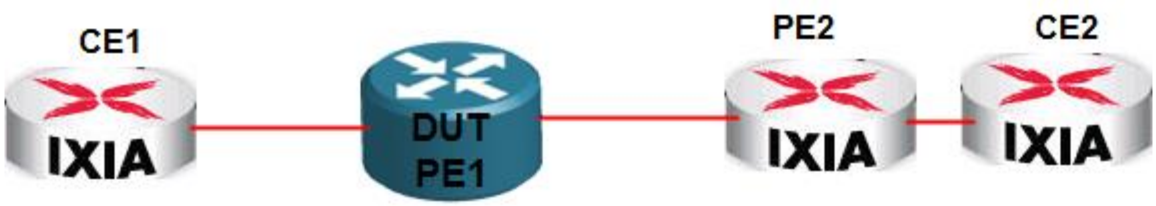


Figure 446. Test Setup for Single Home Test Scenario

Step-by-Step Instructions

Note: Currently there is no EVPN or PBB-EVPN wizard to help user configure basic test scenarios. If you are familiar with IxNetwork and comfortable in manually configuring BGP, LDP, and OSPF/ISIS, then you can complete most test steps without the help of a wizard. If not, you can use existing L3VPN wizard to configure the BGP and LDP part automatically for you. Then you will need to manually modify the wizard generated config to suite EVPN and PBB-EVPN test needs. Starting with a L3VPN wizard also gives you extra benefit of configuring ISIS/OSPF and LDP/RSVP-TE automatically. IGP (ISIS or OSPF) is needed if BGP is actually a multi-hop session. LDP/RSVP-TE is needed to provide transport tunnels between the emulated PEs and DUT. It is strongly recommended to always start with L3VPN in order to reduce configuration mistakes.

Below steps will start with EVPN as a comprehensive example. For PBB-EVPN configuration, refer to steps towards the end of this paragraph which are marked as “Steps to Configure PBB-EVPN and Verify Results”.

30. Launch the IxNetwork L3VPN/6VPE Wizard and navigate throughout it. Test Case “Layer 3 MPLS VPN Scalability and Performance Test” in previous sections provides details on how to use the wizard. If you’re not familiar with L3VPN configuration, you should go over that test first.

31. At the time of the writing, all EVPN/PBB-EVPN specifications are still in draft format. In order to support m ulti-vendors, Ixia has opened up all EVPN parameters for user to customize. The default is filled up with convention values based on public interop test. Below is a diagram showing all the open parameters one can customize, including the most important ones such as **AFI/SAFI** value. Note that the **EVPN IP Address Length Unit** (Byte vs. Bit) is also important one for interoperability.

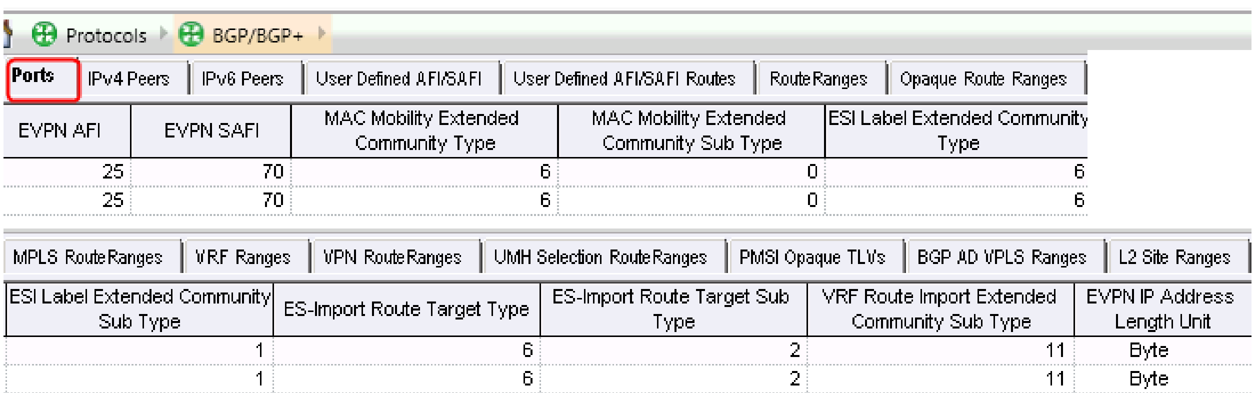


Figure 447. EVPN/PBB-EVPN Open Parameters

32. Once the port level open parameters are set, you need to change the IPv4 peer to include the EVPN and PBB-EVPN capability. First, change **No. of VRF Ranges** to zero to disable any L3VPN VRF generated by the wizard. Then configure value 1 for **No. of Ethernet Segments**. To simulate more Ethernet segments, simply enter the right value. You will need to check to enable **Filter EVPN** and **EVPN** under **Learned Routes Filters** and **Capabilities** bottom tab respectively.

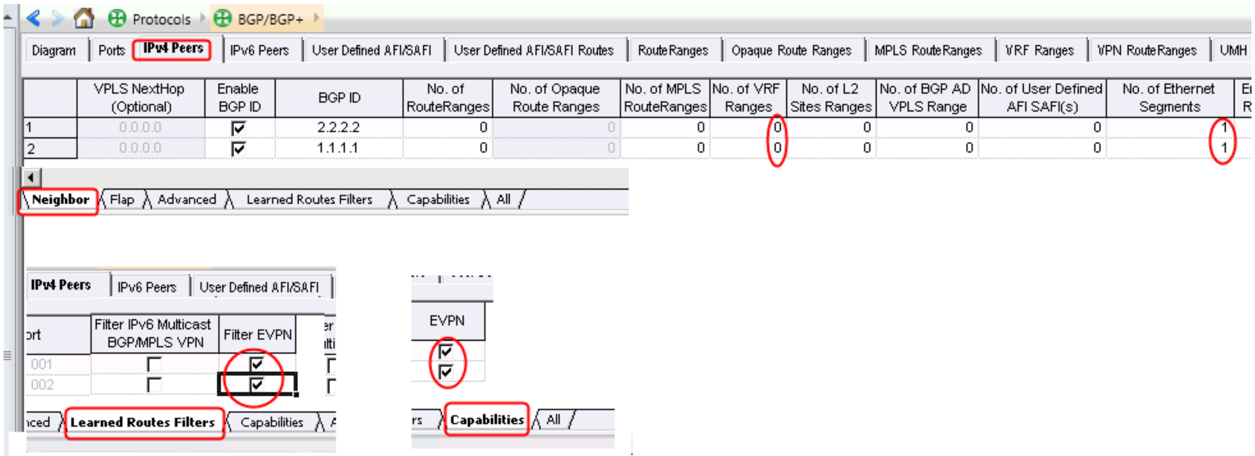


Figure 448. IPv4 Peer Changes for EVPN/PBB-EVPN

33. You can click one at a time, or deep press for continuous clicks, the right arrow in the corner to quickly locate the EVPN/PBB-EVPN related top tabs which are at the very end of BGP tabs

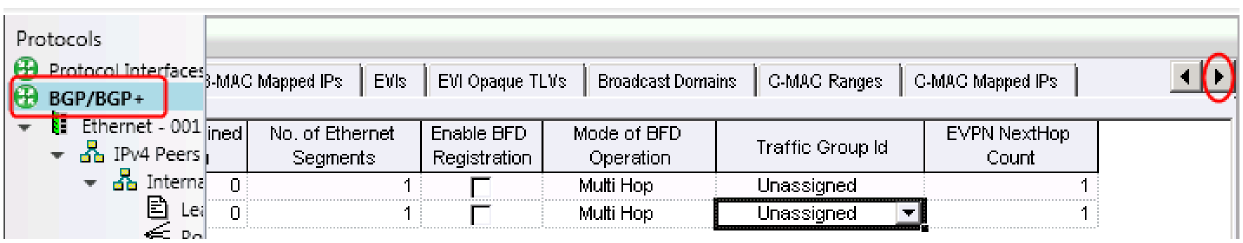


Figure 449. Locate EVPN/PBB-EVPN Related Tabs

34. Start with **Ethernet Segment** tab. Choose **EVPN** as **Type of Ethernet**. Set ESI value all zero to indicate this is a Single Home test scenario. Enter 3 as the **Number of EVIs**. Change it to a proper number if more than 3 EVIs per Ethernet Segment is needed. ESI label is not needed for single home test and leave it as default.

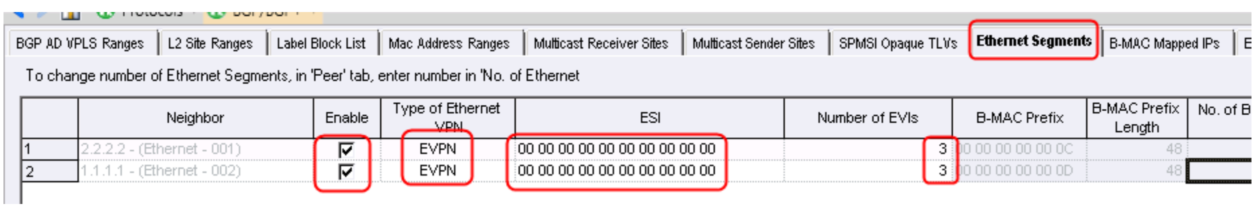


Figure 450. Ethernet Segment tab Configuration

35. Configure the EVIs. Make sure to enter a proper Route Target value. By default, the emulation will automatically set the RD value in IP format, and auto pick up the EVI value for the RD. The Target and Import Target do NOT need to be the same as RD, as shown below. It's critical, though, that Ixia's configured Target and Import Target need to match those of DUT. Below screen shot also shows how to enter a specific value for the Target and then use global "Copy Target to Import Target" to make them the same.

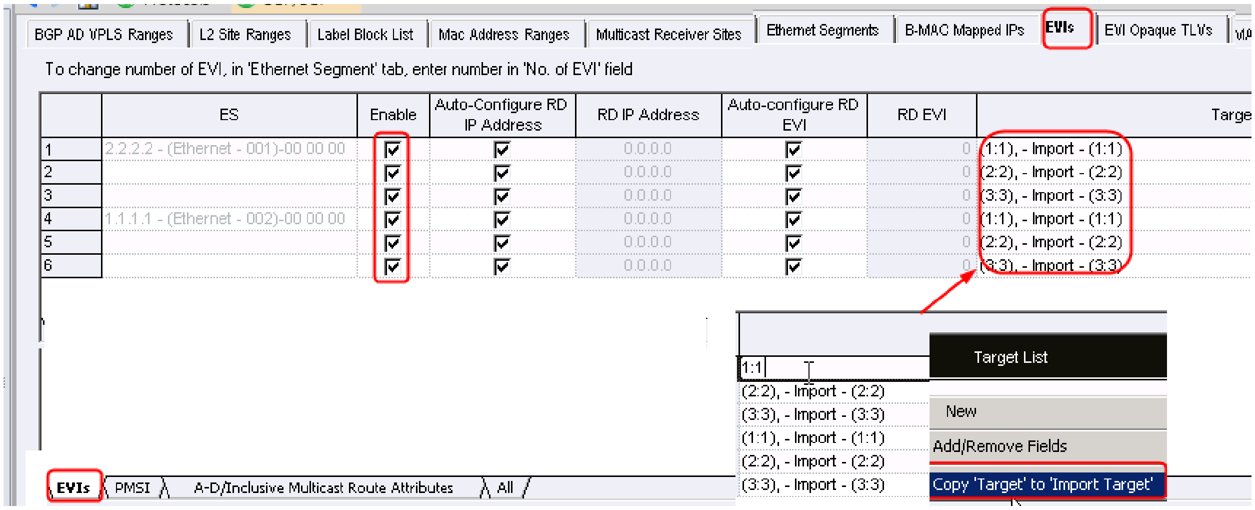


Figure 451. Configure Target and Import Target values

36. Configure the PMSI for the Broadcast, Unknown, and Multicast (BUM) traffic. Make sure to check and enable the "**Include PMSI Tunnel Attribute**" and select "**Ingress Replication**" as tunnel type. Modify the label as appropriate.

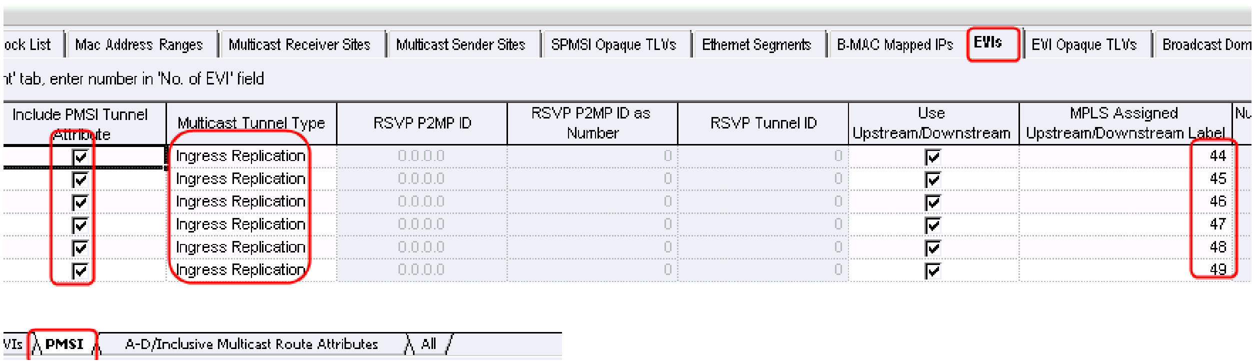
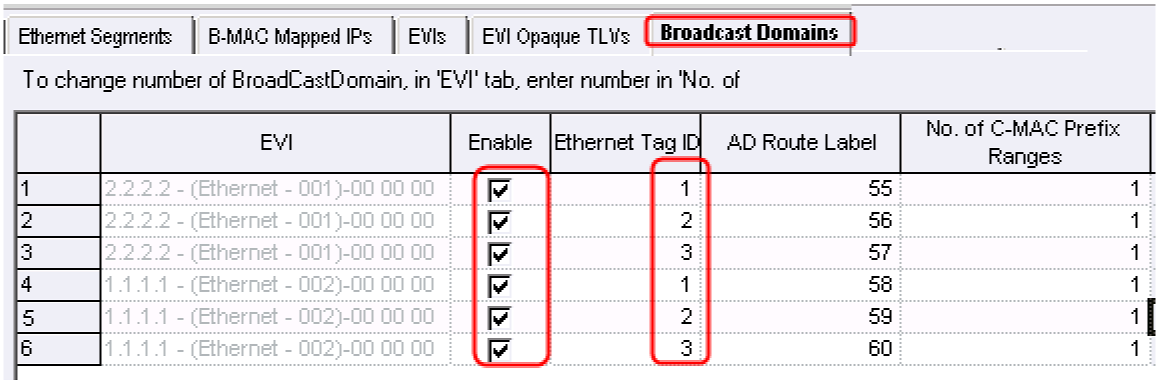


Figure 452. Configure PMSI

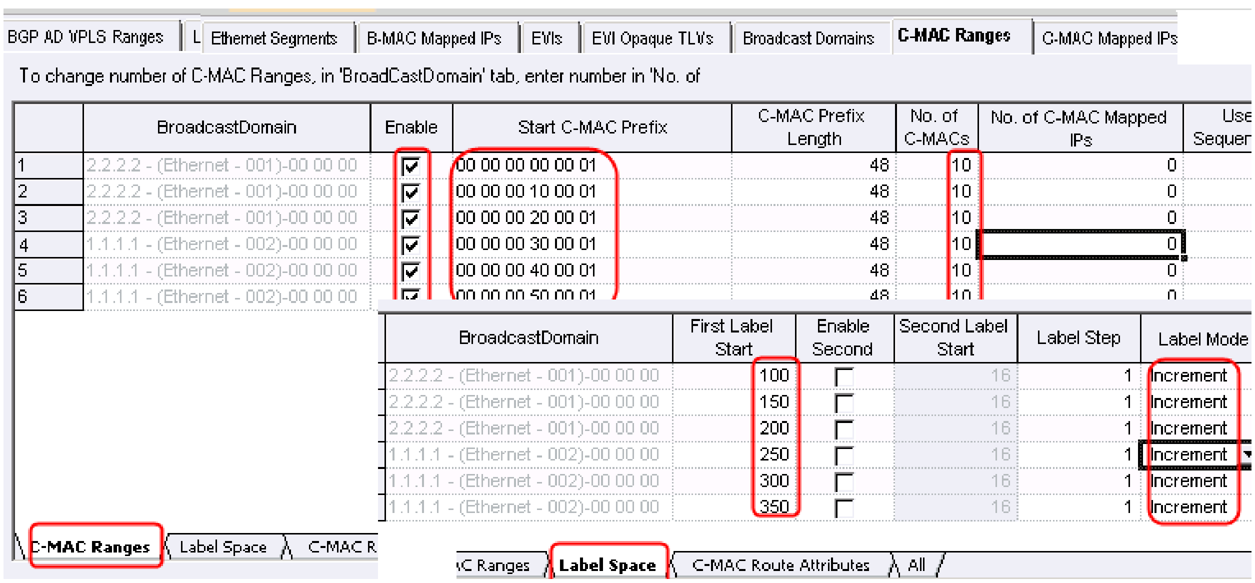
37. Configure the Broadcast domain to indicate the right **Ethernet Tag ID,** and the number of C-MAC ranges.



