Black Book

ixia

Edition 10

Network Impairment

http://www.ixiacom.com/blackbook

October 2013

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, 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

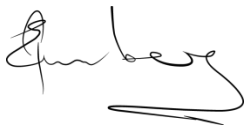
Volume 20 – SDN/OpenFlow

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

Network Emulation

Using Ixia Network Emulators for testing L23 & L47 networks & applications

This book provides use cases where network emulation is used to validate and verify the performance of services, applications, or devices under real world network conditions. Included in this document are pertinent use cases, recommendations, and guidelines for emulating real world networks in a lab test bed.

Introduction

All production networks have unique delays, impairments, and bandwidth limitations that directly impact application performance. Network emulation testing enables you to:

- Predict and characterize the real-world performance of your unique network before deployment
- Avoid costly time to market delays, budget overruns, and customer support nightmares

Without realistic network emulation, you cannot be sure that what you see in the lab is what is available after deployment. Regardless as to which part of the network you may be testing – access, edge, core or applications running across a WAN, the best way to ensure that a network allows for the correct functioning of applications, services or protocols is pre-deployment network emulation testing.

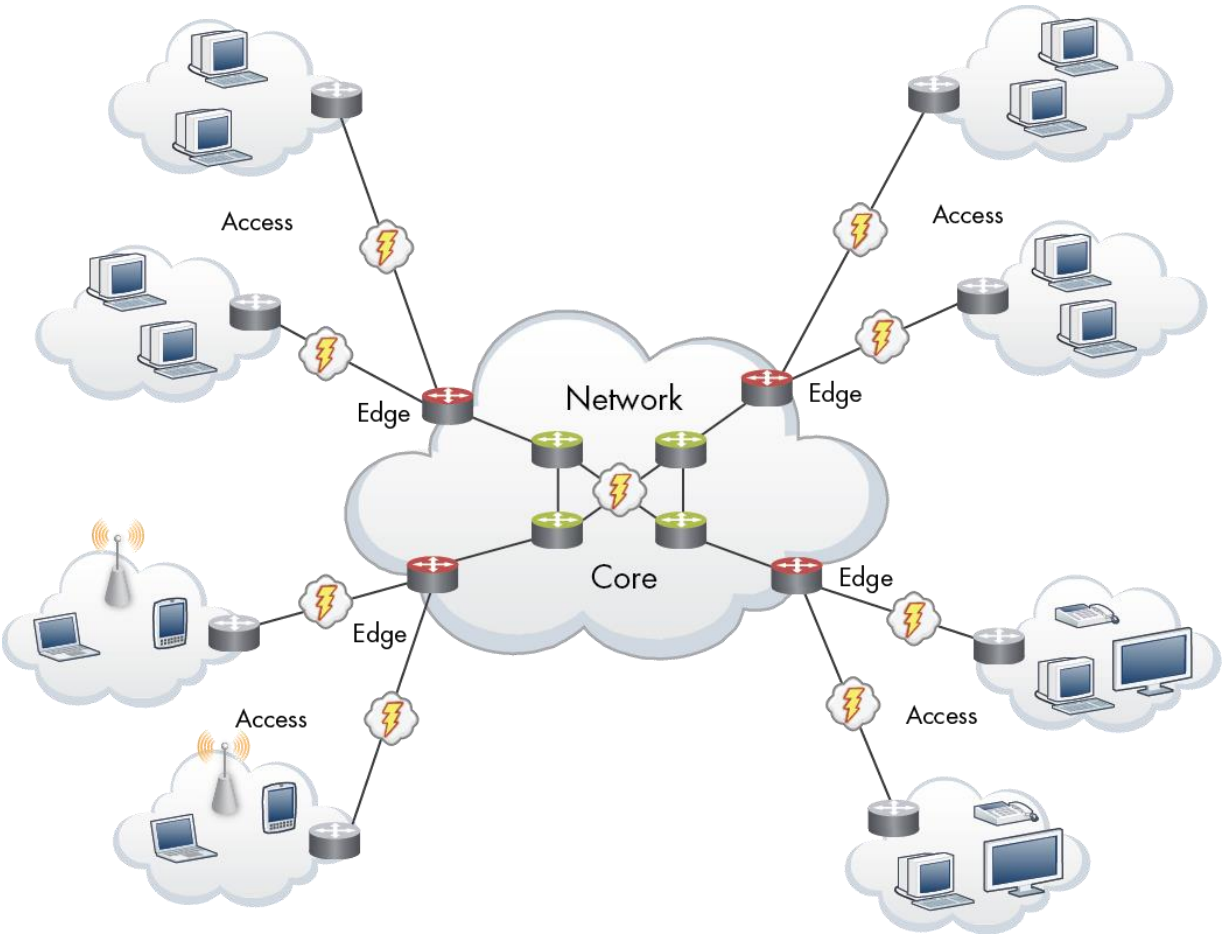


Figure 1. Locations where network impairments can occur

The benefits of network emulation testing using Ixia Network Emulators include:

- Realistic and repeatable network impairment conditions in the lab
- Improved productivity and time-to-test
- Increased reliability of your network, reducing support costs
- Ability to reproduce and quickly resolve issues occurring in the field
- Integration with traffic generation and analysis tools
- Full true dynamic control of impairments (manually or programmatically)
- Multiprotocol (L2-L7) support
- Line rate performance regardless of frame size
- Full APIs for testing automation
- Industry standard test suites and models
- Ability to record and playback live network impairment characteristics
- Preconfigured solutions for a wide range of applications
- High port scalability
- Support for Ethernet, SONET, SDH, OTN, FC, and CPRI

Ixia ImpairNet™ and Ixia-Anue Network Emulators

ImpairNet and Ixia-Anue Network Emulators are Ixia's comprehensive hardware-based impairment solutions that offer ultra-high performance network emulation capability at industry-leading scalability and precision levels.

Conceptually ImpairNet and Anue Network Emulators work by impairing traffic passing through the ports of the ImpairNet Load Module or Anue Network Emulator. These ports are controlled either through Ixia applications or, in the case of Ixia Anue Network Emulators, the ports can be configured through a web interface. Note that there are also Tcl automation features that allow ports to be configured.

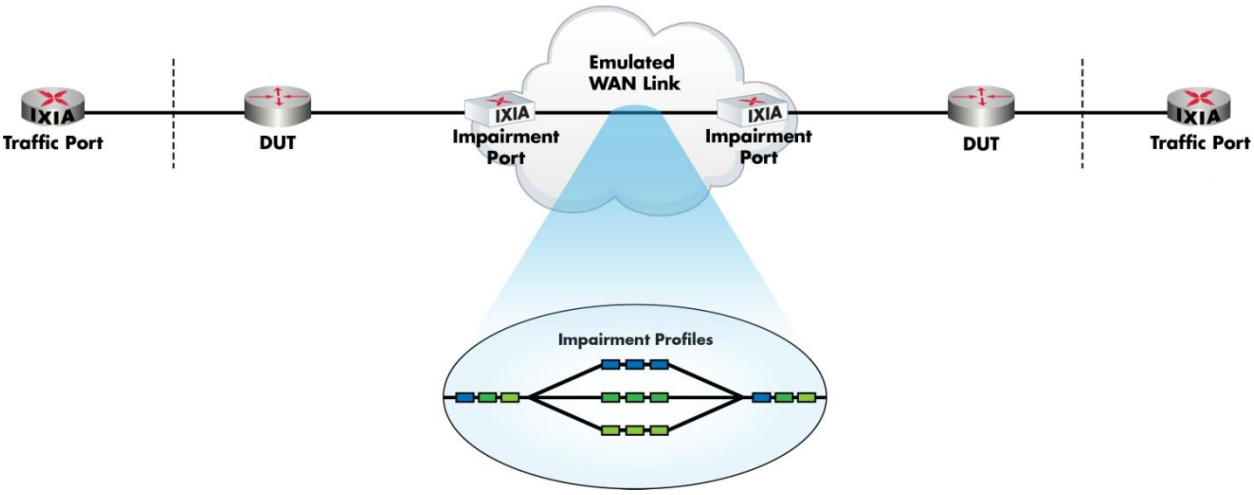


Figure 2. ImpairNet conceptual topology

Packets that pass between the network emulator ports are checked against configured Network Profiles. When a packet matches the classifier of a Network Profile, the impairments configured on that profile are applied to the packet. Keep in mind that all of the above occurs at any packet size up to full line rate.

Note that Ixia load modules (such as IxLoad) can be used in conjunction with ImpairNet. This feature provides unparalleled ease for configuring control plane protocols and traffic loads as well providing integrated statistics that eliminates the need to switch back and forth between multiple applications to look at the control plane, traffic, and impairment statistics separately.

Test Case: Impairment Testing For Layer 3 QoS Mechanisms

Overview

Real world networks suffer from network conditions such as drop, jitter, and delay. To monitor and troubleshoot a network issue, routers and switches provide statistics to measure delay and drops. Service Providers and NEMs need to test that routers and switches are showing reliable statistics.

To test the capability of the router/switch under impaired conditions, an impairment generator is used. The statistics provided by the impairment tool and the router/switch are compared to assess the reliability of the loss and delay measurements. This test case aims to introduce impairment tool setup.

Objective

The objective of this test is to impair the traffic based on precedence value. The traffic will carry packets with precedence 0, 4, and 7. ImpairNet module is configured to selectively drop and delay the packets classified with precedence value.

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

At the end of this test other test variables are discussed that provide more performance test cases.

Setup

Two Ixia ports are used in this example. Traffic is sent from Ixia Port 1 towards Ixia Port 2 with three QoS values configured. The DUT processes the packets based upon the TOS precedence values in the IPv4 headers. Ixia ImpairNet ports are introduced in between the DUT and Port 1.

The DUT is configured to prioritize packet TOS values 7, 4, and 0 (in that order).

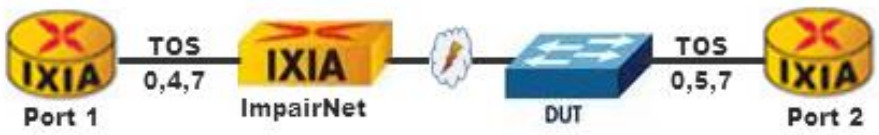


Figure 3. Impairment testing – Layer 3 QoS Mechanism

Step-by-step Instructions

These instructions result in Delay, Jitter, and Drop impairment testing for the Layer 3 QoS topology shown in Figure 3. The steps below guide you to build other impairment test scenarios.

1. Open the IxNetwork GUI (Graphical User Interface), and add two physical ports to the configuration.

2. Under **Protocol Interfaces**, configure two connected protocol interfaces with the following parameters:

IP Type	First IP / Subnet	Mask Width	Gateway	MTU
IPv4	20.1.1.2	24	20.1.1.1	1500
IPv4	20.1.2.2	24	20.1.2.1	1500

Table 1: Summary of protocol interface parameters

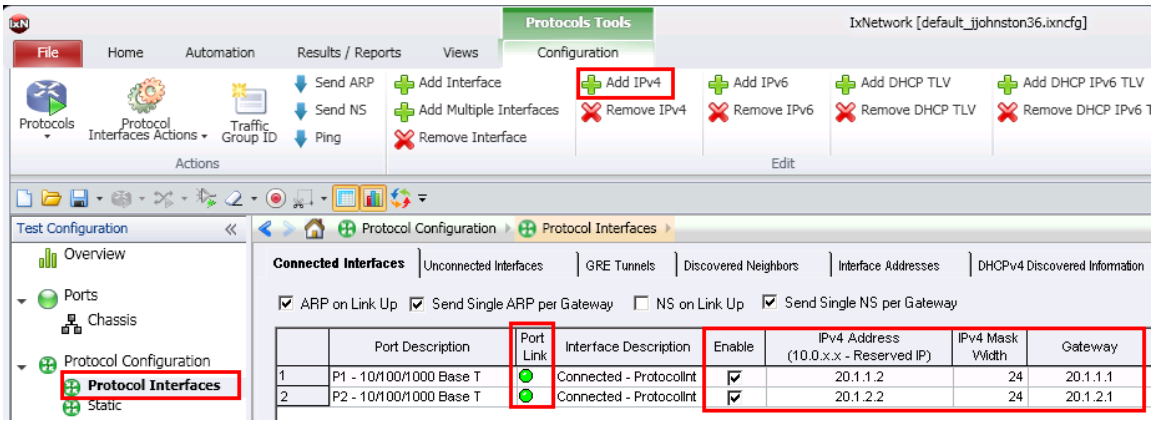


Figure 4. Configuring IP addresses in IxNetwork

Note: The DUT should have the same IP addresses as configured in the **Gateway** column.

3. Click the **Discovered Neighbors** tab to verify connectivity. Send traffic from the Ixia port 1 (IP address 20.1.1.2) to port 2 (IP address 20.1.2.2).

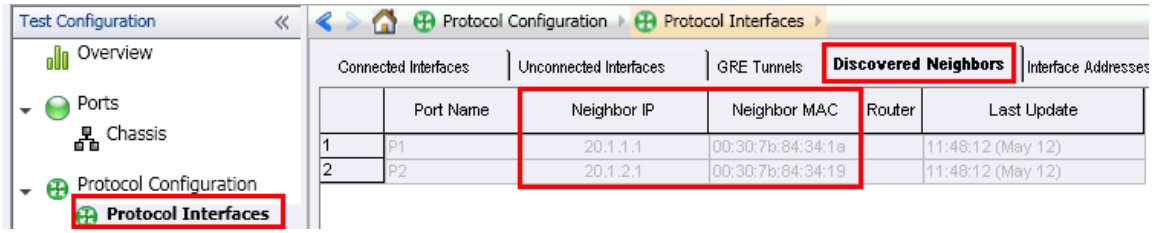


Figure 5. Verifying IP connectivity

4. In the left window, click **Traffic Configuration,** and then start the advanced traffic wizard.

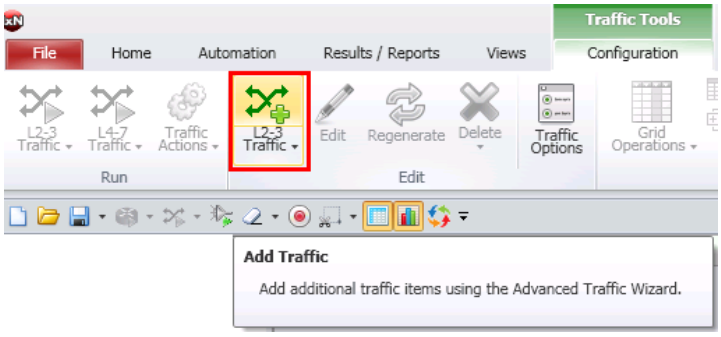


Figure 6. Starting Advance Traffic Wizard

5. In **Source/Destination Endpoints**, select Port 1 as the source and Port 2 as the destination port. Click the down arrow to add the **Endpoint Pair** to the test.

6. Configure the IP priority TOS values of 0, 4, and 7 in the **Packet/QoS** screen.

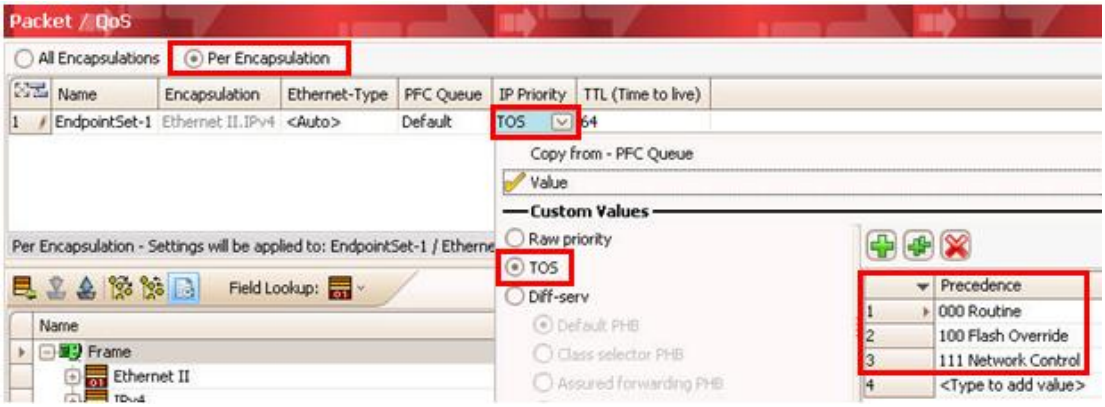


Figure 7. TOS values

7. After configuring the TOS values, create the flow groups. In the **Flow Group Setup** step, select use default distribution option.

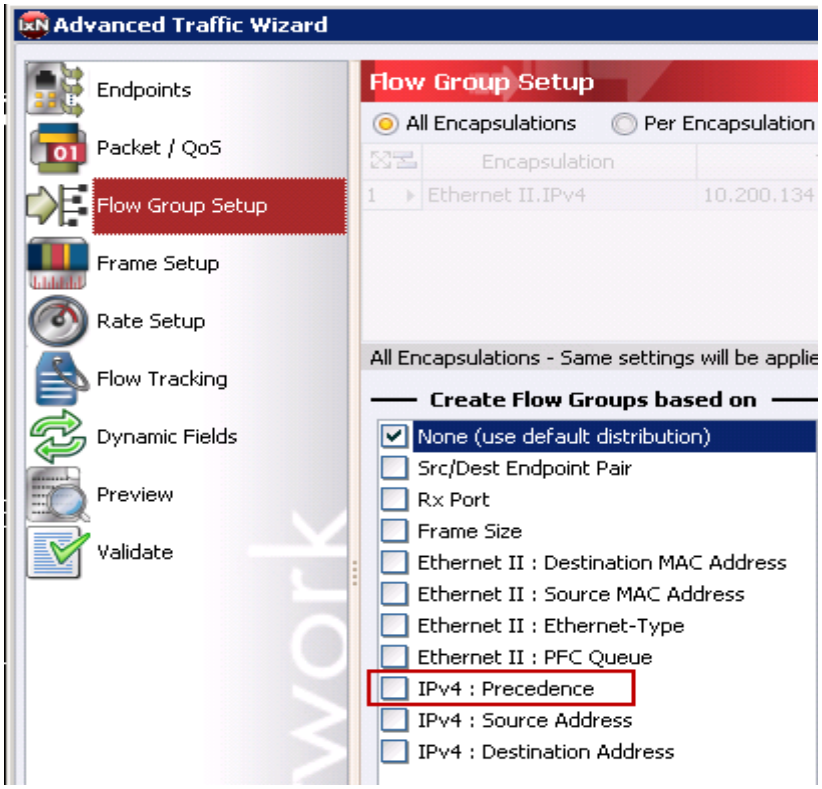


Figure 8. Flow Grouping based on IPv4 precedence

8. In the **Frame Setup**, configure a fixed frame size of 512.

   Note. This dialog also allows you to configure frame parameters such as **Frame Size, Payload**, **CRC Settings**, and **Preamble Size**.

9. In the **Rate Setup**, configure a line rate of 2 percent.

   Note. This dialog allows you to configure the **Transmission Modes** for traffic items and flow groups.

10. In **Flow Tracking**, set the **Track Flows by** value to **IPv4: Precedence**. In addition, also configure **Egress Tracking** for the IPv4 TOS precedence field.

    Note: This configuration tracks the IP Precedence (TOS) field from the DUT ingress and egress side. In some cases the DUT changes the TOS value as traffic flows through the DUT. This happens when the DUT is configured to prioritize certain TOS values over others, and/or to ensure higher priority traffic gets through with low latency and high throughput. This is especially useful in test cases like this, where packet contents are being modified, that are oversubscribing the DUT Egress port.

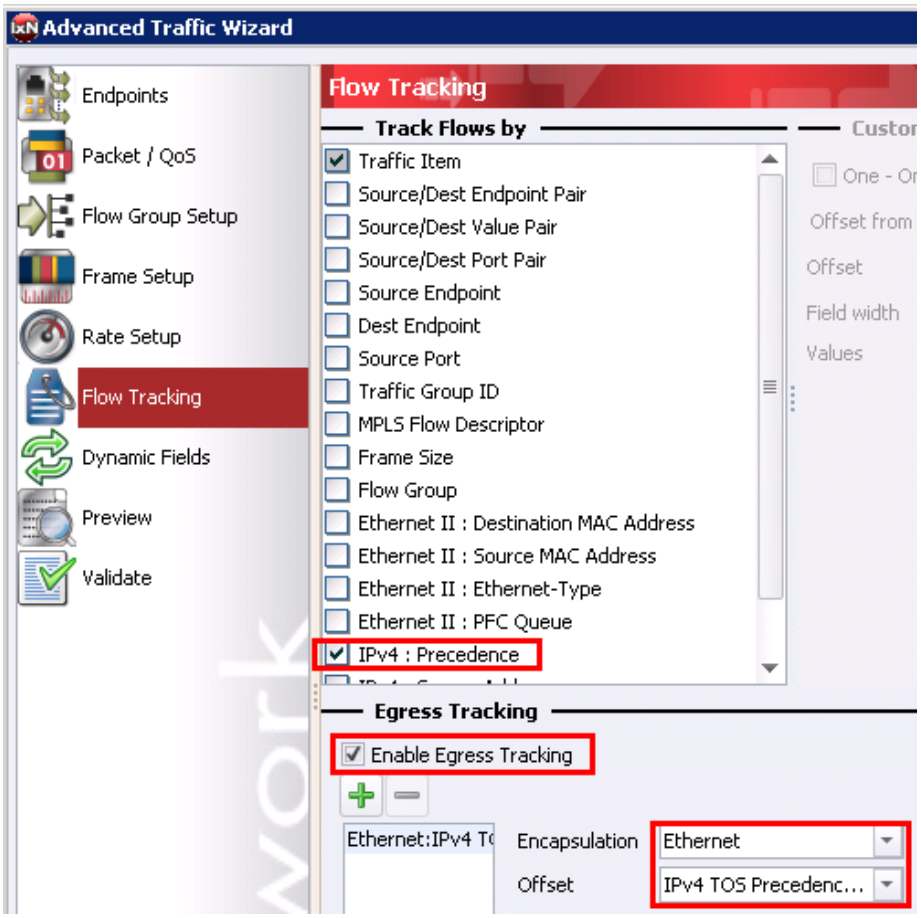


Figure 9. Flow tracking

11. Do not configure or select anything on the **Dynamic Fields** screen.

12. In the preview step, click **View Flow Groups/Packets** to verify that the flow groups are created.

13. The final **Validate** screen is optional. This screen allows you to validate if the settings used in this run of the traffic wizard are correct and gives other useful information such as number of Flow Groups and Flows.

14. Click **FINISH**

15. Apply and start Traffic.

16. Add two impairment ports in IxNetwork configuration. 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.

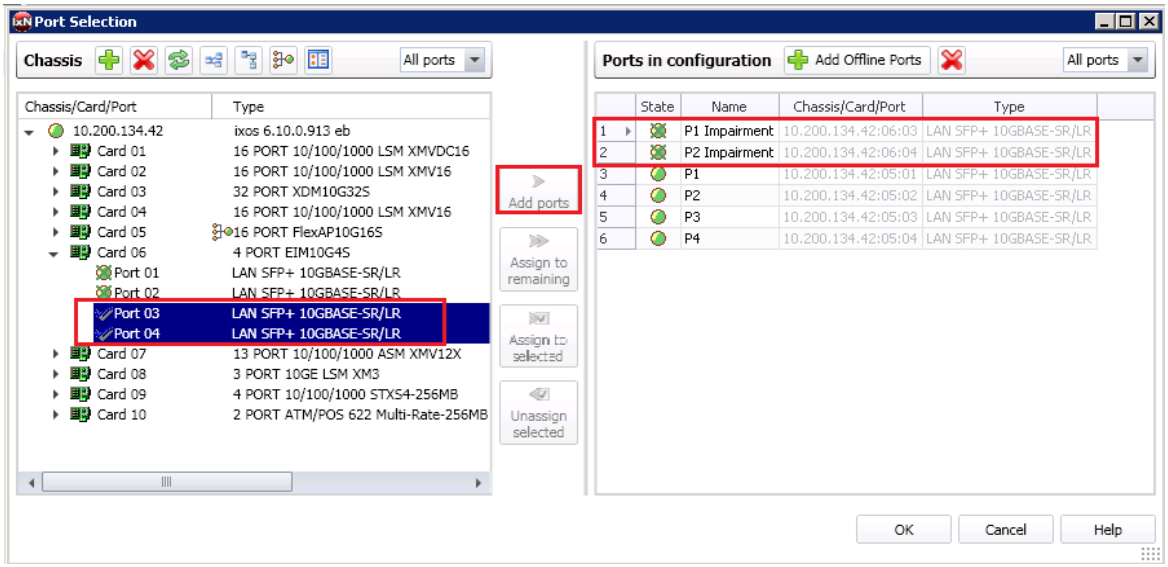


Figure 10. Impairment Port Selection

Optionally, rename the ImpairNet ports for easier reference throughout the IxNetwork application.

Note: ImpairNet ports do not allow for protocol or traffic to be configured on them.

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

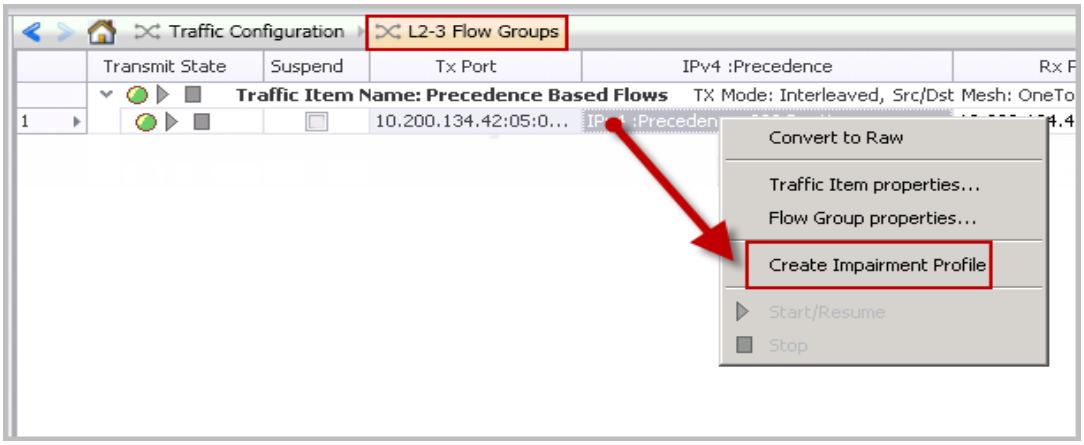


Figure 11. Impairment Profile Creation

Note: The view changes from **L2-3 Flow Groups** view to **Impairments** view after you click **Create Impairment Profile**.

18. The Impairments 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. This view has multiple tabs at the bottom for different impairments.

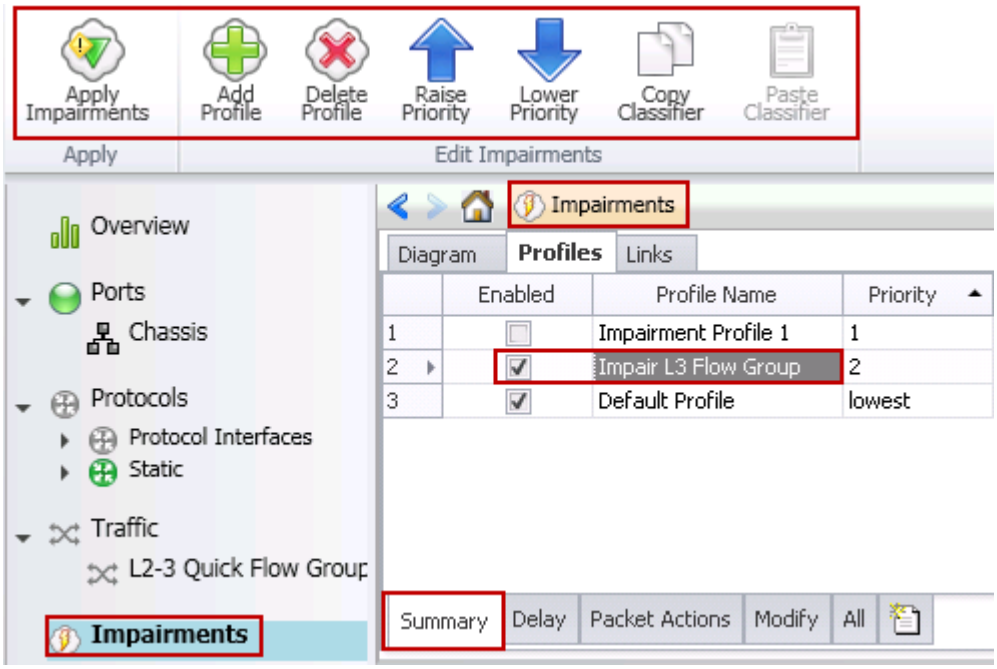


Figure 12. Impairments view

Optionally, change the name of the impairment profile in the Profile Name grid for easy reference.

Note:

- The Impairments view has commands for creation, deletion, and raising or lowering the priority of the impairment profiles.
- The created impairment profile is enabled by default. Each profile has a checkbox to disable or enable it.
- 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.
- By default, there are two profiles created – Default Profile and Impairment Profile 1. Impairment Profile 1 is not enabled. You may leave it as it is or delete it. It has no bearing on this test case. We will leave the profile in screenshots for reference.

19. Click the **Classifier** grid in the **Impairments** -> **Profiles** tab. The **Packet Classifier** dialogue opens.

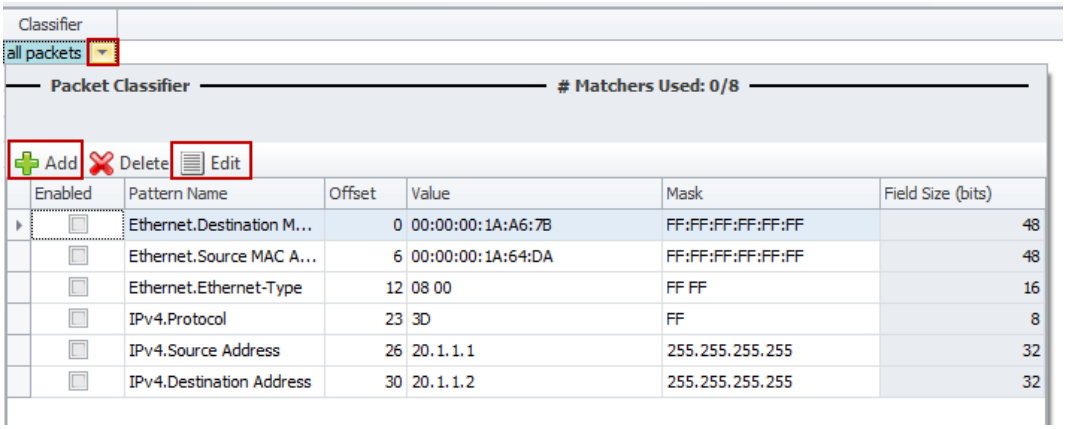


Figure 13. Open Traffic classifiers

20. Click the **Add** icon to add a new classifier pattern. Select **Precedence** in the **Packet Templates Manager** window.

    Note: The selected field offset and size are shown at the bottom for reference. Optionally, remove all of the unused classifier patterns.

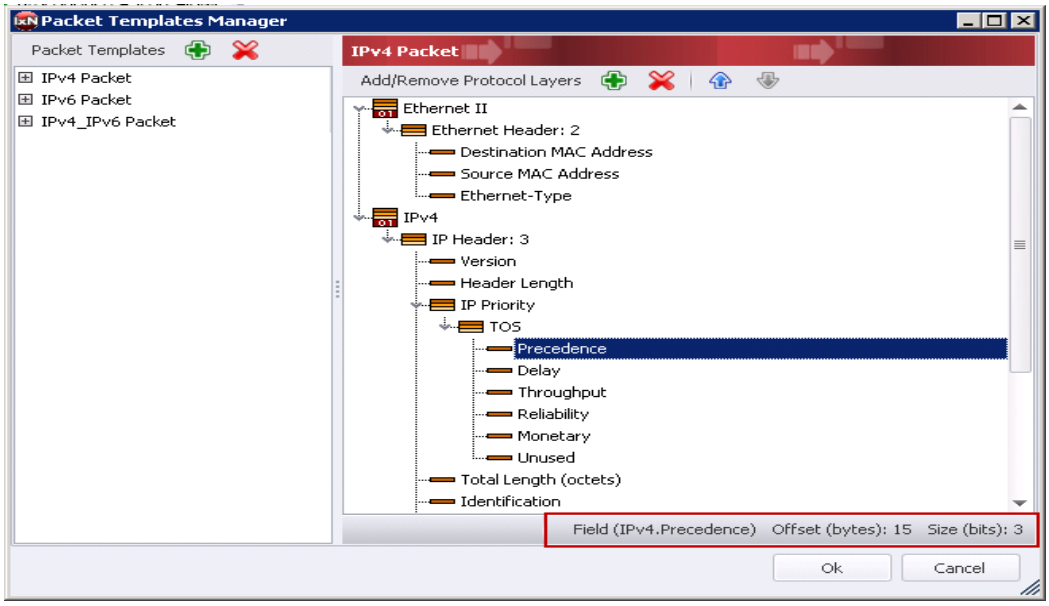


Figure 14. Packet Templates Manager

21. Click **Ok** to close the **Packet Templates Manager** window. The field offset and size are automatically updated in the **Packet Classifier** dialogue.

    The classifier pattern value has hexadecimal format and is aligned to an octet boundary. The unused bits in the value is ignored by using don't care bits in the mask.
    In this test case, the traffic flow with precedence value **00** is impaired. The field size is 3 bits hence the other 5 bits should be ignored. The mask is 1 byte octet value and should be set to **E0**.
    After the classifier is configured successfully, the pattern can be seen in the classifier grid.

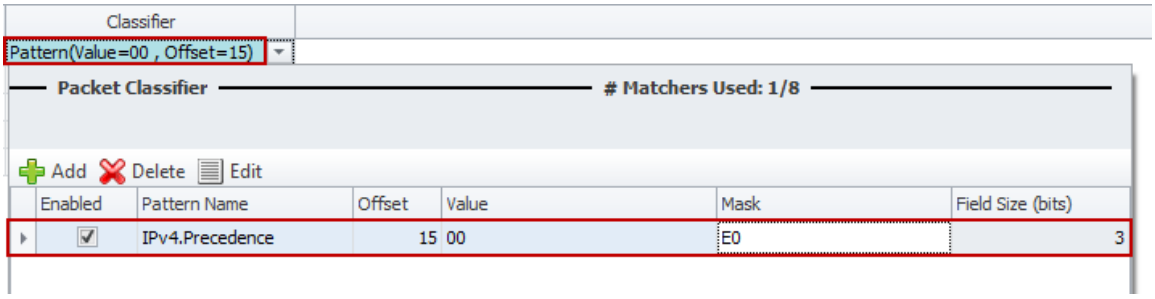


Figure 15. Configure Traffic classifiers

22. Click **Add Profile** icon twice to create two profiles in **Impairments Configuration** ribbon. Optionally, name the profiles.

23. Select the classifier added in **step 9** and click the **Copy Classifier** icon. You can paste this classifier across multiple impairment profiles. Select the profiles created in **step 10** individually and click **Paste Classifier** icon.
24. Edit the classifier to impair traffic for Precedence values 4 and 7. Only the value should be changed in the classifier.

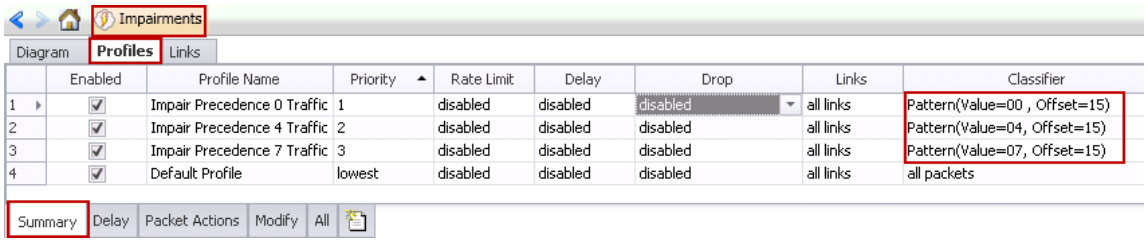


Figure 16. Copying Traffic Classifiers across impairment profiles

25. Each impairment port pair has two links that denote the direction of traffic flow between the two impairment ports. Right click the **Links** grid of the desired impairment profile. Select the link so that the traffic flowing through the DUT is impaired. Configure the links for the other two profiles.

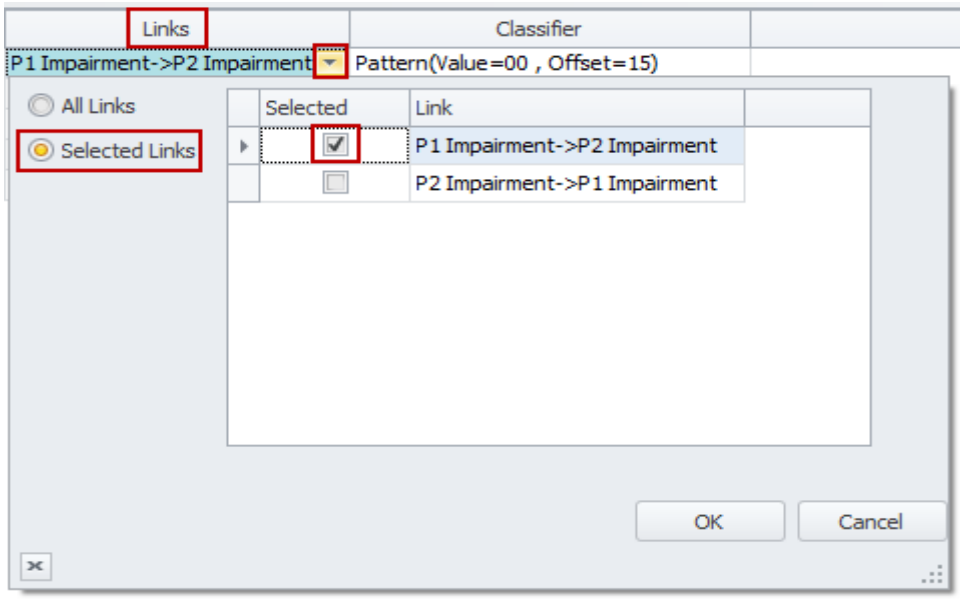


Figure 17. Impairments Link Selection

26. Click the **Drop** grid of the first impairment profile. Select the **Enabled** checkbox and enter the drop percentage as *50%*.Configure drop for the second and third profiles similarly.