	EVI	Enable	Ethernet Tag ID	AD Route Label	No. of C-MAC Prefix Ranges
1	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	1	55	1
2	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	2	56	1
3	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	3	57	1
4	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	1	58	1
5	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	2	59	1
6	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	3	60	1

Figure 453. Configure the Broadcast Domain

38. Configure the C-MAC ranges with proper address, and total counts. Also configure the label values used for the MAC. These labels will be used for sending traffic to these MAC addresses.



	BroadcastDomain	Enable	Start C-MAC Prefix	C-MAC Prefix Length	No. of C-MACs	No. of C-MAC Mapped IPs	Use Sequer
1	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	00 00 00 00 00 01	48	10	0	
2	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	00 00 00 10 00 01	48	10	0	
3	2.2.2.2 - (Ethernet - 001)-00 00 00	☑	00 00 00 20 00 01	48	10	0	
4	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	00 00 00 30 00 01	48	10	0	
5	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	00 00 00 40 00 01	48	10	0	
6	1.1.1.1 - (Ethernet - 002)-00 00 00	☑	00 00 00 50 00 01	48	10	0	

BroadcastDomain	First Label Start	Enable Second	Second Label Start	Label Step	Label Mode
2.2.2.2 - (Ethernet - 001)-00 00 00	100	☐	16	1	Increment
2.2.2.2 - (Ethernet - 001)-00 00 00	150	☐	16	1	Increment
2.2.2.2 - (Ethernet - 001)-00 00 00	200	☐	16	1	Increment
1.1.1.1 - (Ethernet - 002)-00 00 00	250	☐	16	1	Increment
1.1.1.1 - (Ethernet - 002)-00 00 00	300	☐	16	1	Increment
1.1.1.1 - (Ethernet - 002)-00 00 00	350	☐	16	1	Increment

Figure 454. Configure C-MAC Ranges and Labels

39. Make other parameter adjustments as needed. You need to run the control plane and verify the learned info. Either start to run all protocols at once, or run them one by one (OSPF, LDP, and BGP). Make sure OSPF, LDP and BGP are all up. Otherwise, fix the configuration error before proceeding to the verification phase.

40. Go to BGP **Learned Routes** and select the correct route types and then click **Refresh** button in the ribbon area. **EVPN MAC** shows the all the MAC addresses and their associated labels from the DUT. **EVPN Multicast** shows the learned PMSI tunnel type, and labels. Expand the **Tunnel Identifier** column to see the labels at the end of the string. These labels will be used for building BUM traffic. **EVPN Ethernet Segment** shows the learned Ethernet Segment routes. **EVPN Ethernet AD** shows all learned segment or individual EVI auto-discovery routes with the ESI labels. These labels are also known as the Split-Horizon label in multi-home test scenarios

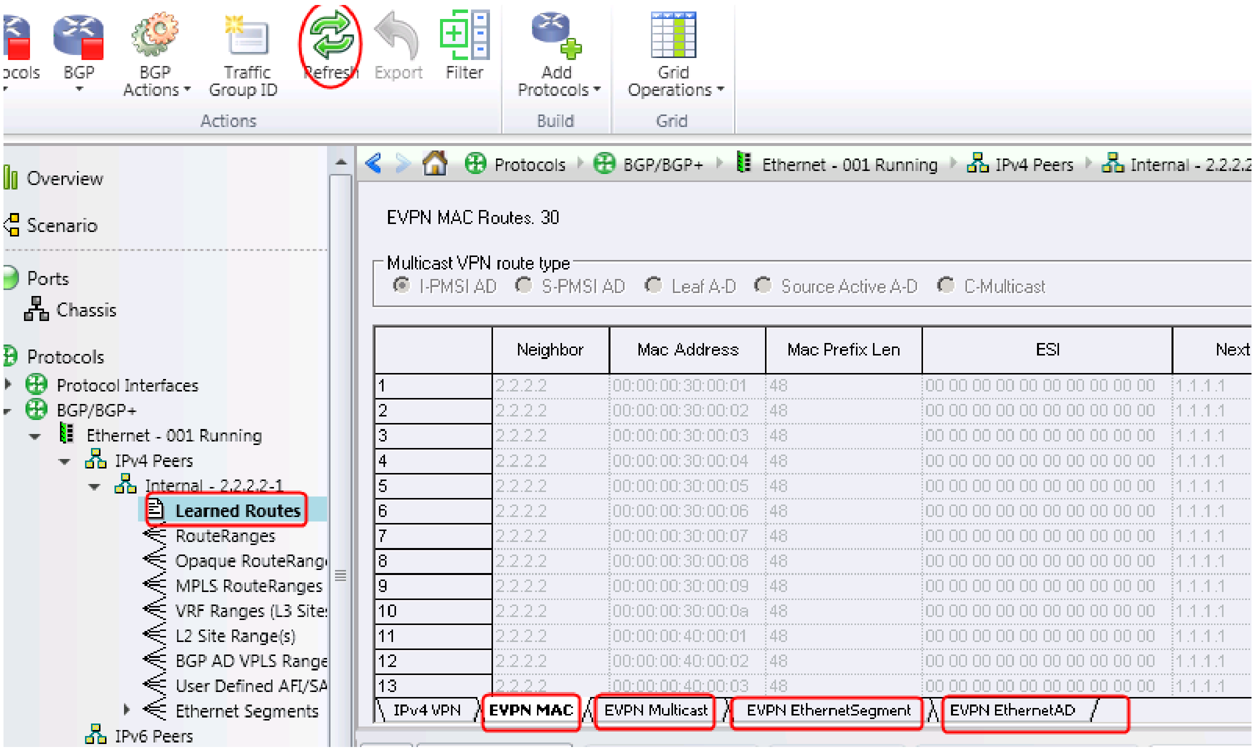


Figure 455. Configure Target and Import Target values

41. Once the control plane is up and running with no issues, it's time to build traffic. Start with the known MAC which is advertised by BGP. Select the **Type of Traffic**, **Traffic Mesh**, and the end points per below screen capture.

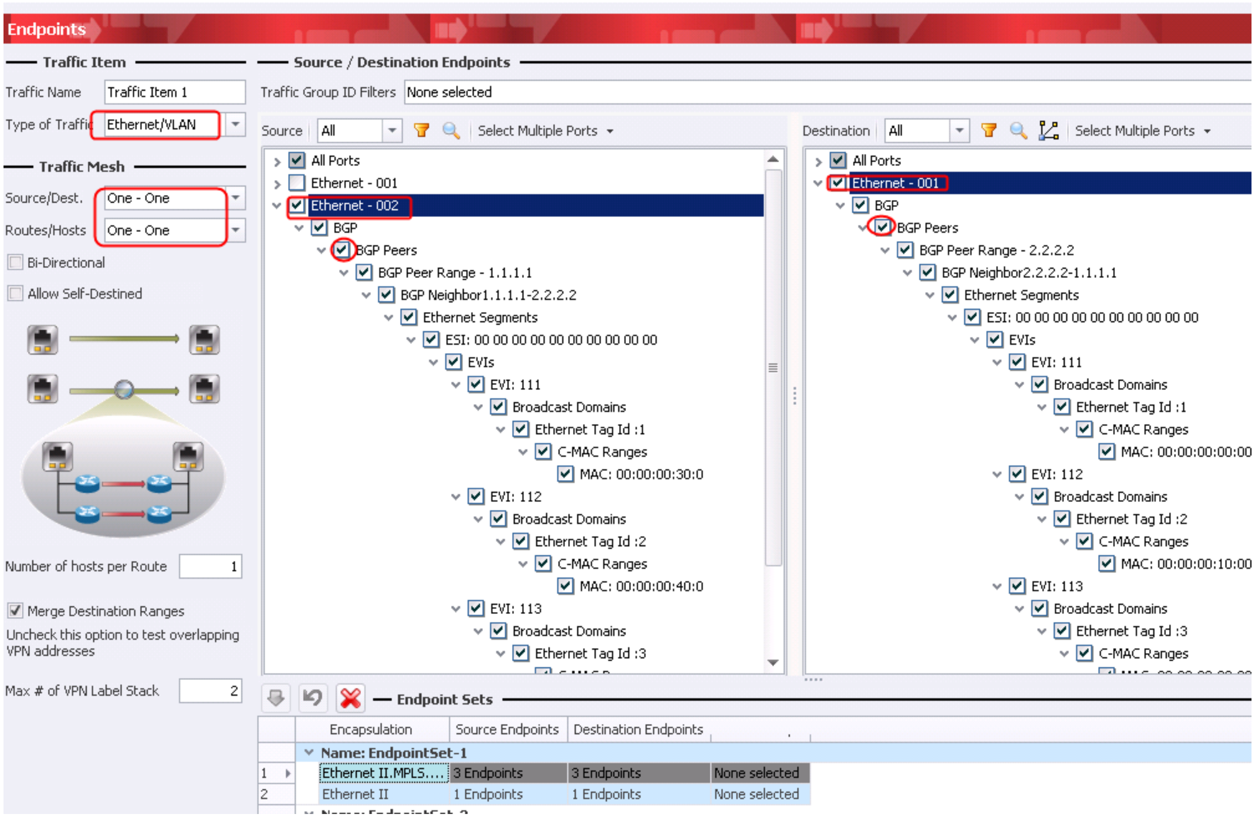
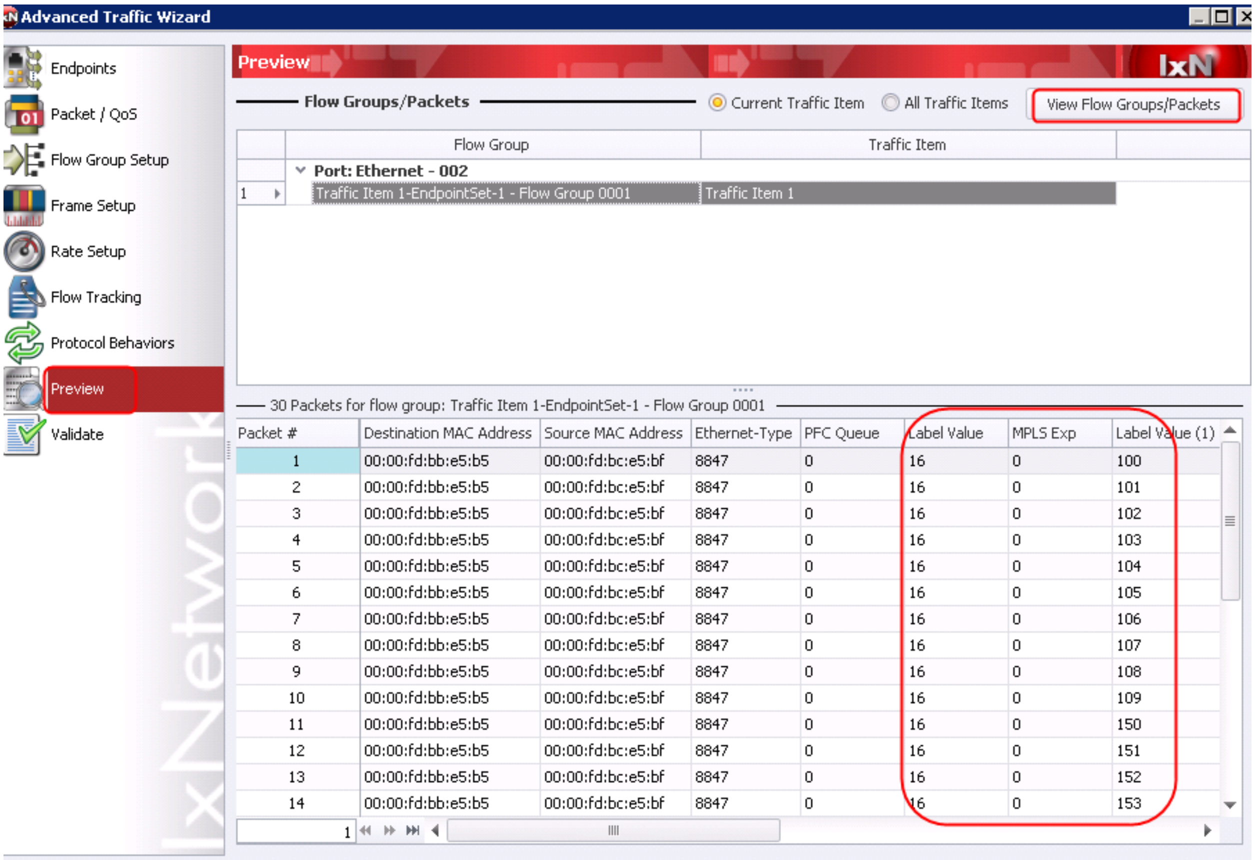


Figure 456. Build Traffic to Known MACs

42. You can verify the traffic via **Preview**. Make sure the inner MPLS labels are corresponding to the **EVPN MAC** tab under the BGP **Learned Routes,** and the outer MPLS label matches the LDP **Port Learned Info** (next-hop for the Mac Advertisement Routes).



Packet #	Destination MAC Address	Source MAC Address	Ethernet-Type	PFC Queue	Label Value	MPLS Exp	Label Value (1)
1	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	100
2	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	101
3	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	102
4	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	103
5	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	104
6	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	105
7	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	106
8	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	107
9	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	108
10	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	109
11	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	150
12	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	151
13	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	152
14	00:00:fd:bb:e5:b5	00:00:fd:bc:e5:bf	8847	0	16	0	153

Figure 457. Verify Traffic for Known MAC through Preview

43. Now proceed to build traffic for BUM. The easiest way to create BUM traffic is to define a few static MAC under the **Static** folder. As the name indicates, these static MAC addresses are static and won't be advertised by BGP Mac Advertisement Routes. Traffic destined to these MAC will be treated as BUM. Another way to build and send BUM traffic is to define some C-MAC ranges behind the EVIs, but do not enable them, so that they are not learned by pee PE routers.