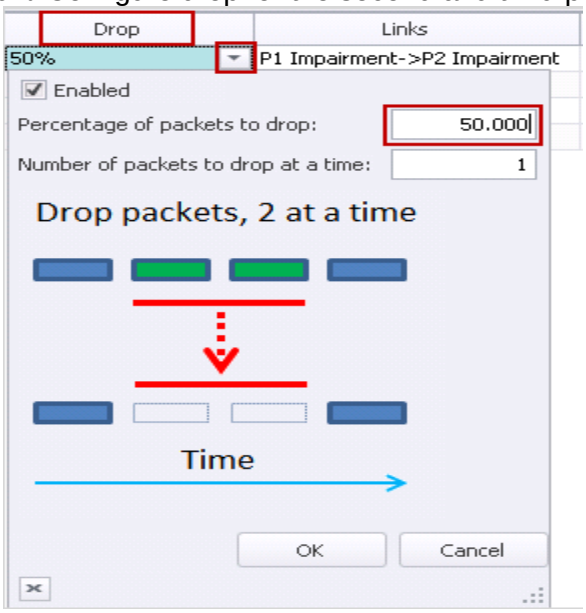


Figure 18. Drop Impairment Configuration

27. To configure delay and jitter impairments, change the bottom tab to **Delay**. To configure **Delay** and **Delay Variation** impairments, in **Impairments** -> **Profiles** tab, select the impairment profile and click the **Delay** grid. Select the **Enabled** checkbox and enter the delay as *300 microseconds.* Click **OK.**

28. Similarly configure delays for the second and third profiles.

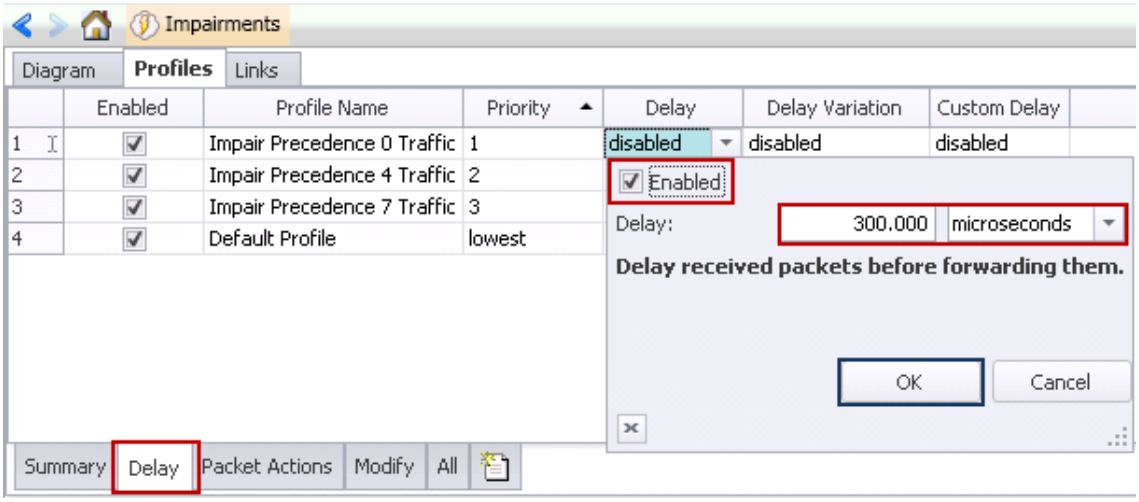


Figure 19. Delay Impairment Configuration

29. Select the impairment profile and click the **Delay Variation** grid. Select the **Enabled** check box and select the *Gaussian* as the delay variation. Enter *10 microseconds* as the value of **Standard Variation** as shown in the figure below. Similarly configure delay variation for the second and third profiles.

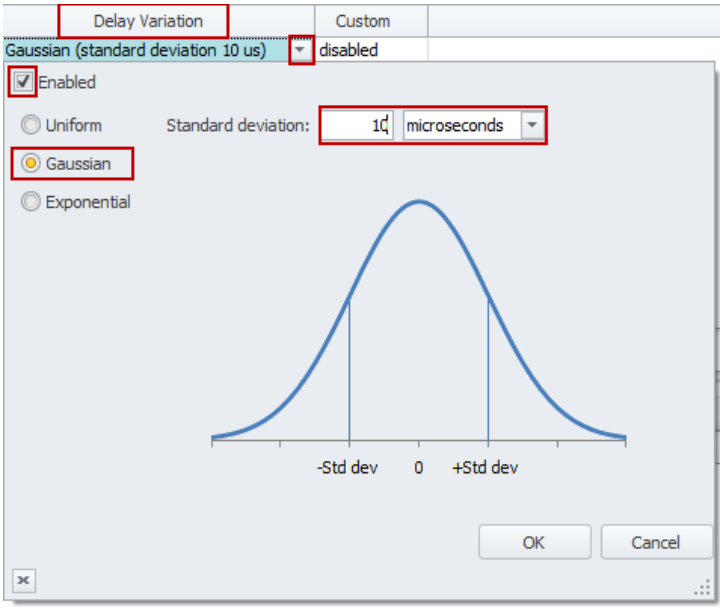


Figure 20. Delay Variation Impairment Configuration

30. To apply the impairment profile in the hardware, click the **Apply Impairments** icon in the **Configuration** ribbon. See the figure below. Only the enabled profiles are applied to the hardware. If applying impairment profile changes is successful, then the exclamation mark on the **Apply Impairments** icon disappears.

Figure 21. Apply Impairments Icon Change

Note: If the impairment profile contains configuration errors, then the exclamation mark is visible and an error notification pop-up appears on the right hand side bottom corner of the IxNetwork GUI. For further troubleshooting, follow the instructions in the Troubleshooting Tips section.

31. After applying impairments, the sytem initiates to update impairment statistics. Select **Impairment Profile Statistics** and click the **Dropped** tab at the bottom in the **Impairment Statistics** view as depicted in the following figure.

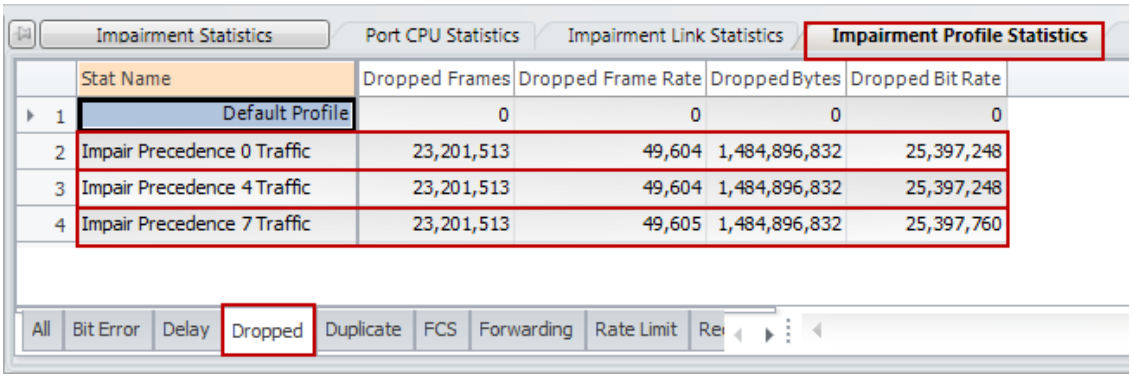


Figure 22. Drop Impairment Profile Statistics

Only the profiles with drop impairment enabled drop the packets as seen above. Check that the packets are dropped as per the configured rate.

32. To check the dropped packet statistics for each link direction, select **Impairment Link Statistics** tab in the **Impairment Statistics** view. Select **Dropped** tab at the bottom as shown in the following figure. Note that the link drop statistics are aggregate of the profile drop statistics.

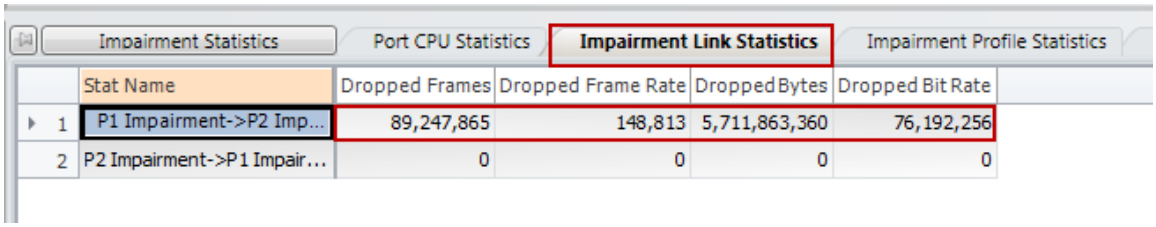


Figure 23. Drop Impairment Link Statistics

33. Select **Impairment Profile Statistics** tab and select the **Delay** tab.

Note: The Delay Values will vary based on the traffic flowing through the ImpairNet module and inter packet gap.

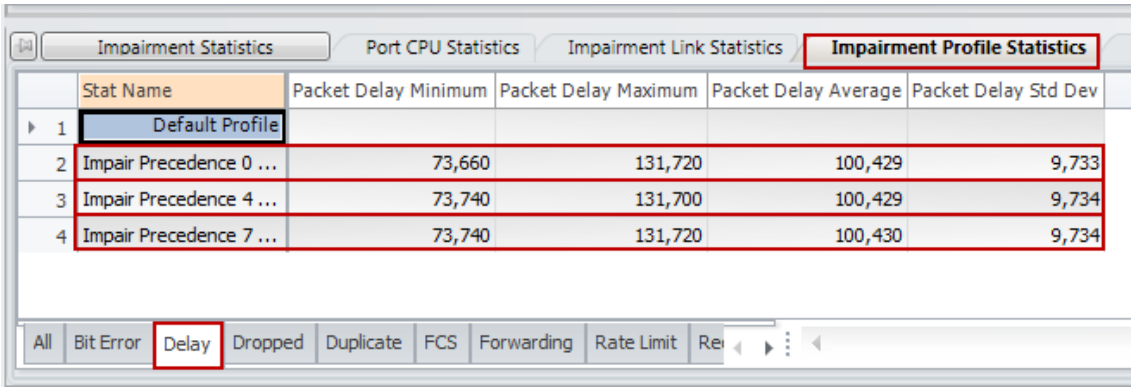


Figure 24. Delay Impairment Profile Statistics

34. Click **Impairment Link Statistics** tab, and then click the **Delay** tab.

Note: The **Link Delay** Statistics shows the aggregated delay for all the traffic flowing through this link and varies from the impairment profile statistics.

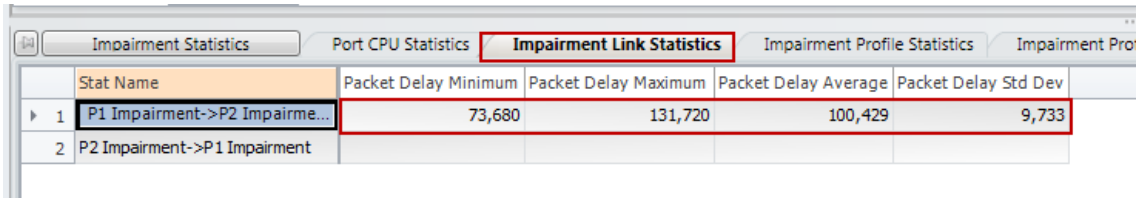


Figure 25. Delay Impairment Link Statistics

Test Variables

You can use each of the following variables in separate test cases to test the DUT. They use the test case detailed above as a baseline, and modify a few parameters in the same Impairments view. You can create various scalability tests to fully stress the DUT's capability as a PE router operating in presence of real world network impairments.

Performance Variable	Description
Apply multiple profiles	Figure 26. You can create up to 32 bidirectional or 64 unidirectional impairment profiles per impairment load module.
Use multiple classifiers	**Figure 27.** 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 **Impairments Configuration** tab. A maximum of 16 classifiers can be added for each link direction.

Performance Variable	Description
Apply impairments in both link directions	**Figure 28.** You can select to impair either one or both the links.
Apply different drop rates	**Figure 29.** Apply drop rates from 0-100% in clusters, to a maximum of 65535 packets.
Apply different packet impairments	**Figure 30.** Apply, reorder, and duplicate BER impairments in addition to drop impairment. Reorder and duplicate impairments are present in the **Packet Actions** tab.
Increase Delay	Figure 31. Introduce delay to a maximum of 6s for every impairment profile on a 1G impairment module and to a maximum of 600 ms for a 10 G impairment module.
Apply different kind of delays	Figure 32. Introduce delay in us, ms or km. 1 km of WAN Link cause a delay of 5 us.
Apply different delay variations	Figure 33. You can apply uniform, exponential, and customized delay variations.

Results Analysis

The test verifies that drop and delay impairments can be introduced in the traffic stream based on precedence based traffic classifiers. The impairment profiles are independent of each other and each traffic flow is impaired independently. You can use the drop and delay measurements to verify the statistics report generated by the DUT.

Troubleshooting Tips

Issue	Troubleshooting Solution
Impairment profiles are enabled but impairment statistics are not updated.	Figure 34. Check that the **Apply Impairments** icon does not have any error mark. Check that the traffic is flowing and the drop rate is not configured to *100%* for all the profiles.
No traffic is flowing through the impairment links.	Figure 35. Disable all the impairment profiles except default profile. Make sure that the default profile is not set to *100%* drop. Apply Impairments, and check that Rx/Tx Frames statistics for the impairment link correspond to the traffic. Also, check that both the links for the impairment port pair are forwarding, that is, in the **Links** tab, clear the checkbox for **Interrupt Forwarding**.
An error window pops up in the right hand side bottom when **Apply Impairments** is clicked.	Figure 36. Check for impairment profile configuration error. Ensure that the impairments are applied with in the configuration limits.

Issue	Troubleshooting Solution
	Check ImpairNet module specifications for the configuration limits.
Traffic is not impaired though the Apply Impairment icon is not showing any exclamation mark.	Figure 37. Check that the classifier value, mask and offset are set correctly. Also ensure that a profile with more generic classifier does not have a higher priority than that of the desired impairment profile. Also ensure that the **Enabled** checkbox is selected for the configured impairments.

Conclusions

This test explains how to impair traffic based on a particular packet field (Precedence). You can easily create impairments for other fields to test the DUT's capability to generate accurate statistics report

.

Test Case: Impairment Testing - Drop and Delay CCM Messages

Overview

CCM messages play an important role in delay and loss measurement. This is achieved by adding sequence number and timestamp to the CCM messages. If the CCM messages are impaired by the underlying E-Line service or MPLS-TP based transport network, the network device can measure the loss and delay based on CCM messages received. It is important to validate that the network device is measuring the loss and delay of CCM messages accurately, because the loss and delay reported by these devices are used to monitor the performance of the network.

The following sections explain how to configure Ixia's ImpairNet module to introduce drop, delay, and jitter impairments in the CCM messages.

Objective

The objective of this test is to introduce drop, delay, and jitter in the CCM messages flowing through the ImpairNet module.

Though the focus of this test is to impair CCM messages, you can apply the same procedure to impair other OAM messages and Ethernet/VLAN Traffic.

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

Setup

The setup is similar to the setup in the previous test case except that an impairment module is inserted between the Ixia test port and Ethernet CFM DUT.

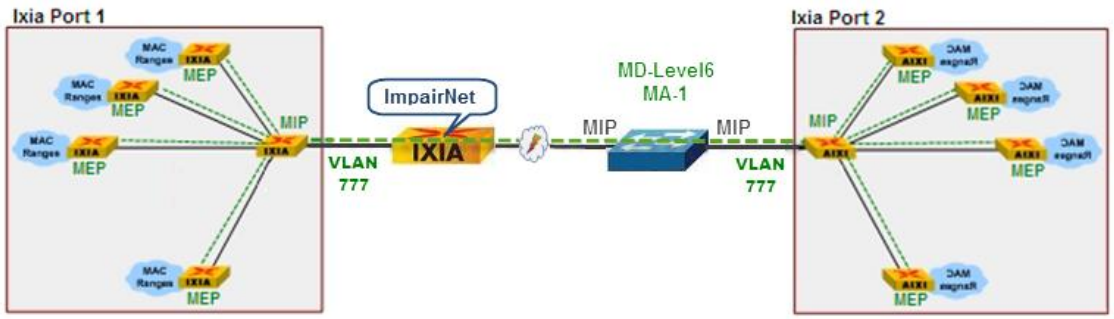


Figure 26. Impairment testing – Drop and Delay CCM Messages

Step-by-step Instructions

The instructions provided in this section helps to perform Delay, Jitter, and Drop impairment test for the CFM topology. You can use the steps below as a guide to build other impairment test scenarios.

1. Click 

to reserve two ports.

2. Launch the **CFM/Y.1731 Wizard** and select the ports reserved in the previous step.

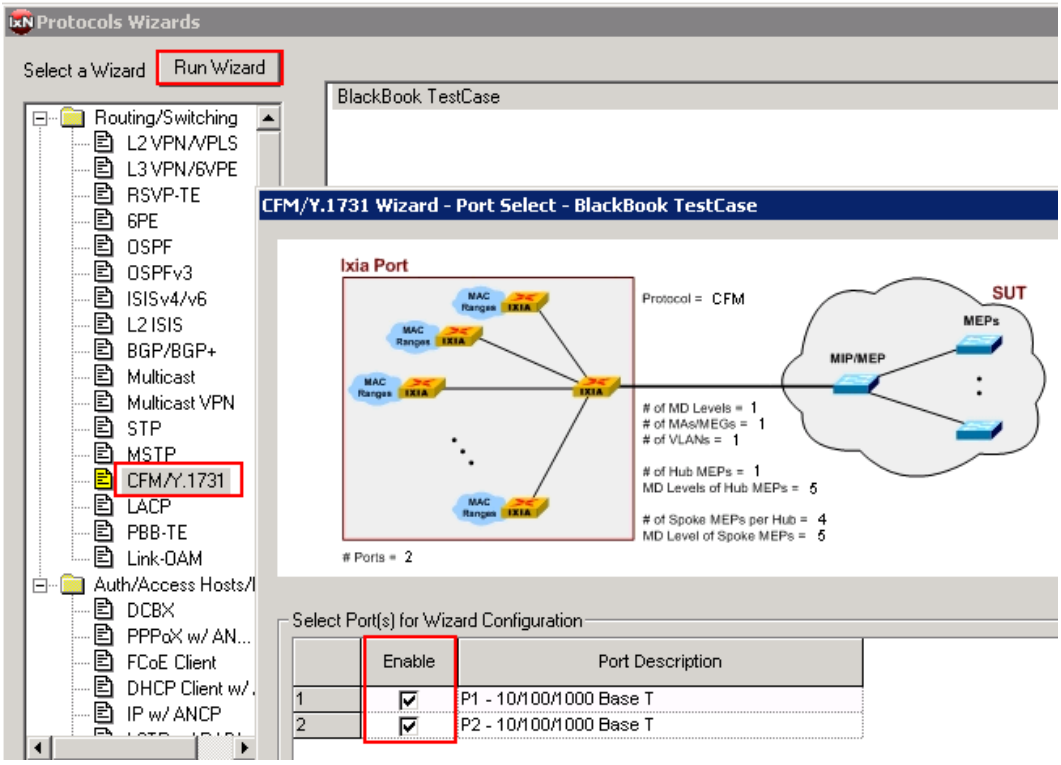


Figure 27. Launch CFM/Y.1731 Protocol Wizard

The **Operation Mode** window configures the protocol, Topology type, and Maintenance Association (MA).

3. Change the **CCI Interval** to *3.33ms*. This action verifies that the DUT can handle the fastest rate for Continuity Check messages for all 8 Endpoints (MEPs). This number needs to match the DUT.

4. Change the **Short MA Name** to *MA-1*. If the **Increment Short MA name** remains unchecked, then all configured MEPs belong to the same service.

5. Optionally:

   Change the **Operation Mode** to *Y.1731.* The wizard changes slightly to match the technology described in Y.1731, however it is very similar (actually a superset) to CFM. Change the **Topology type** to *Tree Topology.* The picture and wizard changes to match. See the Ethernet CFM Application note at http://www.ixiacom.com/solutions/testing_carrier_ethernet for more information on the tree topology.

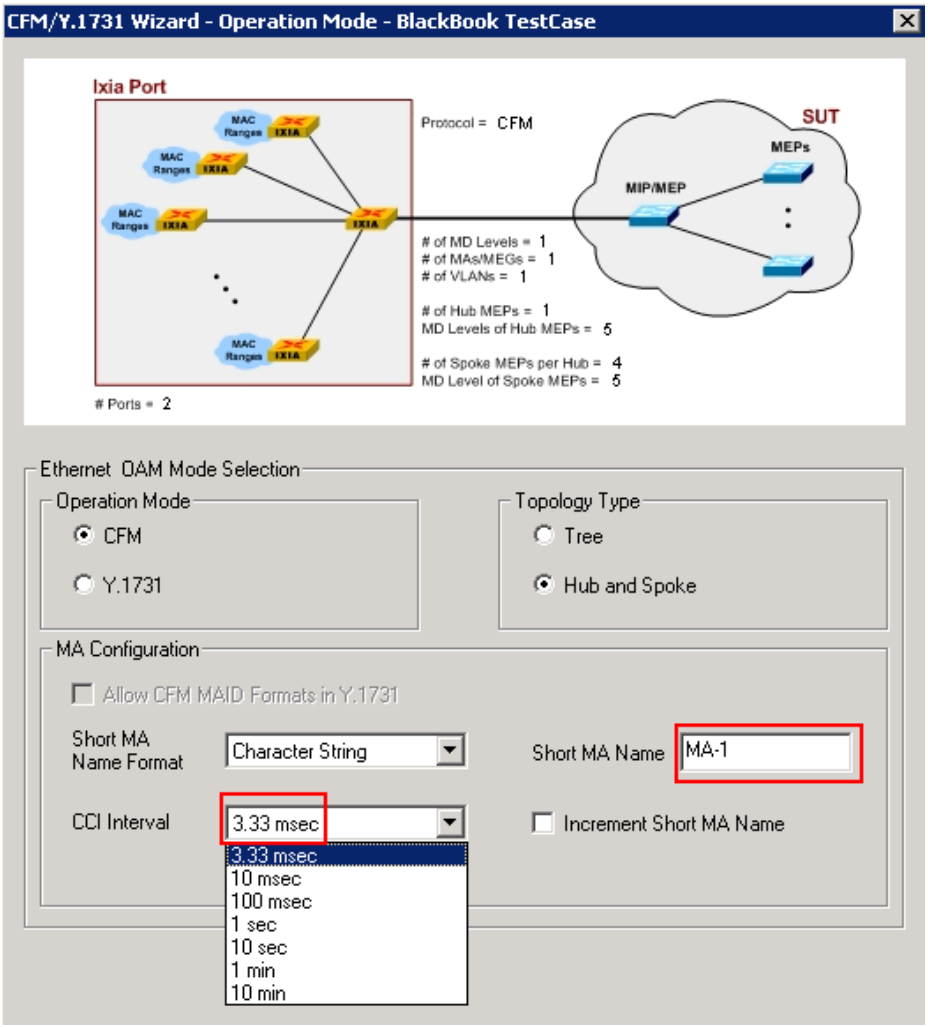


Figure 28. CFM/Y.1731 Protocol Wizard

The **CFM Topology Type** window configures the MAC addresses and number of MEPs to be used.

6. Change the **Number of Spoke MEPs per MIP** to *4.* This action creates a topology the same as shown in the figure, below.

7. Optionally, configure the Starting MAC address and MEP ID/Step as desired.

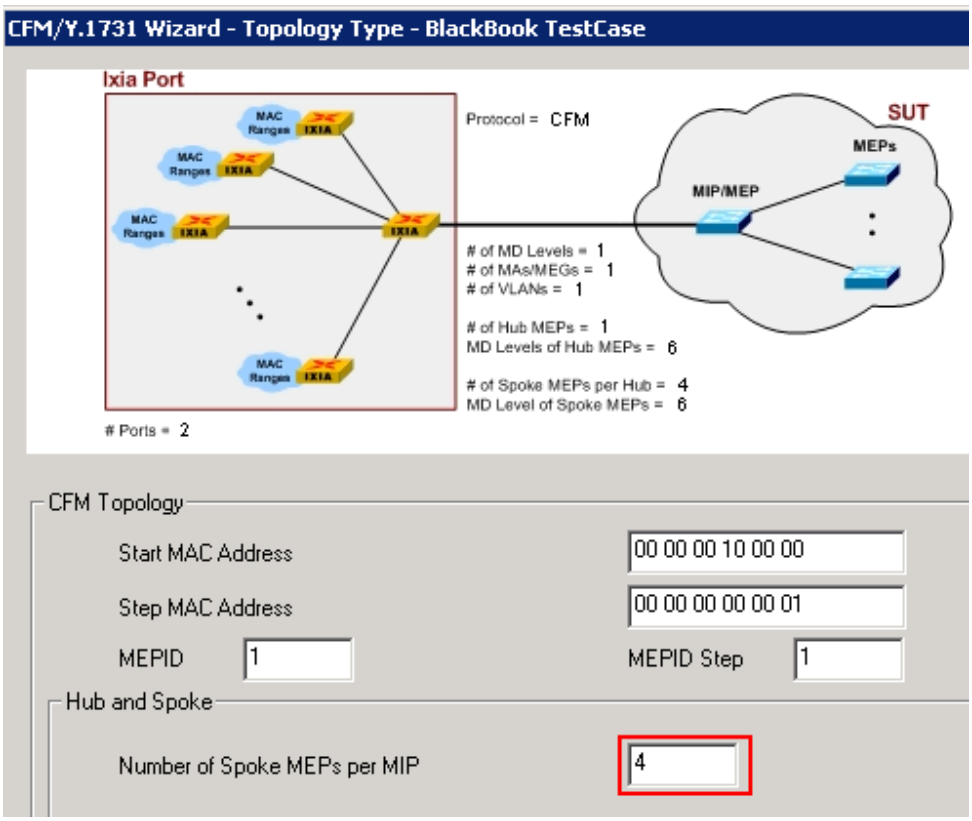


Figure 29. CFM/Y.1731 Protocol Wizard

The **CFM MD Level** window configures the number of Maintenance Domain (MD) levels to use, their *name* and Level ID.

8. Change the **MD** Level ID to *6* as shown in the Setup section of this test case. This number must match the DUT.

9. Change the **MD name** to *MD-Level6* as shown in the Setup section of this test case.

10. Optionally, change the number of MD Levels to greater than 1 to create multiple Management Domains within the same wizard run. You can then configure each one for its MD Level ID and MD Name.

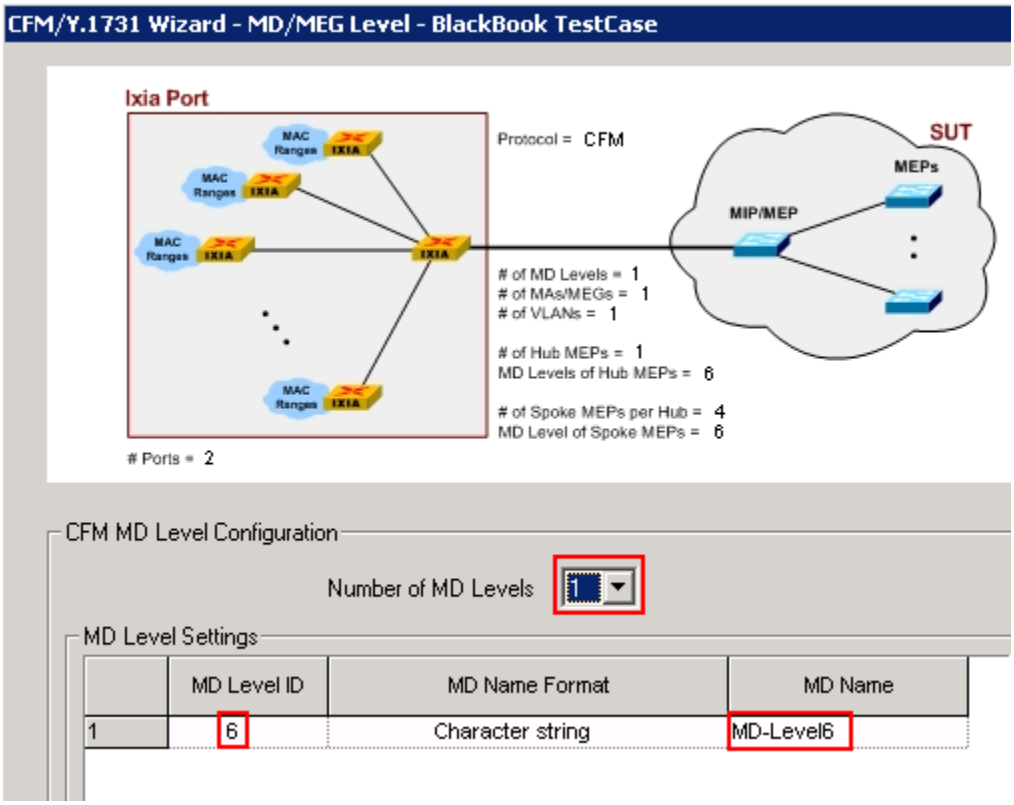


Figure 30. Link CFM/Y.1731 Protocol Wizard

The **CFM MD Level assignment** allows each level of the Topology tree to be configured at different MD level.

- Note at **Topology Depth 1**there are no MEPs. This represents the MIP at the front of the Ixia port. This is also depicted in the Setup section of this test case.
- Note at **Topology Depth 2** there are 4 MEPs. This represents the MEPs at the back of the Ixia port (using the Tree Topology). This is also depicted in the Setup section of this test case.

11. **Optionally**, if multiple MD Levels are configured, you can change the MD Level ID here. In some cases IxNetwork may not allow ascending or descending numbers, as described in the standard.

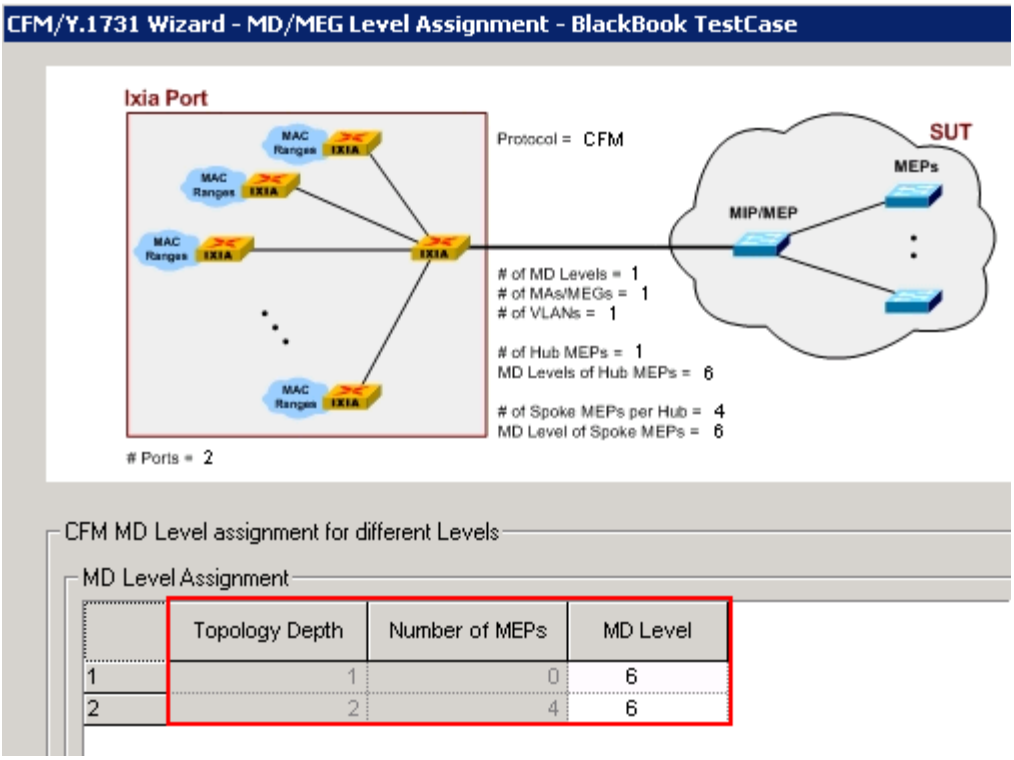


Figure 31. CFM/Y.1731 Protocol Wizard

The **MAC/VLAN Configuration** page allows VLANs, QinQ, and Traffic Sources and Destinations to be configured.

12. In most cases check the **Enable VLAN.** This action encapsulates the CFM messages over a VLAN.

13. Choose **Single VLAN** or **Stacked VLAN (QinQ)**. This action adds S-VLANs and C-VLANs respectively. In this case use VLAN *777*

14. Optionally, configure the VLAN Priority.

15. **Optionally:** check the **Enable MAC Range** to create Source and Destination **MAC Ranges** in the CFM Protocol grid. The MACs show up as Sources and Destinations in the traffic wizard when using the Ethernet/VLAN encapsulation.

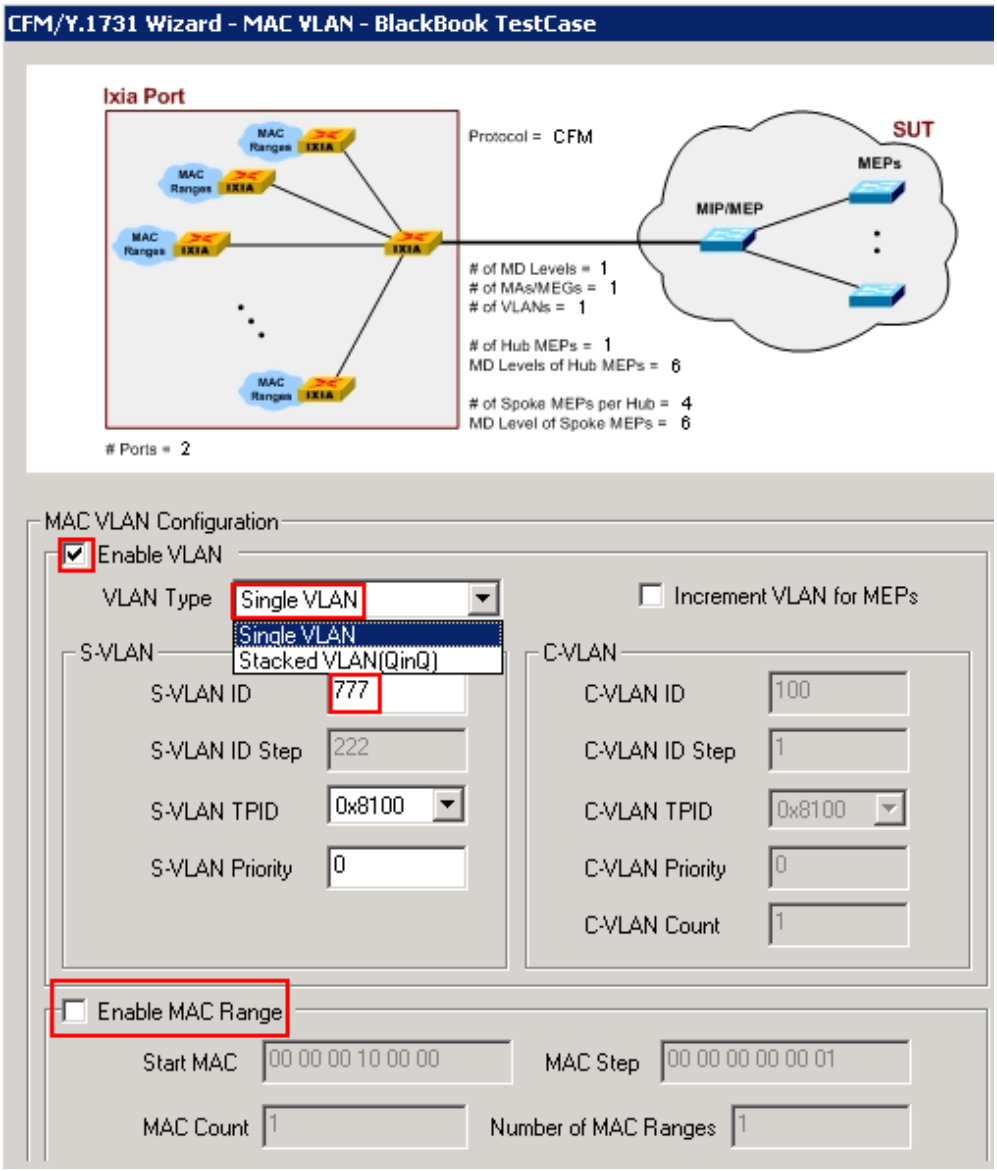


Figure 32. CFM/Y.1731 Protocol Wizard

16. On the last screen of the **CFM/Y.1731** wizard (figure 45), assign a meaningful name and then select either option 3 or 4 to save and overwrite the configuration to the IxNetwork GUI.

    Note: The diagram in the upper panel displays the configuration details. See how this matches the Topology setup for this test case.

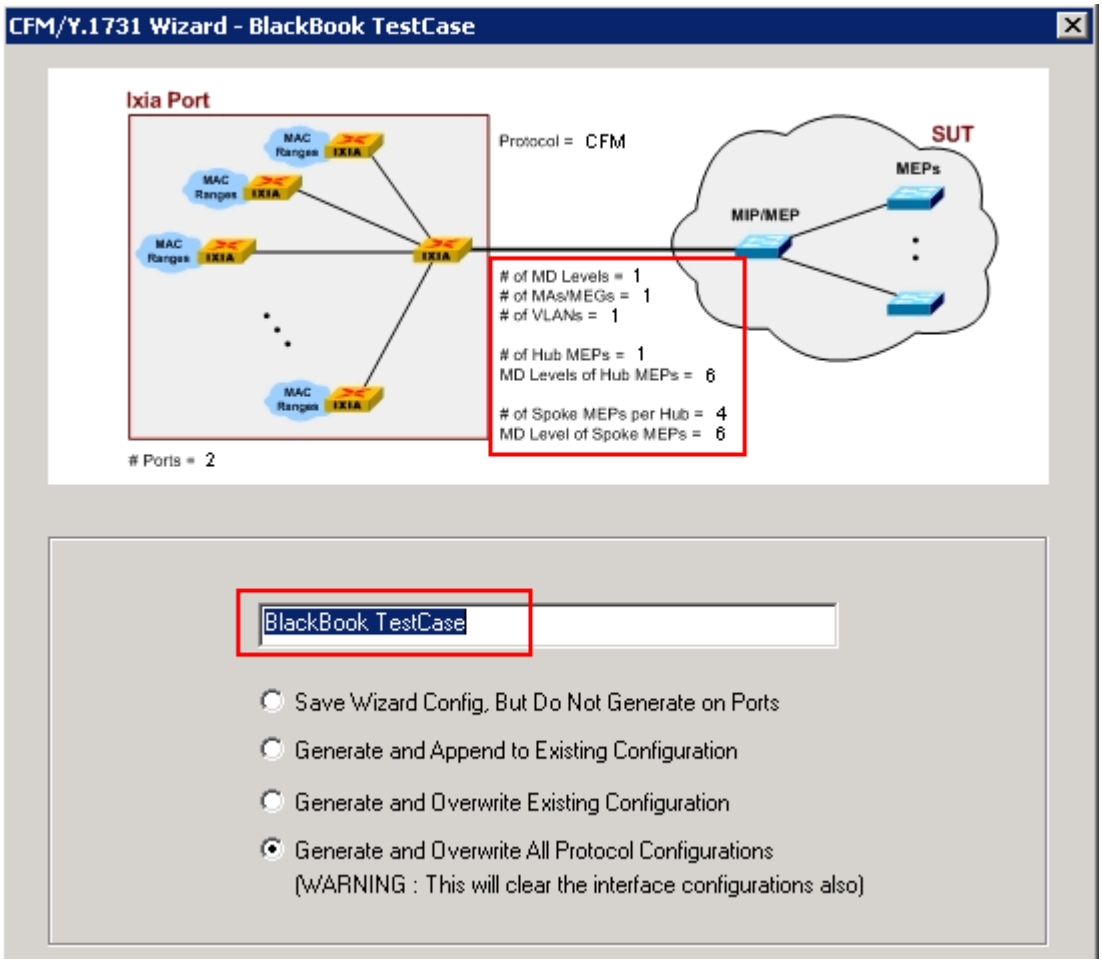


Figure 33. CFM/Y.1731 Protocol Wizard

Once the configuration is complete using the wizard, you can navigate to the main GUI to start the protocol, make protocol-specific changes, and observe DUT behavior. You can achieve many functional verifications using this method. Below are a few examples that show how to achieve specific test objectives relating to CCMs

17. Start the CFM Protocol on both ports. 

18. View the CFM **Learned Info – CCM DataBase** on each port to see what is coming from the neighbor MEPs (in this case from Port2).