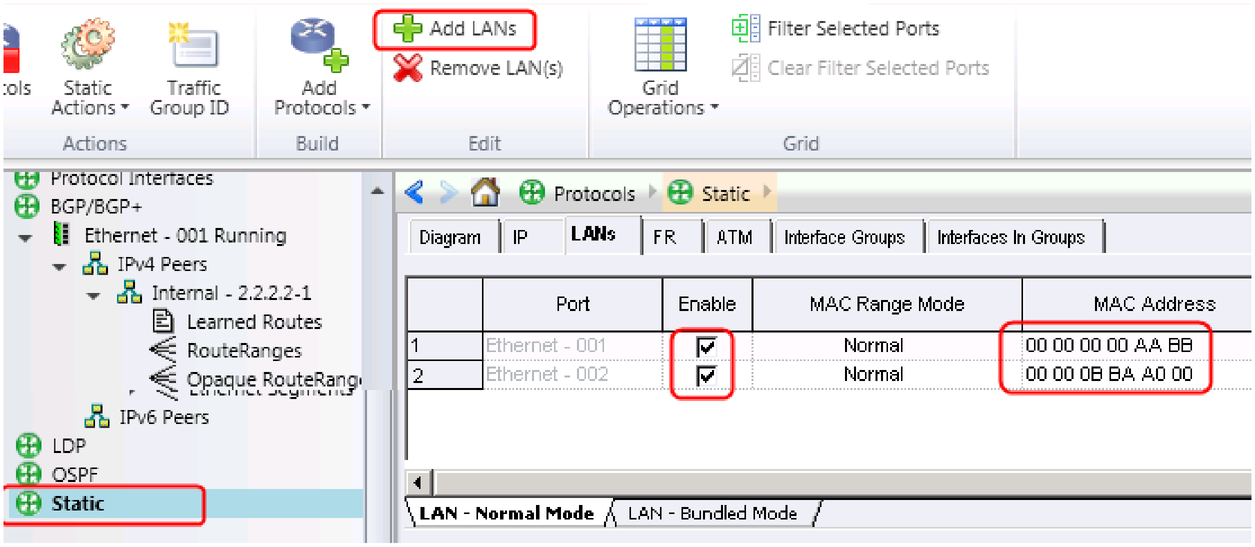


Figure 458. Create Static MAC for BUM Traffic

44. Create a new traffic item for BUM. Make sure to select Static MAC as **Destination**

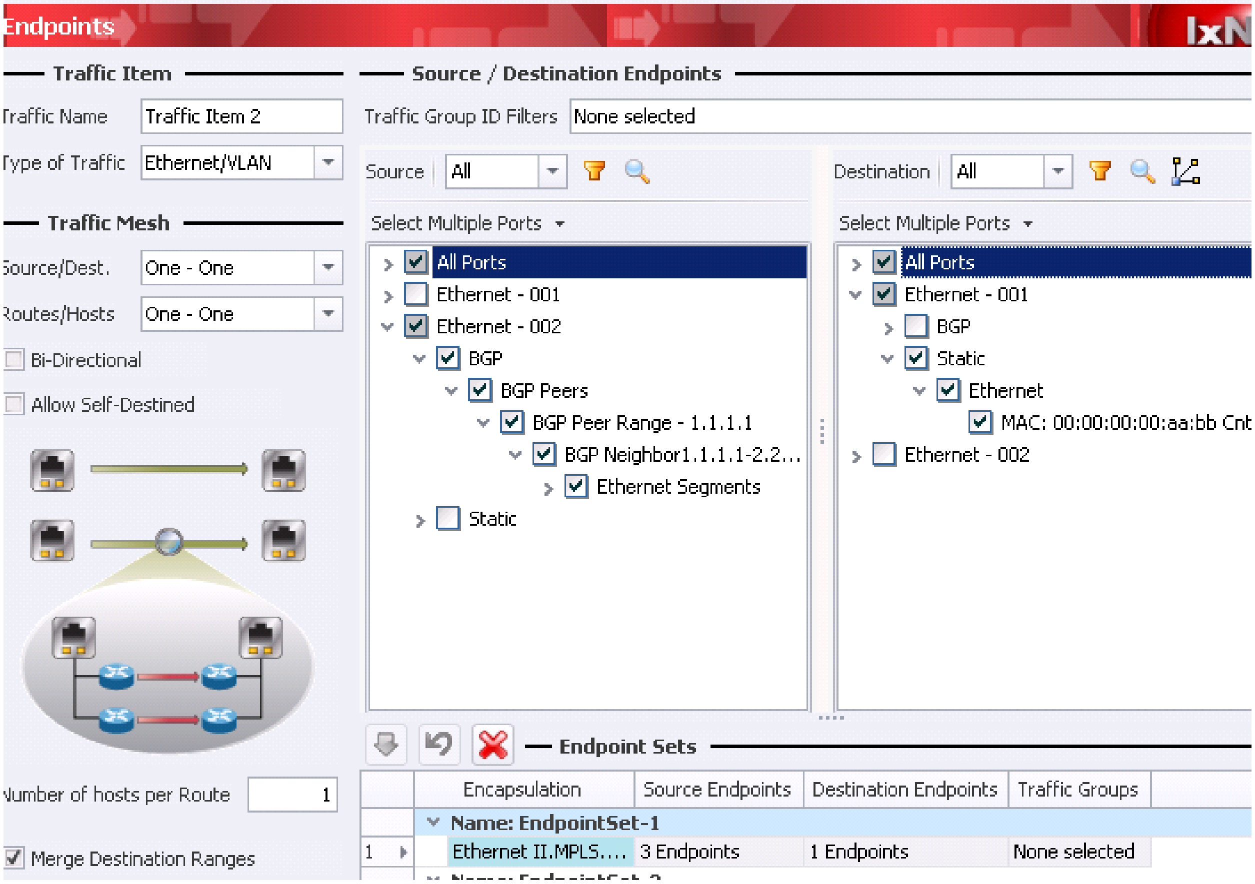


Figure 459. New Traffic Item for BUM – Static MAC as Destination

Preview page should show the correct MPLS labels. The bottom label comes from LDP, and the top label comes from **EVPN Multicast** tab learned info which is known as **Inclusive Multicast Route** in the EVPN sense.

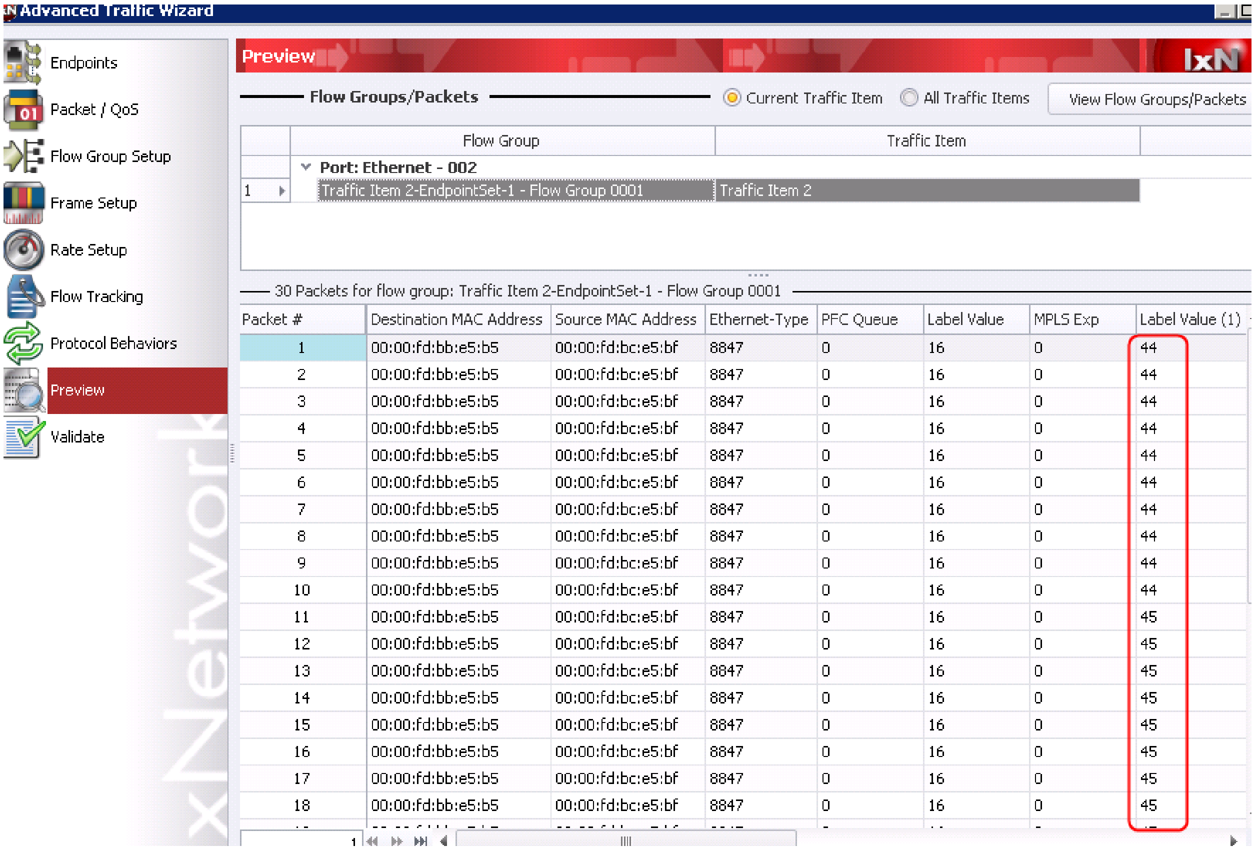


Figure 460. Verify Correct MPLS Labels for BUM Traffic

Note: you can refer to Appendix C: "EVPN/PBB-EVPN Label Stack and Label Resolution Procedures" for more details on how labels are constructed for all valid EVPN/PBB-EVPN use cases including various P-Tunnel methods

Steps to Configure PBB-EVPN and Verify Results

Make sure you review above steps to configure EVPN first. Below steps will detail the difference in configuration steps and result likely seen when testing PBB-EVPN.

1. Select **PBB_EVPN** as the **Type of Ethernet VPN**. Set the ESI all zero to indicate single home testing. Configure the B-MAC Prefix and length, and the proper labels for advertising the B-MAC prefix to all other PEs in the network. Note that in the case of PBB-EVPN, individual C-MAC will lose its meaning in the core and won't carry any labels as they are hidden behind the B-MAC and meaningless to the core. This is key advantage in order to scale to millions of C-MAC.

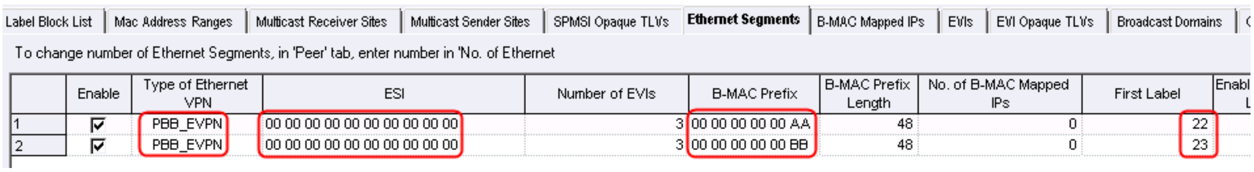


Figure 461. PBB-EVPN Configuration

2. Configure the **Broadcast Domain** with proper Ethernet Tag ID

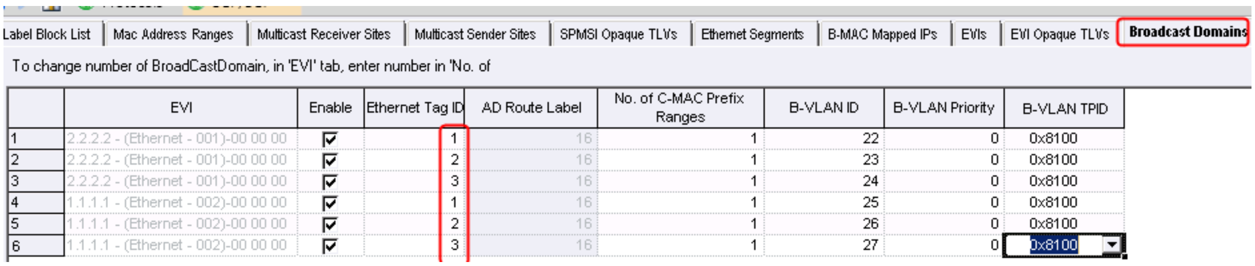


Figure 462. Broadcast Domain Ethernet Tag ID

3. Configure each EVI with proper Target and Import Target value in order for the learned info stored in the right EVI table for label lookup. Set **Multicast Tunnel Type** as **Ingress Replication** with proper Upstream/Downstream assigned MPLS label. This is for BUM traffic. Note that even though we use Ingress Replication as an example, the user is encouraged to use other tunnel types such as RSVP-TE P2MP and mLDP P2MP. When selected, it’s also needed to configure the appropriate P2MP tunnel in order for the traffic to work.

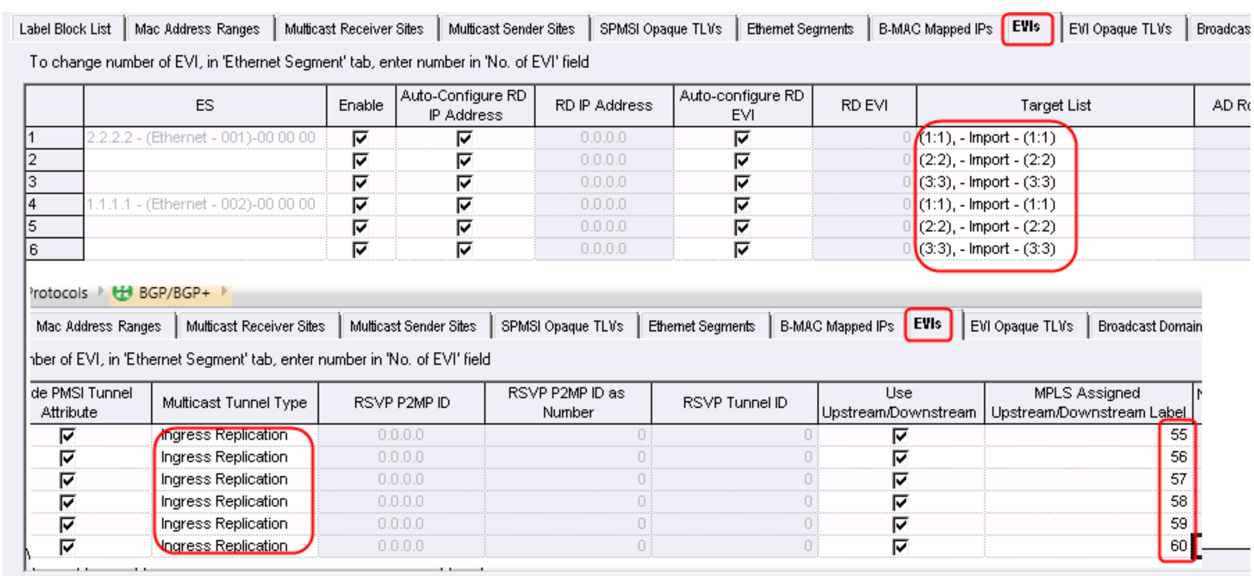
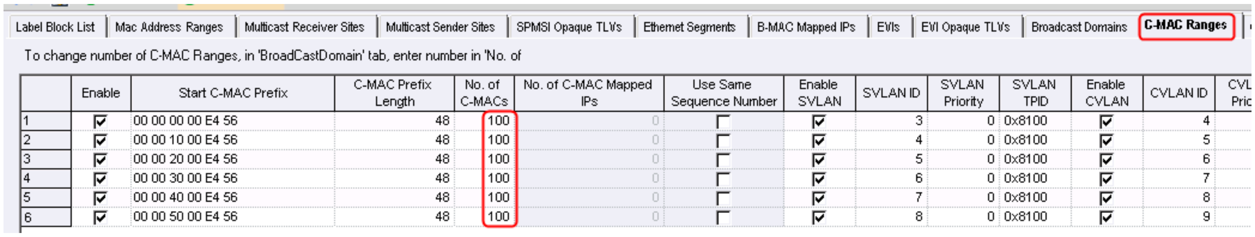


Figure 463. Target and Importat Target , PMSI configuraiton

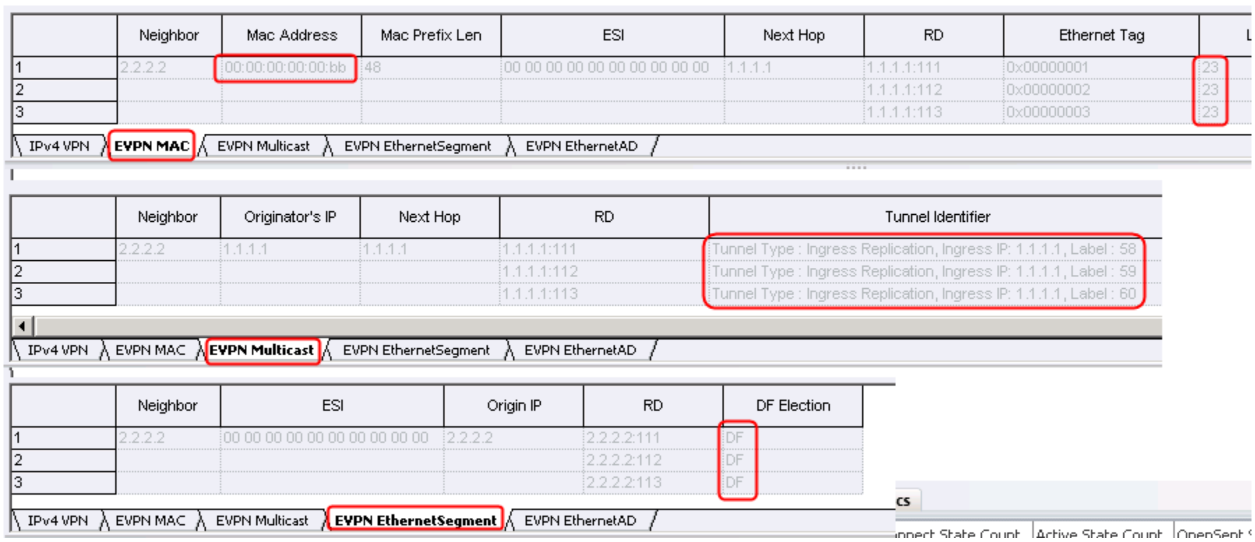
4. Set some number of C-MAC for traffic purpose. Note again that each C-MAC won't carry label info because they are hidden behind the B-MAC.



	Enable	Start C-MAC Prefix	C-MAC Prefix Length	No. of C-MACs	No. of C-MAC Mapped IPs	Use Same Sequence Number	Enable SVLAN	SVLAN ID	SVLAN Priority	SVLAN TPID	Enable CVLAN	CVLAN ID	CVL Pric
1	☑	00 00 00 00 E4 56	48	100	0	☐	☑	3	0	0x8100	☑	4	
2	☑	00 00 10 00 E4 56	48	100	0	☐	☑	4	0	0x8100	☑	5	
3	☑	00 00 20 00 E4 56	48	100	0	☐	☑	5	0	0x8100	☑	6	
4	☑	00 00 30 00 E4 56	48	100	0	☐	☑	6	0	0x8100	☑	7	
5	☑	00 00 40 00 E4 56	48	100	0	☐	☑	7	0	0x8100	☑	8	
6	☑	00 00 50 00 E4 56	48	100	0	☐	☑	8	0	0x8100	☑	9	

Figure 464. C-MAC Configuration

5. Start all protocols and verify the learned info. Note that it's the B-MAC that is advertised with a specific label instead of individual C-MAC. Also notice the Ingress Replication label to be used for BUM traffic. As a single home PE, it's always in DF role. There is no Ethernet AD routes needed for PBB-EVN which simplifies implementation significantly.



	Neighbor	Mac Address	Mac Prefix Len	ESI	Next Hop	RD	Ethernet Tag	L
1	2.2.2.2	00:00:00:00:00:bb	48	00 00 00 00 00 00 00 00 00 00	1.1.1.1	1.1.1.1:111	0x00000001	23
2						1.1.1.1:112	0x00000002	23
3						1.1.1.1:113	0x00000003	23

	Neighbor	Originator's IP	Next Hop	RD	Tunnel Identifier
1	2.2.2.2	1.1.1.1	1.1.1.1	1.1.1.1:111	Tunnel Type : Ingress Replication, Ingress IP: 1.1.1.1, Label : 58
2				1.1.1.1:112	Tunnel Type : Ingress Replication, Ingress IP: 1.1.1.1, Label : 59
3				1.1.1.1:113	Tunnel Type : Ingress Replication, Ingress IP: 1.1.1.1, Label : 60

	Neighbor	ESI	Origin IP	RD	DF Election
1	2.2.2.2	00 00 00 00 00 00 00 00 00 00	2.2.2.2	2.2.2.2:111	DF
2				2.2.2.2:112	DF
3				2.2.2.2:113	DF

Figure 465. Learned Info

6. Create traffic item for unicast to known C-MAC. Select destination from C-MAC defined behind each EVI. Verify the encapsulated packets to ensure right labels are picked up. Note that even though a total of 300 C-MAC are defined, only one label value (23) is used which corresponds to the B-MAC advertised by the DUT.

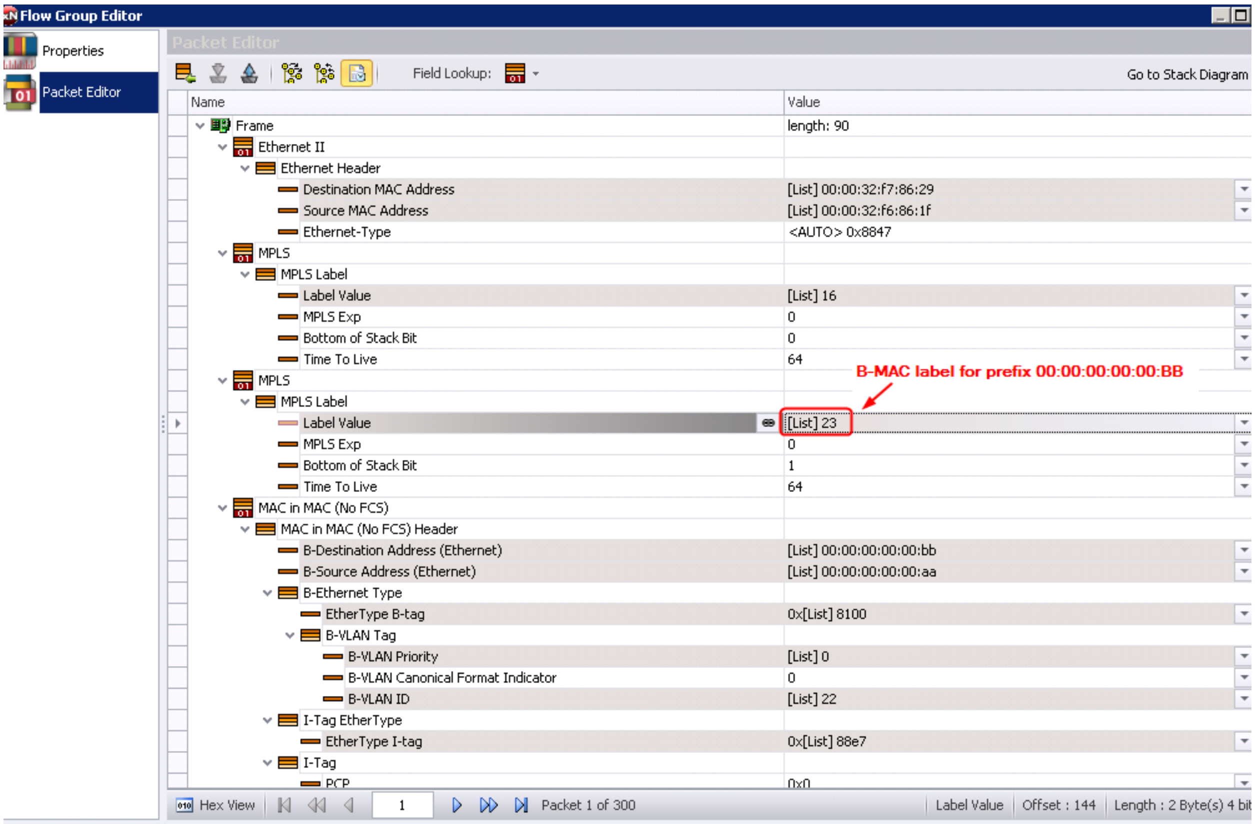


Figure 466. Known Unicast Traffic Creation and Verification

7. Create a traffic item for BUM traffic. To simulate BUM traffic, simply define a few static MACs that are unknown to the control plane. Verify the content to ensure that the Ingress Replication label is used instead of the B-MAC label. Also notice that the Dest B-MAC is using I-SID converted multicast address based on **802.1ah** spec.

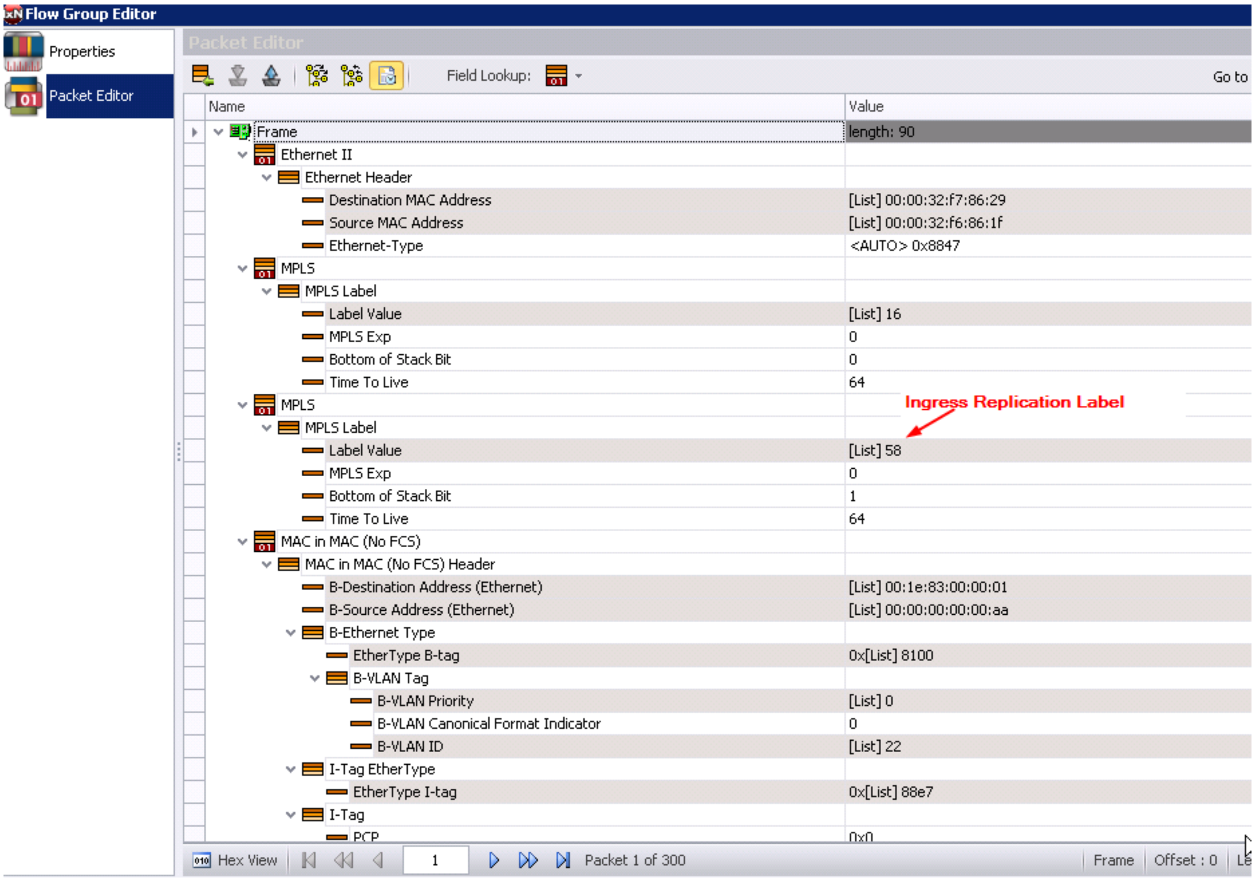


Figure 467. BUM Traffic Creation and Verification

8. To verify if DUT is encapsulating the packets in the same way as Ixia, you can do a capture on data plane to decode the packets. Make sure to send the traffic a slower rate so capture buffer won't be congested.

   Note: you can refer to the appendix "EVPN/PBB-EVPN Label Stack and Label Resolution Procedures" for more details on how labels are constructed for all valid EVPN/PBB-EVPN use cases, including various P-Tunnel types

Test Variables

Consider the following list of variables to add in the test in order to make the overall test plan better.

Functional/Performance Variable	Description
While we use **Ingress Replication** as the example throughout this chapter on EVPN/PBB-EVPN testing, obviously the other types, **RSVP-TE P2MP** and **mLDP P2MP** types should be tried out – if the DUT supports them.	If P2MP tunnel is used instead of Ingress Replication, control plane will work very much the same as in the case of using Ingress Replication. The difference is in the traffic encapsulation using different labels. In the case of known unicast traffic, P2MP will use the corresponding P2MP labels learned from RSVP-TE P2MP or mLDP protocols instead of LDP or RSVP-TE P2P. The second label still comes from the MAC advertisement route. For BUM traffic, the transport traffic also comes from P2MP protocol just as in the case of unicast. The multicast label will come from the user configured Upstream/Downstream assigned label. Everything else is the same. Refer to Appendix C: "EVPN/PBB-EVPN Label Stack and Label Resolution Procedures" for a complete understanding of label stacks and label resolution procedure for both Ingress Replication and P2MP tunnel types.
The B-MAC and C-MAC mapped IP addresses	You can define one or more IP addressed mapped to B-MAC or C-MAC to test ARP table cache.
The number of Ethernet Segments and EVIs per segment	Increase both numbers to test DUT scalability in terms of total number of Ethernet Segments and maximum number of EVIs supported per segment.
The number of C-MAC addresses per Broadcast domain	Increase the number of C-MAC per broadcast to test DUT's MAC table capacity
Flap BGP peer, Ethernet Segment, EVI, MAC to stress test DUT stability	Introduce flaps to different levels to increase stress to DUT.

Test Case: EVPN and PBB-EVPN Multi-Home Test Scenario

Overview

Multi-home test is more complex than single home testing. One of the very reasons for EVPN coming to existence is that it supports multi-homing. Some of the key functions of multi-homing PEs are:

- Load balancing
- Resilience against failure
- Designated Forwarding to avoid packet duplication
- Split Horizon to avoid forwarding loops

These key functions need to be verified in order to guarantee a robust implementation. IxNetwork feature rich EVPN emulation software, coupled with hardware unique ability to perform egress tracking, and convergence time measurement up to ms accuracy, can be used to verify all above important functions.

Objective

This test is to verify all key functions in a multi-homing EVPN and PBB-EVPN setup, including load balancing, convergence time against failure, Designated Forwarding, and Split Horizon.

Setup

In the load balancing and convergence time test, two Ixia test ports are required as depicted below. One test port emulates CE and one test port emulates two PEs and the single homed CE.

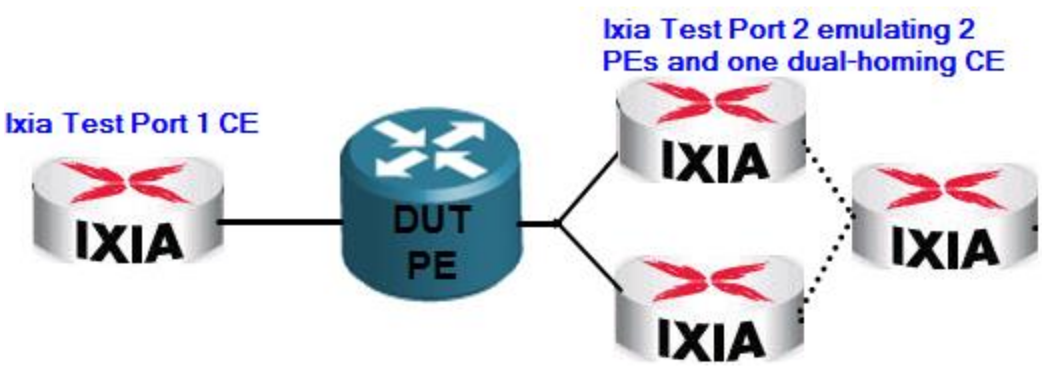


Figure 468. Multi-Home Scenario for Load Balancing Test

In the Designated Forwarding and Split Horizon test, three test ports and two DUTs are required. One test port is emulating CE1 connected to DUT1 who is a multi-homing PE to CE1. Ixia test port will be emulating a multi-homing PE (PE3) which also simulates CE1 behind (dotted line). The third Ixia test port will be emulating remote CE2 connecting to another DUT (PE2). In addition to control plane configuration, traffic will be built and sent between various pairs in order to verify the functions.

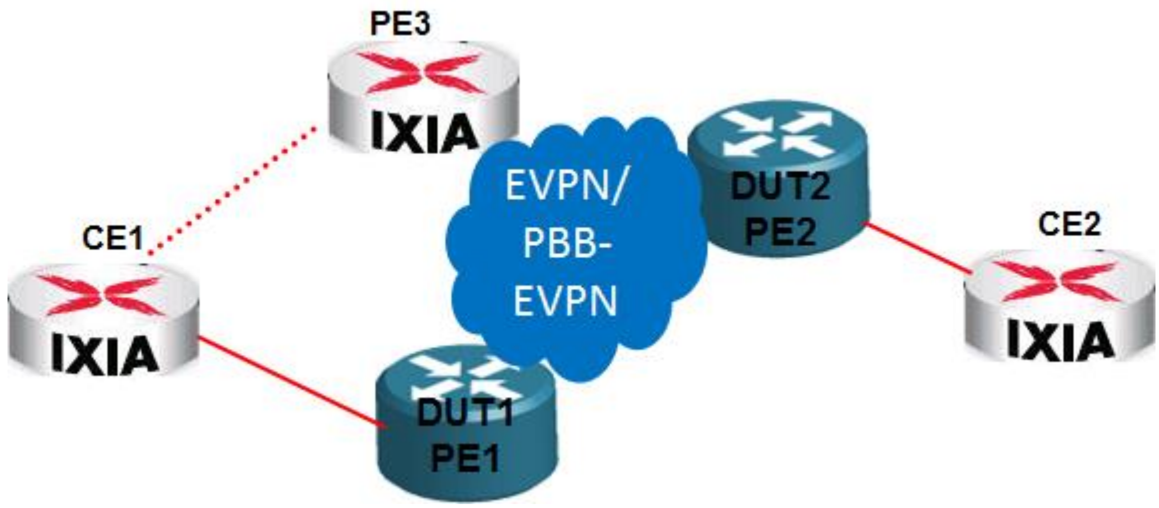


Figure 469. Multi-Home Scenario for Split Horizon and Designated Forward Test

Step-by-Step Instructions

Note: You need to review basic steps descried in the single home EVPN and PBB-EVPN test case to get yourself familiar with basic configuration steps and operation skills. The steps below are on a much higher level and will only describe what are required in order to achieve the test objectives. Also, we will focus on EVPN first to illustrate key steps and then list the differences when configuring PBB-EVPN.

Multi-Homing Testing for Load Balancing and Convergence Time Measurement

1. Configure some static MACs behind Ixia test port 1 which emulates the CE router.
2. Configure Ixia test port 2 with 2 PE routers which is to emulate dual-homed PEs in the load balancing and convergence test.
3. Ensure both PEs are configured with identical ESI values (non zero).