    - If there are many MDs, S-VLANs, or C-VLANs configured, use the **Advanced Filter** options to only show the MEPs of choice.

    - Verify there are no Alarms (RDI, Defects, AIS).

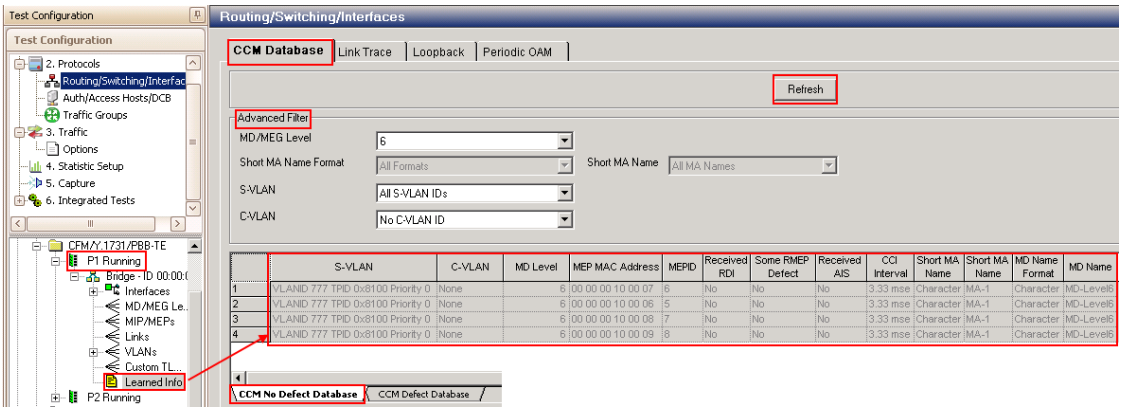


Figure 34. Viewing Learned CCM Info.

19. 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 pair of ports.

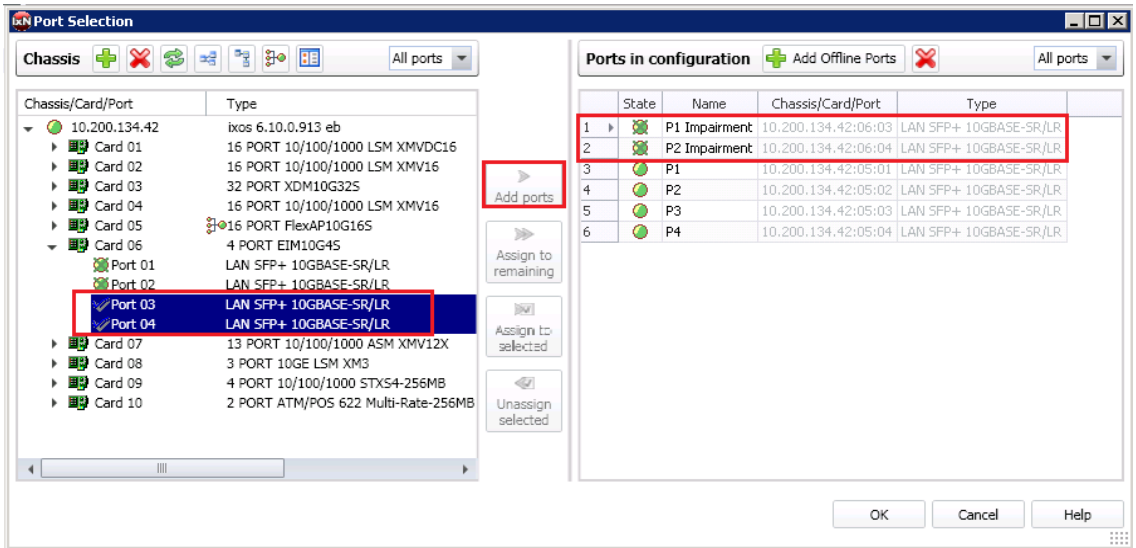


Figure 35. Impairment Port Selection

Optionally, rename the ImpairNet ports just like any other test ports for easy reference throughout the IxNetwork application.

20. Click the **Impairments** icon on the **Test Configuration** pane to switch to the Impairments view. Select the **Profiles** tab.

    Click **Add Profile** to create an impairment profile.
    Notes:
    a. The exclamation mark on the **Apply Impairment** icon indicates that the previous impairment profile changes are not applied to the hardware.
    b. By default, there are two profiles created – Default Profile and Impairment Profile 1. For the purpose of this test, Profile 1 is not used, so it stays disabled.

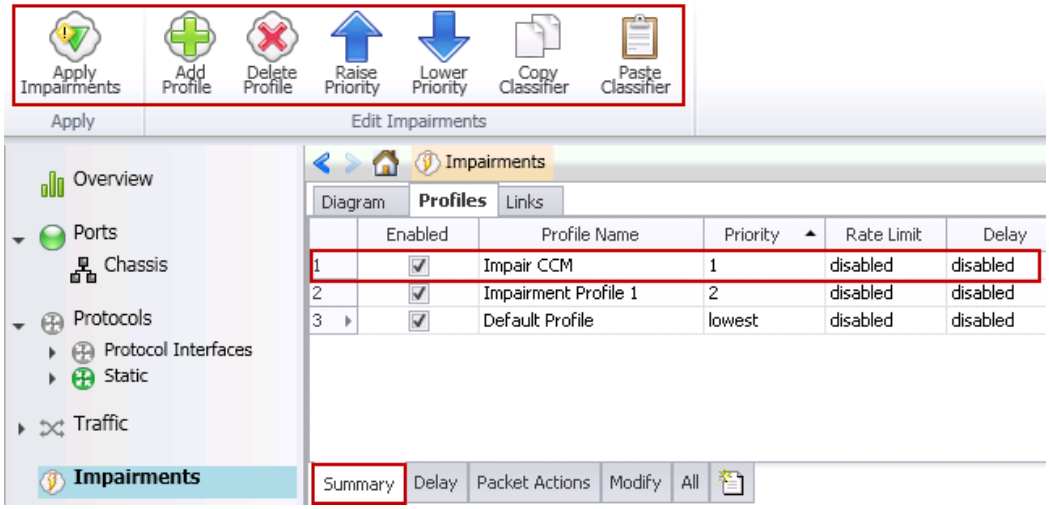


Figure 36. Impairments view

Optionally, click the **Profile Name** grid to change the name of the impairment profile. The profile has been named *Impair CCM* here.

Note: Each profile has a checkbox to enable or disable the profile. You cannot disable the impairment profile *Default Profile*.

Optionally, you can create impairment profile for the Ethernet/Service Traffic. Switch to the L2-3 Flow Groups view. Select the traffic flow group, right click, and select **Create Impairment Profile** from list.

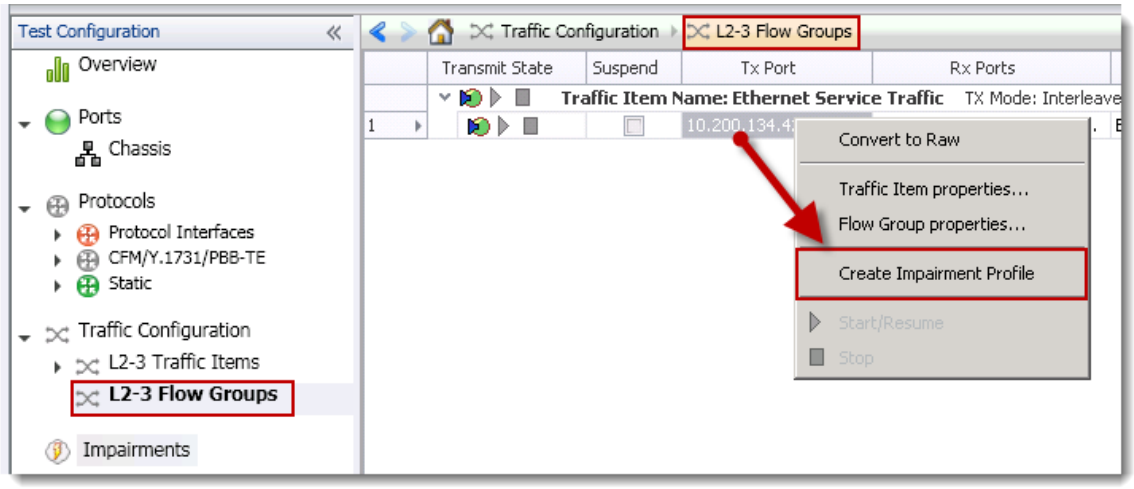


Figure 37. Create Impairment Profile from Traffic

Creating impairment profile directly from the traffic flow group has the advantage that all the L2-3 traffic classifiers are automatically added to the traffic classifier for this profile. This saves time and effort spent on creating Classifiers.

Note: After creating the profile, the view automatically switches to Impairments view.

21. Click the **classifier** grid of the *Impair CCM* profile. The classifier pattern value has hexadecimal format, and is aligned to an octet boundary. The unused bits in the value are ignored using ‘don’t care bits’ in the mask.

    Click the **Add/Edit** icon to open **the Packet Templates Manager**. Add the Ethernet -> VLAN -> CFM protocol layers and select **CFM Op Code**. Set the Op code value to *01* and mask to *FF* in the Packet Classifier.
    Note: The offset and field-size values are already set when you select the field from **Packet Templates Manager**. Select the classifier.

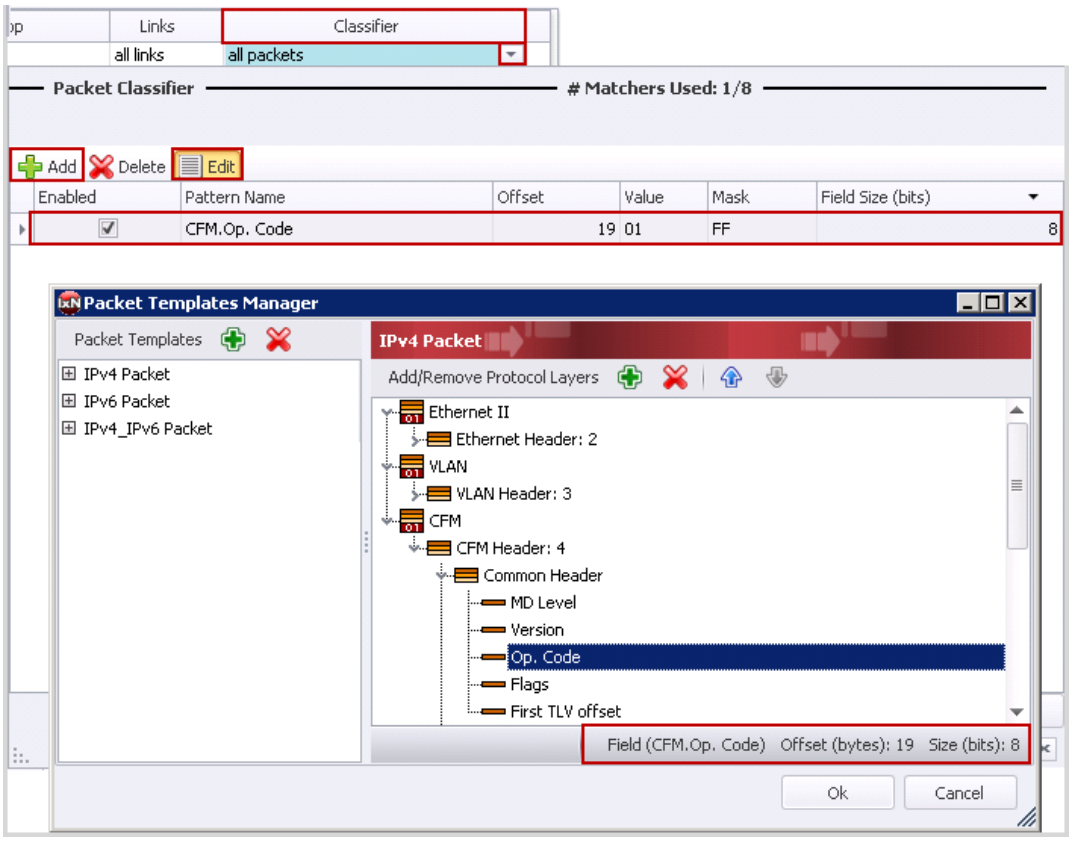


Figure 38. Adding CCM Traffic classifier

22. Click the **Links** grid of the *Impair CCM* profile. These links denote traffic direction inside impairment module. Select the links so that the impaired traffic passes through the DUT.

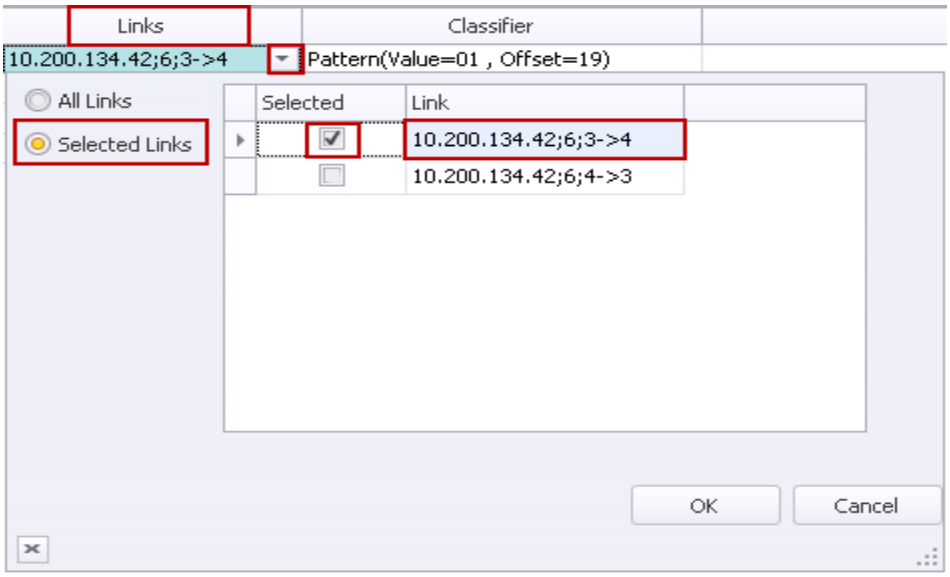


Figure 39. Impairment Link Selection

23. Select the **Delay** tab, to apply delay and jitter impairments in **Impairments** -> **Profiles** tab. Select the impairment profile and right click on **Delay** grid. Select the **Enabled** checkbox and enter delay as *300 microseconds*.

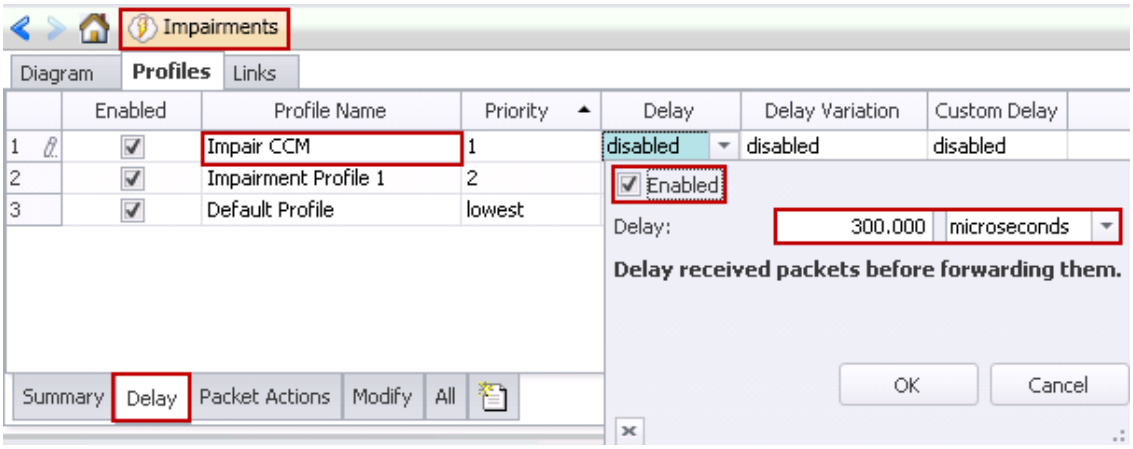


Figure 40. Delay Impairment Configuration

24. Select the impairment profile and right click on **Delay Variation** grid. Select the **Enabled** checkbox and select *Gaussian* delay variation. Enter the value of Standard Deviation as *50 microseconds*.

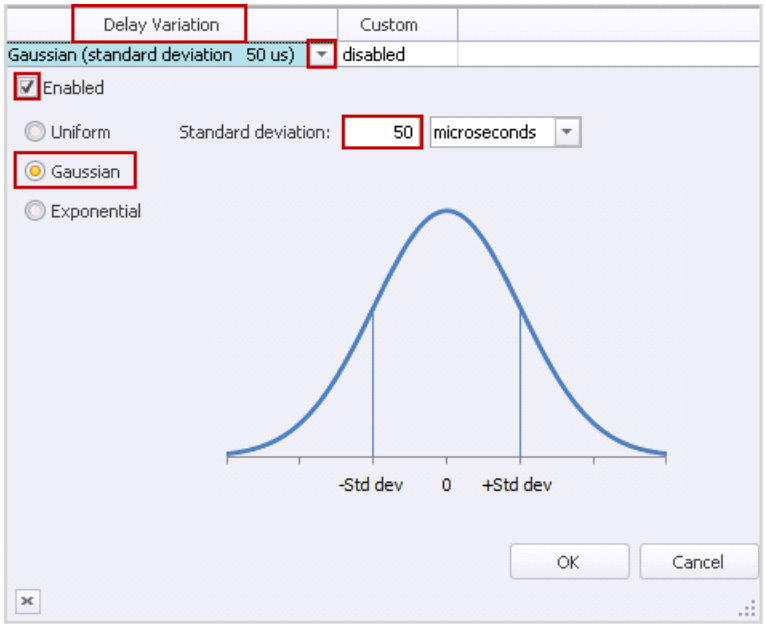


Figure 41. Jitter Impairment Configuration

25. Click the **Apply Impairment** icon, in the **Configuration** ribbon, to apply the impairment profile in the hardware. Only Enabled profiles are applied to the hardware. If applying impairment profile changes is successful, the exclamation mark on the **Apply Impairment** icon disappears.

Figure 42. Apply Impairment Icon Change

Note: If the impairment profile contains configuration errors, the exclamation mark remains, and an error notification window appears. For further troubleshooting, follow the instructions in the **Troubleshooting Tips** section.

26. Select **Impairment Profile Statistics** and click the **Delay** tab.

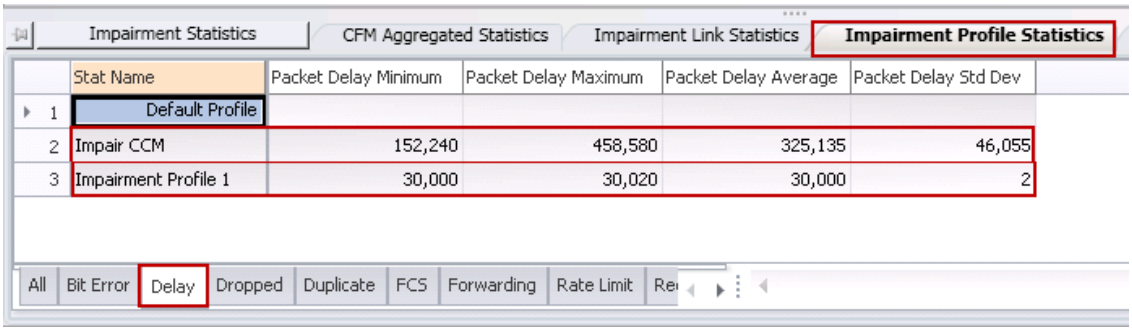


Figure 43. Delay Impairment Profile Statistics

Note: Two profiles show delay statistics, *Impair CCM* Impairment profile, and *Impairment Profile 1. Impairment Profile1* shows an intrinsic delay of 30 us.
As per delay variation configuration, delay is expected in the range from ~150 us to ~450 us and is achieved in this setup. However, the amount of delay applied, varies with the spacing between packets and the amount of traffic flowing through the ImpairNet module.

27. Select **Impairment Link Statistics** tab in the **Impairment Statistics** view, and select **Delay** tab, to check the packet delay/jitter statistics for impairment links.

Note: Unlike impairment profile statistics, impairment link statistics show delay statistics for all packets passing through the links; therefore, Link statistics values vary from the Profile statistics values.

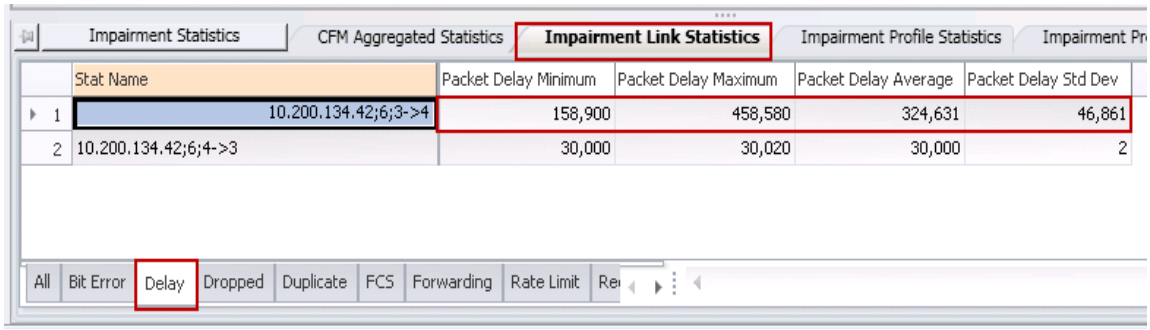


Figure 44. Delay Impairment Link Statistics

28. Right-click the **Drop** grid of *Impair CCM* impairment profile, to apply drop impairment. Select the **Enabled** checkbox and set the drop percentage to *50%*.

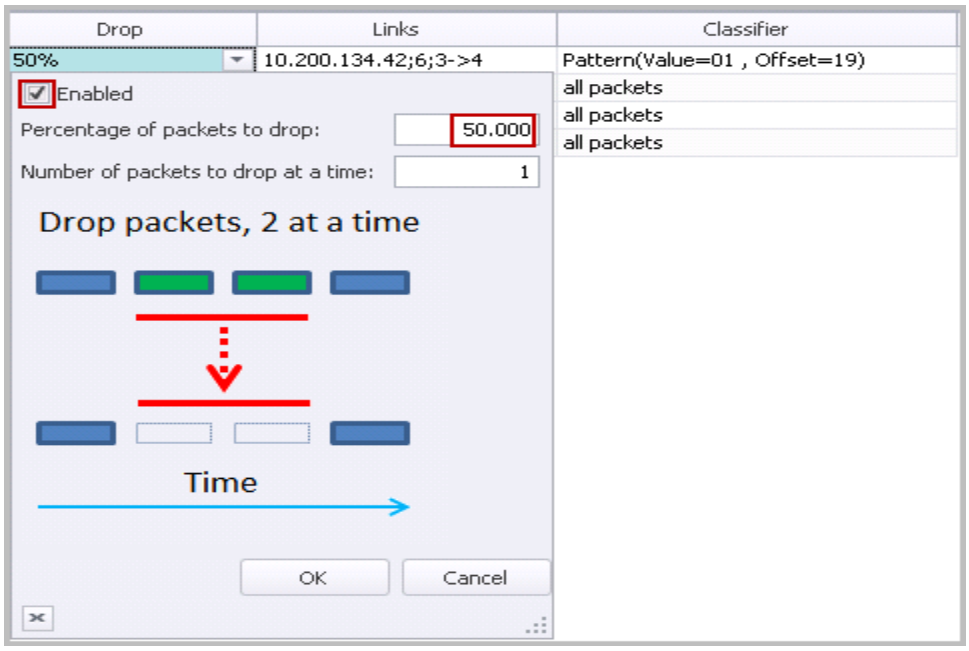


Figure 45. Drop Impairment Configuration

29. The **Apply Impairment** icon shows an exclamation mark as the latest impairment profile changes are not yet applied to hardware. Click the **Apply Impairment** icon to apply the impairment profile changes.

    Note: The impairment profile changes are applied without disrupting the traffic flowing through the ImpairNet module.

30. Select **Impairment Profile Statistics** tab and click the **Dropped** tab.

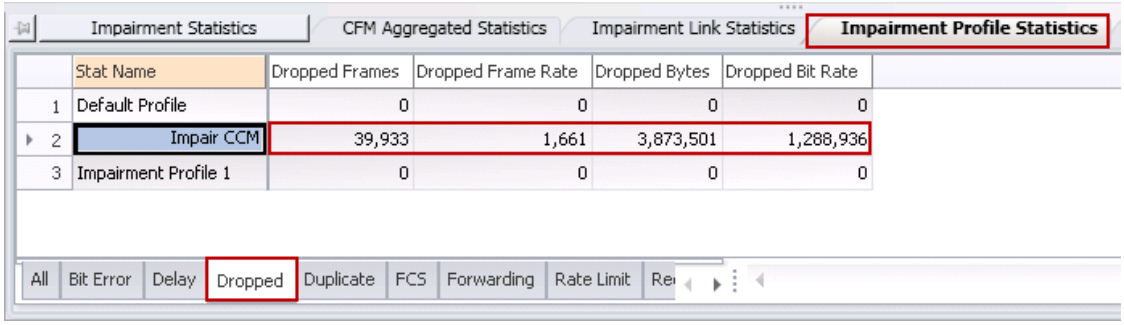


Figure 46. Drop Impairment Profile Statistics

31. Select **Impairment Link Statistics** tab in the Impairment Statistics view and select **Dropped** tab, to check the dropped packet statistics for each link direction of the *Impair CCM* Impairment profile.

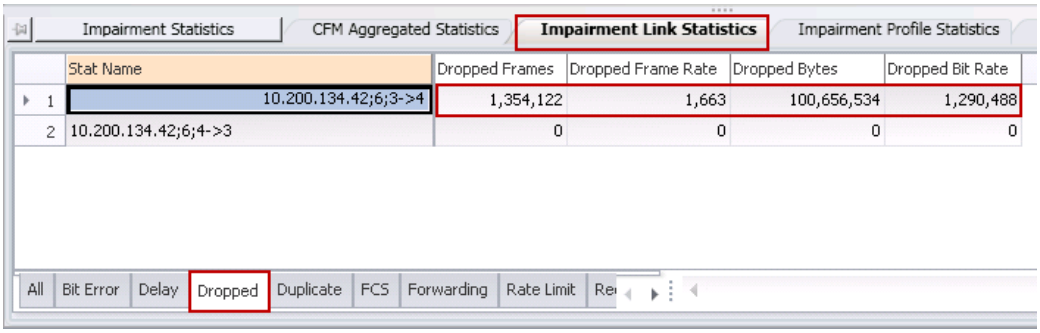


Figure 47. Drop Impairment Link Statistics

Ensure that the packets are dropped as per the configured rate.

Test Variables

You can use each of the following variables in separate test cases. These variables use the test case detailed above as a baseline, modifying a few parameters in the same Impairments view. You can create various scalability tests to utilize the DUT operating completely in presence of actual world network impairments.

Performance Variable	Description
Create multiple profiles	You can create up to 32 bidirectional, or 64 unidirectional impairment profiles per impairment port pair.
Add multiple classifiers	You can add multiple classifiers in a single impairment profile. Use Copy Classifier and Paste Classifier commands in the **Impairments Configuration** tab to copy and paste the Classifiers across impairment profiles. You can add a maximum of 16 classifiers for each link direction.
Apply impairments in both link directions	You can select to impair one or both the links.
Increase Delay	Introduce delay to a maximum of 6s for every impairment profile on 1G impairment module, and to a maximum of 600 ms for every impairment profile on 10G impairment module.
Select among different kinds of delay units	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 drop rates	Apply drop rates from 0-100% in clusters, to a maximum of 65535 packets.
Apply different packet impairments	Apply, reorder, and duplicate BER impairments in addition to drop impairments. Reorder and duplicate impairments are present in the **Packet Actions** tab.
Apply BER impairment	Apply BER impairment in the **Other** tab. Optionally, select to correct L2 FCS error, or, drop the packet with L2 FCS errors in the **Checksum** grid.

Results Analysis

This test proved that you can successfully emulate WAN Link conditions such as delay, jitter, and drop. Also, you can select CCM messages to impair.

In this test only CCM messages were impaired. Similarly, you can also impair other OAM messages like LMM, LMR, DMM, DMR, 1DM and 1DR to completely test the delay and loss measurements reported by the network device.

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 error. Make sure that traffic is flowing through the module and the drop rate is not set to *100%*.
No traffic is flowing through the impairment links.	To ensure that traffic flows through the impairment modules: • Disable all the impairment profiles except the default profile. • Apply Impairments and check that Rx/Tx Frames statistics for the impairment link corresponds to the traffic. • Verify that both the links for the impairment port pair are forwarding, that is, the checkboxes for **Interrupt Forwarding** are cleared.
An error window appears, on clicking Apply Impairments.	To overcome this error: • Ensure that there is no impairment profile configuration error. • Make sure that the impairments are applied with in the configuration limits. • Check ImpairNet module specifications for the configuration limits.
Traffic is not impaired though the Apply Impairment icon is not showing any error.	To overcome this error: • Ensure that the classifier value, mask, and offset are set correctly. • Make sure that a profile with generic classifier does not have a lower priority than that of the desired impairment profile. • Verify that you have selected the **Enabled** check box for the configured impairments.

Conclusions

This test verified that the device or system under test is reporting loss and delay statistics accurately and these statistics match that of Impairment load module.

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.

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 are discussed that 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.

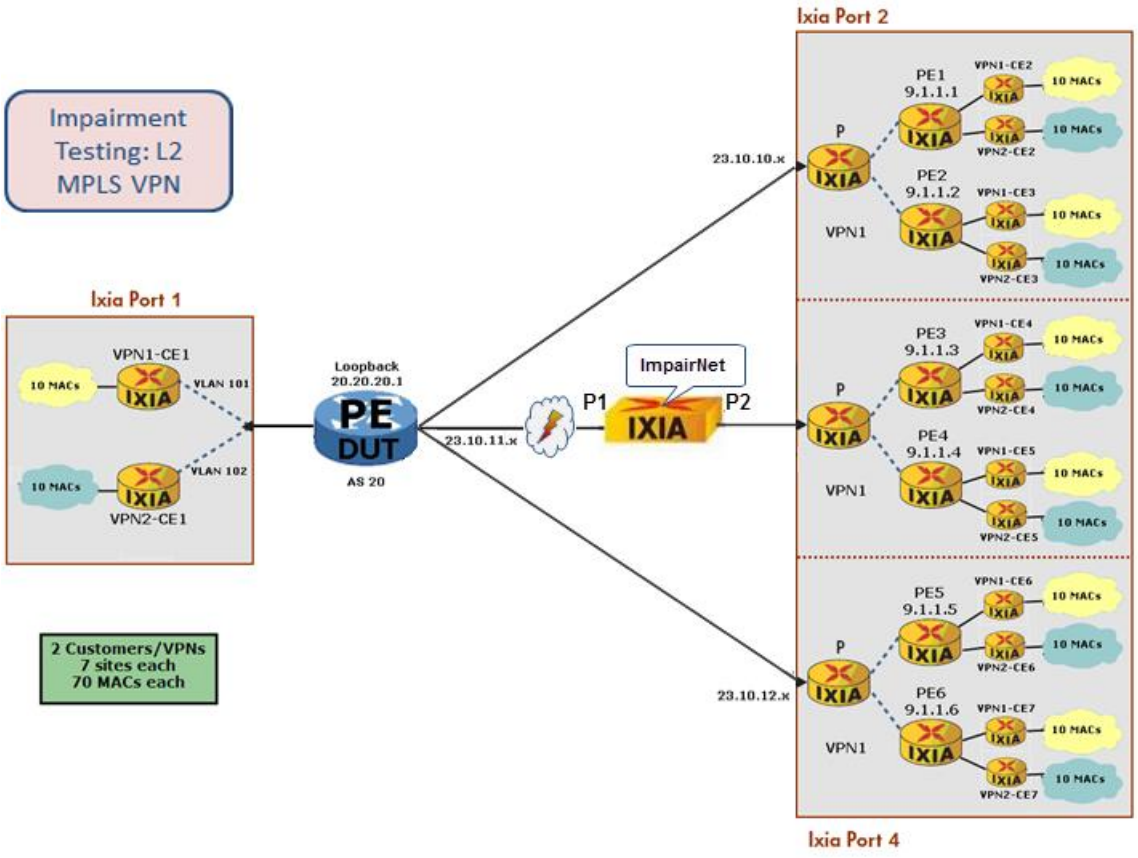


Figure 48. Impairment testing - Ixia emulated layer 2 MPLS VPN network

Step-by-step Instructions

These instructions create a Layer2 VPN – VPLS performance test for the topology shown in figure above. Then these instructions create Delay, Jitter, Drop, and Rate Limit Impairment tests of the Layer2 MPLS VPN topology. You may also use these steps as a guide to build other Impairment test scenarios.

1. Reserve four ports in IxNetwork.

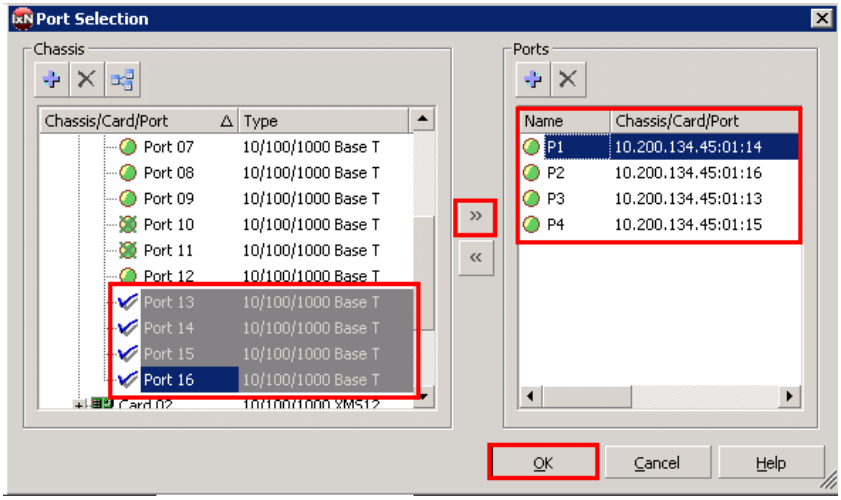


Figure 49. Port reservation

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

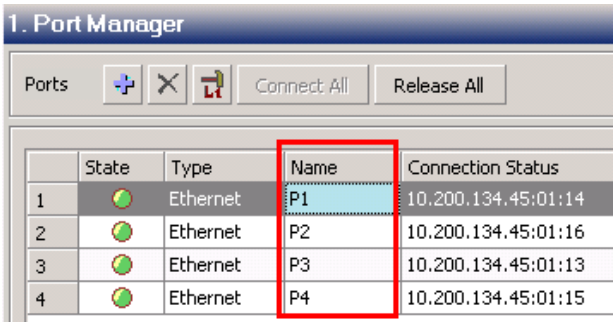


Figure 50. Port naming

3. In the IxNetwork application, click **Protocol Wizards.**

Figure 51. Protocol wizards

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

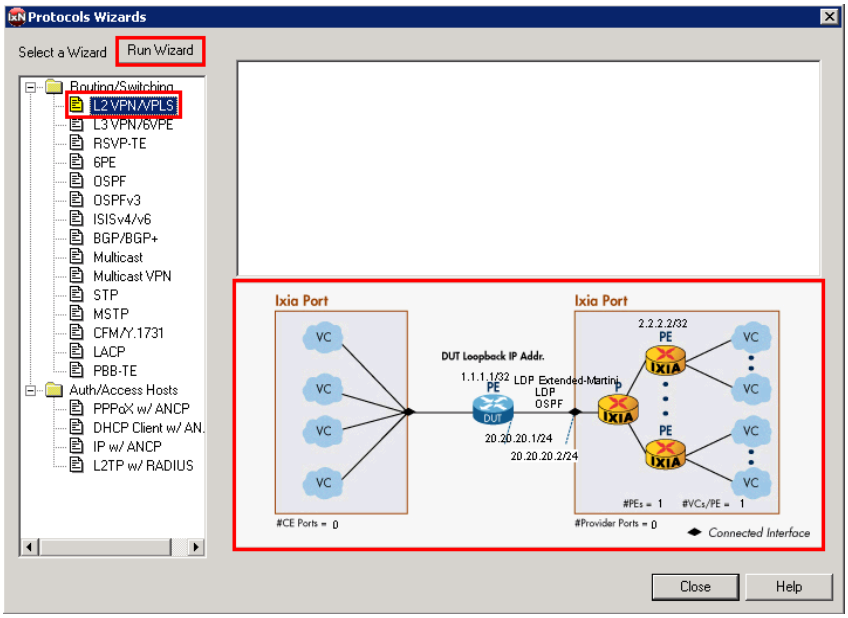


Figure 52. L2 VPN wizard

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**.

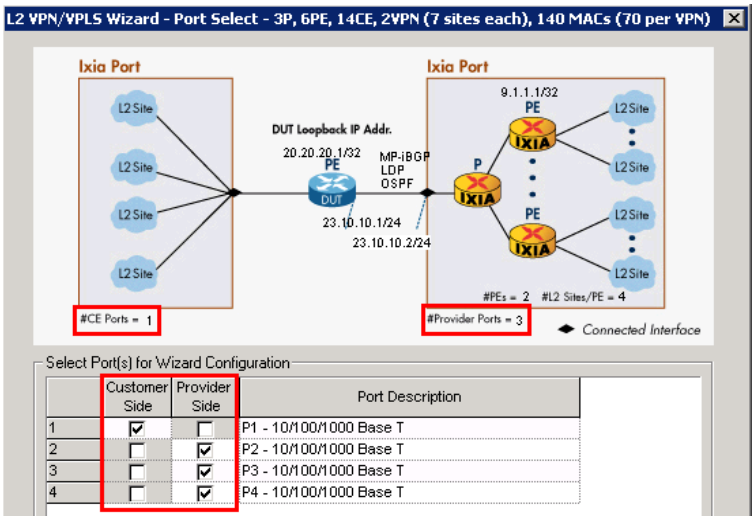


Figure 53. L2 VPN Wizard Screen1 of 6

Note: The configuration in the screen above updates 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 (depicted in the image below) 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
    a. 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:
    Disable (clear) **Enable P Routers**. In this case, Ixia ports(s) would then only emulate PE routers (that is, no P router emulation), and 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.
- Select the **Enable VLAN** checkbox (not shown) to run these protocols over VLANs. Enter the first **VLAN ID** and choose to increment.