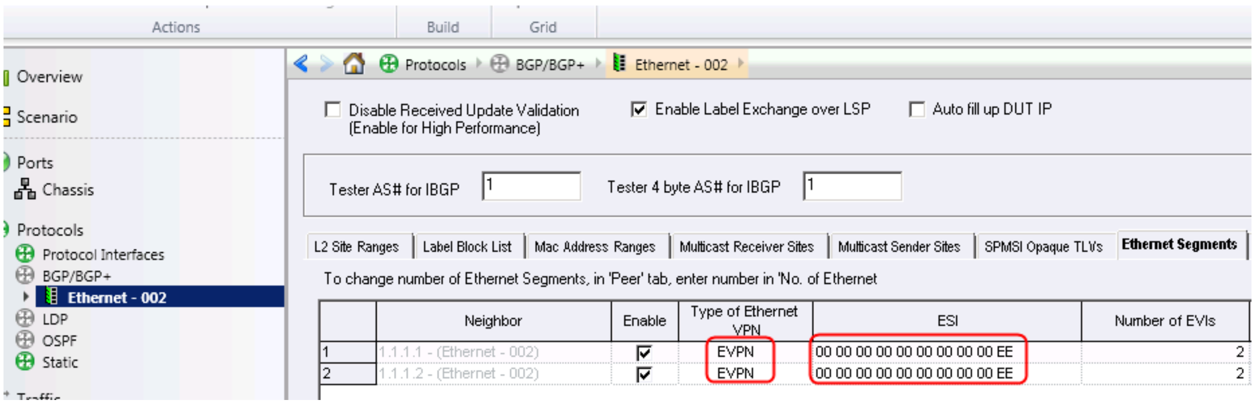


Figure 470. Multi-Homing ESI Configuraiton

4. Enable Ingress Replication for PMSI to deliver BUM traffic
5. Configure the EVI with appropriate Target and Import Target values

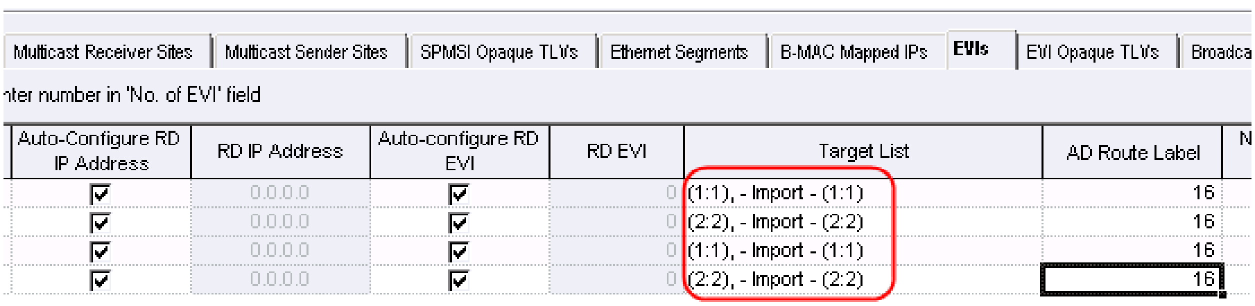


Figure 471. Target and Import Target Configuration

6. Configure identical C-MAC behind the same EVI. Set up appropriate label start value. The DUT will learn multiple NextHops for the same MAC and will perform load balancing.

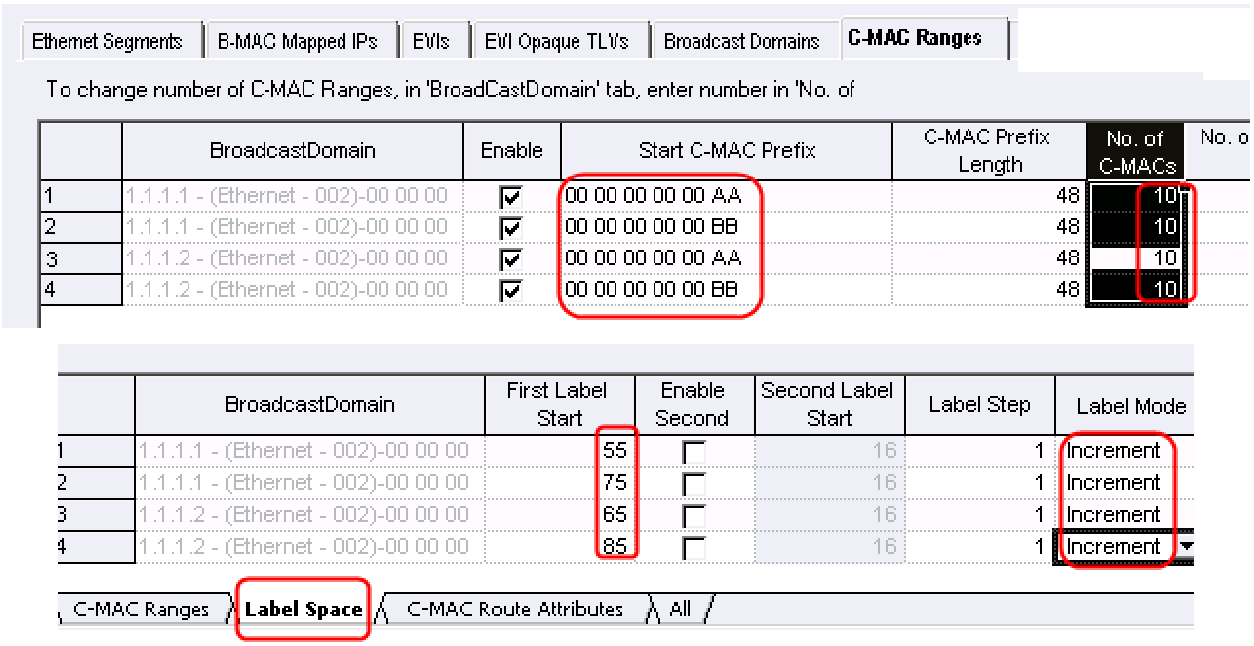


Figure 472. Dual-Homed CE Configuration

7. Start all control plane protocols and make sure they are all up with the correct learned info.

8. Use traffic wizard to build traffic source from static MAC behind Ixia test port1, and destined to C-MAC for the first EVI behind Ixia test port 2.

9. Enable **Packet Loss Duration** under Test Options. This will deliver the convergence time when one of the active links is under flap.

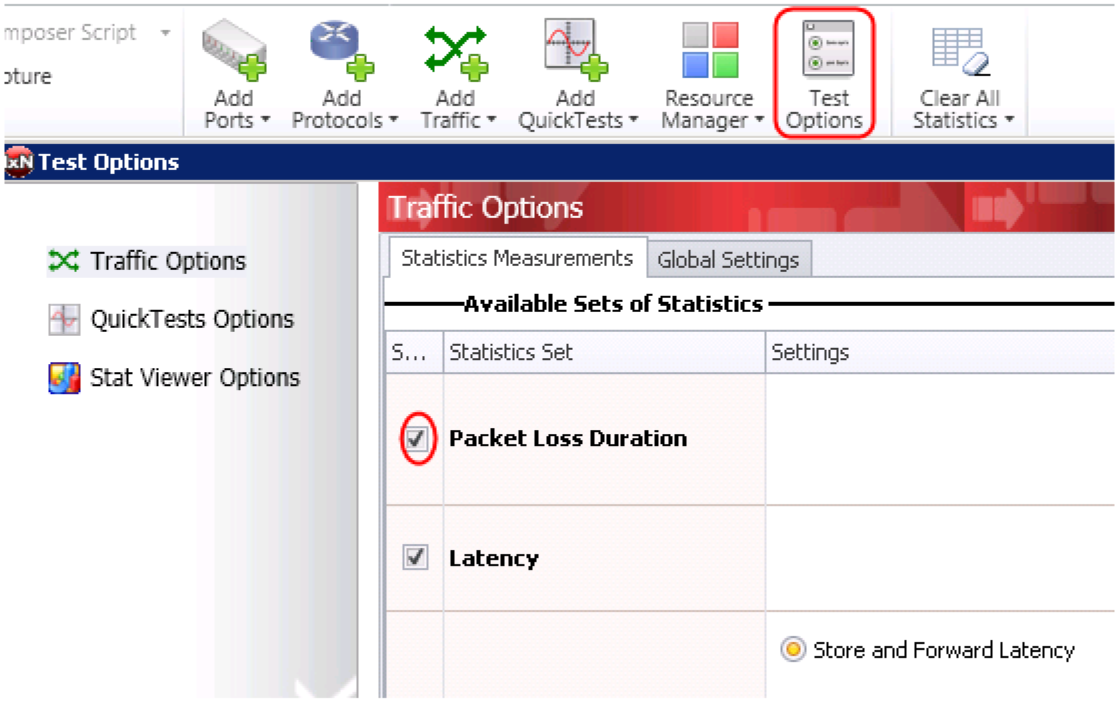


Figure 473. Enable Packet Loss Duration for Convergence Time Measurement

10. The key to track if load balancing is done appropriately by DUT is to use a unique feature in Ixia called “Egress Tracking”. See below screen capture for how it is configured. We will use the **Use Custom Settings** and **Raw Offset** in bits to track the actual label encapsulated by the DUT. Here is a brief explanation how value 156 and 8 are derived: We know the second MPLS label starts at offset 18 bytes. Turn this to bits and it becomes 144 bits. Now there are 20 bits for MPLS label value and we know our advertised MPLS label is under 256 therefore the values will only change in the last 8 bits. So we don’t really need to track all 20 bits to avoid large number of display with nil value entries – only the last 8 bits need to be tracked in order to view all legal values. So we increase the offset by another 12 bits which makes the offset at 156 bits and only 8 bits need to be tracked – hence the offset 156 and width 8 settings.

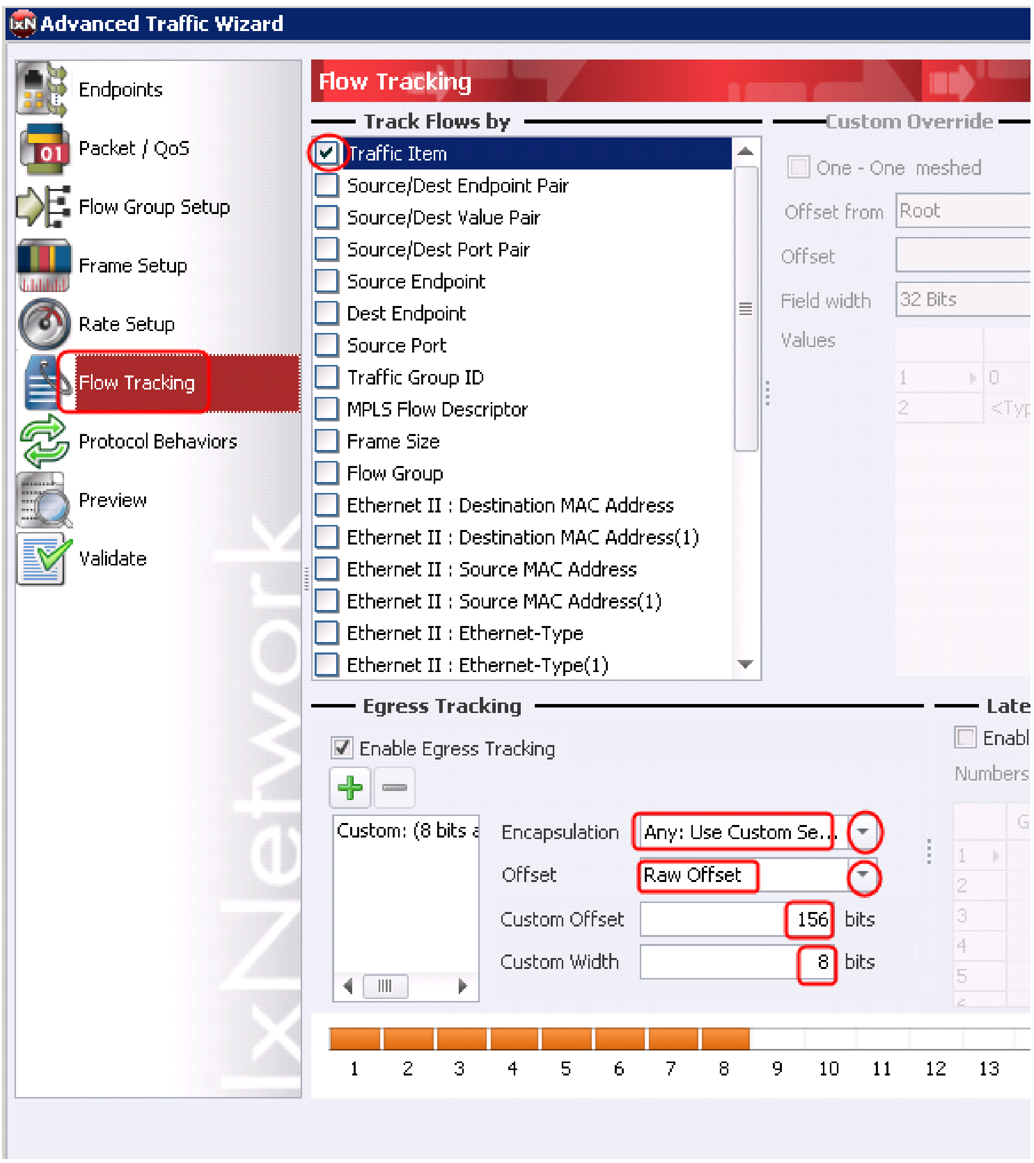


Figure 474. Configure Egress Tracking for Load Balancing Verification

Note that you can also do egress tracking on the first MPLS label which is the LDP FEC lable for the two PE loopbacks. In this case, simple descrease the offset value by 4 bytes or 32 bits.

Note also that at least one ingress tracking items need to be selected. In above example, the "Traffic Item" is selected. The egress tracking results will show "port level load balancing". If the DUT is actually doing on per VLAN basis, you should select "VLAN ID" as the ingress tracking. The egress tracking results will then show the load balancing on per VLAN basis.

11. Start traffic generation. On traffic item level, right click to choose Ingress/Egress Statistics->Show All Egress.

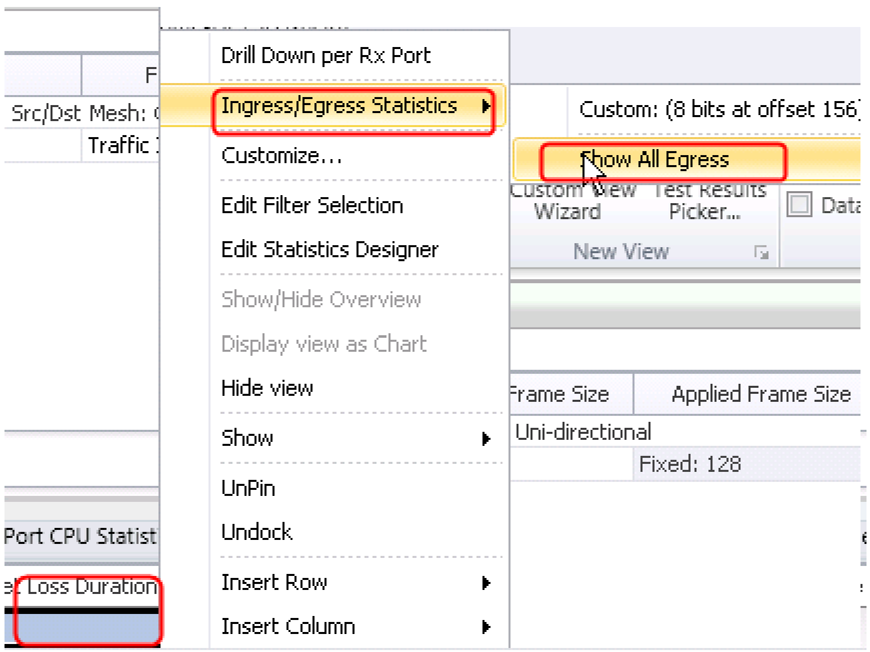


Figure 475. Enable Ingress/Egress Tracking Correlation

12. The ingress/egress view will show all legitimate MPLS labels (second label that correspond to Ixia's emulated PE MAC Advertisement Routes). This proves that DUT is doing the load balancing correctly. Expand this test to have more emulated PEs to test if DUT is doing the load balancing across all legal nextHops. An extra step is to verify the RX rate for each of the MPLS labels to verify if DUT is doing load balancing evenly or whatever rates that are configured per load balancing policy configured on the DUT.

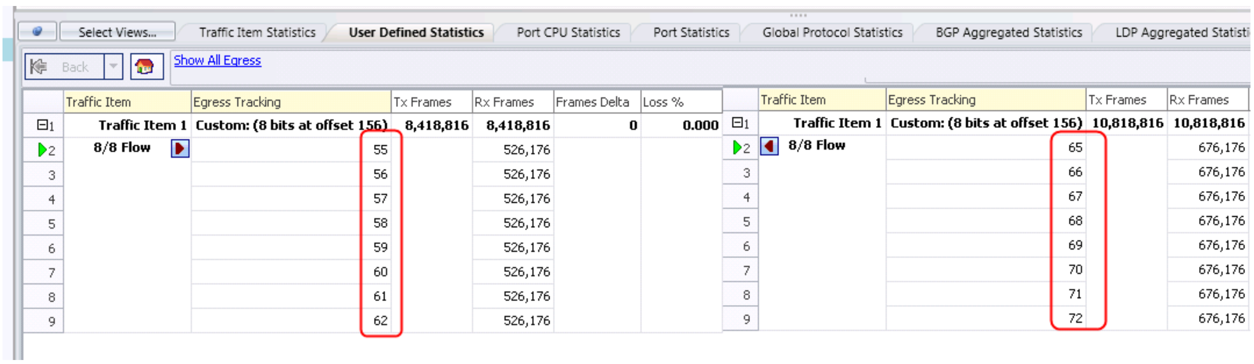


Figure 476. Ingress/Egress Tracking Stats for Load Balancing Verification

13. You should build a second traffic item for the second EVI and perform similar steps to prove DUT is also doing the load balancing for the second EVI.