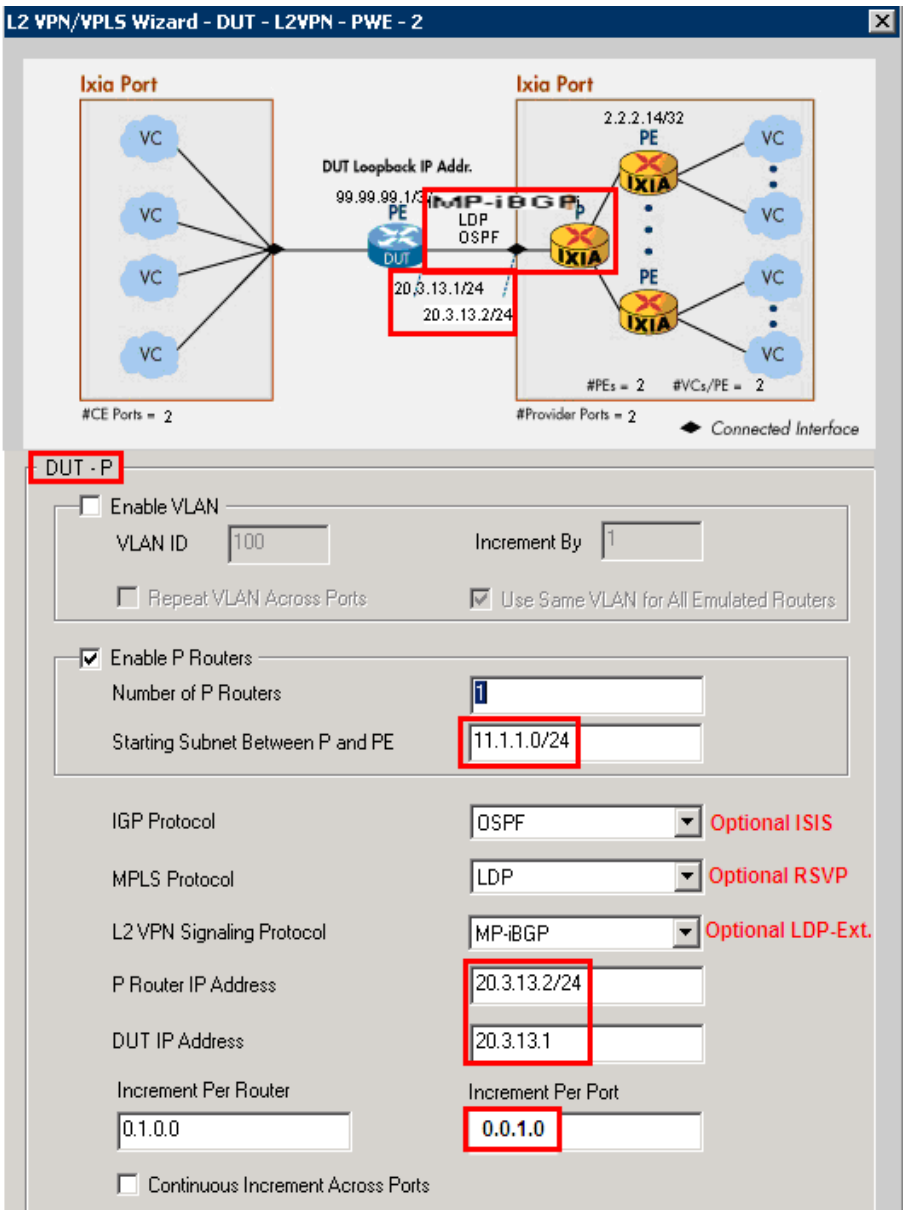


Figure 54. L2 VPN wizard screen 2 of 6

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

7. This window (depicted in the image below) 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 configuration 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 gets *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 action tests the DUT's ability to peer with many PE routers with potentially many VPNs/VCs.

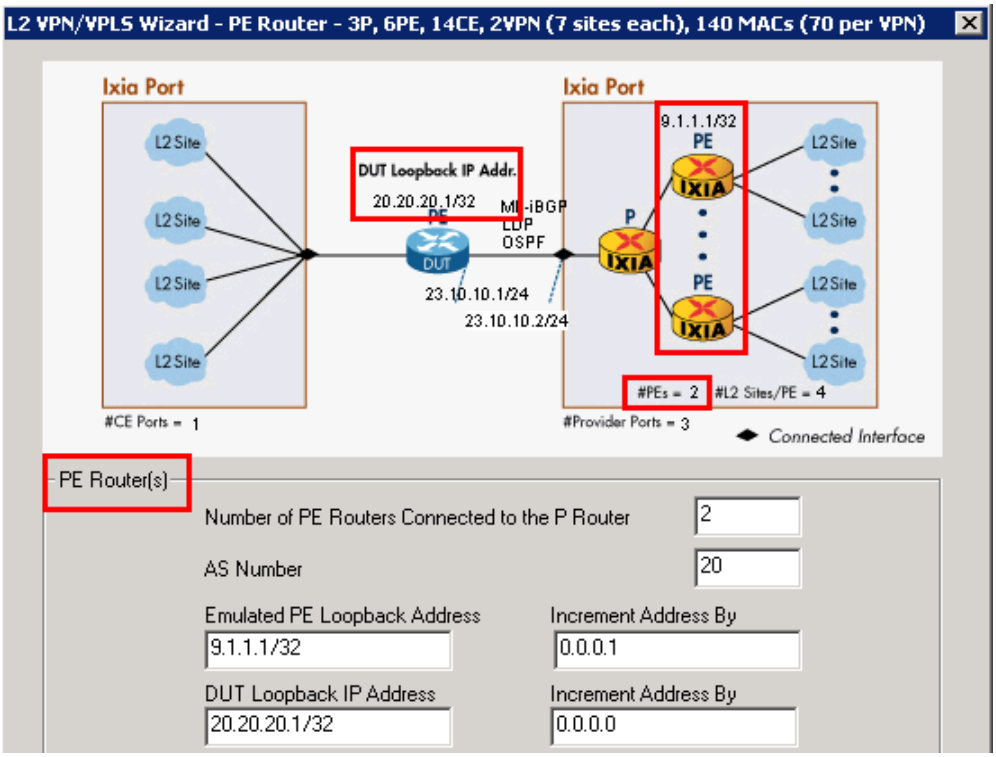


Figure 55. L2 VPN wizard screen 3 of 6

8. This window (depicted in the image below) 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 uses 151:2.
   c. Configure the **Number of VPNs per PE Router**. This configuration partially determines the number of customers/VPNs that are used in the test. This number also determines the number of CE routers 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**. Ensure that the site ID is unique for each circuit within a given VPN.
      - In this test they are *101* and *201*, respectively
      - 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 action tests 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.

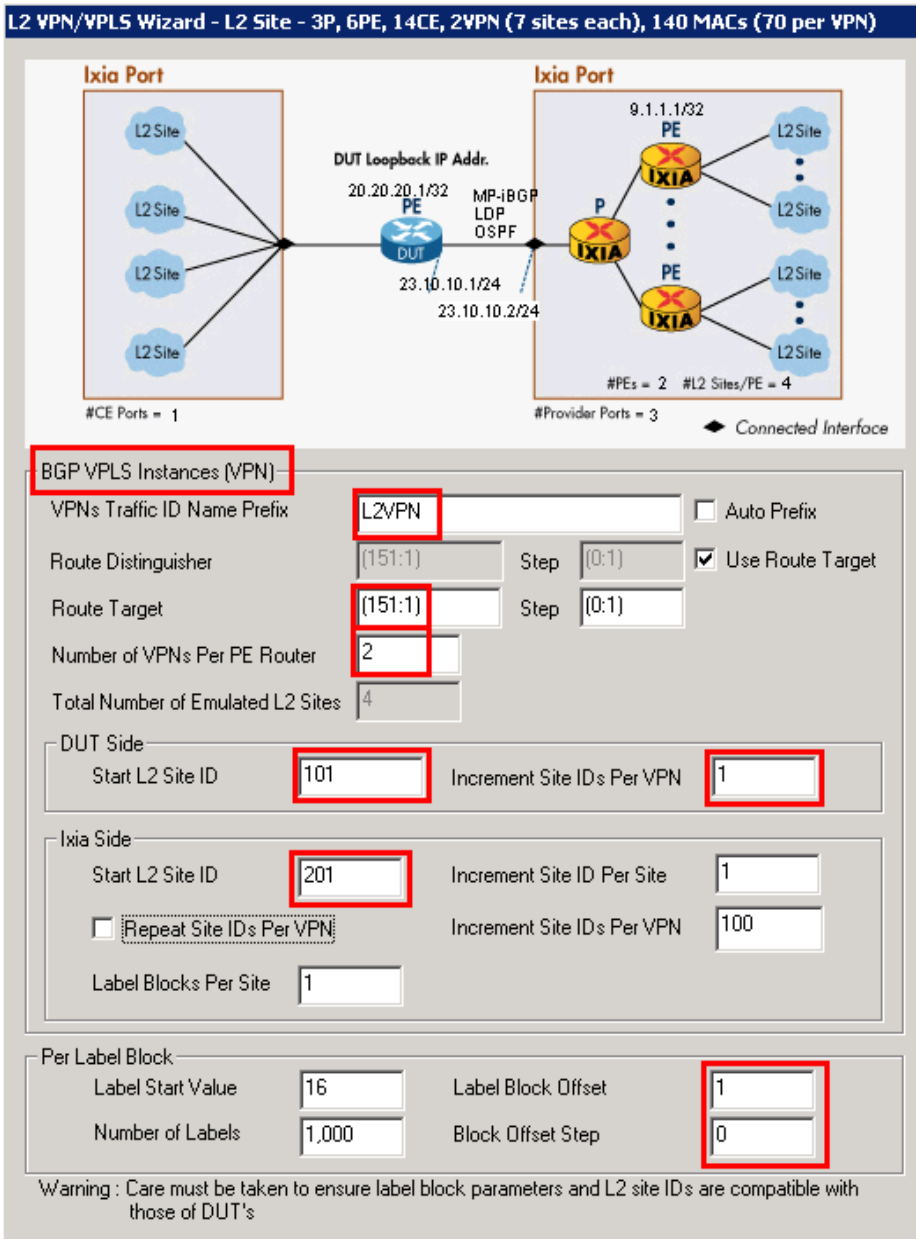


Figure 56. L2 VPN wizard screen 4 of 6

9. This window (depicted in the image below) 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 are used per VPN site (70 MACs per VPN total).

b. Enter the **First VLAN ID** for the first VPN on P1.
   - In this test it is *101*.
   - The second VC on P1 uses 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 stresses the DUT's ability to handle many MAC addresses on each VPN.

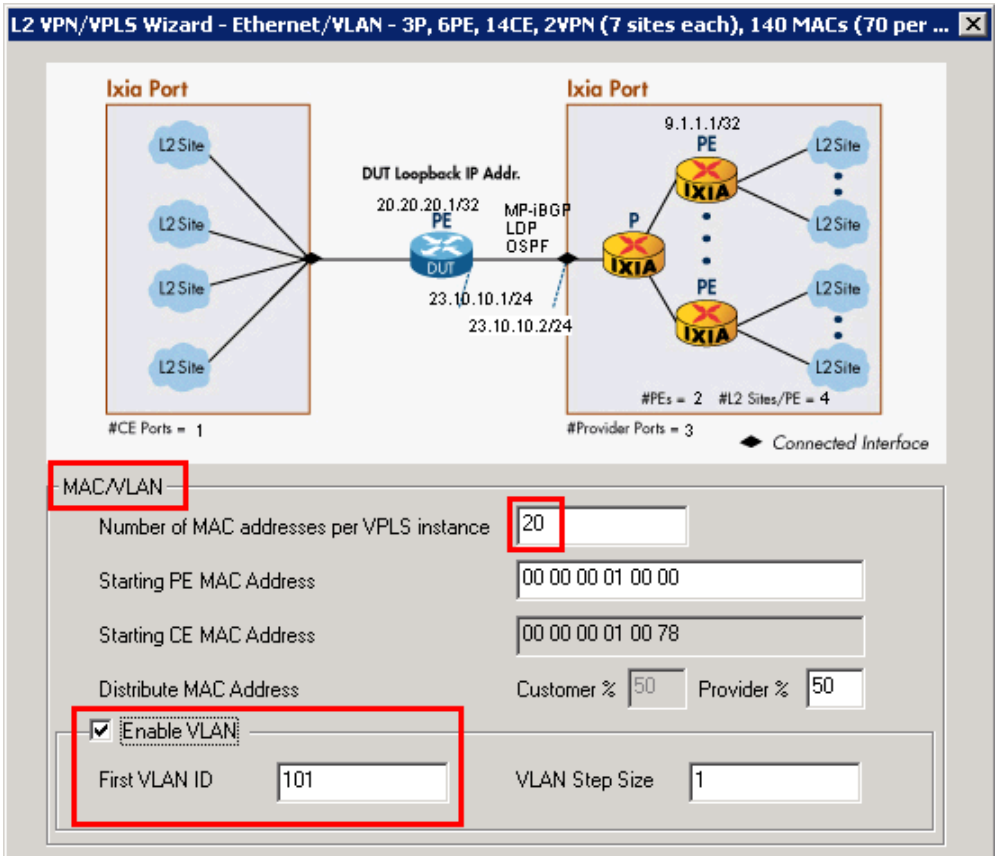


Figure 57. L2 VPN Wizard Screen 5 of 6

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

10. This window (depicted in the image below) 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 action overwrites all previous configurations.

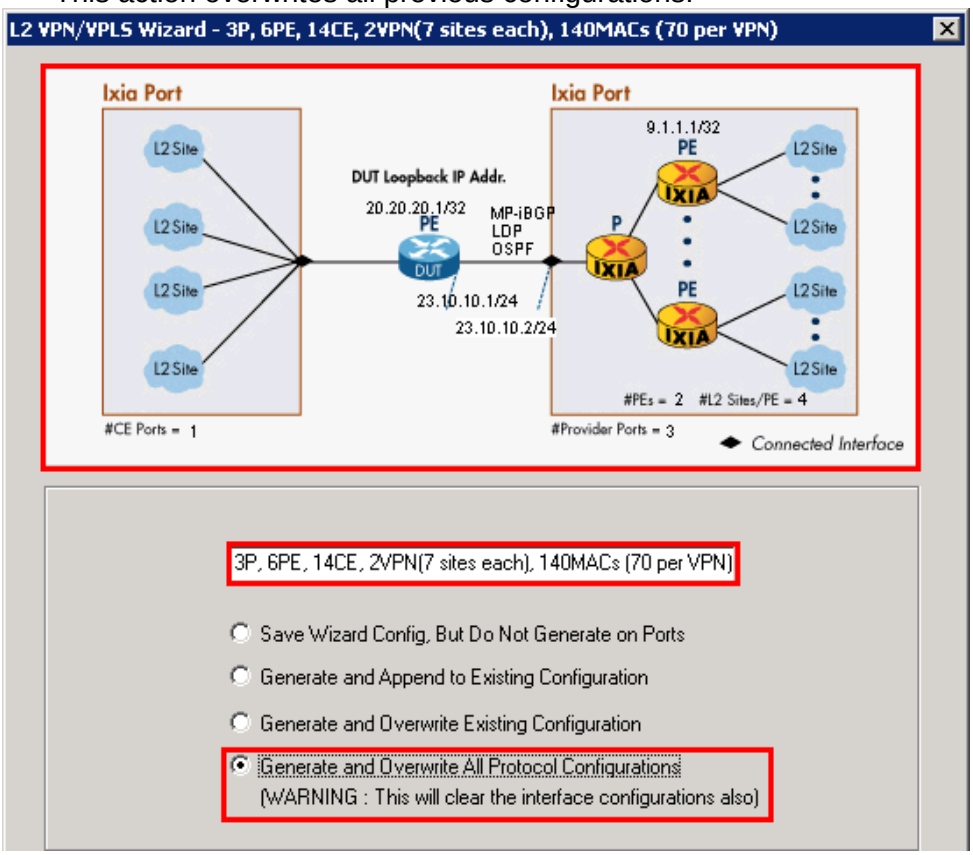


Figure 58. L2 VPN Wizard Screen 6 of 6

11. This window (depicted in the image below) shows the saved wizard template.

    a. Click **Close** to finish the wizard configuration.
    b. ***Optionally***, when using saved wizard templates, you may:
        - Revisit the same wizard to 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.

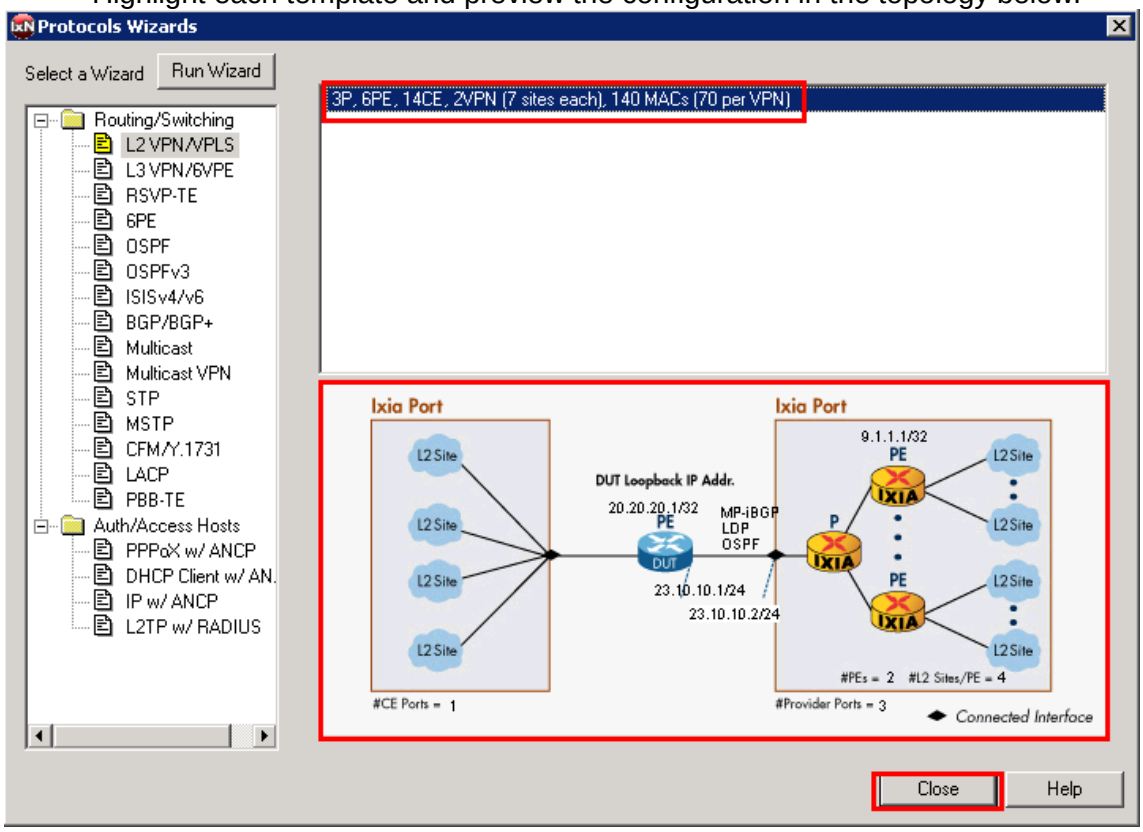


Figure 59. L2 VPN wizard saved wizard template

12. In the Test Configuraton pane, click **Routing/Switching/Interfaces**, and **BGP/BGP+** protocol. Note how the wizard incremented the fields and check that the settings function with the DUT configuration. For example:

    a. On **P2, P3, P4**, view the **Local IP** (also known as, 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 as required. Another option is to highlight columns and right-click to customize with **Same** or **Fill Increment** options.

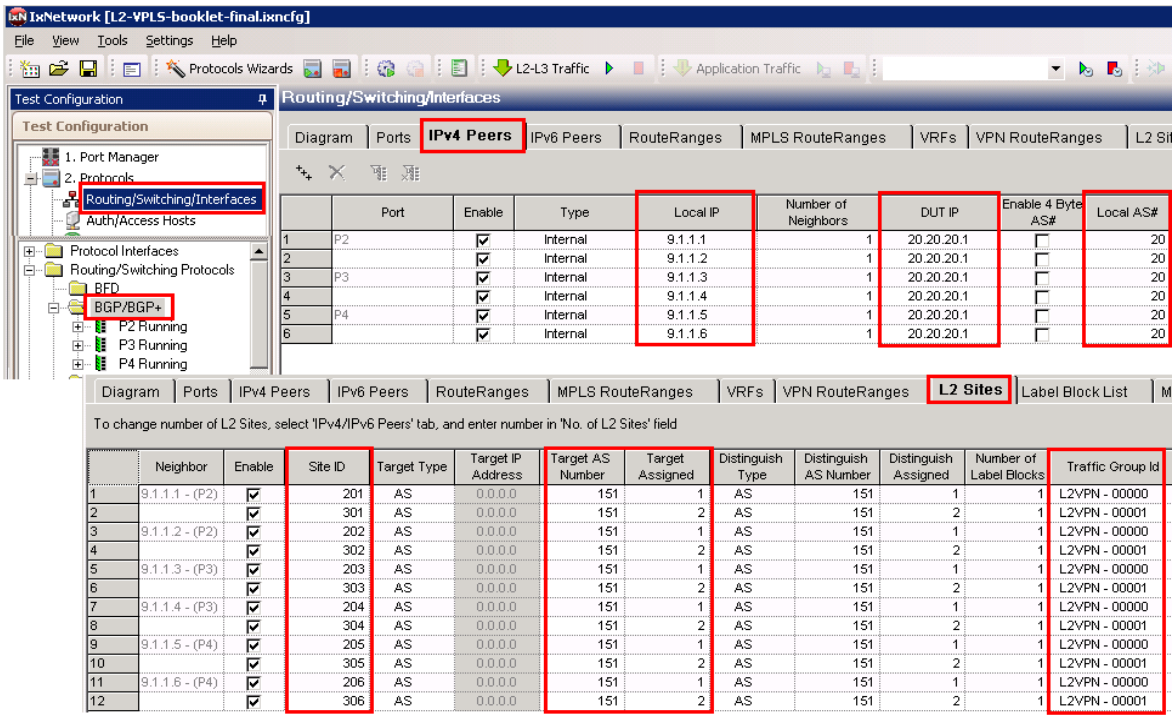


Figure 60. Protocol configuration window

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

14. Click **Global Protocol Statistics** to view the summary of all protocols running on each port.

Check whether all of the BGP, OSPF, and LDP sessions are functioning.

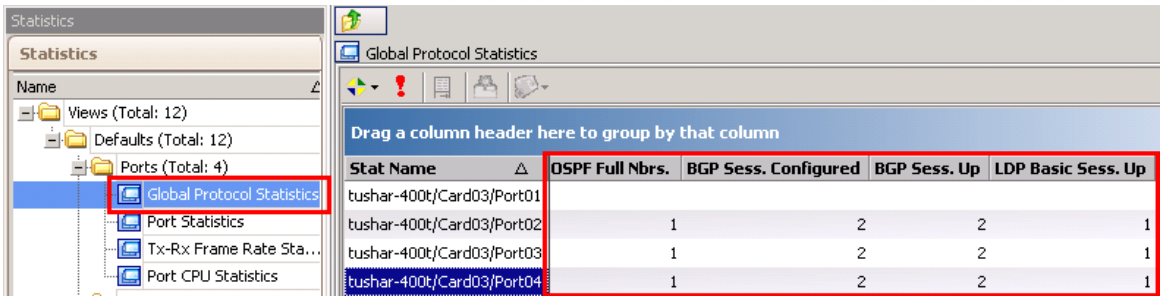


Figure 61. Global protocol statistics window

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 functioning:

- Navigate 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 starting the protocols, 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. In the Test Configuration pane, click **Learned Routes,** and then **Refresh** button to see the labels learned by the Ixia peer. In this test case, verify that there are **two** BGP-VPLS labels learned from the DUT (PE) to the Ixia PE at 9.1.1.1. Check it against the DUT.

Optionally,

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

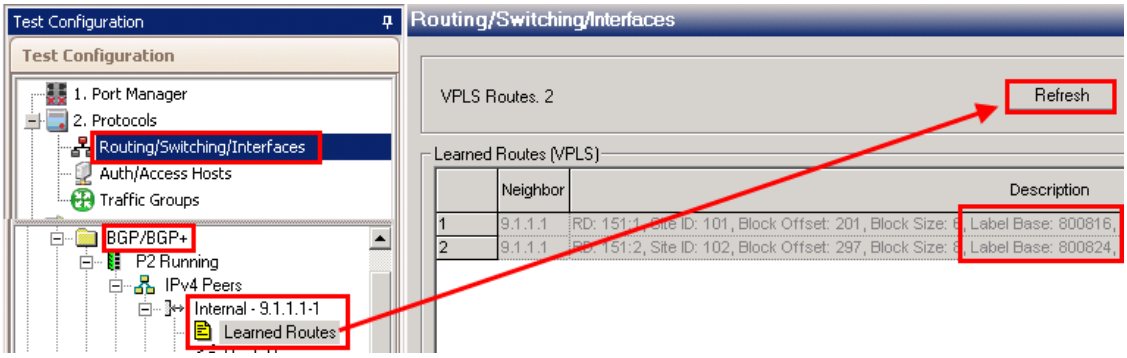


Figure 62. Protocol learned info

16. After all of the sessions are functioning, build bidirectional traffic from CE-PE, and from PE-CE. Click the **+** sign. to launch the **Advanced Traffic Wizard**.

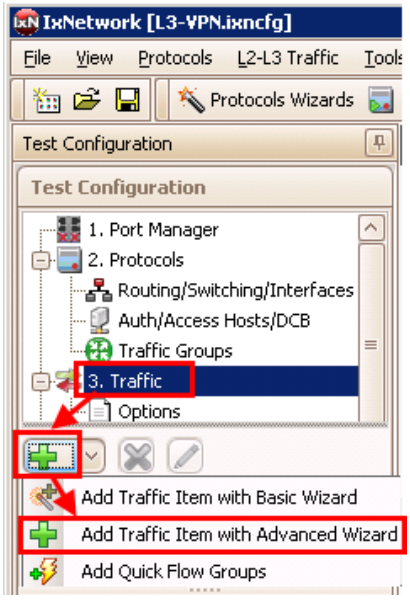


Figure 63. Create traffic

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.**
       - This configuration filters 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.
       - 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 action further filters the source/destination tree for CE-PE traffic.
    f. Select the **Source – Static Mac VLAN Ranges** checkbox.
       - This option 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 option is a global option to select ALL of the LDP MAC VLANs for the destination ports.
    h. Click the down arrow to add 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 them 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.

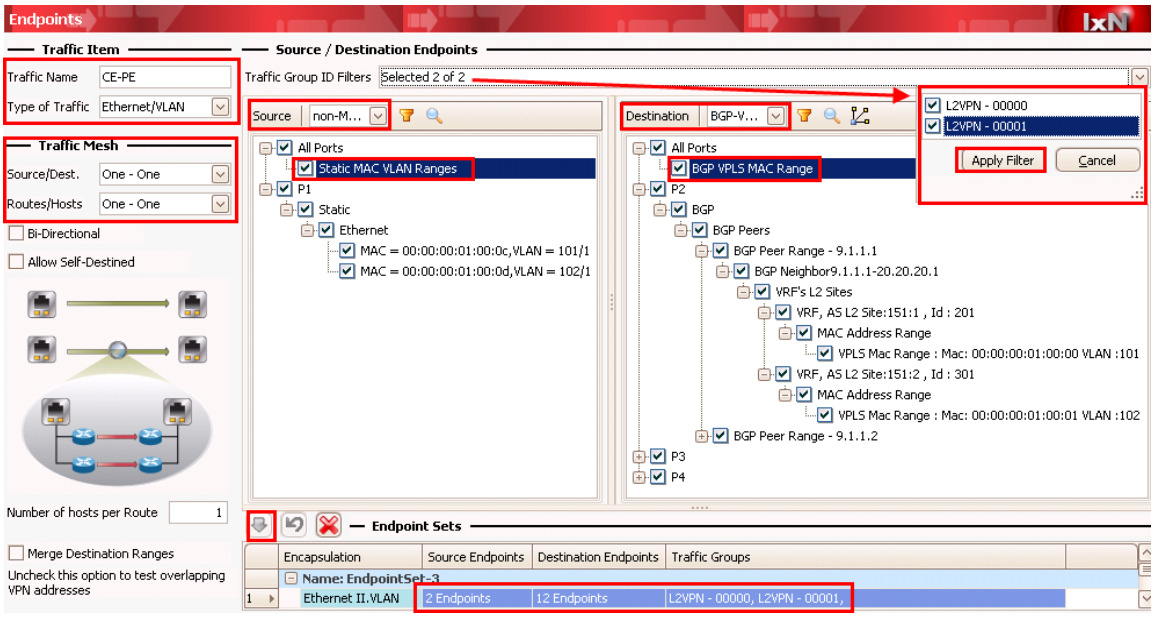


Figure 64. Advanced Traffic wizard screen 1

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

19. Optionally, use the **Flow Group Setup** window (not shown) to, separate (in this case,) 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.

20. 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. You can modify these two parameters in the **Traffic Grid** window after completing the wizard.

21. 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 creates a trackable flow for every combination of the selected items. Each flow provides full statistics (rate, loss, latency, and so on.)
    - Click **Next.**

    Note: These options are also available as **Drill-down** views in the **Statistics** windows. In this case, there is an aggregated **Traffic Item** statistics that shows all of the combined statistics for every flow within this Traffic Wizard. Then, you can right-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 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 select each check box. Also use the **Validate** window to understand the precise number of resources used.

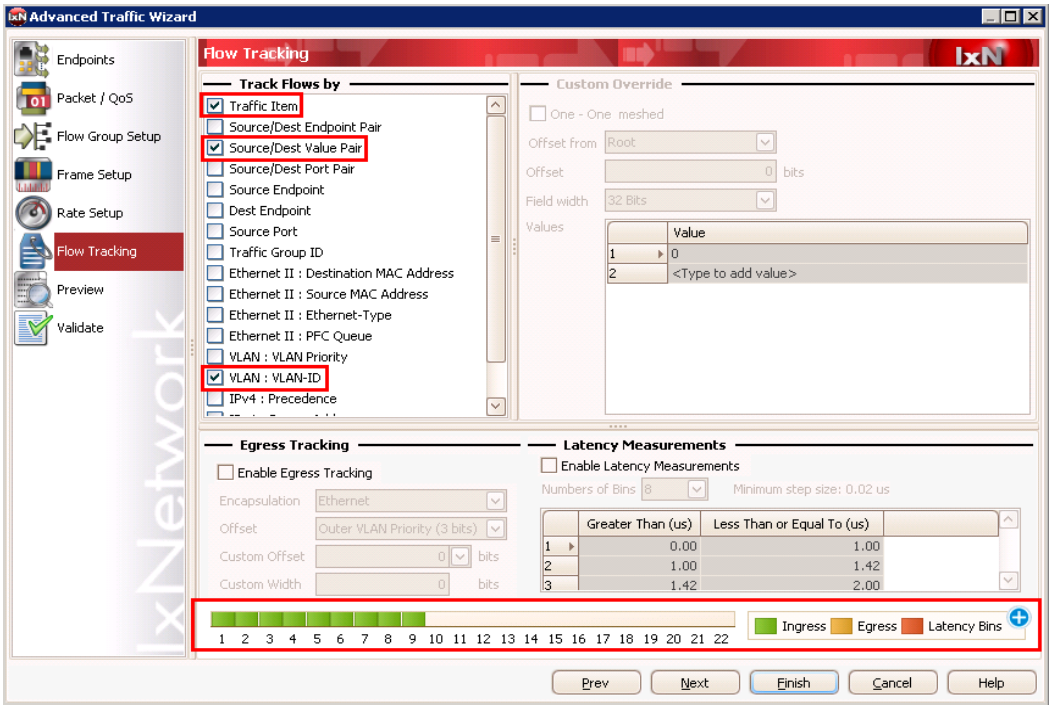


Figure 65. Advanced Traffic wizard screen 6

22. Optionally, in the **Preview** window, click the **View Flow Group/Packets** to view the exact packets the system can transmit from each Port/Flow Group.

    a. In this case on P1, Flow Group 1, there are 12 unique packets/flows ready for transmission. As shown in the Setup topology, 10 MACs from each of the two VPNs on P1 transmit to the 60 MACs on the same VPN on P2, P3, and P4.

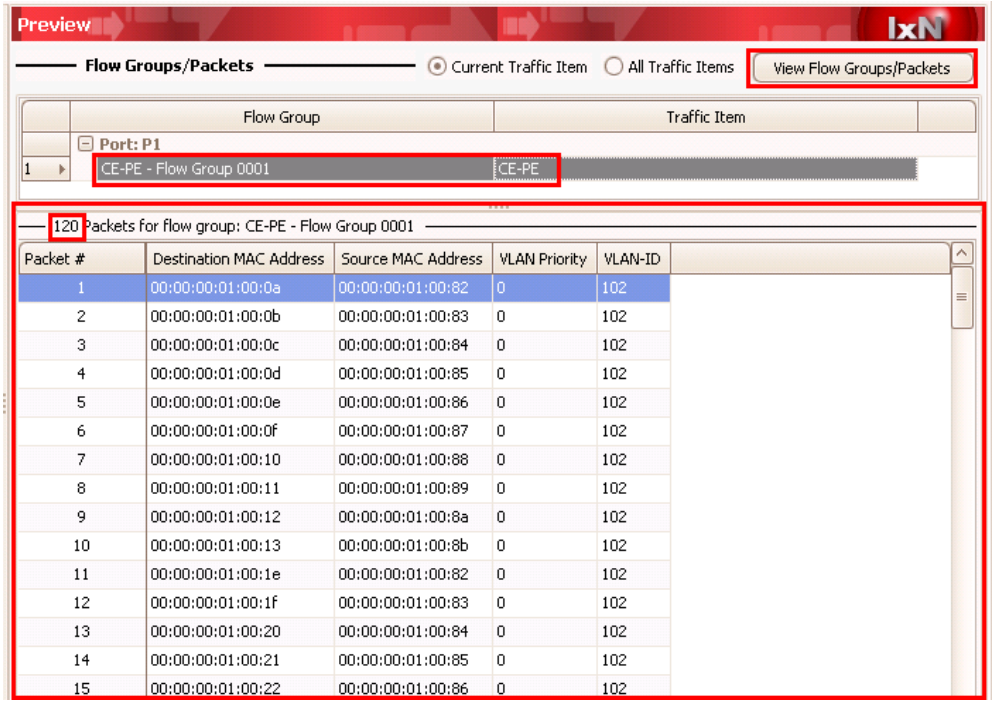


Figure 66. Advanced Traffic wizard screen 7

23. 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.**

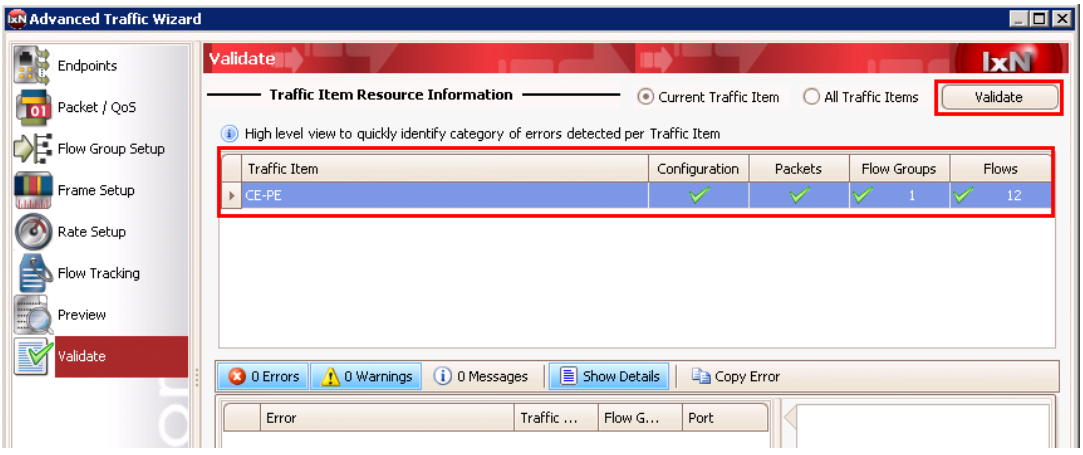


Figure 67. Advanced Traffic wizard screen 8

Troubleshooting Tip:

If errors are generated after finishing the tasks, see the **Errors** pane at the bottom of the window. Follow the explanation/steps provided. In this type of test, it is likely that 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 the task, right-click the affected **Traffic Item** and select **Regenerate.**

Also, perform **Regenerate**, if the DUT sends new label information – for example if a topology change or flapping occurs. The symptom of this occurrence is usually when certain flows are experiencing 100% loss.

1. Now configure the PE-CE traffic. Click the the **+** sign again to run the **Traffic Wizard**. The configuration steps are exactly similar to CE-PE, but in the reverse order. The following steps provide a brief description about PE_CE configuration.

    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 traffic Endpoint Set.
    i. Click **Next**
2. Optionally, use the **Packet/QOS** window (not depicted) to add an IP/TCP or IP/UDP header, for example.

3. Optionally, use the **Flow Group Setup** window (not depicted) 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.

4. Set the **Frame Setup** and **Rate Setup** windows (not depicted) to the desired settings. Start with a simple configuration such as 128 byte frames and 1000 pps rate. You can modify these two parameters in the **Traffic Grid** window after completing the wizard.

5. Select the **Flow Tracking** options for PE-CE traffic (not depicted).

    a. For this direction of traffic it is better to choose **Traffic Item, Traffic Group ID, MPLS Label (1),** and **Source/Dest Value (MAC) Pair.**
    b. All possible combinations from all options create a track able flow in the statistics, including rate, loss, and latency.
6. Optionally, in the **Preview** window, click the **View Flow Group/Packets** to view the exact packets that are ready for transmission from each Port/Flow Group.

In this case on P2, Flow Group 1, there are 40 unique packets/flows that are ready for transmission. As shown in the Setup topology, 20 MACs from each of the two VPNs will transmit to the 10 MACs on the same VPN on P1.