14. To test convergence time, simply go to the **C-MAC Ranges** tab to disable the C-MAC corresponding to the right EVI.

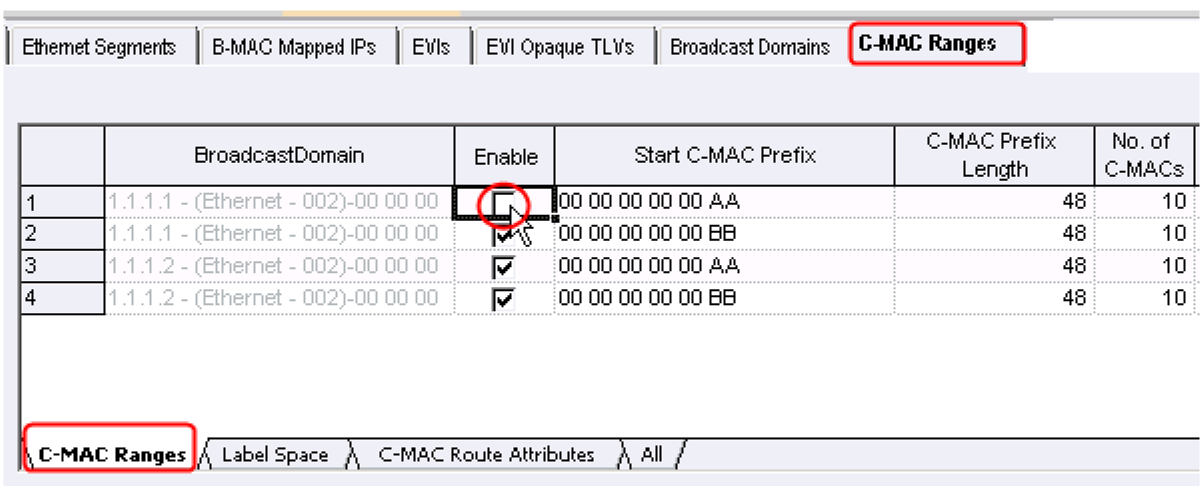


Figure 477. Inject Failure

15. Traffic Item level stat – Packet Loss Duration – will show the correct convergence time. When the traffic rate is low, DUT may have enough buffer so the convergence time is zero. You should increase the rate to ensure expected convergence time is observed.

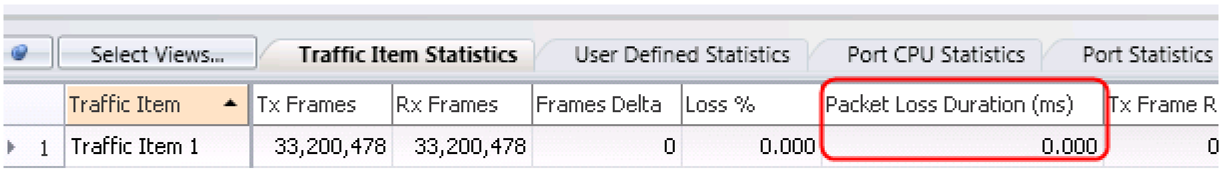


Figure 478. Convergence Time

Confiuration Steps for PBB-EVPN to Verify Load Balancing and Measure Convergence Time

1. To configure PBB-EVPN multi-homing, make sure to select **PBB_EVPN** as the **Type of Ethernet VPN**. Set identical non-zero value for the ESI, and set the same B-MAC prefix for both PEs. Advertise a different label value for load balancing verification.

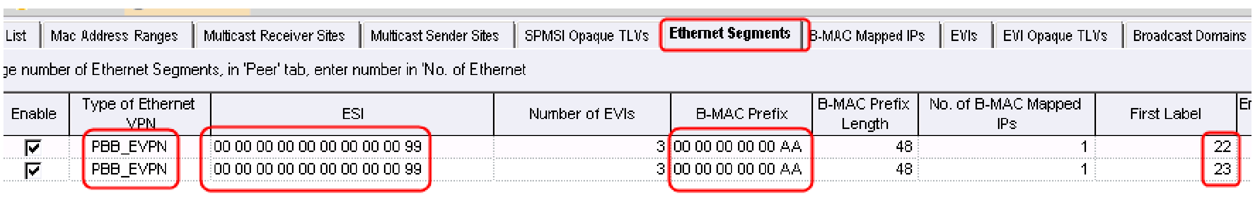


Figure 479. PBB-EVPN Configuration

2. Configure the same Target and Import Target for the same EVI, and set the ingress replication as the **Multicast Tunnel Type**. Make sure to enter a unique MPLS label.

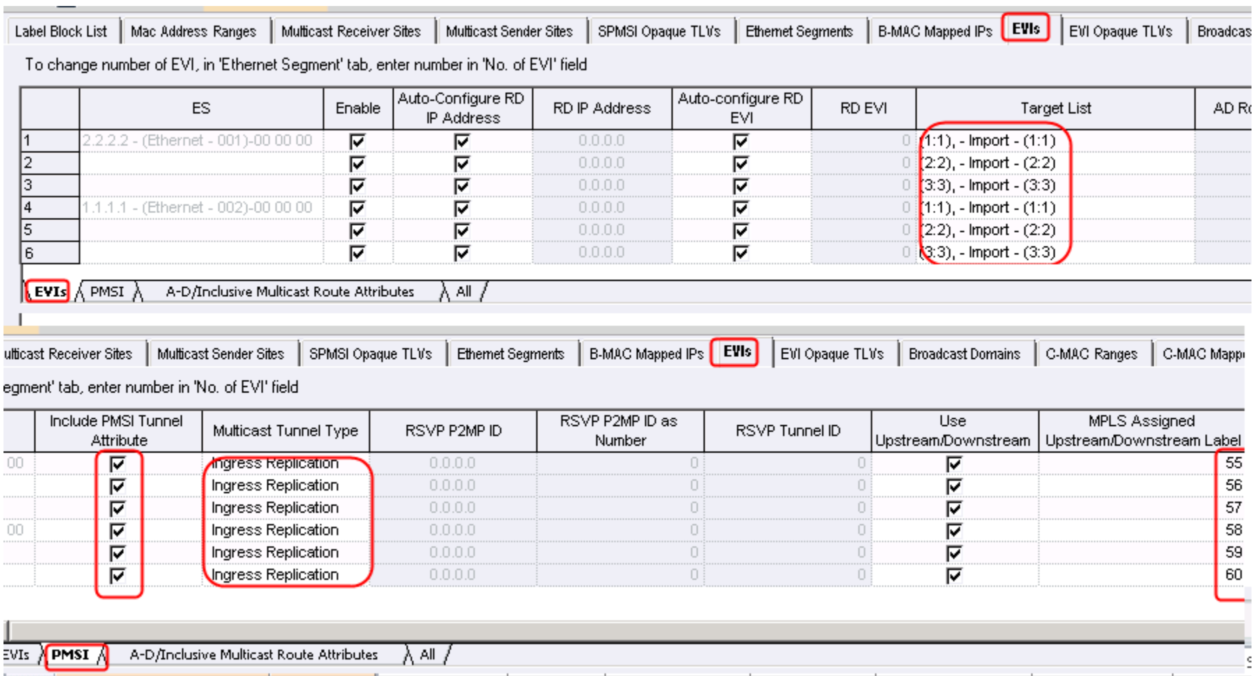


Figure 480. Target and Import Target, PMSI Configuration

3. Set the **Broadcast Domain** with unique **Ethernet Tage ID** for each different EVI, but the same across both emulated PEs for the same EVI.

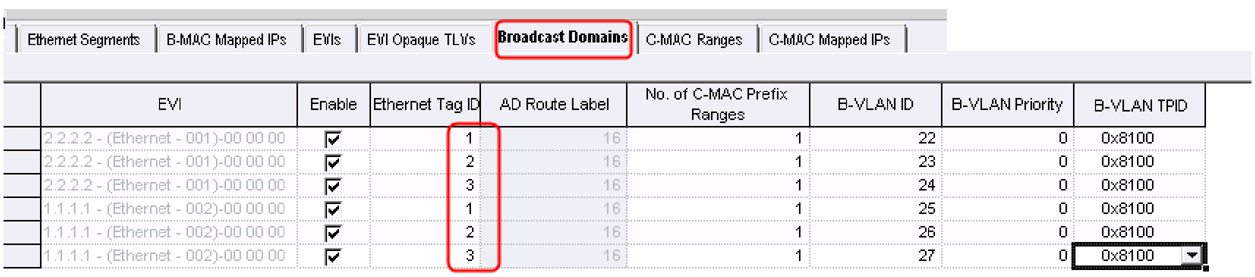


Figure 481. Broadcast Domain Ethernet Tage ID

4. There is no need to change the Egress Tracking offset and bit width from what is configured and fully explained in the EVPN multi-homing section. This is because the PBB encapsulation is after MPLS header. If DUT is doing load balancing on I-SID, you do need to enable I-SID as ingress tracking.

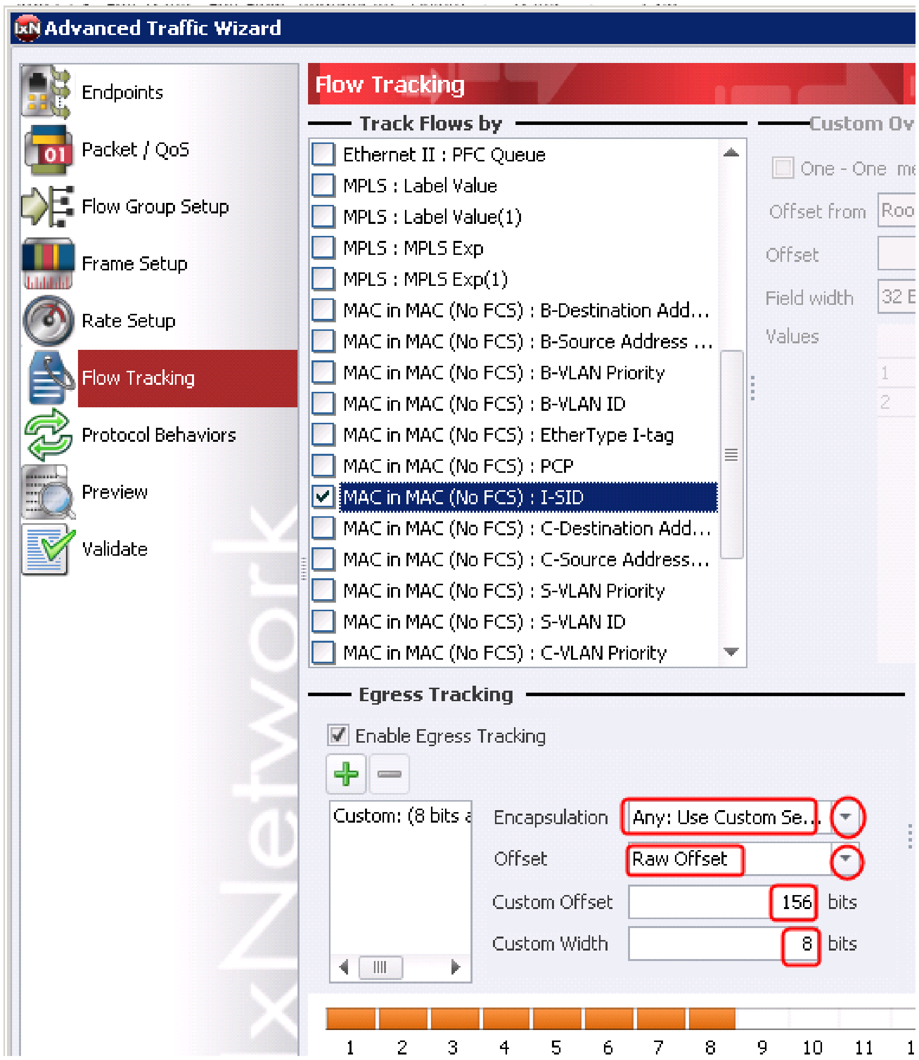


Figure 482. Enable Egress Tracking to Verify Load Balancing based on ISID

5. Use the **Flush Remote CMAC Forwarding Table** button which is only available under PBB-EVPN to induce flaps and use Packet Loss Duration as indiactor of convergent time in case of any loss during the control plane flap. Increase the traffic rate in order to observe the expected results.

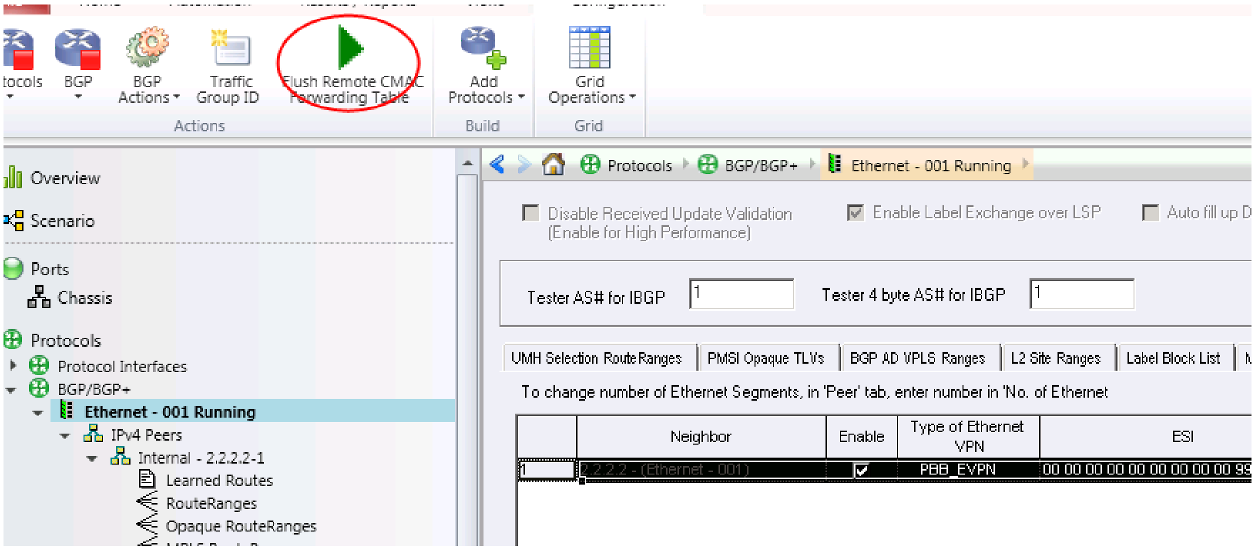


Figure 483. Inject Failre to Measure Convergence Time

Multi-Homing Testing for Split Horizon and Designated Forwarding

Again, we will use EVPN as a comprehensive example how to configure the IxNetowork to achieve test objective. PBB-EVPN related steps will be highlighted toward the end of this section.

1. Configure a few static MACs behind the CE1 (test port 1) and CE2 (test port 3) for traffic purpose. Being a CE router in EVPN setup, there is no control plane invoved. DUT1/PE1 will learn these MACs and propagate them to other PEs in the diagram.

2. Configure PE3 (test port 2) with the right BGP info per below screen capture. The ESI value must be non zero (indicating multi-homing) and must match DUT1/PE1's ESI to indicate they are connected to the same CE1. Enter appropriate number of EVIs in the segment. Make sure the **Support Mult-Homed ES Auto Discovery** is enabled, and the **Enable Active-Stanby** is disabled. Enter a valid ESI Label value.

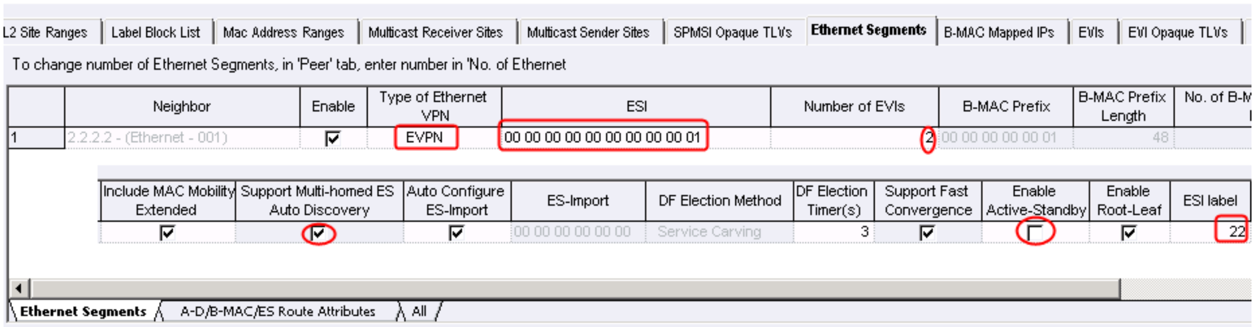


Figure 484. BGP Configuration for Multi-Home EVPN DF and S-H Tests

3. Set appropriate values for the Target and Import Target under EVI tab

4. For PMSI, make sure to select Ingress Replication and enter proper value of the labels used for ingress replication.

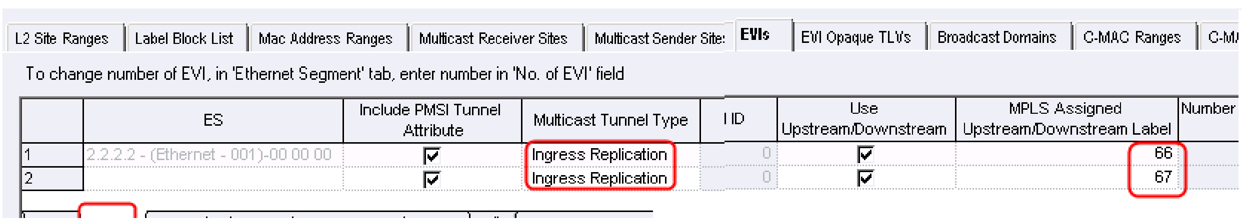


Figure 485. PMSI Tunnel Configuration

5. Configure the same MAC as defined as static behind CE1 as the C-MAC behind PE3 Broadcast domain.

6. Start all control plane protocols and make sure they are all up with learned info. Verify that DUT PE1 is the elected as DF for the dual-homed CE1.

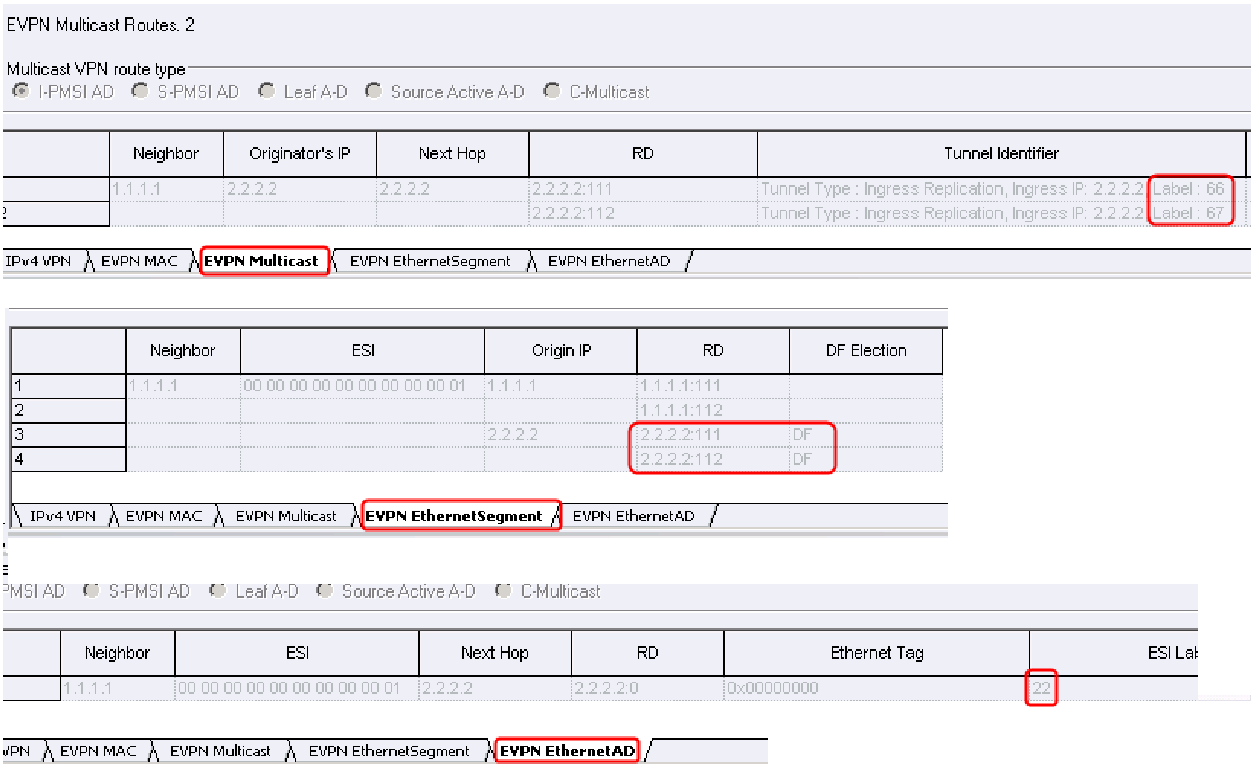


Figure 486. Learned Info

Above learned info shows that DUT PE1 (2.2.2.2) is sending Ixia PE3 Ingress Replication labels 66 and 67 (two EVIs configured), and an ESI label of 22. DUT is elected as the DF.

7. Build a BUM traffic from Ixia test port (PE3) – using static MAC behind CE2 for example. Verify the label stack sent by Ixia – 3 labels as shown below.

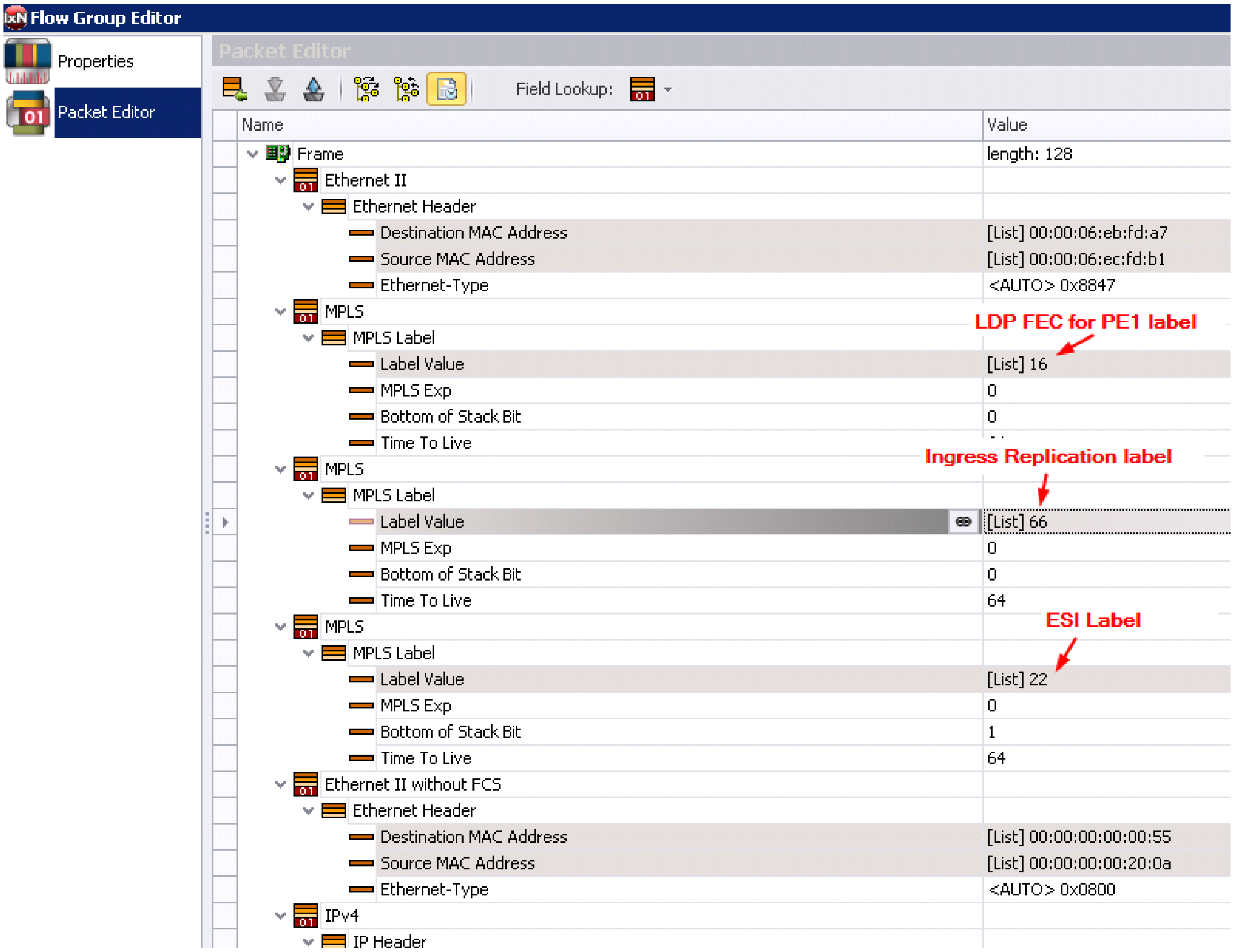


Figure 487. BUM Traffic Creation and Verification

8. Traffic received by DUT PE1 from Ixia PE3 (test port 2) should NOT be forwarded to CE1 (test port 1). This is the Split Horizon rule.

9. Likewise, force DUT1 to be **non DF** and Ixia PE3 to be **DF** (change DUT loopback lower in value, or change Ixia PE3 address to be higher in value). Verify traffic by Ixia test port1 (CE1) to an unknown MAC will carry three labels stack. This can be done using data capture on Ixia test port 2 (PE3).

10. Build traffic from Ixia test port 3 (CE2) and send traffic to test port 1 (CE1). Verify when DUT is in **DF** role, it fowrads all traffic to CE1 (no loss). When Ixia PE3 is in DF role, no traffic should be forwarded to CE1 (100% loss).

Steps to Configure PBB-EVPN for Multi-Homing Split Horizon and Designated Forwarding Testing

1. The PBB-EVPN Split Horizon rule is actually made very simple. There is NO ESI labels involved. The requirement of B-MAC to be identical for the common Etherent Segment actually make the decision simpler: if the packets carry the same B-MAC address, then it is coming from the same segment and there is no need to forward in order to avoid loops. Even though there is no control plane action involved, you must still verify it from data plane perspective by sending the traffic between Ixia test port 1(CE1) and Ixia test port 2 (PE3) and observe if any forwarding occurs.

2. There are no changes in the DF election procedure in PBB-EVPN therefore procedures defined in the EVPN multi-homing case for DF forwarding verification apply here.

Test Variables

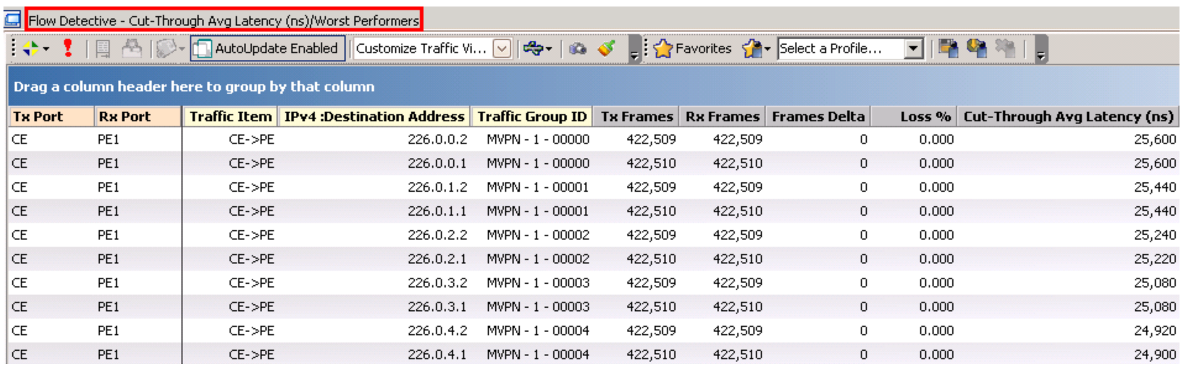
Consider the following list of variables to add in the test in order to make the overall test plan better.

Funtional/Performance Variable	Description
While we use **Ingress Replication** as the example throughout this chapter on EVPN/PBB-EVPN testing, obviously the other types, **RSVP-TE P2MP** and **mLDP P2MP** types should be tried out – if the DUT supports them.	If P2MP tunnel is used instead of Ingress Replication, control plane will work very much the same as in the case of using Ingress Replciation. The difference is in the traffic encapsulation using different labels. In the case of known unicast traffic, P2MP will use the corresponding P2MP labels learned from RSVP-TE P2MP or mLDP protocols instead of LDP or RSVP-TE P2P. The second label still comes from the MAC advertisement route. For BUM traffic, the transport traffic also comes from P2MP protocol just as in the case of unicast. The multicast label will come from the user configured Upstream/Downstream assigned label. Everything else is the same. Refer to Appendix C: "EVPN/PBB-EVPN Label Stack and Label Resolution Procedures" for a complete understanding of label stacks and label resolution procedure for both Ingress Replication and P2MP tunnel types.
The B-MAC and C-MAC mapped IP addresses	You can define one or more IP addressed mapped to B-MAC or C-MAC to test ARP table cache.
The number of Ethernet Segments and EVIs per segment	Increase both numbers to test DUT scalability in terms of total number of Ethernet Segments/B-MAC table size and maximum number of EVIs supported per segment.
Flap BGP peer, Ethernet Segment, EVI, MAC to stress test DUT stability	Introduce flaps to different levels to increase stress to DUT.

Appendix A: Data MDT for Topology

Topology 1 can be used to test a PE device's capability to join a data MDT. The basic test procedure and configuration are the same as above except for a few differences in the Ixia emulation.

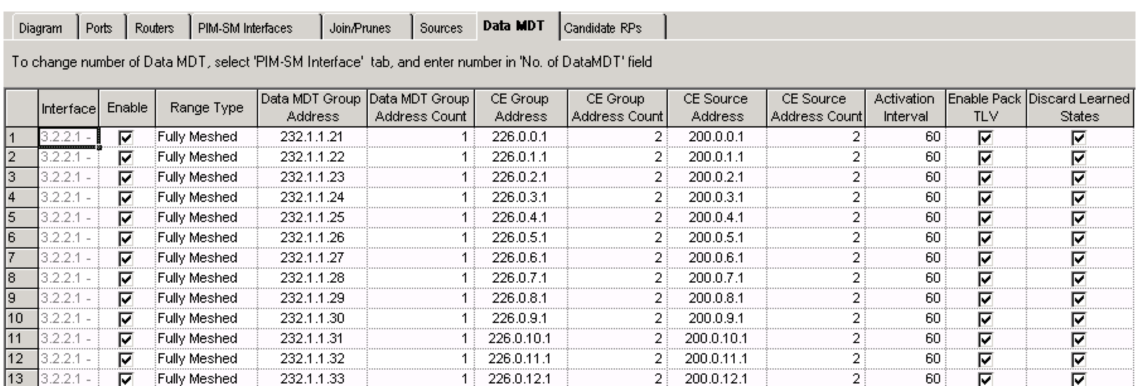
1. While configuring data MDT parameters in the mVPN protocol wizard, one parameter is specific to this test – **Switchover Interval**. The Ixia emulation does not monitor the multicast traffic flow rate as a real router does in order to decide when to switchover to data MDT. Instead, the Ixia emulation switchover is controlled by a timer. After the time elapses (from starting PIM protocol), the Ixia emulated PE router will send a data MDT join TLV to signal the data MDT.