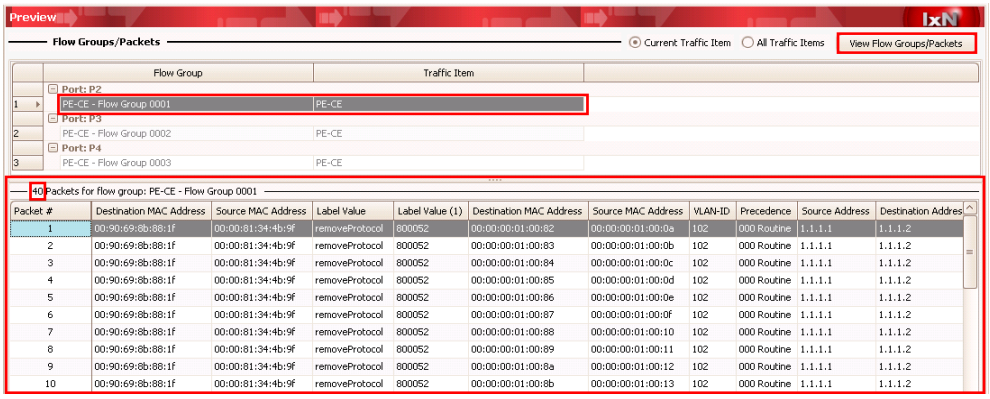


Figure 68. Advanced Traffic wizard screen 7

7. 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.**

8. Optionally, after you finish the Traffic Wizard, the Traffic (grid) window appears. Here, you can perform many operations including:

   - Add new (tab) views
   - Add new columns to existing views, including packet contents fields.
   - Many grid operations, including multi-select, and copy down/increment.
   - Change the rate/frame size on the fly without stopping traffic.
   - Configure the properties/packet contents of a flow group.

   Performance test variables:

   - You can accomplish manual performance testing of the data plane by increasing the frame size and data rate.
   - You can accomplish automatic throughput tests using IxNetwork's integrated tests as discussed in the *Test Variables* section below.

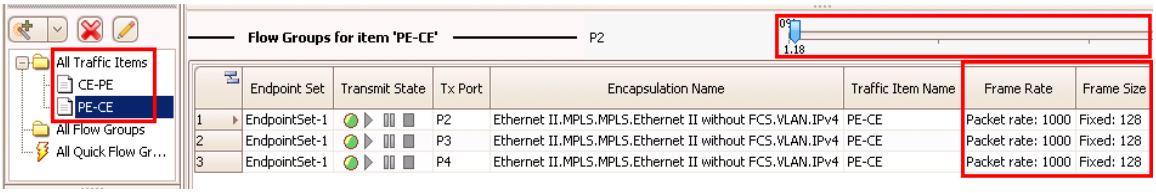
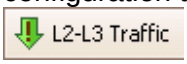


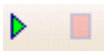
Figure 69. Post-Wizard Traffic Grid

9. **Apply,** and **Start** the traffic.

   a. Click **Apply Traffic** at the top of the window. This action sends the Traffic Item configuration to the test port.

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



10. View the traffic statistics.

    a. Click **Statistics** -> **Traffic Item Statistics**. This action shows 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.

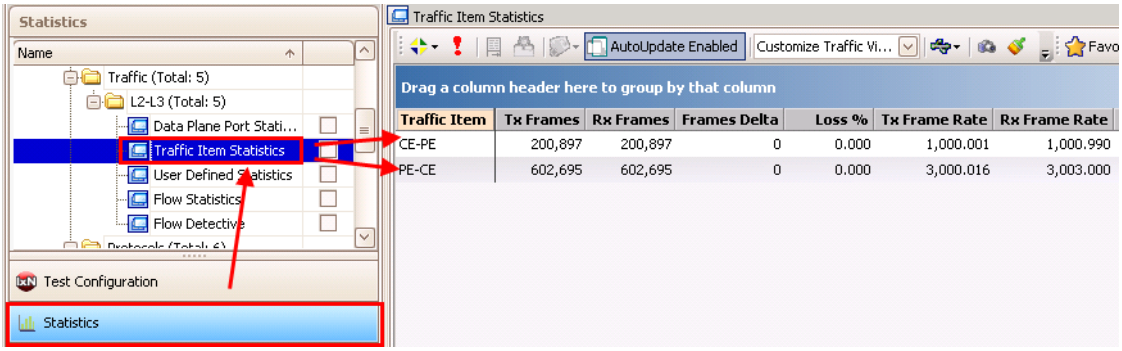


Figure 70. Statistics -> Traffic Item View

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

a. Right-click the CE-PE Traffic Item to Drill Down and find the Flow Tracking options as defined in the Traffic Wizard. In the example below, click **Drill Down per VLAN ID** to view 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: The above statistics is very helpful to accurately view the problematic VLAN (that is, customer VPN).

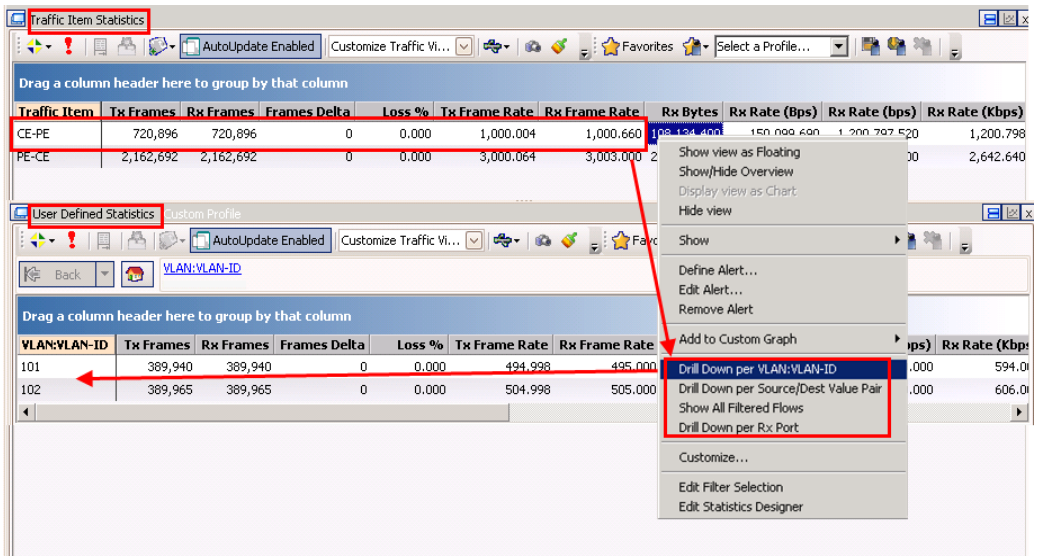


Figure 71. Statistics -> Drill down from Traffic Item to VLAN ID

b. Right-click **Drill down per Src/Dst Value (MaC Pair)** to again **Drill down** on VLAN 101. You can view all 60 MAC flows within VLAN 101 from the CE-PE side.

Note: The above statistics is very helpful to accurately view the problematic Src/Dst MAC within the given VLAN (that is, customer VPN).

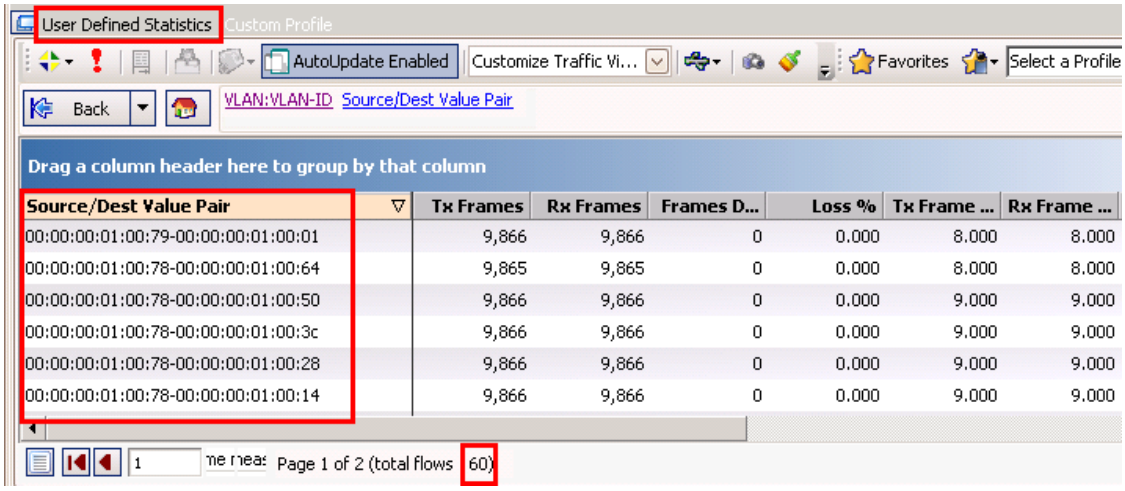


Figure 72. Statistics -> Drill down from VLAN ID to Src/Dst Value (MAC) pair

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

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

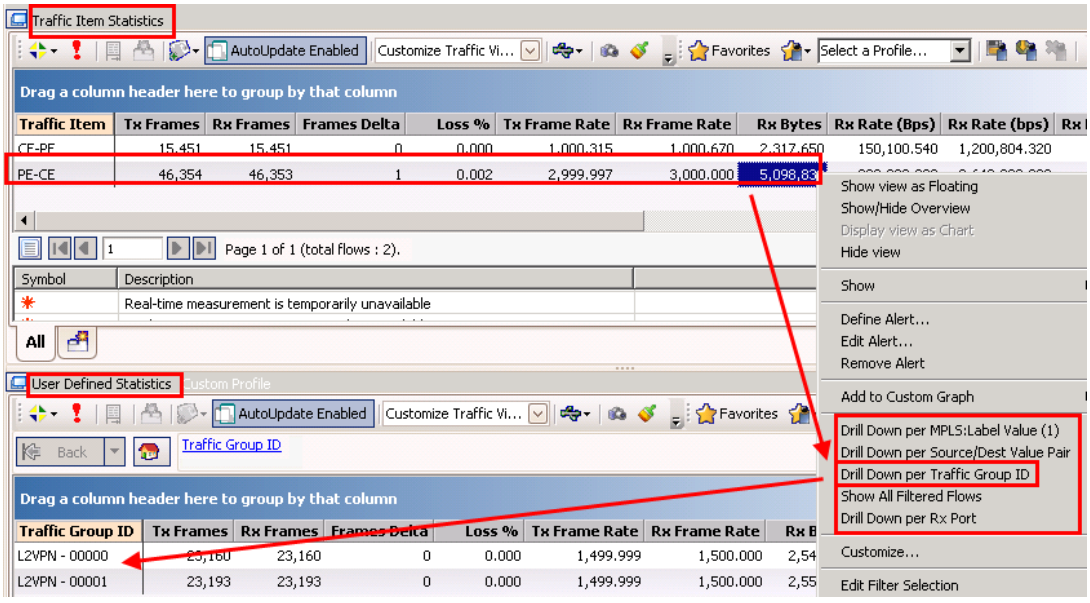


Figure 73. Statistics -> Drill down from Traffic Item to Traffic Group ID

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

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

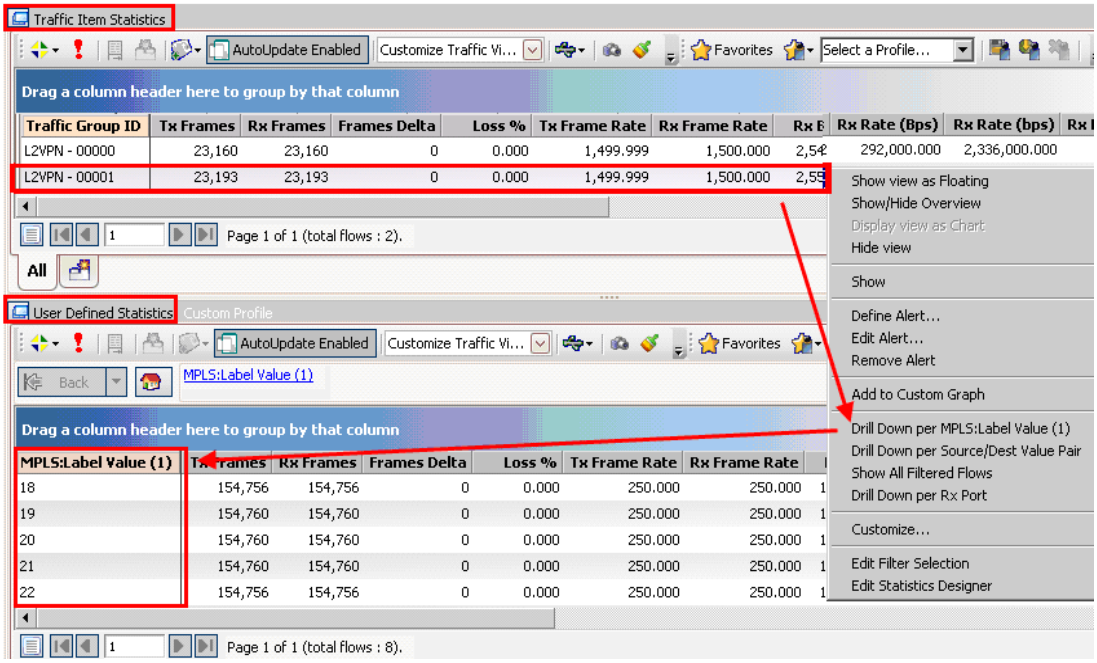


Figure 74. Statistics -> Drill down from Traffic Group ID to MPLS label

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

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

Note: **Drill-down per Rx Port** is a standard by default with every drill-down view. In this case, it helps to determine which RX port on the CE side is receiving the suspect MPLS traffic from the PE side. It may help to 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 completely synchronizes the results. No test tool can measure Tx and Rx instantaneously, because the traffic must go through the DUT first. If the frame delta is continually increasing, however, there is a loss likely to happen.

11. Reserve the 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.

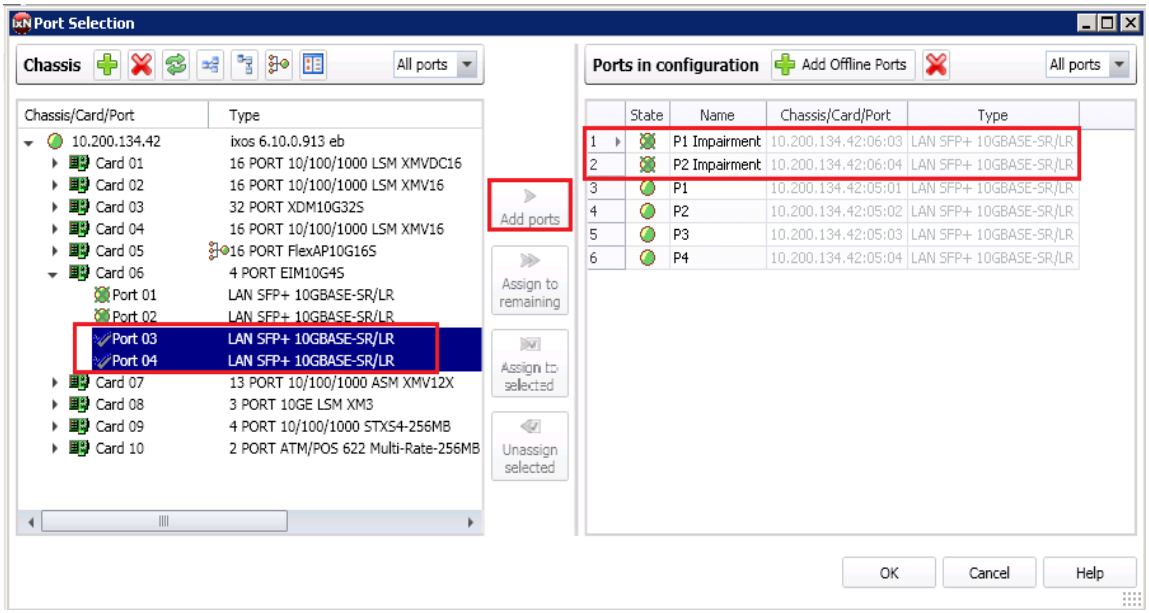


Figure 75. Impairment Port Selection

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

12. 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.

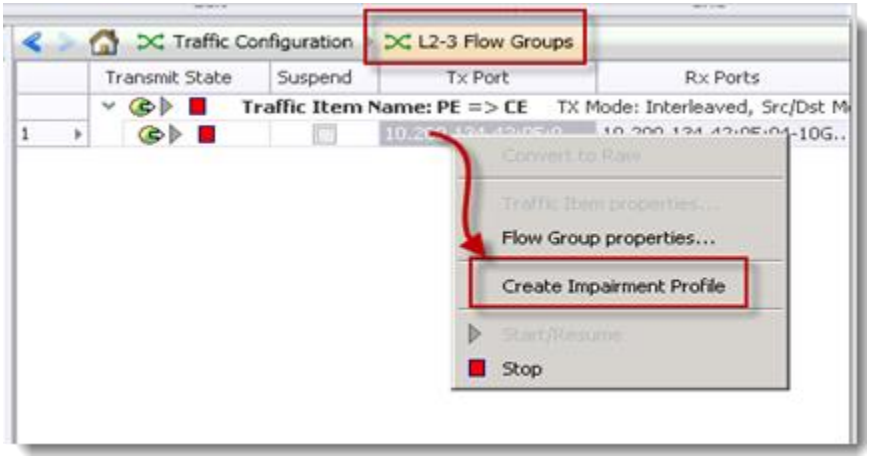


Figure 76. Impairment Profile Creation directly from Traffic Flows

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 Impairments view on clicking **Create Impairment Profile**.

13. The Impairments 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.

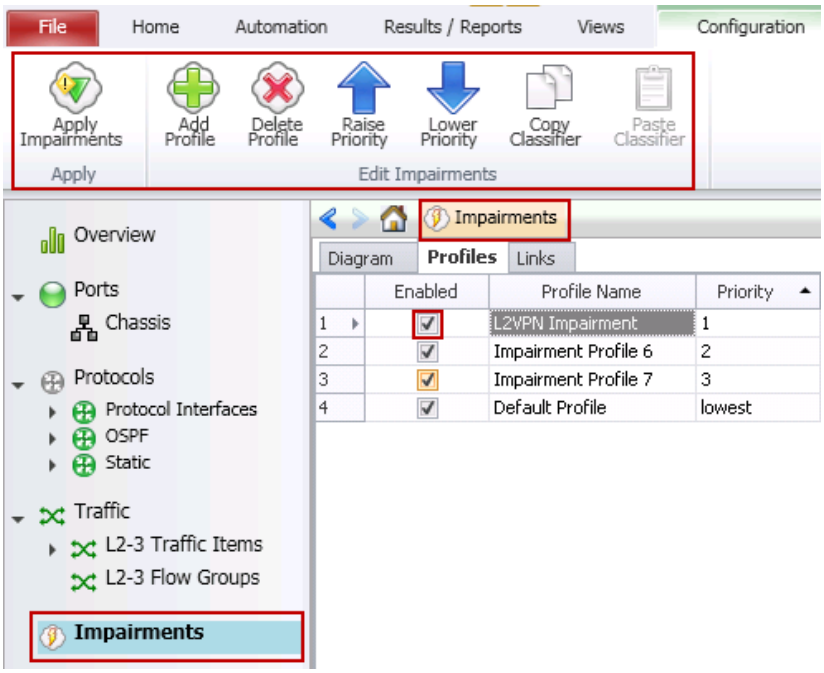


Figure 77. Impairments view

Optionally, change the name of the impairment profile. You can easily reference a named profile throughout the IxNetwork application. In this example, we are changing the newly created profile to 'L2VPN Impairment'.

Note:

- The Network Impairment view has commands for creation, deletion, and raising or lowering priority of impairment profiles as shown in Figure 12.
- 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.

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

    There are two MPLS label values. 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. You can ignore the unused bits in the value 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.*

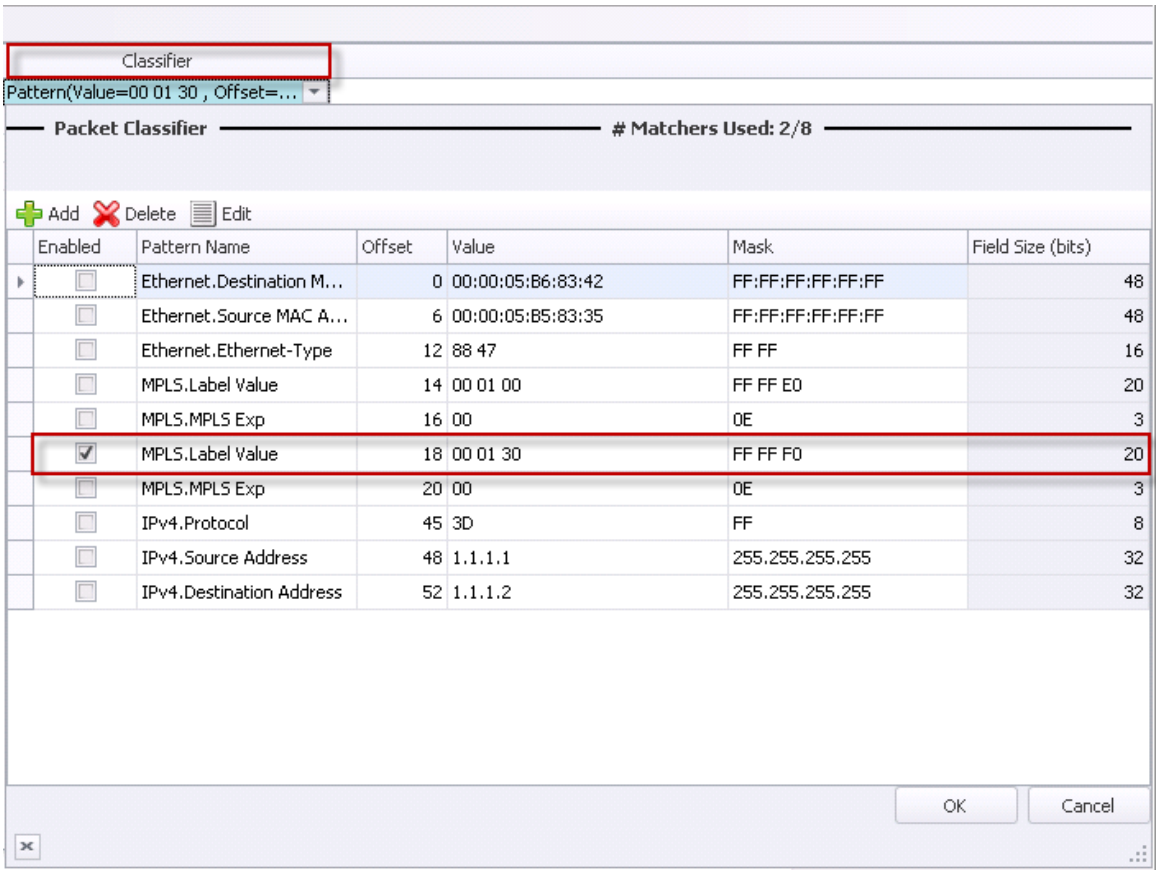


Figure 78. Traffic classifiers

15. 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.

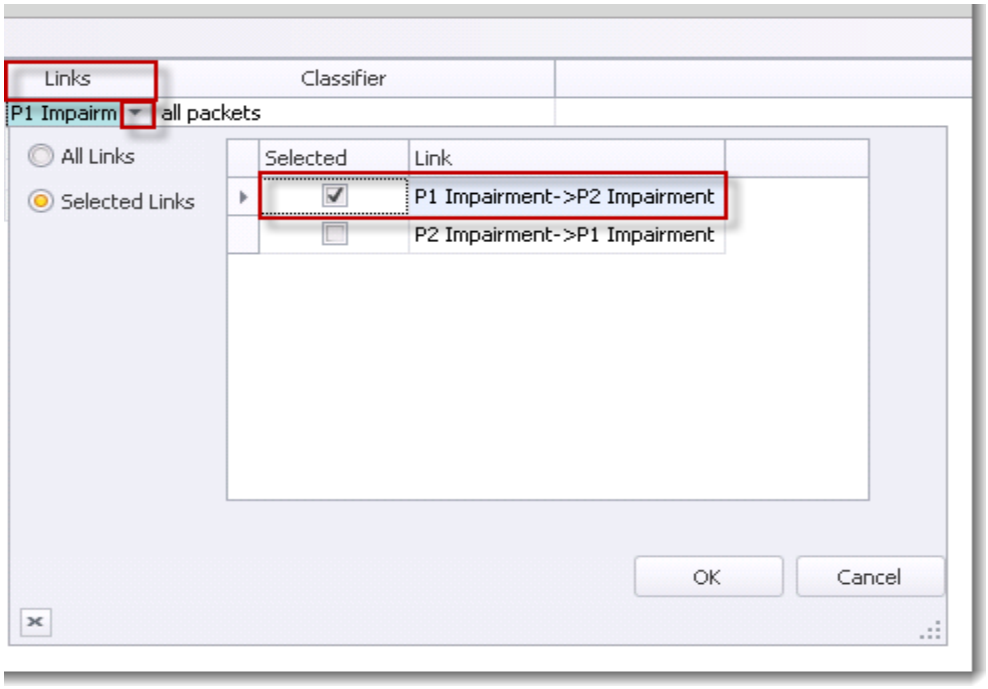


Figure 79. Impairment Link Selection

16. 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%.*

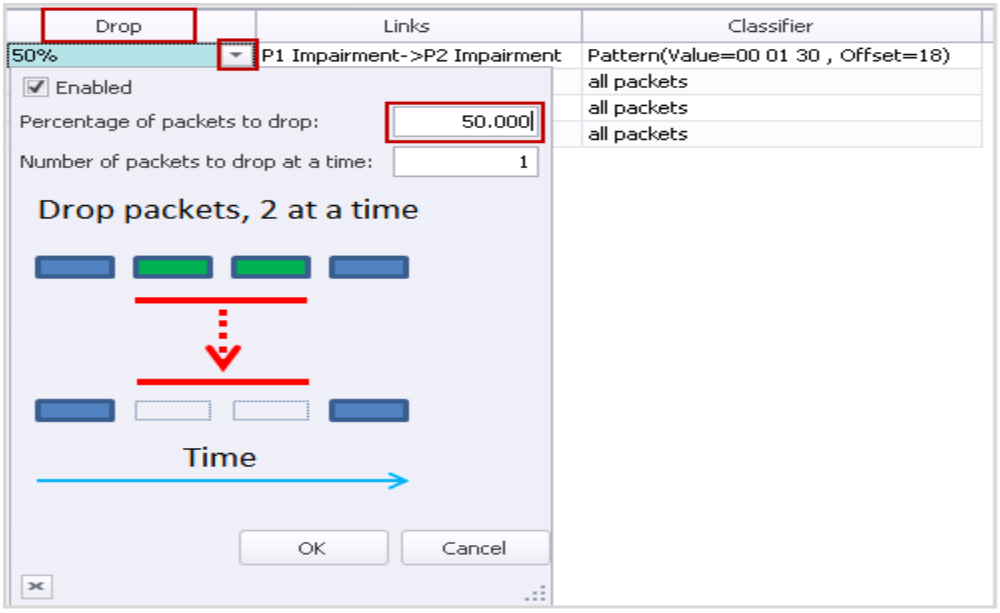


Figure 80. Drop Impairment Configuration

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

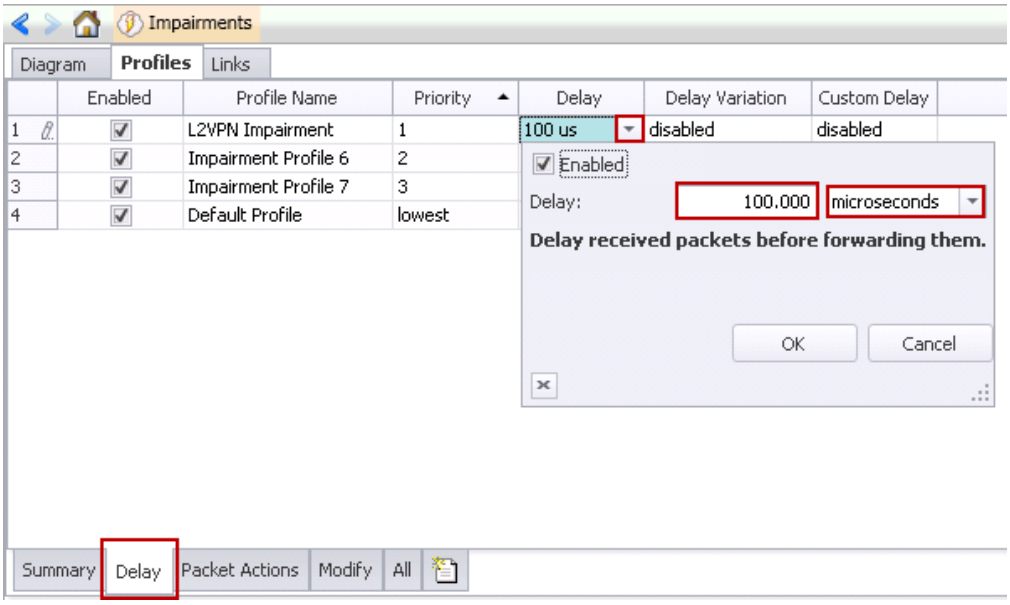


Figure 81. Delay Impairment Configuration

18. 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*.

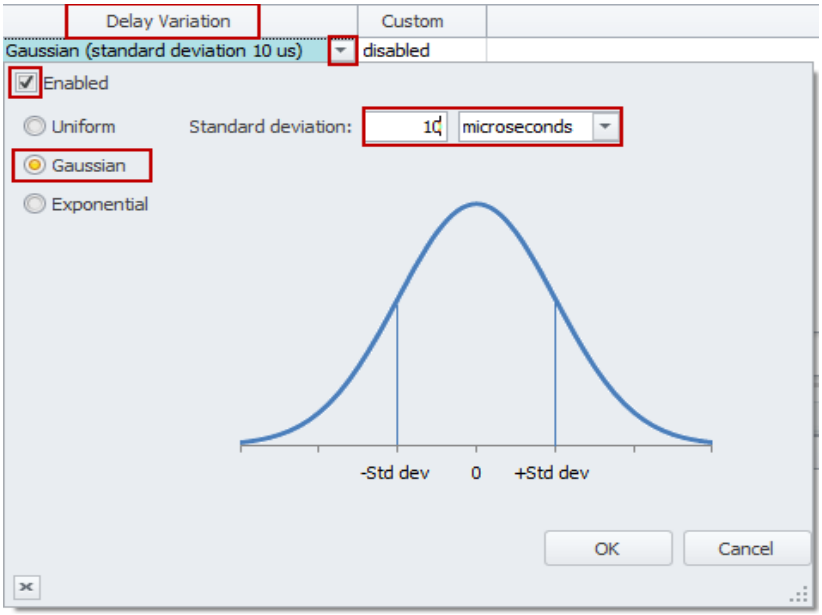


Figure 82. Jitter Impairment Configuration

19. 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 disappears.

Figure 83. Apply Impairment Icon Change

Note:

- Only the enabled profiles are applied to the hardware.
- If the impairment profile contains configuration errors, the exclamation mark remains and a pop-up window appears on the right hand side bottom corner of the IxNetwork GUI. For further troubleshooting, follow the instructions in the Troubleshooting Tips section.

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

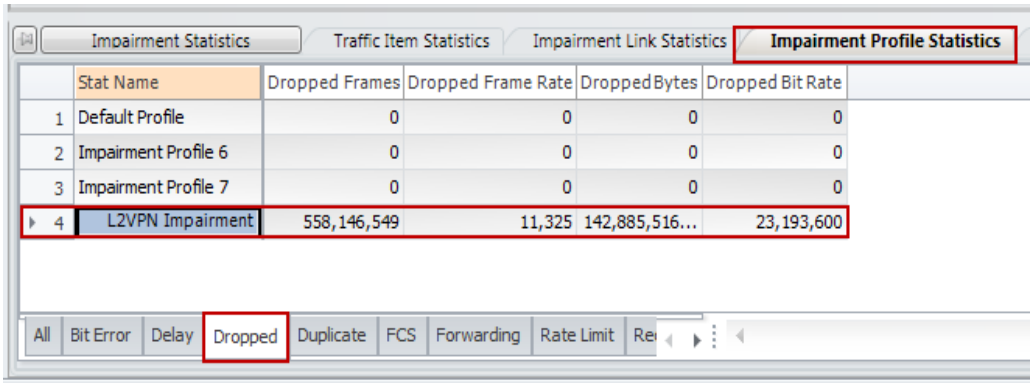


Figure 84. Drop Impairment Profile Statistics

21. Only the profiles with drop impairment enabled 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.

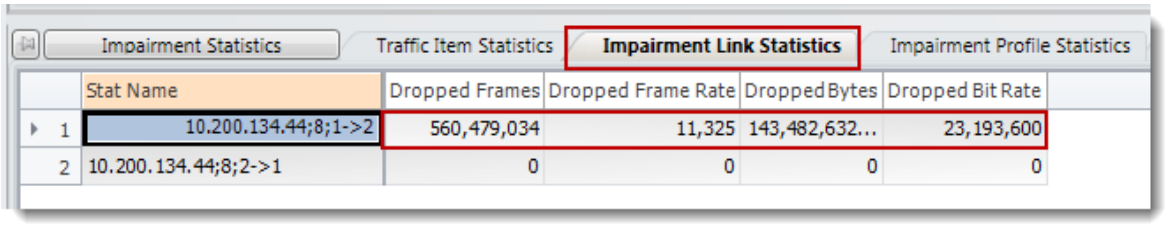


Figure 85. Drop Impairment Link Statistics

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

22. 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. All the traffic classified under Impairment Profile 6 experiences a delay of 30 us, because ImpairNet module has an intrinsic delay of 30 us.

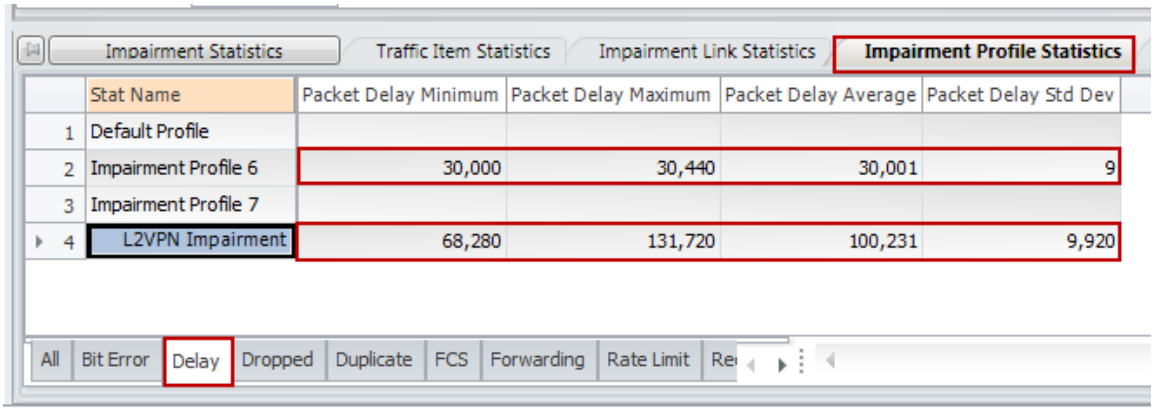


Figure 86. Delay Impairment Profile Statistics

23. 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.

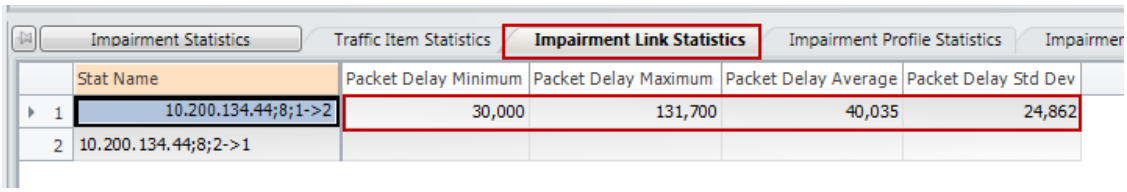


Figure 87. Delay Impairment Link Statistics

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.

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

Go to **Profiles** Tab in the 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*.

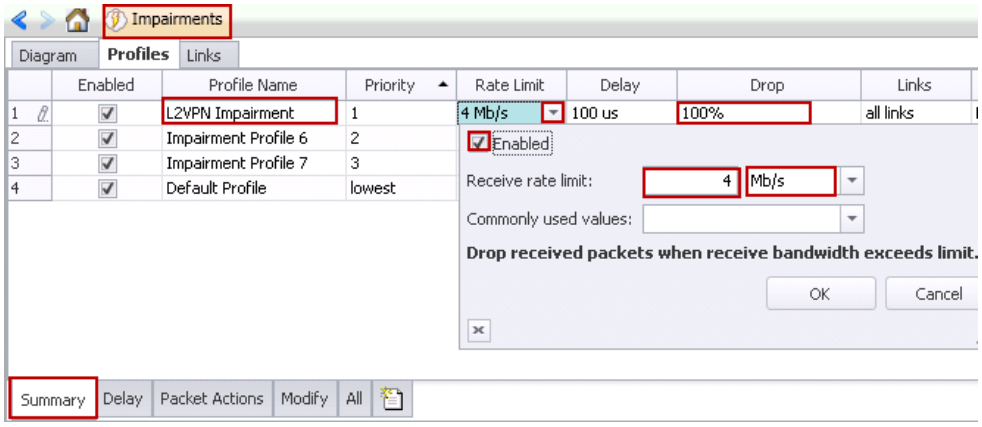


Figure 88. Rate Limit Impairment configuration

Note: For this test setup, the configuration of L2 MPLS VPN parameters is 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 vary.

25. 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 displays an exclamation mark. Click the **Apply Impairment** icon again to apply the impairment profile changes.

Note: You can apply Impairment profile changes 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.

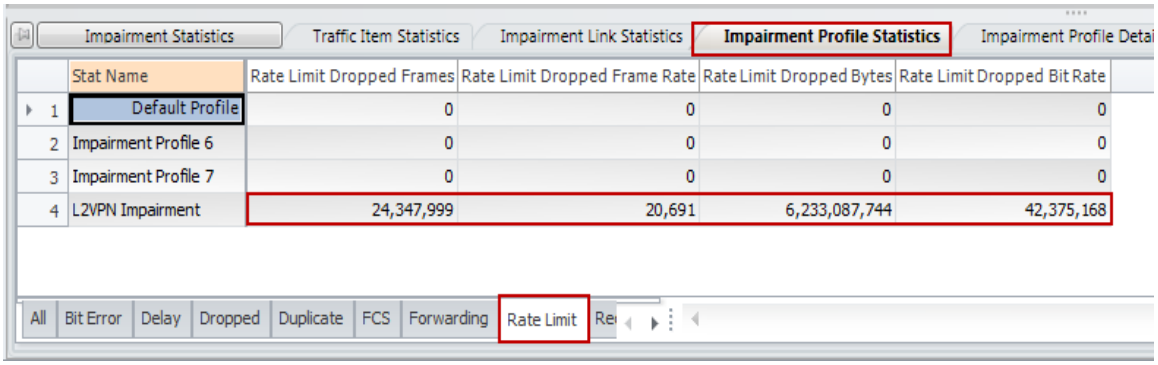


Figure 89. Rate Limit Statistics for Impairment Profile

26. 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.

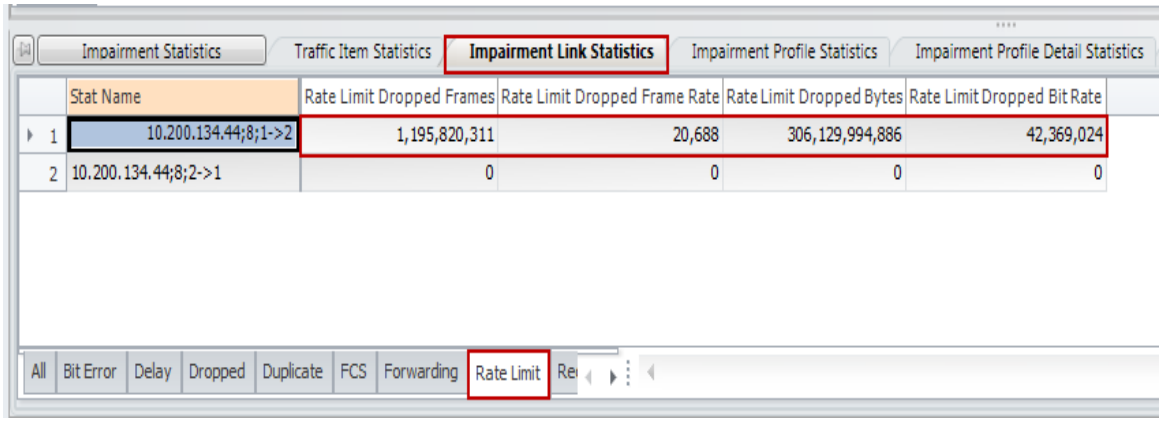


Figure 90. Rate Limit Statistics for Impairment Link

27. 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.

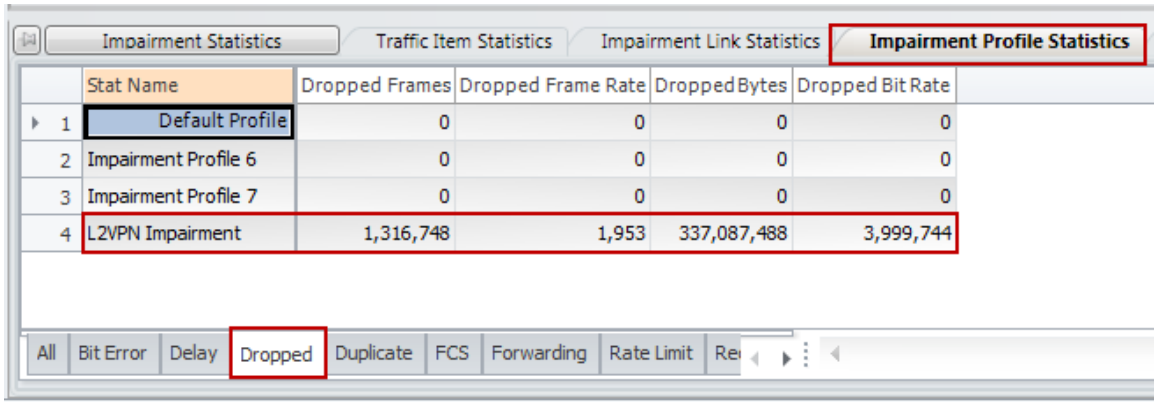


Figure 91. Dropped Statistics with Rate Limit for Impairment Profile

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

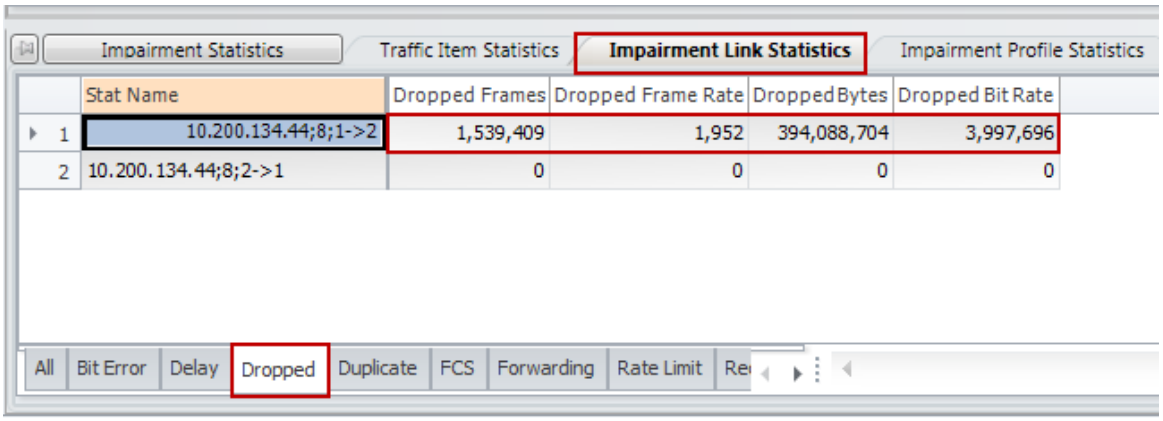


Figure 92. Dropped Statistics with Rate Limit for Impairment Link

Test Variables

You can use each of the following variables 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. Use Copy Classifier and Paste Classifier commands in the Impairments Configuration tab to copy and paste Classifiers across impairment profiles. You can add a maximum of 16 classifiers 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 600 ms for a 10 G impairment module.
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 Service Level Agreements (SLA) 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 marks. 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 you cannot disable. 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 cleared in the **Links** tab.
An error is displayed when Apply Impairments is clicked.	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.
Traffic is not getting impaired although the Apply Impairment icon does not show any error.	Ensure that the classifier value, mask, and offset are set correctly. Verify that a profile with more generic classifier does not have a lower priority than that of the desired impairment profile. Ensure that you select the **Enabled** checkbox 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 practical L2 VPN – MPLS Network.

Test Case: Modifying Packets to Validate Robustness

Overview

In practical networks, there can be many events that cause particular parts of packets being populated with invalid values. This may lead to unpleasant behavior in network systems – devices may crash, allow unauthenticated access to hackers, slow down services to the point of breakdown. Many a times, hackers employ the man-in-the-middle attacks, where they intercept packets and overwrite them to gain access or impair network services.

The possibility of unauthorized access and the resultant loss of revenue and prestige make testing of abnormal inputs a priority for sensitive applications.

However, these types of problems are the toughest to find, because they are dependent not just on the implementation of a single equipment, but also its ability to withstand protocol packets that are outside the parameters defined in standards. This problem could lead to one faulty device causing havoc with the rest of the network. Additionally, the developer may not even be aware of their presence.

Testing for these impairments, where certain fields within an otherwise perfectly normal packet have incorrect values, allows for catching these kind of bugs earlier in the development/deployment process.

Testing of the robustness of network applications, devices, and systems is of importance to network equipment and software application manufactures, carriers, service providers, Government organizations, defense organizations, financial institutions, and enterprises.

Objective

The objective of this test is to overwrite a field in the IP packets that are passing between two devices.

Impairment ports are placed in any location between the two devices, allowing for the ability to modify packets as they pass back and forth between the two devices. The packet field that we modify is the IP version field.

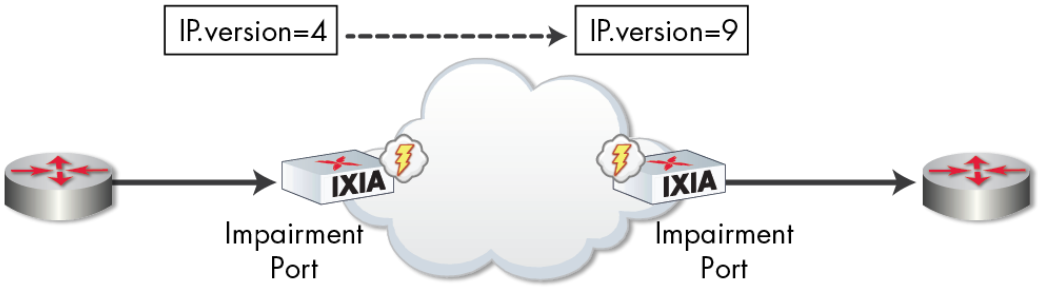
At the end of this test, other test variables are discussed that provide ideas for many more packet modification tests.

Setup

This test setup requires the following equipment:

A. Two devices that are exchanging IPv4 packets between the two of them.

B. Two ImpairNet ports that are connected in-line between these two devices.



This test includes modifying IPv4 packets going in one direction. The IP Version field value is changed from 4 to 9 by the ImpairNet load module.

Step-by-step Instructions

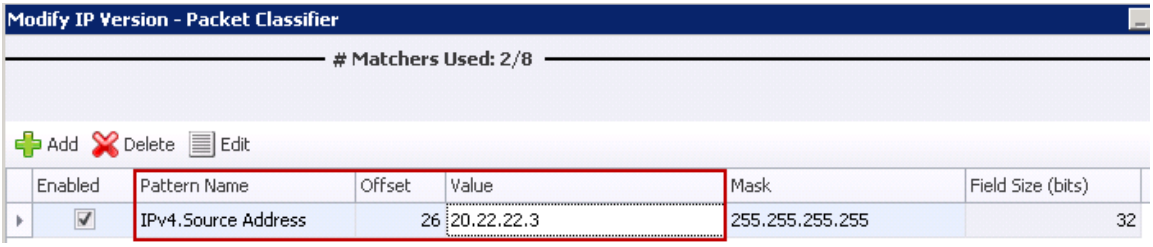
1. Click the 

button to create a new impairment profile.

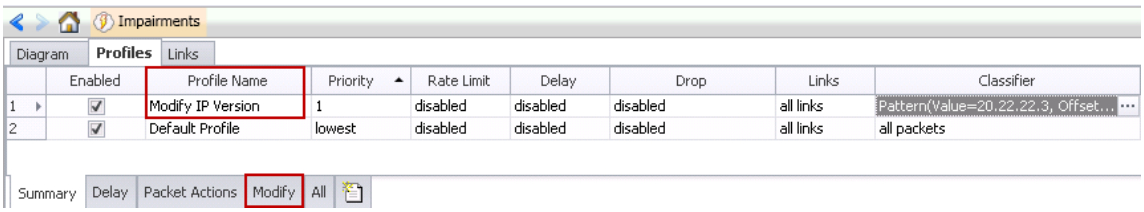
2. You may rename the default profile name to a different one to make it easier to identify. We are using ‘Modify IP Version’ in this example. (Optional)

3. Click on classifier and enter the source IP address of one of the traffic sources. **Note**: Make sure that the mask entered is 255.255.255.255 so that only one traffic flow is classified to be impaired.

   Click **OK**.



4. Back on the profile, the Classifier displays the pattern you entered above.

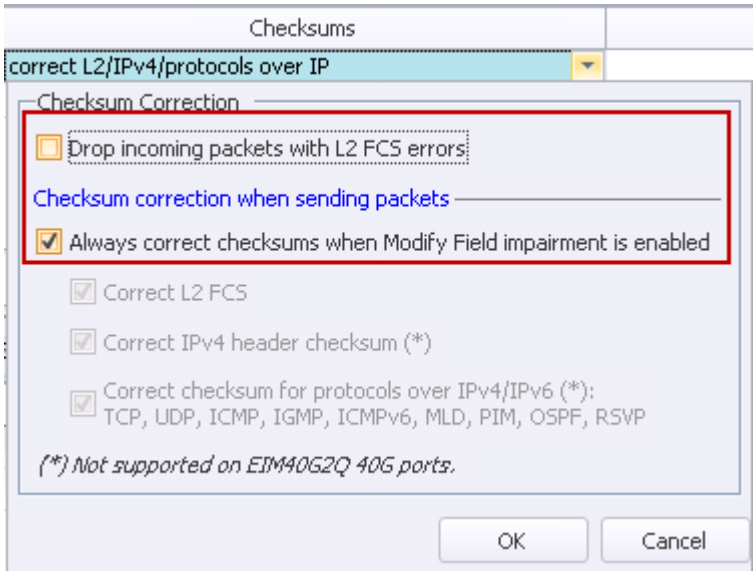


5. Click the **Modify** tab.

   This action displays the modification configuration associated with a profile.

6. Click the **Checksums** column to show checksum options.

7. Select **Always correct checksums when Modify Field impairment is enabled**. This selection ensures that the modified packets have correct checksums.



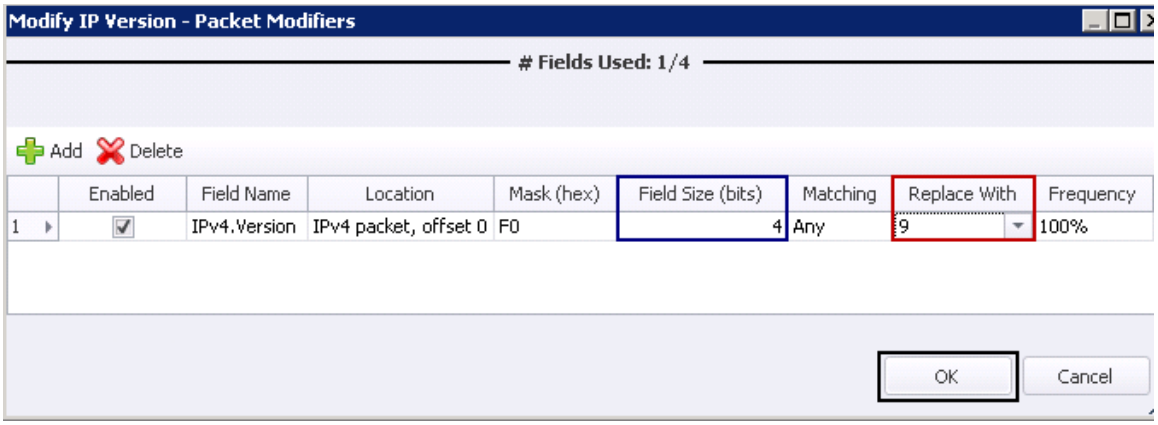
8. Modify IP version information from value 4 to value 9.

   This value is configured in the **Packet Modifiers** action.

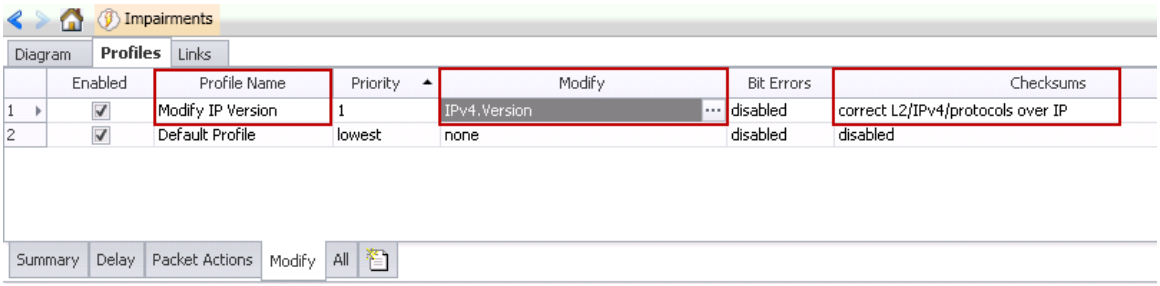
9. Just as with packet classifier, select the field to be modified. In this case, it is IP version field.

10. The next step is to instruct ImpairNet what values to modify. You may enter those values in the **Matching column**. The values in **Replace with** column replace the **Matching** column values.

11. Click OK.



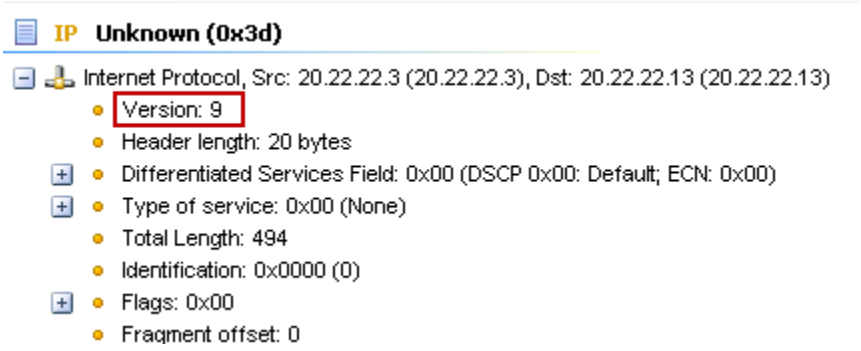
12. Verify that **Modify** step includes the values configured above.



13. Click the **Apply Impairments** icon to apply the impairments. The exclamation mark in the icon disappears indicating that changes in the impairment configuration are applied to ports.

14. Capture packets leaving the ImpairNet ports.

    Packet capture reveals that only packets from source IP address 20.22.22.3 have the IP version value of 9. The rest of the packet flows will have the normal IP version value of 4.



Results Analysis

This test proves the ability of ImpairNet ports to modify real-time packets as they pass between the ImpairNet ports. We also verified that only those packets that match the classifier criteria are modified, while the rest of the traffic is not affected by packet modification.

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 error. Make sure that traffic is flowing through the module and the drop rate is not set to *100%*.
No traffic is flowing through the impairment links.	To ensure that traffic is flowing through the impairment modules: • Disable all the impairment profiles except the default profile • Apply Impairments and check that Rx/Tx Frames statistics for the impairment link corresponds to the traffic. • Ensure that both the links for the impairment port pair are forwarding, that is, the checkboxes for **Interrupt Forwarding** are cleared.
An error window appears, on clicking Apply Impairments.	To overcome this error: • Ensure that there is no impairment profile configuration error. • Make sure that the impairments are applied with in the configuration limits. • Check ImpairNet module specifications for the configuration limits.
Traffic is not modified though the Apply Impairment icon is not showing any error.	To overcome this error: • Ensure that the classifier value, mask and offset are set correctly.

Issue	Troubleshooting Solution
	• For packet modification, make sure that you selected the correct field to be modified and that field is actually present in the packets on the wire. • Verify that a profile with generic classifier does not have a lower priority than that of the desired impairment profile. • Confirm that you have selected the **Enabled** checkbox for the configured impairments.

Conclusions

This test verified ImpairNet functionality for packet modification. Packet modification allows the user to proactively test his network infrastructure for vulnerabilities arising from malformed or malicious packets.

Test Case: Impairment Testing For Bandwidth Limitations

Overview

Practically, customers possess a limited amount of bandwidth guaranteed for the service access towards the Internet. Typically the service providers allow maximum rate of traffic during non-peak hours and guarantee minimum channel capacity during high density customer usage. This implies a different network dynamic and end-user experience during an extended period of time.

To test the capability of the service access gateway under limited bandwidth conditions, a network cloud emulator, such as ImpairNet, is used to simulate a congested network or limited bandwidth resources similar to when working on backup connection. The data from the powerful statistics provides user experience characteristics for the impaired types of traffic.

For content aware gateways bandwidth limit network emulation is required to determine the optimum data rates for different classes of user profiles.

Objective

The objective of this test is to impair the traffic between the content servers and the emulated clients. ImpairNet load module is configured to limit the packets classified with rate limit configured for all the transactions in execution. This will challenge the SYN stability testing for the TCP based traffic and also deliver the key performance indicators for application delivery.

The impairment module can be inserted in any link where it is needed. You can apply the steps used in this test case for Layer 3 VPN, access router, or service delivery gateway.

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

Setup

The setup consists of IXIA ports acting as clients on two individual IP private ranges, with ImpairNet module in between the simulated users and DUT. This setup emulates an enterprise branch office accessing resources from the main branch datacenter. The impairment active on the network emulates the usage of backup line connection with limited data transfer while traffic is in the peak hours with different rate profile for each of the user IP range.

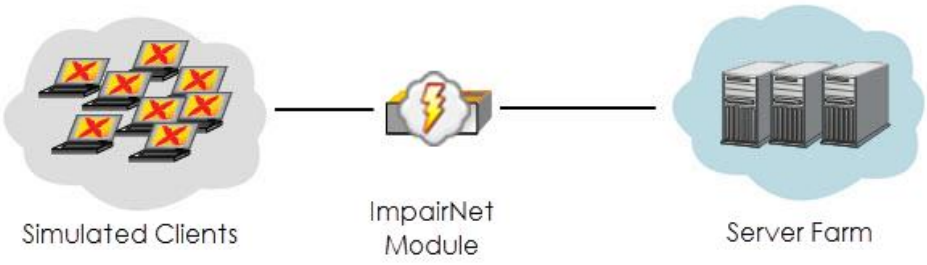


Figure 93. ImpairNet Testing – Bandwidth limiting topology

Step-by-step Instructions

Performing the step-by-step instructions explained in the this section will result in bandwidth limiting Impairments test for the access network topology.

1. Configure a HTTP Get activity for a large file size. In this test we configure a file size of **1MB**. Depending on the scope of test, you can configure different sizes depending on network topology or scope of the traffic.

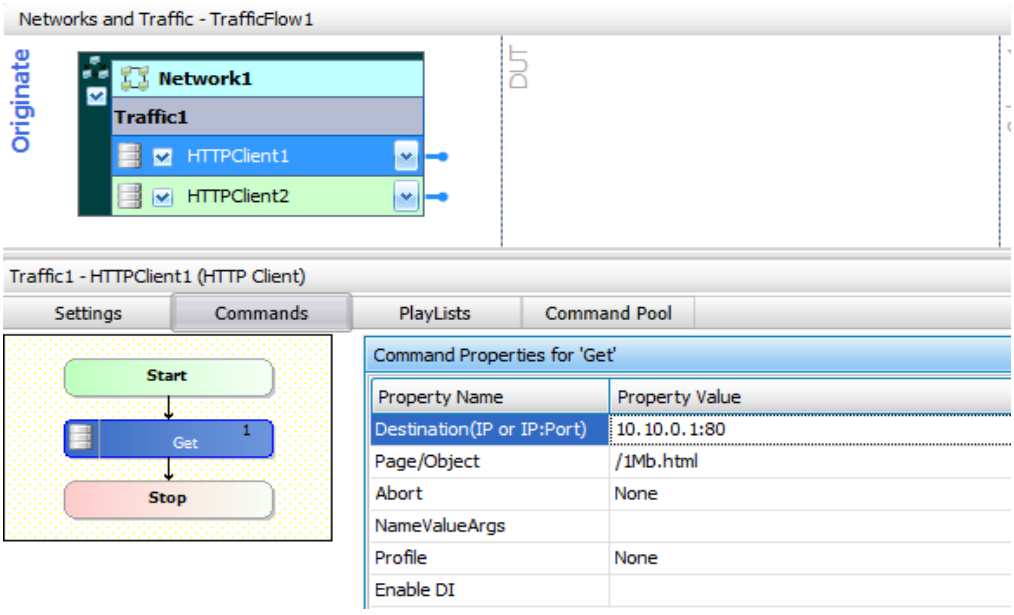


Figure 94. HTTP Activity – Target destination and object configuration

2. Reserve two impairment ports in IxLoad. 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 pair of ports.

3. Configure the test objective to simulate *1,000* concurrent users for the all the activities with *50%* of users per IP range client simulation with a *10 minutes* sustain time.

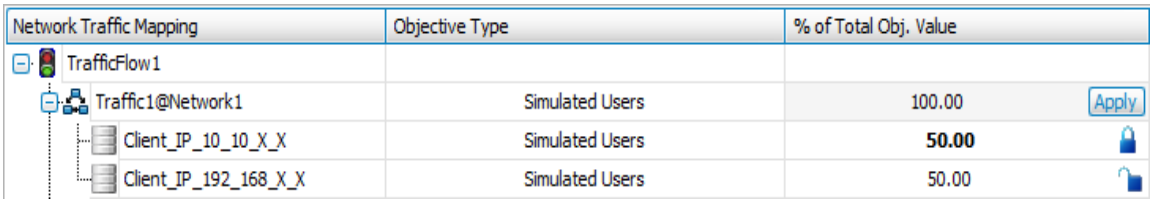


Figure 95. HTTP Activity – Objective distribution

Note: You can configure advanced timeline for a wider range of user connection behavioral patterns. This allows distortion in the objective values such as pulses or bursts with multiple segments of target objectives to mimic the actual behavior of users.

4. **Enable ImpairNet** for the current activities from the **Traffic** command tab. A new menu automatically appears once enabled in the left tree as part of test configuration.

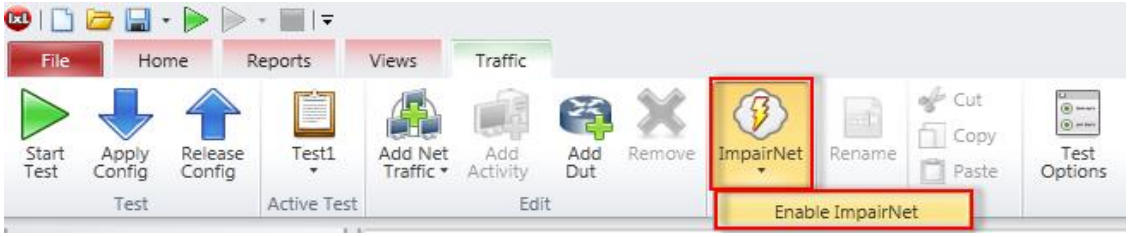


Figure 96. Enabling ImpairNet for test execution

5. Access **ImpairNet** menu and select **Profiles** tab to enable the configuration screen.

6. Add a new profile from the **Add Profile** ribbon command. This action adds a new configuration row on top of the default profile. The newly added profile is used to match and impair the traffic form the current test case.

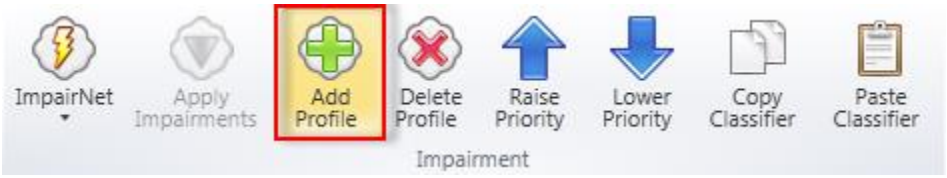


Figure 97. Adding a new impairment profile command

7. Configure the newly added profile to limit the rate by enabling the **Rate Limit** function.

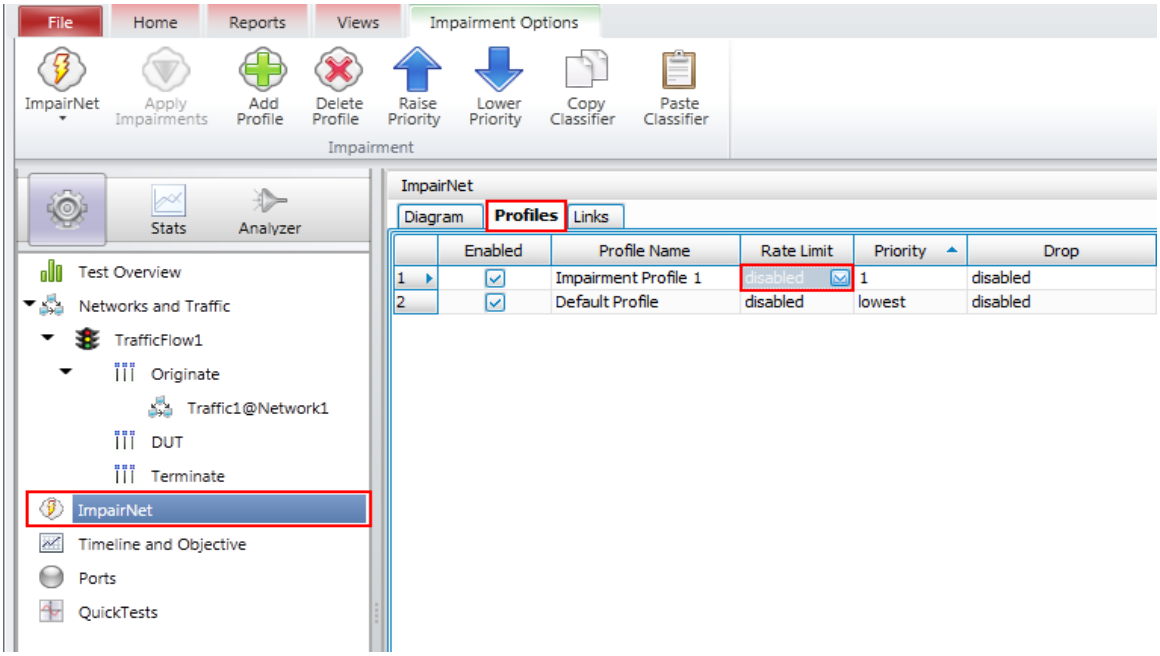


Figure 98. Enabling the Rate Limit impairment

8. Set Rate limit to *100Mbits*. Predefined profiles are available for user convenience that emulates commonly used access interfaces rates.

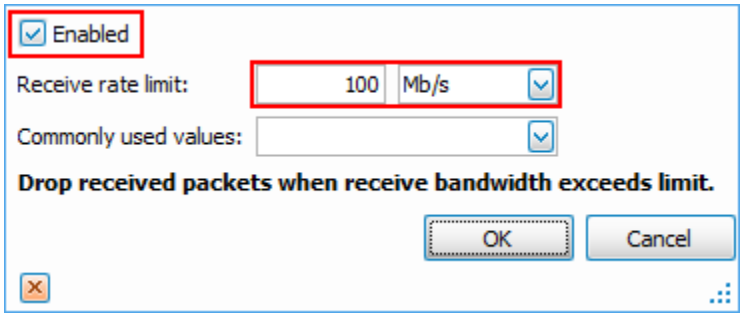


Figure 99. Configuring the test objective rate limiting value

Note: In order to limit the desired packets, you must configure proper classifiers in order to impair the targeted traffic. All the unclassified traffic matches the default profile configured rules of impairment. By design, default profile will not impair any type of traffic.

9. Enable the **Classifier** configuration screen for the profile created to impair the target traffic.

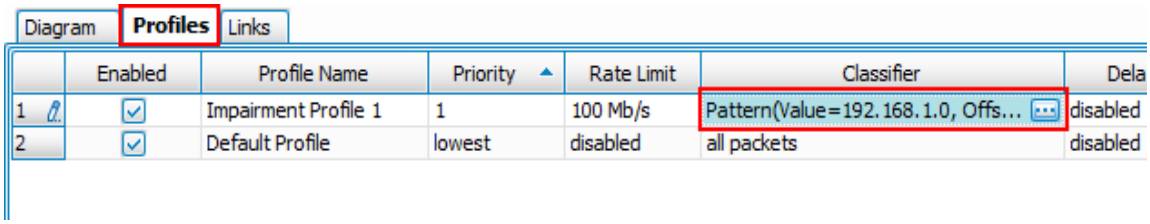


Figure 100. Accessing the classifier configuration screen

10. **Add** a new classifier as **destination IP** address and set the target destination address according to test configuration.

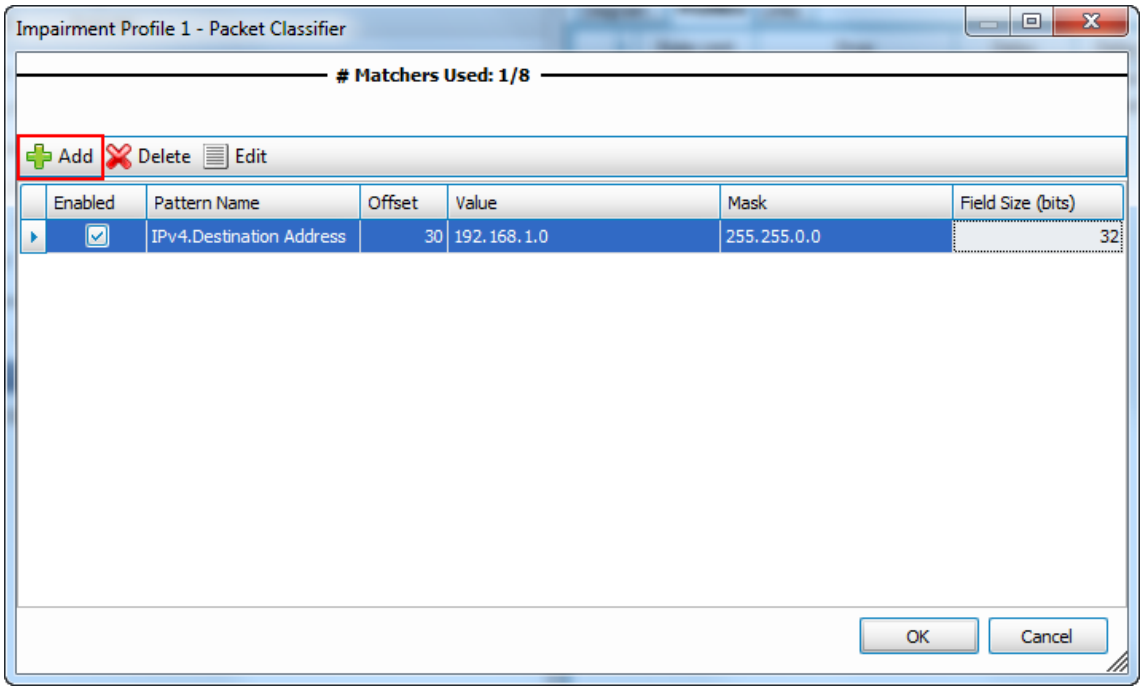


Figure 101. Adding a new impairment packet classifier

11. Configure the target field desired to match the traffic. You can configure up to 8 protocol layers for a high granularity configuration and to assure that a specific traffic type is affected.

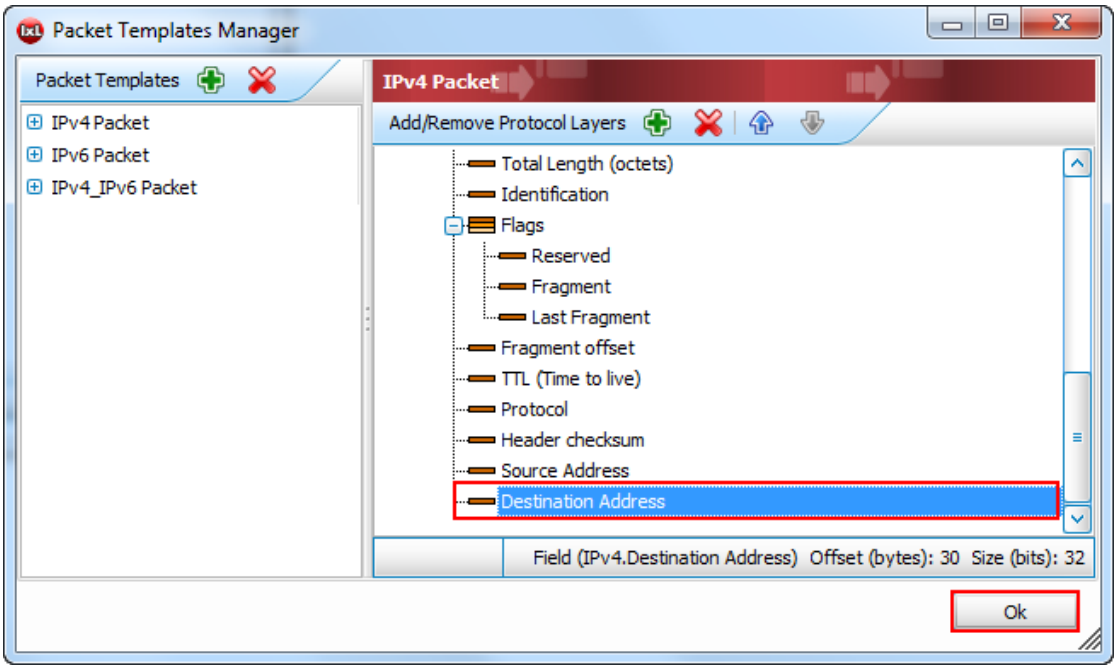


Figure 102. Selecting the protocol layer targeted for impairment

12. Assign the ports according to existing network topology to execute the test. ImpairNet ports are assigned in pairs (ingress and egress traffic).

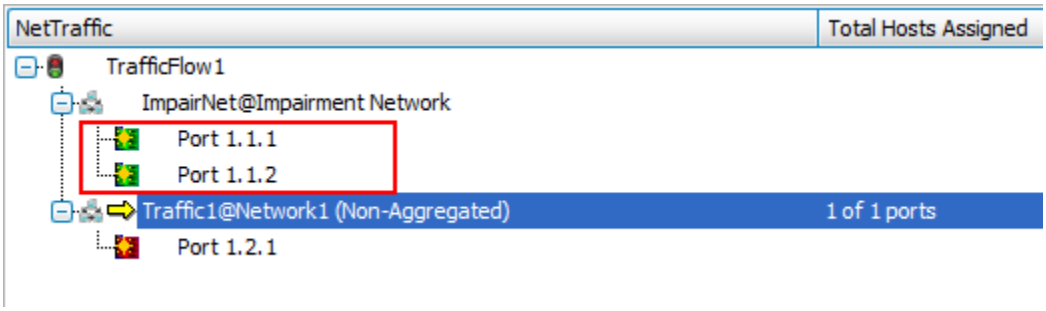


Figure 103. Assigning ImpairNet ports

13. At this point the traffic is configured and the profiles for impair populates with the limited target destination traffic. Execute the test by accessing the ribbon icon named **Start Test**. IxLoad begins the required configuration deployment and starts the test execution.

14. Select the **HTTP Client – Throughput Objective** and **Impairment Link Statistics** check box to access the run-time statistics for the test activity.