Tx Port	Rx Port	Traffic Item	IPv4 :Destination Address	Traffic Group ID	Tx Frames	Rx Frames	Frames Delta	Loss %	Cut-Through Avg Latency (ns)
CE	PE1	CE->PE	226.0.0.2	MVPN - 1 - 00000	422,509	422,509	0	0.000	25,600
CE	PE1	CE->PE	226.0.0.1	MVPN - 1 - 00000	422,510	422,510	0	0.000	25,600
CE	PE1	CE->PE	226.0.1.2	MVPN - 1 - 00001	422,509	422,509	0	0.000	25,440
CE	PE1	CE->PE	226.0.1.1	MVPN - 1 - 00001	422,510	422,510	0	0.000	25,440
CE	PE1	CE->PE	226.0.2.2	MVPN - 1 - 00002	422,509	422,509	0	0.000	25,240
CE	PE1	CE->PE	226.0.2.1	MVPN - 1 - 00002	422,510	422,510	0	0.000	25,220
CE	PE1	CE->PE	226.0.3.2	MVPN - 1 - 00003	422,509	422,509	0	0.000	25,080
CE	PE1	CE->PE	226.0.3.1	MVPN - 1 - 00003	422,510	422,510	0	0.000	25,080
CE	PE1	CE->PE	226.0.4.2	MVPN - 1 - 00004	422,509	422,509	0	0.000	24,920
CE	PE1	CE->PE	226.0.4.1	MVPN - 1 - 00004	422,510	422,510	0	0.000	24,900

Figure 488. mVPN protocol wizard screen #4 - data MDT

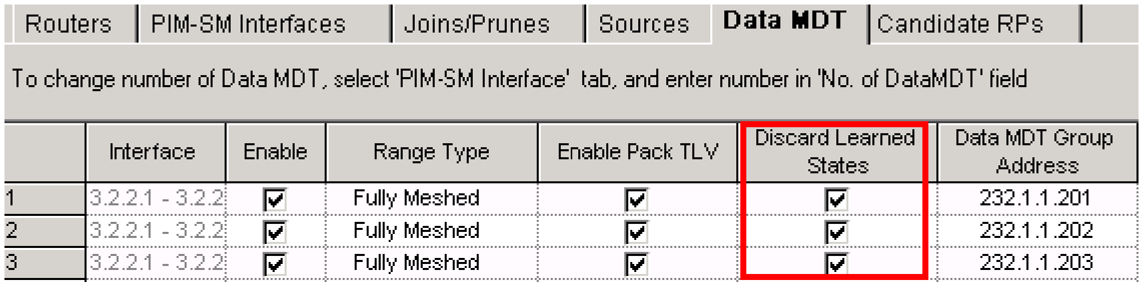
2. After running the mVPN protocol wizard, a data MDT range is created on the Ixia PE port. There is one row per mVPN per PE that specifies the C-multicast group and source address pair and the data MDT group associated with the pair. After the switchover time, a data MDT join TLV will be sent for each mVPN that an emulated PE supported.



	Interface	Enable	Range Type	Data MDT Group Address	Data MDT Group Address Count	CE Group Address	CE Group Address Count	CE Source Address	CE Source Address Count	Activation Interval	Enable Pack TLV	Discard Learned States
1	3.2.2.1 -	☑	Fully Meshed	232.1.1.21	1	226.0.0.1	2	200.0.0.1	2	60	☑	☑
2	3.2.2.1 -	☑	Fully Meshed	232.1.1.22	1	226.0.1.1	2	200.0.1.1	2	60	☑	☑
3	3.2.2.1 -	☑	Fully Meshed	232.1.1.23	1	226.0.2.1	2	200.0.2.1	2	60	☑	☑
4	3.2.2.1 -	☑	Fully Meshed	232.1.1.24	1	226.0.3.1	2	200.0.3.1	2	60	☑	☑
5	3.2.2.1 -	☑	Fully Meshed	232.1.1.25	1	226.0.4.1	2	200.0.4.1	2	60	☑	☑
6	3.2.2.1 -	☑	Fully Meshed	232.1.1.26	1	226.0.5.1	2	200.0.5.1	2	60	☑	☑
7	3.2.2.1 -	☑	Fully Meshed	232.1.1.27	1	226.0.6.1	2	200.0.6.1	2	60	☑	☑
8	3.2.2.1 -	☑	Fully Meshed	232.1.1.28	1	226.0.7.1	2	200.0.7.1	2	60	☑	☑
9	3.2.2.1 -	☑	Fully Meshed	232.1.1.29	1	226.0.8.1	2	200.0.8.1	2	60	☑	☑
10	3.2.2.1 -	☑	Fully Meshed	232.1.1.30	1	226.0.9.1	2	200.0.9.1	2	60	☑	☑
11	3.2.2.1 -	☑	Fully Meshed	232.1.1.31	1	226.0.10.1	2	200.0.10.1	2	60	☑	☑
12	3.2.2.1 -	☑	Fully Meshed	232.1.1.32	1	226.0.11.1	2	200.0.11.1	2	60	☑	☑
13	3.2.2.1 -	☑	Fully Meshed	232.1.1.33	1	226.0.12.1	2	200.0.12.1	2	60	☑	☑

Figure 489. PIM-SM configuration - data MDT range

3. You can view the joined data MDT state from PIM **Learned MDT Info**. You must disable **Discard Learned States** under the Data MDT tab before starting the PIM protocol to be able to view **Learned MDT Info**.



Routers	PIM-SM Interfaces	Joins/Prunes	Sources	Data MDT	Candidate RPs

To change number of Data MDT, select 'PIM-SM Interface' tab, and enter number in 'No. of DataMDT' field

	Interface	Enable	Range Type	Enable Pack TLV	Discard Learned States	Data MDT Group Address
1	3.2.2.1 - 3.2.2	☑	Fully Meshed	☑	☑	232.1.1.201
2	3.2.2.1 - 3.2.2	☑	Fully Meshed	☑	☑	232.1.1.202
3	3.2.2.1 - 3.2.2	☑	Fully Meshed	☑	☑	232.1.1.203

Figure 490. PIM-SM Data MDT tab - Discard Learned States

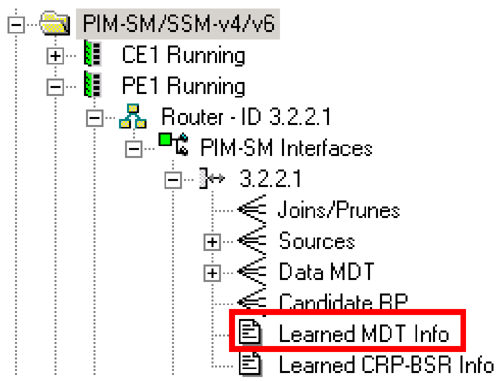
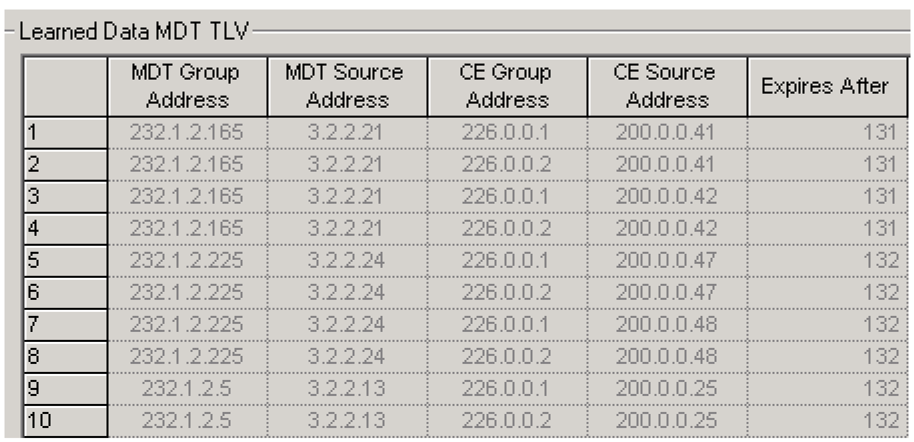


Figure 491. PIM-SM protocol tree - learned MDT info



Learned Data MDT TLV

	MDT Group Address	MDT Source Address	CE Group Address	CE Source Address	Expires After
1	232.1.2.165	3.2.2.21	226.0.0.1	200.0.0.41	131
2	232.1.2.165	3.2.2.21	226.0.0.2	200.0.0.41	131
3	232.1.2.165	3.2.2.21	226.0.0.1	200.0.0.42	131
4	232.1.2.165	3.2.2.21	226.0.0.2	200.0.0.42	131
5	232.1.2.225	3.2.2.24	226.0.0.1	200.0.0.47	132
6	232.1.2.225	3.2.2.24	226.0.0.2	200.0.0.47	132
7	232.1.2.225	3.2.2.24	226.0.0.1	200.0.0.48	132
8	232.1.2.225	3.2.2.24	226.0.0.2	200.0.0.48	132
9	232.1.2.5	3.2.2.13	226.0.0.1	200.0.0.25	132
10	232.1.2.5	3.2.2.13	226.0.0.2	200.0.0.25	132

Figure 492. PIM-SM Learned Data MDT TLV

4. After control plane sessions are up, generate data MDT traffic from the PE to the CE.

5. Launch the **Advance Traffic wizard**. Under **Traffic Mesh**, select **One-One** for **Source/Dest** and **Fully Meshed** for **Routes/Hosts**. At the Source endpoints window, click on the **+** button under **All Ports** and select **PIMSM DataMDT Ranges**. All DataMDT ranges under PE ports will be selected. At the Destination endpoints window, click the **+** button on the CE port and select PIM. Set other parameters as desired, such as frame size, line rate, and so on.

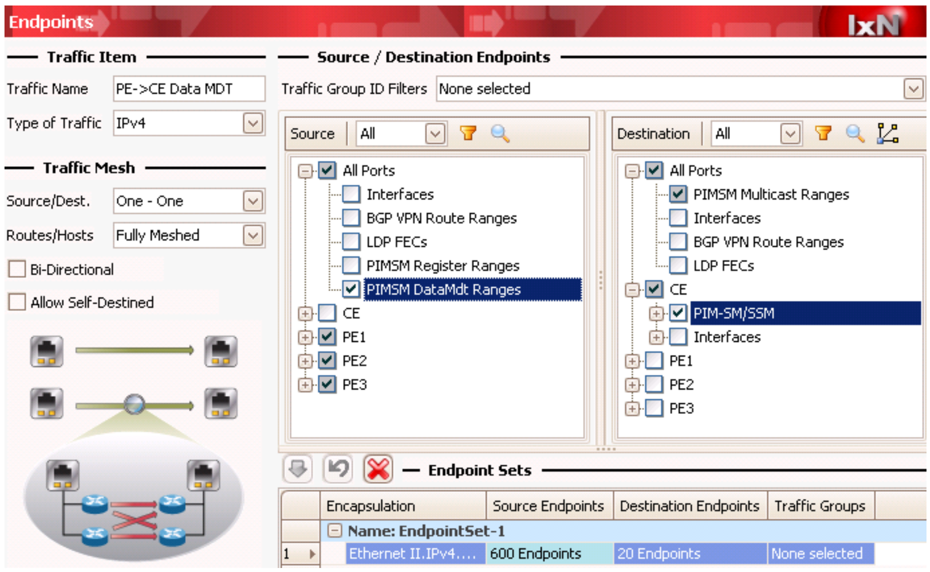


Figure 493. Traffic wizard endpoint selection - data MDT

6. You can view the generated packet using the Packet Editor. The outer IP destination address is the data MDT group address.

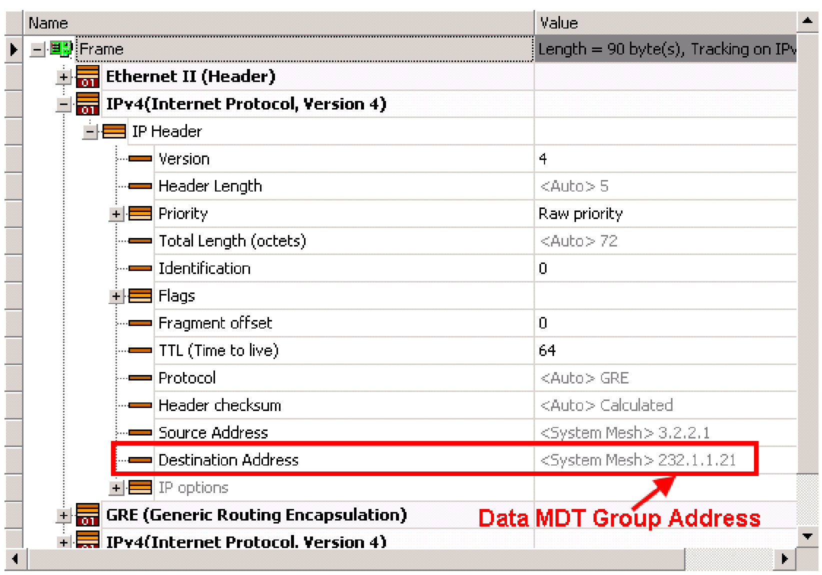


Figure 494. Packet Editor - data MDT encoding

Appendix B: mVPN Wizard

The mVPN wizard append function can be used to append additional configuration to the existing test without interrupting the current test. It can be used to append additional PEs, additional mVPNs, additional C-multicast source, and C-multicast groups. It can also be used to append topology 2 to topology 1 so that bi-directional traffic can be built.

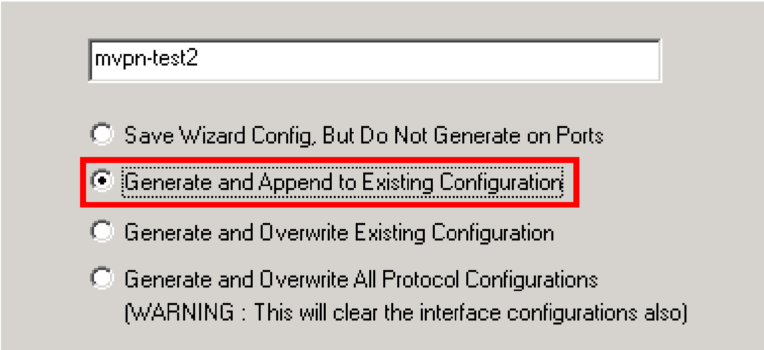


Figure 495. mVPN wizard append option

Appendix C: EVPN/PBB-EVPN Label Stack and Label Resolution Procedures

EVPN/PBB-EVPN Label Stack and Resolution Procedures	Ingress Replication	P2MP (mLDP or RSVP)
EVPN Label Stack	- Tunnel label (Inner Label) - E-VPN ingress replication label obtained from PMSI tunnel attribute advertised by remote PE. - ESI Label (Outer Label)	- P2MP LSP label for which ingress PE is root (Inner Label) PMSI upstream label (assigned) if enabled in GUI - ESI Label (Outer Label)
EVPN Label Resolution Procedures	Tunnel Label: - get the NextHops from the Multicast learned info for this source PE and obtain the LSP tunnel labels for each of the NH from LDP or RSVP-TE P2P which ever is configured PMSI Label: - traffic engine should get all the NextHops learned on this PE (source endpoint) from EVPN multicast learned info. - traffic engine should select only those NH which are having same EVI as that of source endpoint. -traffic engine should get the P-tunnel label from EVPN multicast learned info for this EVI for each of the NH and send same copy of packet (replication) to each NH with the corresponding PMSI tunnel label	P2MP Tunnel Label: - get the tunnel identifier from EVI/PMSI tab for mLDP or RSVP-TE P2MP and query to mLDP/RSVP-TE state machine exactly in the same way as in NG MVPN. PMSI Label: - get this label from the EVI/PMSI tab configuration (this is the configured upstream label). ESI Label: - if source PE is operating in active/standby mode (i.e. this bit is 1) then ESI label value is to be set to implicit null (3). - if operating in all-active mode (i.e. bit value is 0) - if source PE is non-DF then ESI label assigned in the ethernet segment for this PE is used to encode the packet. Note this is the configured

EVPN/PBB-EVPN Label Stack and Resolution Procedures	**Ingress Replication**	**P2MP (mLDP or RSVP)**
	learned from remote peer. ESI Label: - if source PE is operating in active/standby mode (i.e. this bit is 1) then ESI label value is to be set to implicit null (3). - if source PE is operating in all-active mode - if source PE is non-DF then packet must be encapsulated with ESI label advertised by remote PE in AD per ESI route. - if source PE is DF then ESI label encoding is not required.	label. - if source PE is DF then ESI label encoding is not required. This ESI label is to be obtained from EVPN Ethernet AD leanred info for corresponding NH and RD set to 0 and tag set to zero.
PBB-EVPN Label Stack	- Tunnel LSP label (Inner Label) - E-VPN ingress replication label obtained from PMSI tunnel attribute advertised by remote PE (Outer Label)	- P2MP label for LSP for which ingress PE is root (Inner Label) - PMSI upstream label (assigned) if enabled in gui (Outer Label)
PBB-EVPN Label Resolution Procedures	Tunnel Label: - get the NextHops from the Multicast learned info for this source PE and obtain the tunnel labels for each of the NextHops from LDP or RSVP-TE P2P whichever is configured PMSI Label: - **same** as in EVPN mode	P2MP Tunnel Label: - get the tunnel identifier from EVI/PMSI tab for mLDP or RSVP-TE and query to LDP/RSVP exactly in the same way as in ngMVPN. PMSI Label: - get this label from the EVI/PMSI tab configuration (this is the configured upstream label).

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**	**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 Technologies Europe Limited** **Clarion House, Norreys Drive** **Maiden Head SL6 4FL** **United Kingdom** **+44 1628 408750** **FAX +44 1628 639916** **VAT No. GB502006125** **salesemea@ixiacom.com**	**Renewals:** renewals-emea@ixiacom.com **Support:** support-emea@ixiacom.com **+44 1628 408750** online support form: http://www.ixiacom.com/support/inquiry/?location=emea
Ixia Asia Pacific Headquarters **21 Serangoon North Avenue 5** **#04-01** **Singapore 5584864** **+65.6332.0125** **FAX +65.6332.0127** **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/**