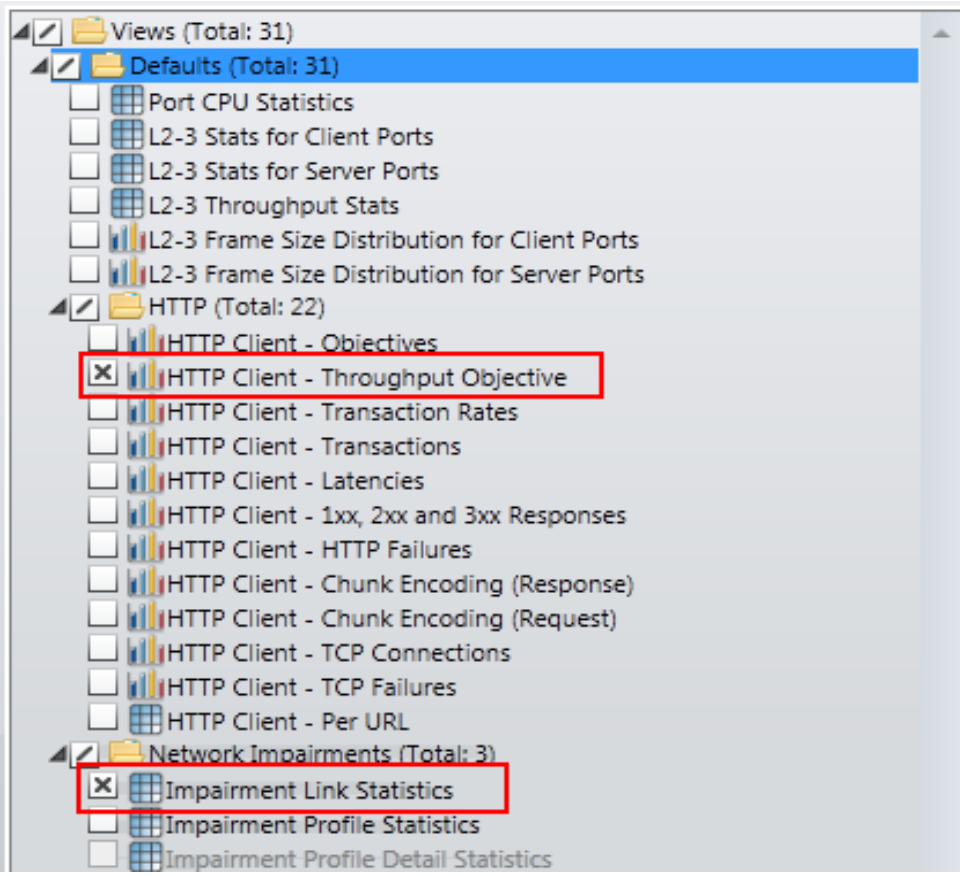


Figure 104. Selecting the Active Views

15. To view the traffic generated for the impaired subnet (traffic limited to the target bandwidth), select **Throughput** from the **HTTP Client** statistics and execute command **Drill-down by Net-Traffic.** This command assists in generating a new view for all the traffic performed by Client Network.

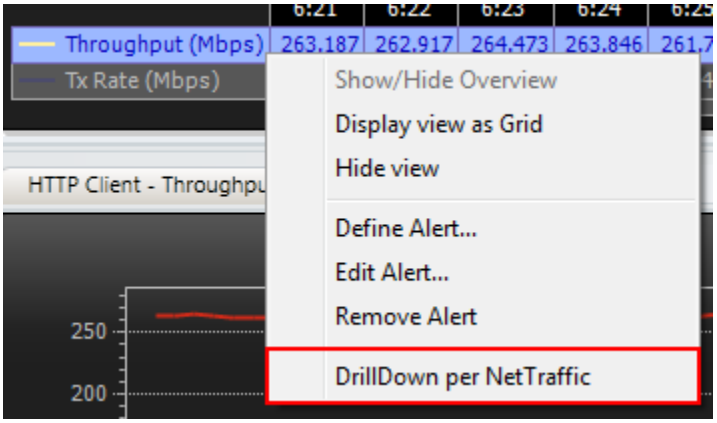


Figure 105. Selecting views specific to the Client Network

16. To view traffic performed independently by each activity, access the Net-Traffic throughput and **Drill-down by Activity**. This action displays the throughput for each activity independently.

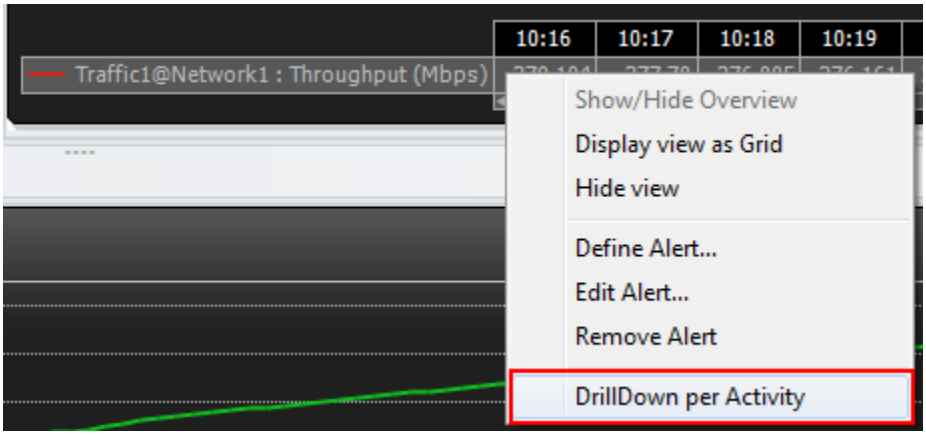


Figure 106. Selecting view specific to the emulated Client Activities

17. From ImpairNet menu, disable the profile. 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 disappears.

Figure 107. Apply Impairment Icon Change

18. You can obtain information regarding the dropped frames rate by accessing the **Impairment Profile statistics** and browsing to the **rate limit** tab. Analyze the displayed information to ensure that the packets are dropped at the desired rate.

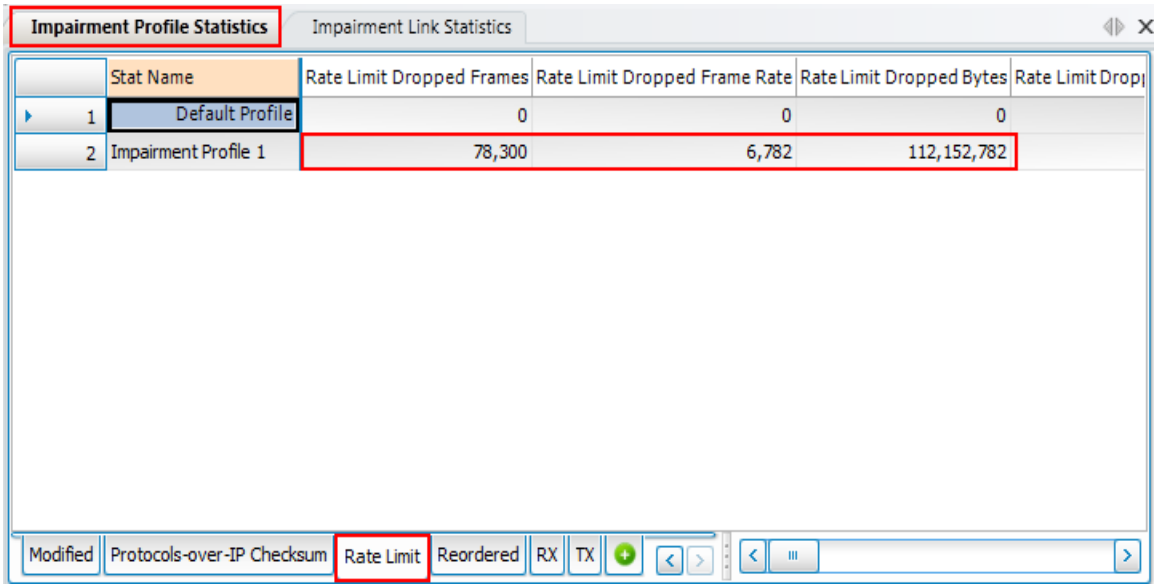


Figure 108. Selecting views specific to configured impairment profile

Test Variables

Use each of the following variables in separate test cases. Use the above test case as a baseline and modify a few parameters in the same Impairments view. You can create various scalability tests to utilize the DUT operating completely in presence of actual world network impairments.

Performance Variable	Description
Create multiple profiles	Create up to 16 bidirectional, or 32 unidirectional impairment profiles per impairment port pair.
Add multiple classifiers	Add multiple classifiers in a single impairment profile. You can copy and paste the classifiers across impairment profiles by using Copy Classifier and Paste Classifier commands in the **Impairments Configuration** tab. A maximum of 8 classifiers can be added for each link direction.
Apply impairments in both link directions	You can select to impair one or both the links.
Increase Delay	Introduce delay to a maximum of 6s for every impairment profile on 1G impairment module, and to a maximum of 600 ms for every impairment profile on 10G impairment module.
Apply different delay variations	You can apply uniform, exponential and customized delay variations.

Performance Variable	Description
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 BER impairments in addition to drop impairments. Reorder and duplicate impairments are present in the **Packet Actions** tab.

Results Analysis

This test proved that WAN Link conditions such limited bandwidth capacity can be successfully emulated and traffic rate can be selected to impair.

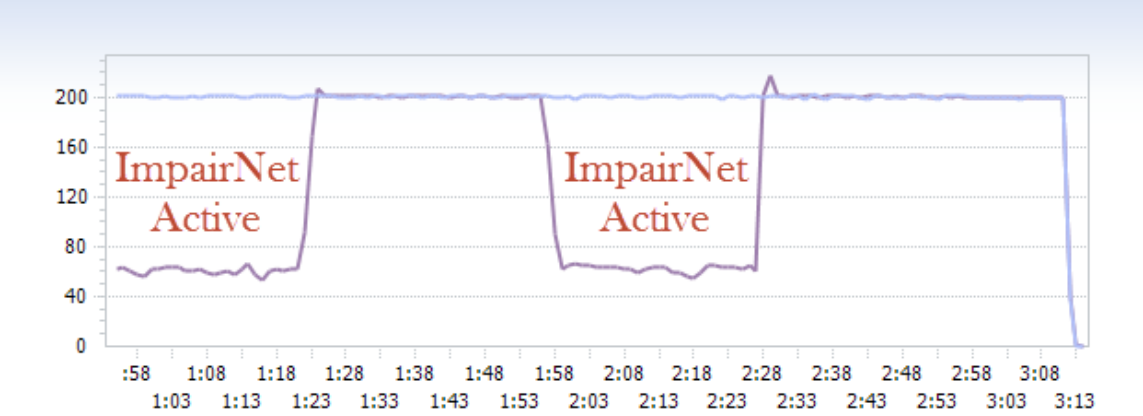


Figure 109. Displayed throughput with impairment conditions

In this test, only traffic for a specific destination IP subnet were impaired, but you can also impair other packet types in a similar way to completely test the device behavior under limited bandwidth connectivity.

Troubleshooting Tips

Issue	Troubleshooting Solution
Impairment profiles are enabled, but impairment statistics are not updated.	Ensure that the **Apply Impairments** icon is error free. Make sure that traffic is flowing through the module and the drop rate is not set to *100%*.
No traffic is flowing through the impairment links.	To ensure that traffic is flowing through the impairment modules: • Disable all the impairment profiles except the default profile. • Apply Impairments and check that Rx/Tx Frames statistics for the impairment link corresponds to the traffic. • Ensure that both the links for the impairment port pair are forwarding, that is, the checkboxes for **Interrupt Forwarding** are cleared.
An error window appears, on clicking Apply Impairments.	To overcome this error: • Ensure that there is no impairment profile configuration error. • Verify that the impairments are applied with in the configuration limits. • Check ImpairNet module specifications for the configuration limits.
Traffic is not impaired though the Apply Impairment icon is not showing any error.	To overcome this error: • Ensure that the classifier value, mask, and offset are set correctly. • Make sure that a profile with generic classifier does not have a lower priority than that of the desired impairment profile. • Verify that you have selected the **Enabled** checkbox for the configured impairments.

Conclusions

This test verified that the device or system under test is functioning correctly under limited bandwidth connectivity and we analyzed the effect of throughput for a target destination IP subnet.

Test Case: Impairment Testing For Real Time Applications

Overview

The late arrivals or out of order stream of packets highly impact the system stability and user experience rating. Such behavior is commonly observed on wide area networks with mixed MTU (maximum transmission unit) limits to maximize bandwidth efficiency and minimize transport overhead on specific network segments. On high load, the packet buffering capabilities of the device under test are challenged and packets are delivered with an incorrect sequence or duplicated due to missing confirmation of arrival for the transmitter.

To test the stability of the voice gateway or media transcoder under packet duplication conditions, a service provider network cloud emulator such as ImpairNet is used to simulate a congested network with exhausted resources and improper buffer handling mechanisms. Data from the powerful statistics provide user experience characteristics for the VoIP quality of service for the impaired type of traffic.

For media transcoding gateways and voice gateways, incorrect order of packets network emulation is required to determine the system stability for memory leaks and voice engine coder/decoder functionality for different types of media traffic.

Objective

The objective of this test is to impair the traffic between emulated VoIP endpoints using ImpairNet load module configured to duplicate and reorder RTP packets. This test challenges the system stability and delivers the key performance indicators for application delivery measuring the user experience quality factor.

The impairment module can be inserted in any link where it is needed. You can apply the steps used in this test case for Layer 3 VPN, access router or media delivery gateway.

At the end of this test other test variables are discussed that provide more performance test cases.

Setup

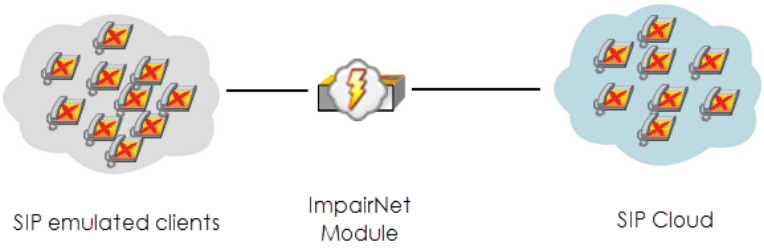


Figure 110. ImpairNet testing - Setup topology for real time application

The setup consists of IXIA ports acting as VoIP clients with ImpairNet module in between the simulated users and DUT. This setup emulates a typical voice delivery service for a branch office or network service provider. The impairment active on the network emulates a wide area network at the capacity limit with congested buffers queues due to intensive traffic as in peak service hours.

Step-by-step Instructions

Performing the step-by-step instructions explained in the following section, result in packet duplication and reordering Impairments test for the access network topology. The following instructions serve as a guide to build other traffic impairment test scenarios.

1. Add two **NetTraffics** for the call initiator and call responder. Configure IP addresses to match the test environment addressing scheme.
2. The configuration of network depends on the physical connection between the devices. Access the **NetTraffics** tab and select the **Ethernet** layer. Set the PHY mode accordingly to the used transmission mode; because the available options are auto media detection, copper, and fiber. This example uses an optical connection.

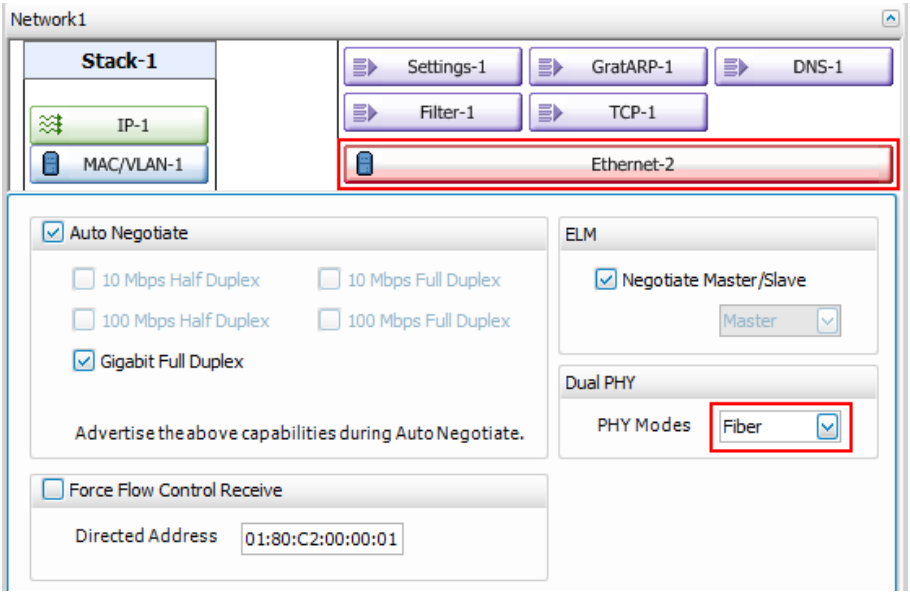


Figure 111. Configuring the physical layer connectivity type

3. Add a **VoIP SIP Peer** activity on each side. In this test, we configure the endpoints using SIP signaling for call establishment and RTP for audio payload transport. Depending on the scope of test, you can configure different call patterns, again depending on the network topology or scope of traffic.

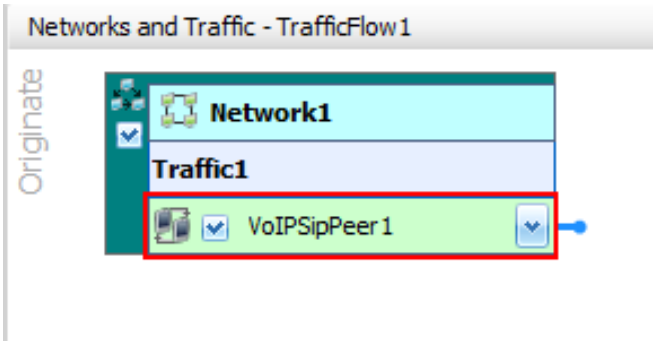


Figure 112. Adding a new VoIP SIP activity

4. Using the symbolic link, drag and drop the cursor to link the two activities.
5. Select a **Basic call with voice** option. Scenario editor automatically populates with the procedures required for signaling and media transmission.

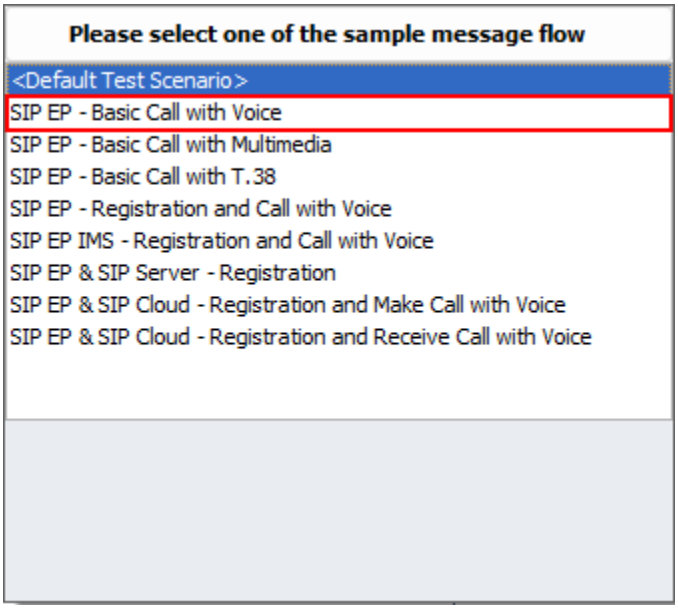


Figure 113. Selecting SIP with RTP activity

6. Select the **VoIPSIPPeer** activity on the call originator endpoint.
7. Select the **RTP** configuration tab. Enable **Calculate advanced statistics** and **per stream statistics**. This selection assists in delivering the metrics for voice quality of service and user experience rating.

8. For the test execution, configure the RTP ports in the range of *10000* to *20000*. Use these values for the RTP payload stream destination when negotiating the SDP capabilities. Impairment is applied using the trigger for the RTP packets configured with these destination ports.

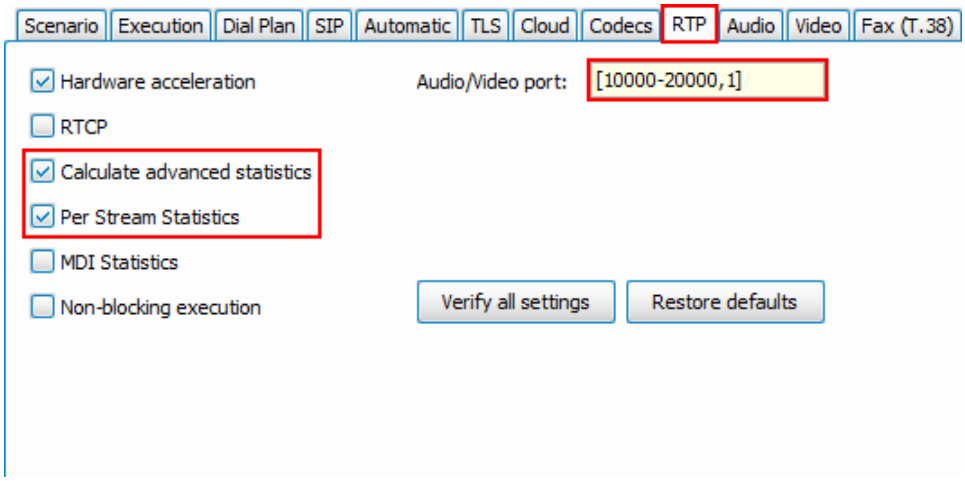


Figure 114. Custom configuration for RTP with quality analysis

9. For configuration of RTP payload, access the **Audio** configuration tab and **Enable audio** for the activity. This action enables execution for all audio script functions from the scenario editor.
10. To enable quality of service rating using E-Model as per ITU-T P.800 recommendations, enable the option **Perform MOS.** The client application automatically enables the **Calculate One Way Delay** option.

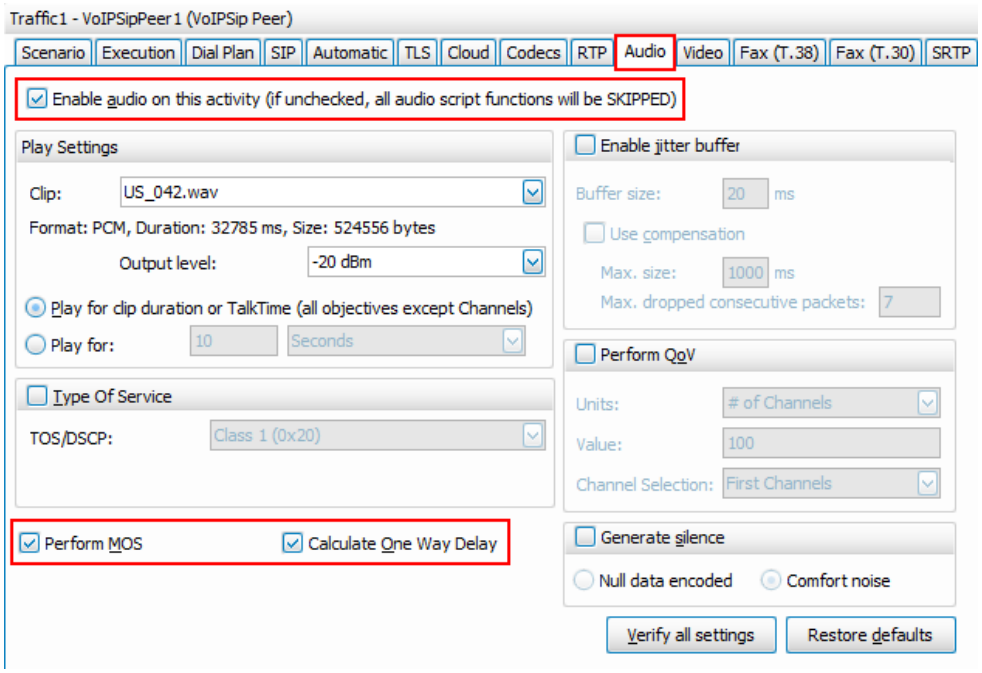


Figure 115. Audio configuration with enabled quality of service

11. Repeat the steps from point 5 for the called endpoint, the one terminating the calls.
12. Enable **ImpairNet** from the ribbon access menu.

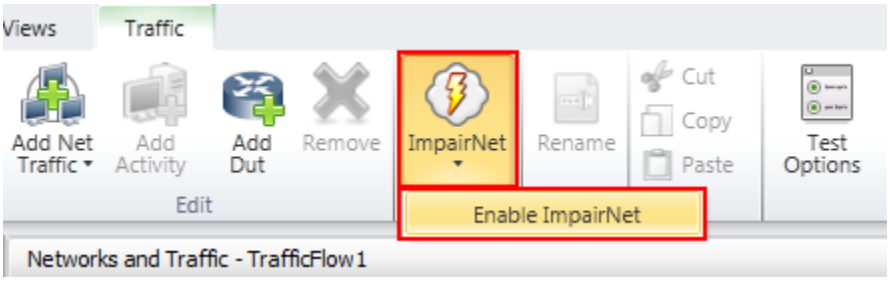


Figure 116. Enabling ImpairNet for test execution

13. Enable **ImpairNet** from the ribbon access menu.
14. Access **ImpairNet** menu from the left tree and add a **New Profile** from the ribbon command.

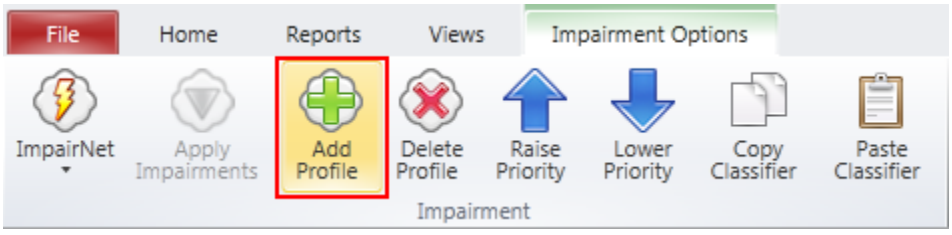


Figure 117. Adding a new profile for impairment

15. In the newly added profile, select **Reorder** option and configure the desired values for the test execution. This scenario reorders packets with a rate of *5%, 3* frames at a time and skips *1* from the streams passing through the engine.

16. Submit the new changes by **enabling** the profile configuration.

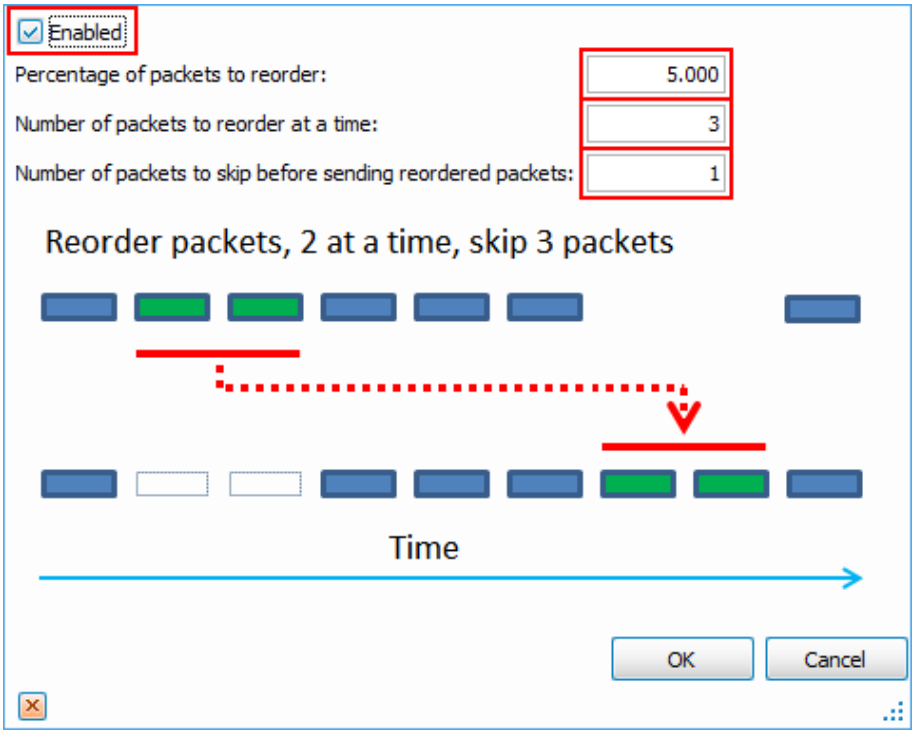


Figure 118. Configuration details for packet reordering

17. In the current profile, select the **Duplicate** option and configure the desired values for the test execution. This scenario duplicates the packets with a rate of *10%, 3* frames at a time and skips *1* from the streams passing through the engine.

18. Submit the new changes by **enabling** the profile configuration.

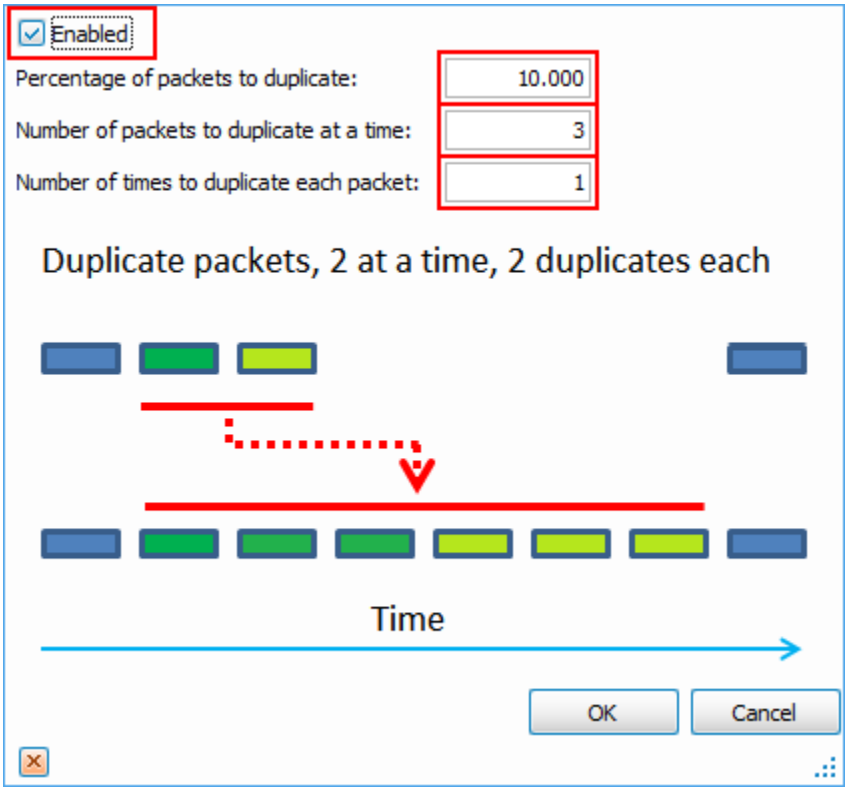


Figure 119. Configuration details for packet duplication

Note: To duplicate and reorder the desired packets, configure the appropriate classifiers in order to impair the targeted RTP traffic. All the unclassified traffic matches the default profile, with the configured rules of impairment. By design, default profile will not impair any type of traffic.

19. Enable the **Classifier** configuration screen for the profile created to impair the target traffic.

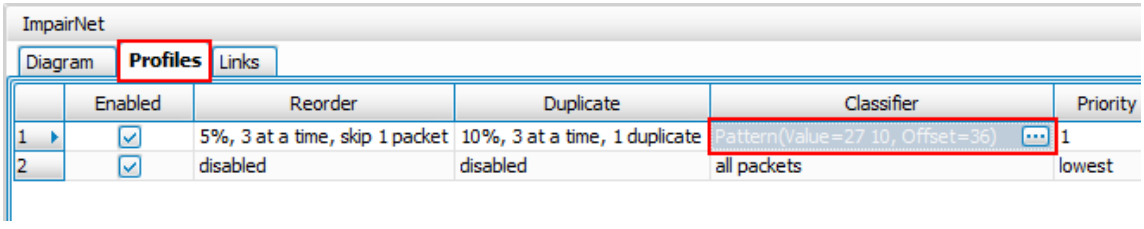


Figure 120. Accessing the classifier configuration screen

20. **Add** a new packet classifier.

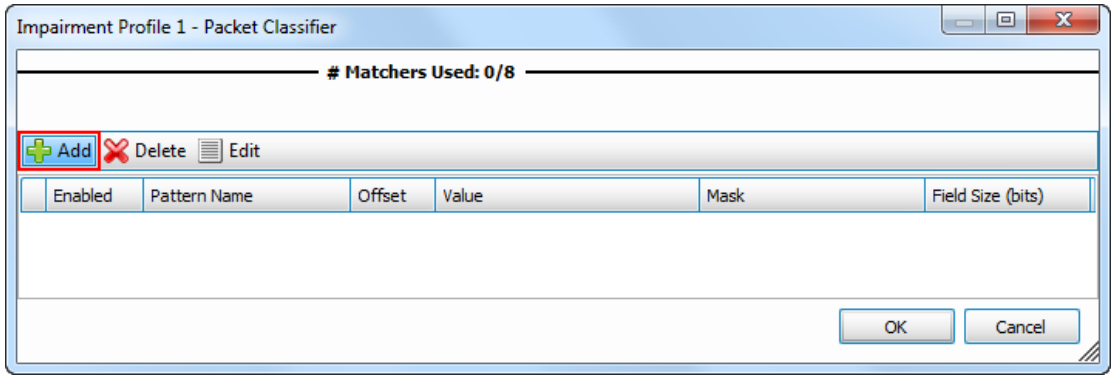


Figure 121. Adding a new packet classifier

21. **Add** a new protocol layer classifier from the templates manager.

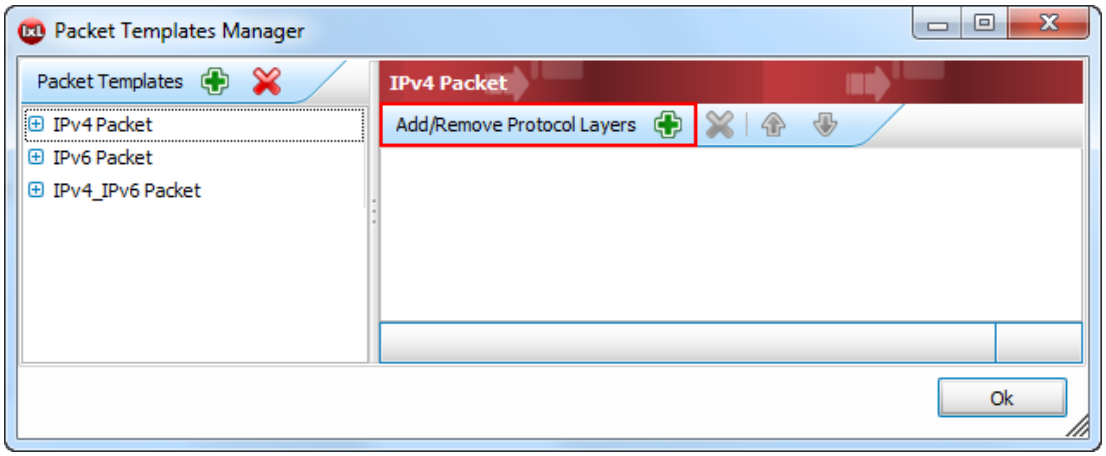


Figure 122. Adding a new protocol layer classifier

22. Select the desired protocol for classification. This example uses **UDP** transport protocol. An extensive list is available for selection for a multitude of L2-7 protocols.

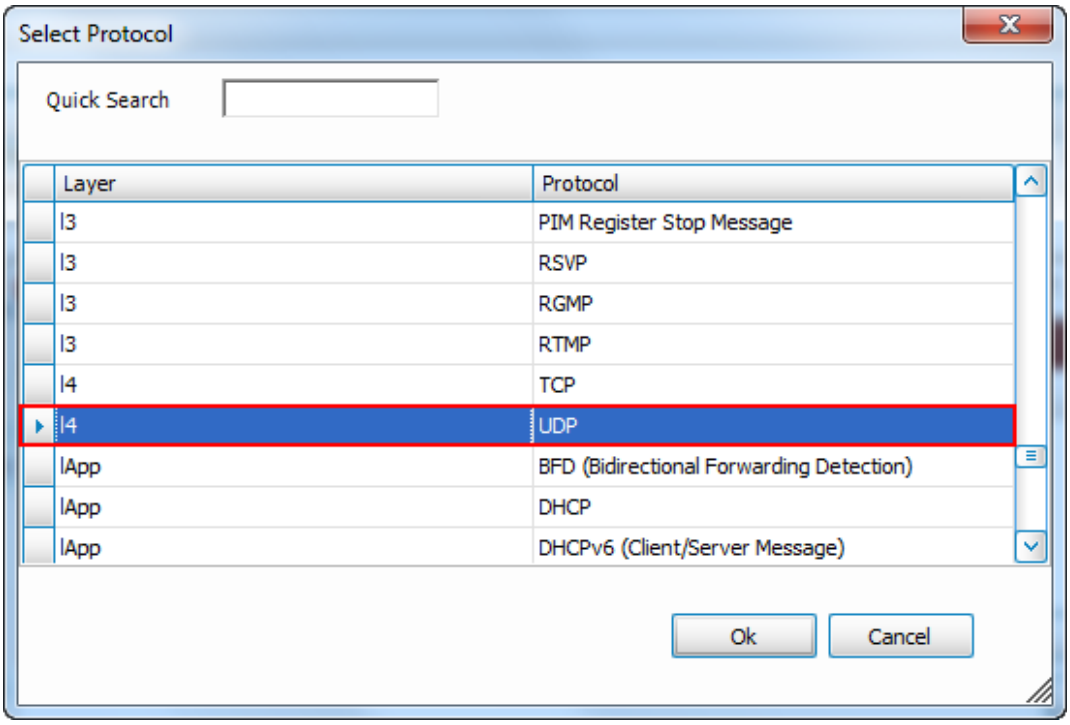


Figure 123. Selecting the protocol for classification

23. After selecting the target protocol, configure the specific fields of the protocols. This example targets for impairment of all RTP traffic based on **UDP Destination Port**. Submit the changes to save the newly added configuration.

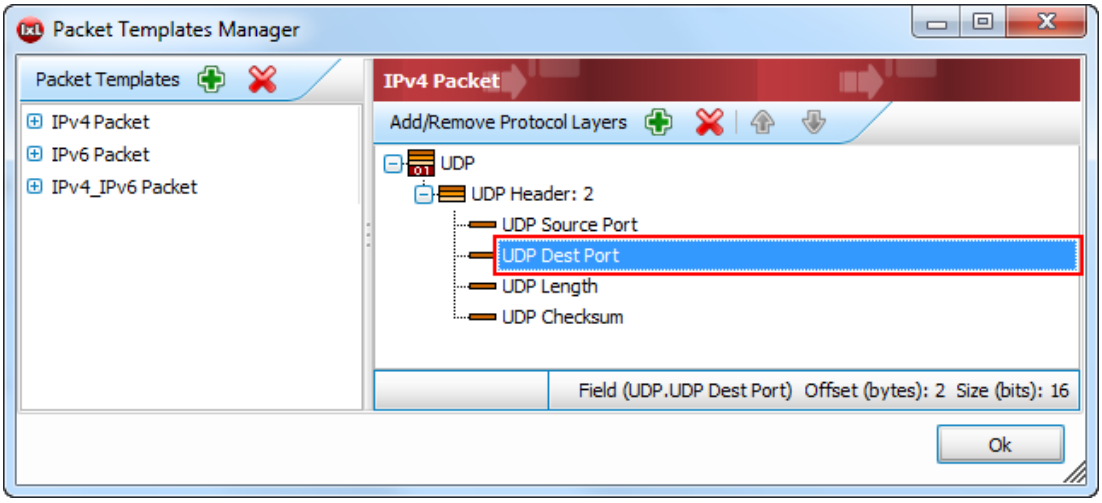


Figure 124. Selecting the protocol fields for targeted traffic

24. Modify the default values for the protocol layer variables to match the considered traffic for impairment. For the current scenario, configuration is adjusted to match UDP destination port *10000*.

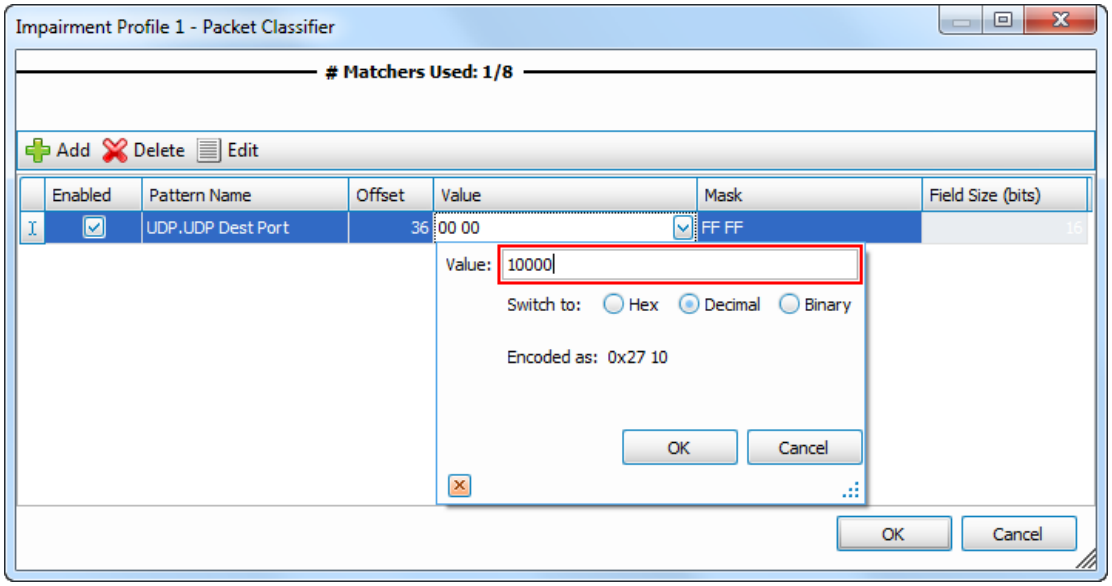


Figure 125. Configuring UDP protocol layer with destination port for packet classification

Note: You can configure up to 8 protocol fields simultaneously to assist a high granularity in the classification of the target traffic. The traffic impairs if all of the configured packet classifiers are matched at the same time.

25. Modify the default values for the protocol layer variables to match the considered traffic for impairment. For the current scenario, configuration is adjusted to match UDP destination port *10000*. This value represents the destination port for all the RTP streams the system generates, and destination for the impairment classification.

26. Assign the ports according to existing network topology to execute the test. ImpairNet ports are assigned in pairs (ingress and egress traffic).

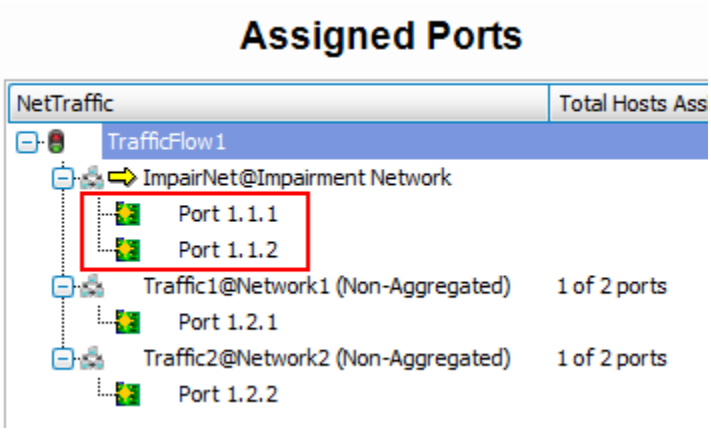


Figure 126. Port assignment option for ImpairNet and user emulated traffic

27. Configure the test objective for the scope of the test. This example uses *1000* active **channels** objective. This value opens 1,000 RTP connections per each direction for the emulated endpoints.

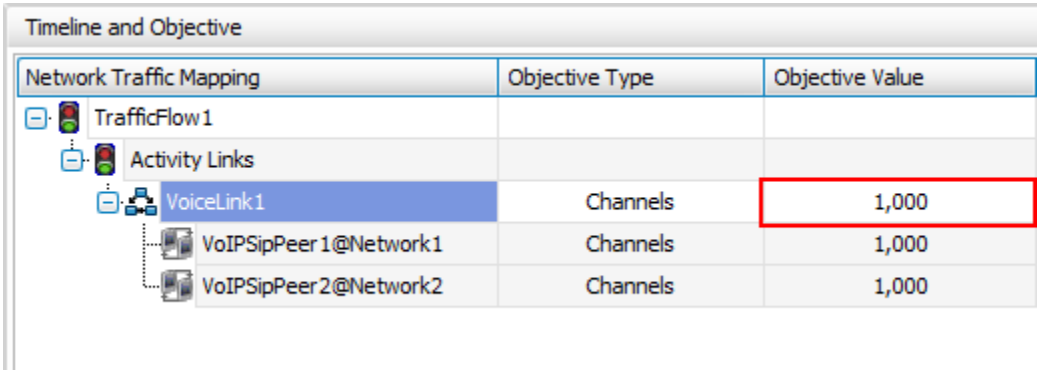


Figure 127. Configuring test objectives

28. Configure the test execution for *10 minutes* sustain time and ramp-up value of *500 channels per second.*

29. At this point, the VoIP traffic is configured and the profiles for impairments populates with the target destination traffic to be reordered and duplicated. Execute the test by accessing the ribbon icon named **Start Test**. IxLoad begins the required configuration deployment and starts the test execution.

30. Select the Impairment Link Statistics and RTP per channel statistics check box to access the run-time statistics for the test activity.

31. From **ImpairNet** menu, disable the profile. 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 in the **Apply Impairment** icon disappears.

Figure 128. Apply Impairment Icon Change

32. To view the packet duplication and reordering statistics for impairment links, click **Impairment Link Statistics** tab in the Impairment Statistics view and then click the **Duplicate** tab. Perform the same steps to access **Reorder** tab statistics.

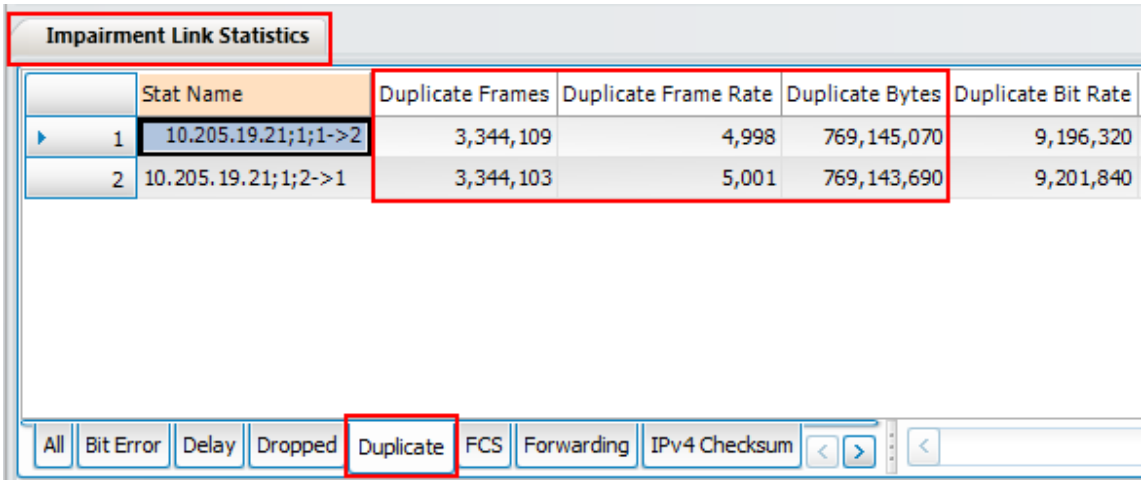


Figure 129. Accessing the Impairment specific statistics

Test Variables

You can use each of the following variables in separate test cases. Use the above test case as a baseline and modify a few parameters in the same Network Impairment. You can create various stability tests to challenge the DUT operating margins similar to practical network impairments.

Performance Variable	Description
Create multiple profiles	Create up to 16 bidirectional, or 32 unidirectional impairment profiles per impairment port pair.
Add multiple classifiers	Add multiple classifiers in a single impairment profile. Use Copy Classifier and Paste Classifier commands in the **Network Impairment Configuration** tab to copy and paste classifiers across impairment profiles. You can add up to a maximum of 8 classifiers for each link direction.
Apply impairments in both link directions	Select this option to impair one or both the links.
Increase Reordering percentage	Introduce a larger number of irregularities in the data stream to measure the influence of out of order packets in the user quality experience.
Apply different pattern variations	Apply different patterns for the impairment engine to handle the streams of data forwarded.
Apply different packet impairments	Apply packet modifications and BER impairments in addition to reordering and duplication impairments. These options are available in the **Modify** packet profiles.

Results Analysis

This test proves that you can successfully emulate WAN link conditions such as packet duplication and reordering. You can also select specific types of traffic to impair.

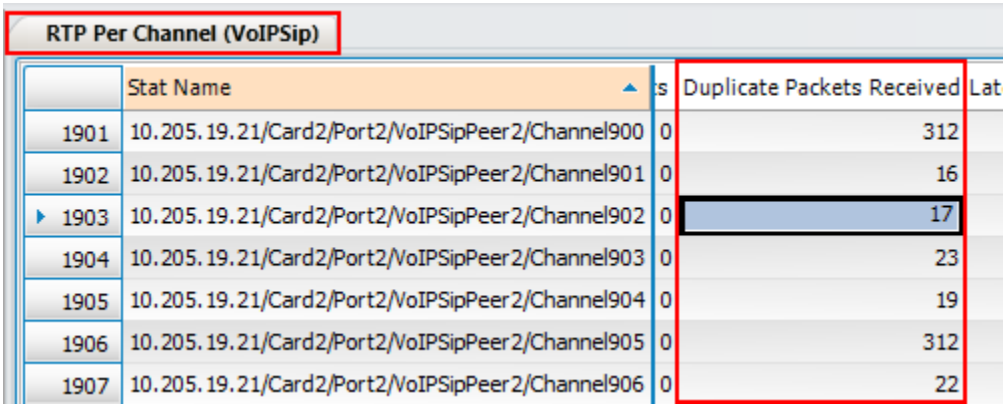


Figure 130. Displayed statistics for RTP received frames

This test impairs only traffic for a specific UDP port destination. Similarly, you can also impair other packet types to completely test the device behavior and stability upon receiving erroneous patterns of packets.

Troubleshooting Tips

Issue	Troubleshooting Solution
Test does not start execution reporting physical link errors	Ensure that correct PHY modes are set for the ImpairNet traffic ports depending on the connectivity type in use (copper or fiber).
Impairment profiles are enabled but impairment statistics are not updated.	To overcome this error: Verify that the **Apply Impairments** icon does not have any error. Make sure that the traffic is flowing through the module and the drop rate is not set to *100%*.
No traffic is flowing through the impairment links.	To ensure that traffic is flowing through the impairment modules: • Disable all the impairment profiles except the default profile. • Apply Impairments and check that Rx/Tx Frames statistics for the impairment link corresponds to the traffic. • Ensure that both the links for the impairment port pair are forwarding, that is, the **Interrupt Forwarding** check boxes are cleared.
An error window appears on clicking Apply Impairments.	To overcome this error: • Ensure that there is no impairment profile configuration error. • Make sure that the impairments are applied within the configuration limits. • Check ImpairNet module specifications for the configuration limits.
Traffic is not impaired though the Apply Impairment icon is not showing any error.	To overcome this error: • Ensure that the classifier value, mask, and offset are set correctly. • Make sure that a profile with a generic classifier does not have a lower priority than that of the desired impairment profile. • Verify that you selected the **Enabled** checkbox for the configured impairments.

Conclusions

This test verifies whether the device or system under test is functioning correctly when receiving incorrect stream of data. The effect of RTP payload data as received by the emulated endpoint is also analyzed.

Test Case: Capture and Replay Network Characteristics To Validate Application Performance

Overview

After understanding the importance of network emulation testing before deployment, the first question that customers usually ask is, “what impairments should I use to validate application, device or service performance?” The Anue Network Emulator provides two answers, 1) Anue Profiler and 2) ITU-T G.1050/TIA-921 IP network models. This section will discuss the Anue Profiler solution.

Profiler is a free, downloadable, software tool that captures network characteristics such as delay, jitter and packet loss by sending ICMP pings to user selected network targets on production networks. The recorded data can then be analyzed in the form of graphed results that display network behavior over specified periods of time.

The network emulator’s Network Playback feature can then be used to playback the recorded network characteristics in a lab, allowing application performance to be validated while subjected to the most relevant real world impairment scenarios.

The following sections explain how to use Profiler to capture live network characteristics and the GEM network emulator to playback the recorded characteristics in the form of delay, drops and jitter.

Objective

The objective of this test is to capture the network characteristics of a customer’s production network and then replay those characteristics in the lab in order to allow application performance to be validated before deployment.

Profiler will be configured to record for two business days in order to get a thorough characterization of network performance.

Setup

The setup for this test case requires that Anue Profiler be installed on a Windows (XP/Vista, Win7) PC that is connected to the production network and has a typical configuration for a user that will be working in the office. The PC should have access to the networks and servers that are used for everyday business transactions. Upon starting Profiler, an attempt will be made to send ICMP pings to defined network targets (computers) and internet websites (as shown in the figure below). The ping response times (delay/delay variation) or lack of response (drops) is logged and graphed in the Profiler in order to capture the network characteristics.

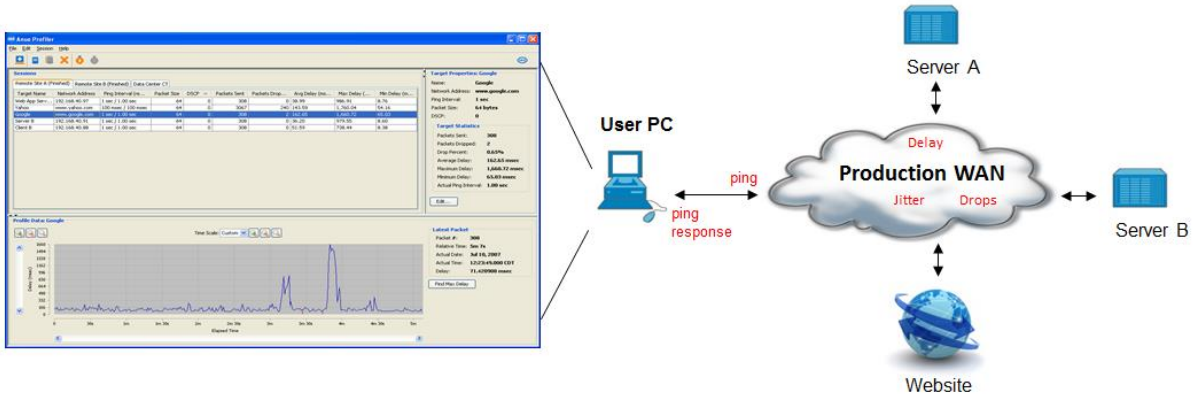


Figure 131. Profiler Capturing Network Impairment Conditions from a Live Network

Once network characteristics data has been gathered, it can be loaded into GEM (which sits inline between the DUTs) and replayed in order to accurately emulate the live network.

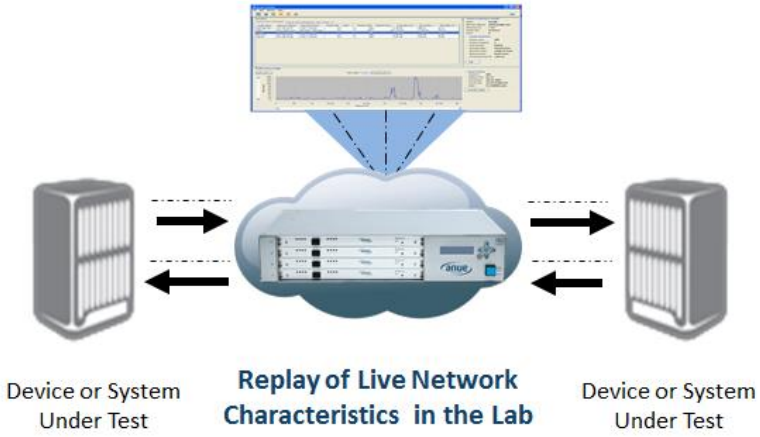


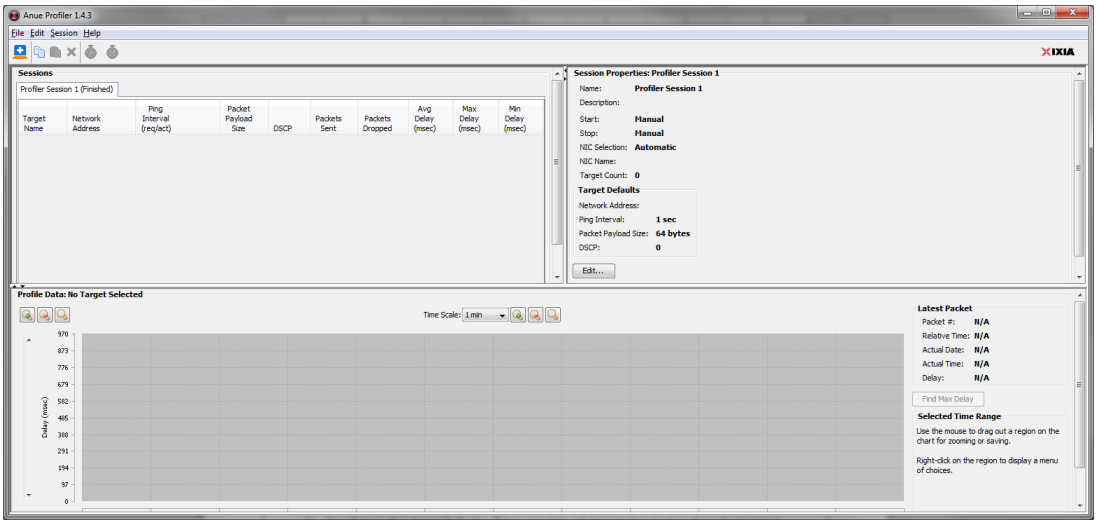
Figure 132. GEM Playback of Network Characteristics Recorded by Profiler

Step-by-step Instructions

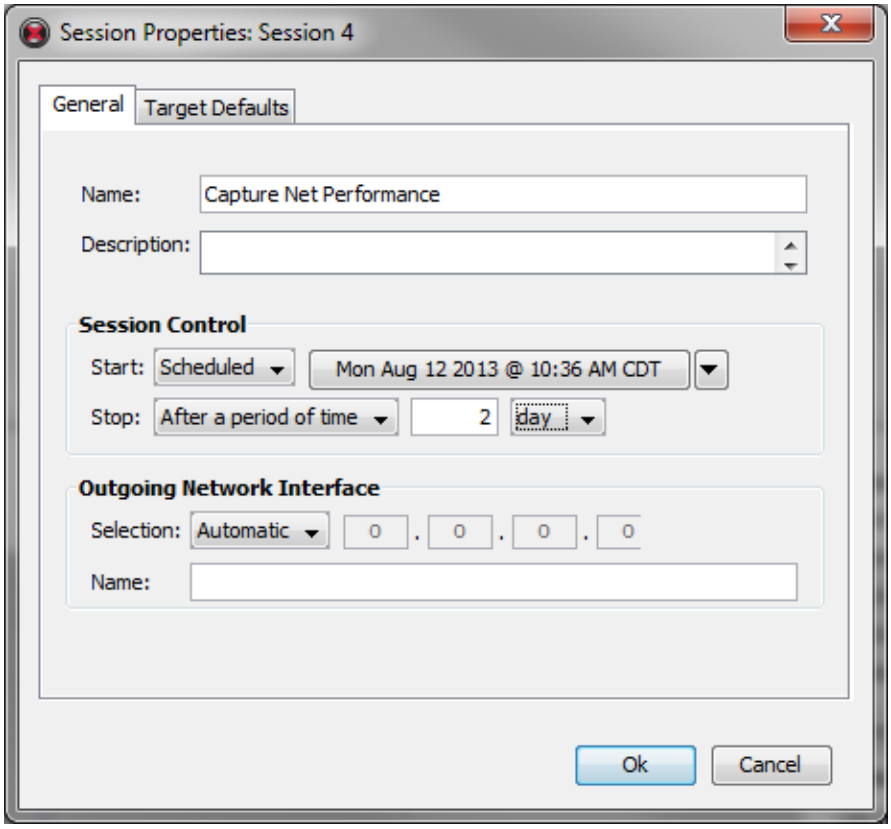
Install Anue Profiler on a production Windows (XP/Vista, Win7) PC that is connected to the network. For example, Profiler can be installed on a PC that is used by the accounting group for daily accounting transactions.

1. Configure the targets (PCs, servers, websites) that will be used to characterize network performance. For example, if Profiler is installed on a PC that is used by a member of the accounting group, the configured target can be a server or a website that is accessed often by the accounting team to retrieve job quotes or access an employee salary database.

    a. Start the Profiler from the Windows Start menu. The Profiler GUI appears as shown in the figure below.

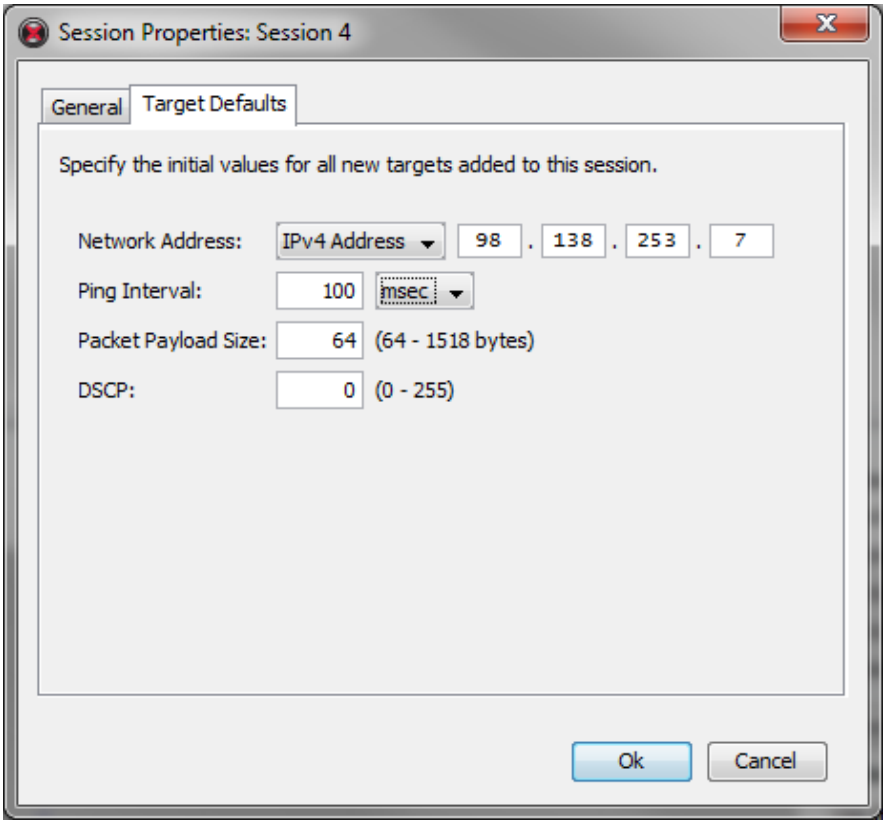


    b. From the menu, click **File> New Session**. The **Session Properties** window appears.



c. In the **General** tab of the **Session Properties** window, you can configure the **Name** and **Description** fields. Note that in this example, the **Session Control** section is configured to start gathering data on a specific date and run for 2 days.

Click the **Target Defaults** tab.



d. Configure the target Network Address using an IPv4 address or DNS Name (click the drop down arrow to select this option). Configure the **Ping Interval** in seconds or milliseconds. Configure the **Packet Payload Size** for the ICMP packet and optionally configure **DSCP** (DiffServ), if you wish to configure Quality of Service settings for the packets. Note that the PC must be rebooted before starting the session if you configure DSCP.

   The settings defined here will become the default settings for any additional targets that are added to this session. This feature is a handy time-saving shortcut when a majority of the targets are on the same subnet or require similar settings.

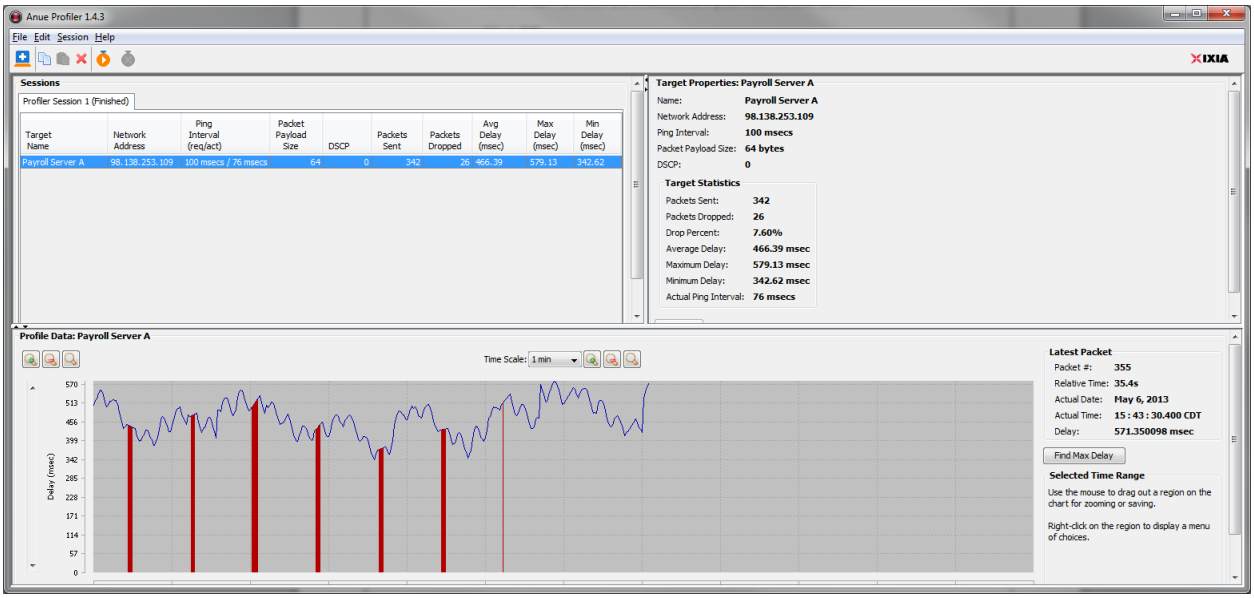
   Click **OK**.

e. If you wish to configure additional targets for this session, click **File > New Target.** The default target settings appear. Modify the target settings as necessary.

Interpreting and Saving Profiler Data

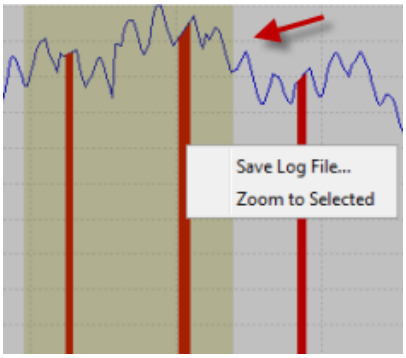
1. The Profiler Session starts at the time and date configured in the Step-by-step Instructions section of this chapter.

   After a few seconds, ping response statistics begin to display along with a graph similar to the one displayed in the figure below. Note that the red lines in the graph indicate dropped packets (ping response was not returned from target) and the blue line indicates delay/delay variation values.



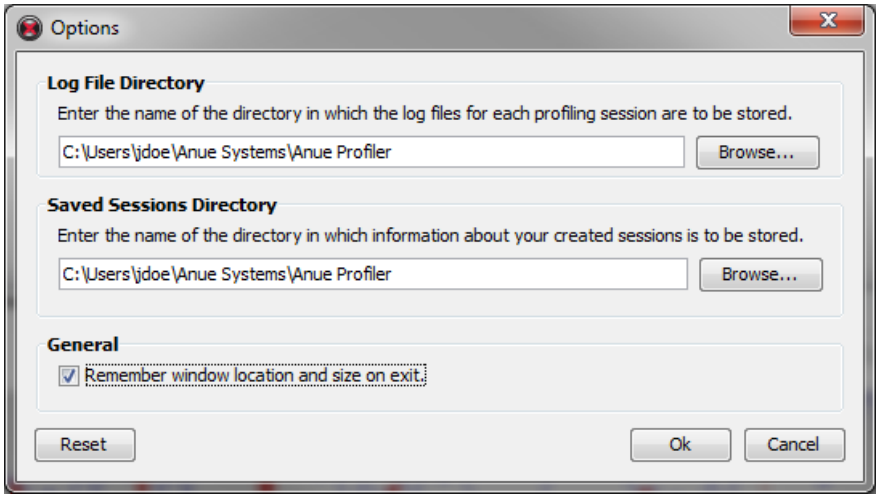
   Over the two day period of recording packet drop, delay, and delay variation, patterns usually appear in the graph that characterize network activity and responsiveness. The Profiler GUI also provides detailed information about each ICMP packet that has been sent.

   Once the Session is complete, the graph can be further analyzed by isolating and saving data from specific time periods or zooming in for greater detail.



2. The network characteristics data is stored in a log file with the extension, .anr. The log file is essential in the next section, when the recorded network characteristics are played back in the lab.

   To locate the log file, select **Edit Options** from the menu. The **Options** dialog displays the default path for the storage of Profiler log files.



   For example, the log file stored for the scenario described above is stored is the following directory, C:\Users\jdoe\Anue Systems\Anue Profiler\Capture Net Performance\20130812-103604.

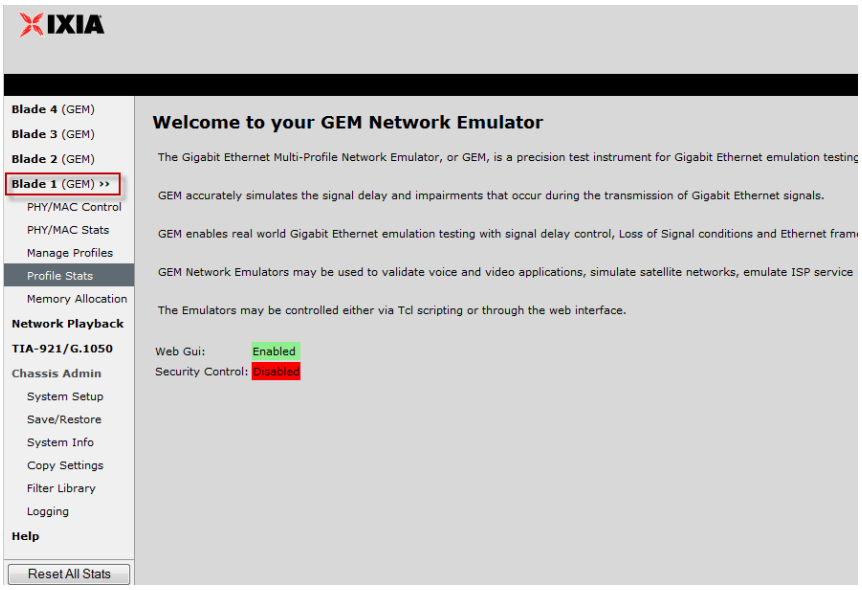
   The Capture Net Performance folder is the name defined for the session in the **General** tab of the Session window. The “20130812-103604” folder is the session start date (20130812), hour (1036) and seconds (04).

Replay the Captured Network Characteristics

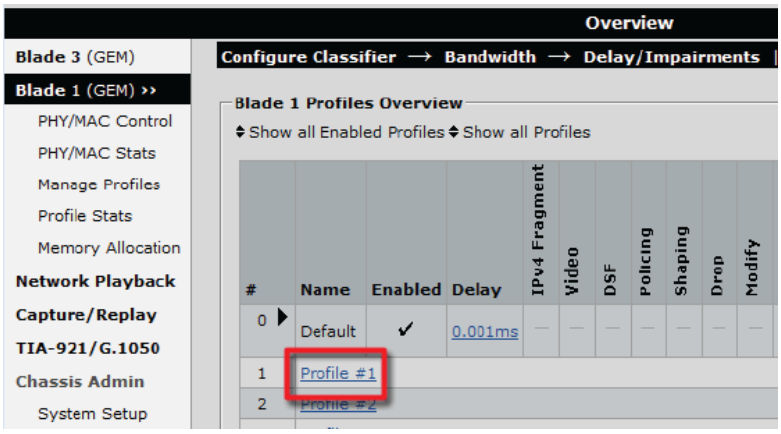
1. Enter the IP address of the GEM Network Emulator IP address into the URL field of your IE or Firefox HTML browser.

   The GEM Welcome page appears.

2. Select **Blade 1** (GEM).



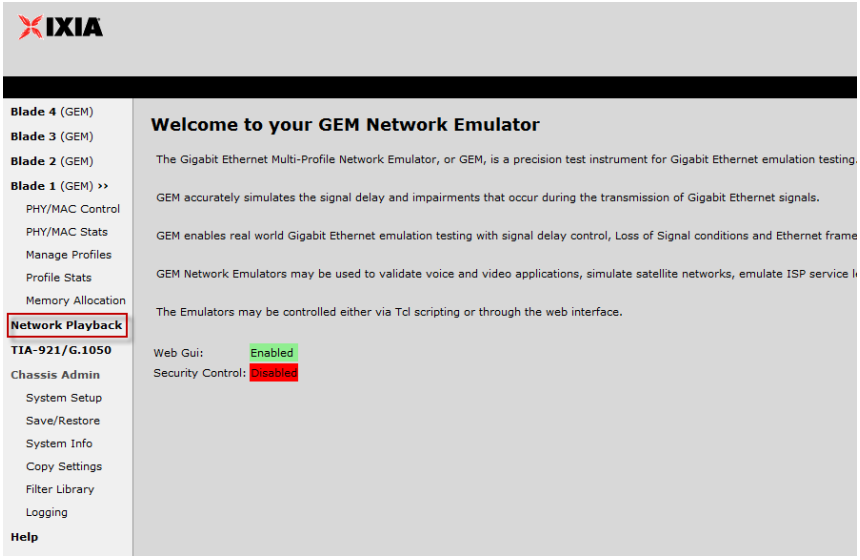
3. The Blade **Overview** page appears. Select **Profile #1**.



4. The **Network Profile Classifier** page appears.

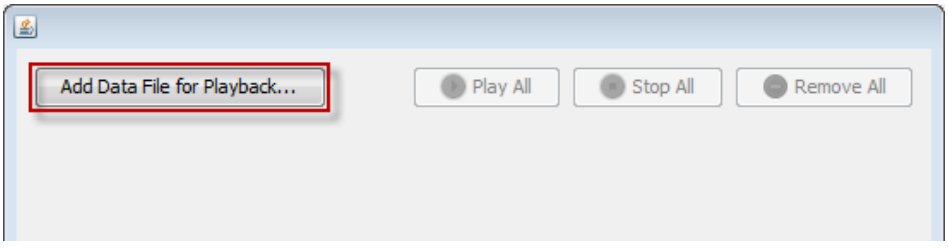
   Configure the Network Profile Classifier to impair traffic destined for the application server (from DUT 1 to DUT 2) and click **Apply**. The example below uses the destination IP address of the application server.

5. In the left pane, click **Network Playback.**



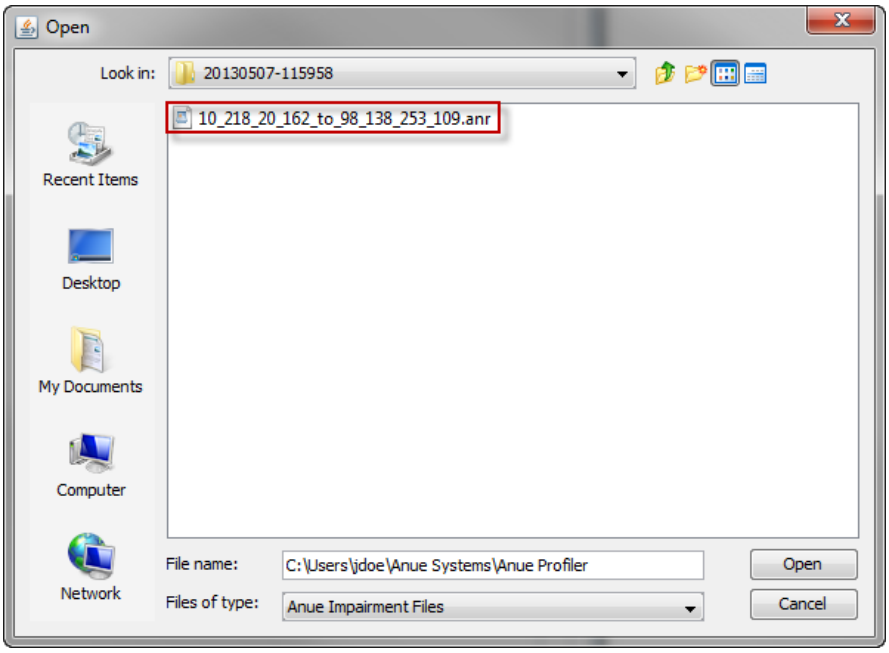
   The **Network Playback** dialog appears.

6. Click **Add Data File for Playback**.

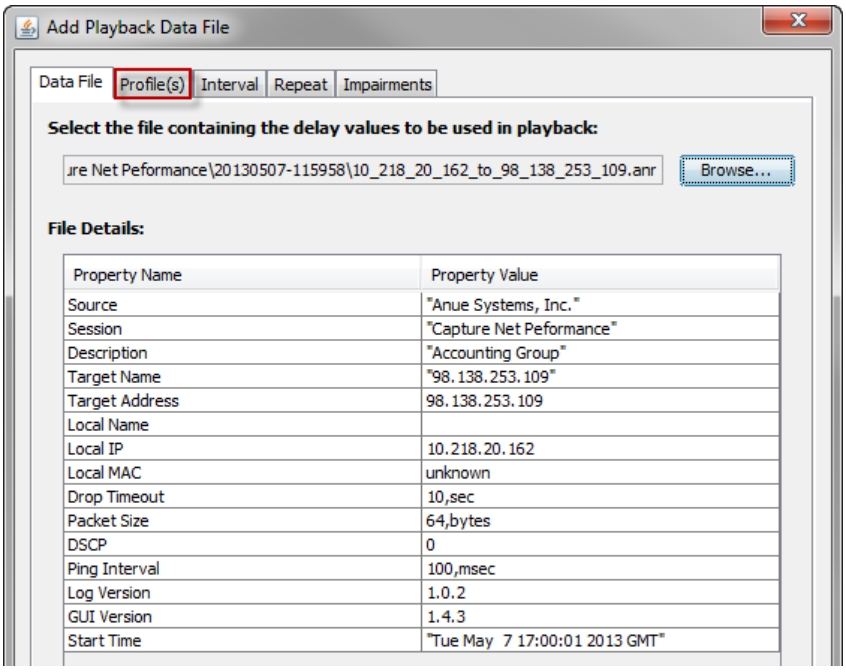


   Then click **Browse**.

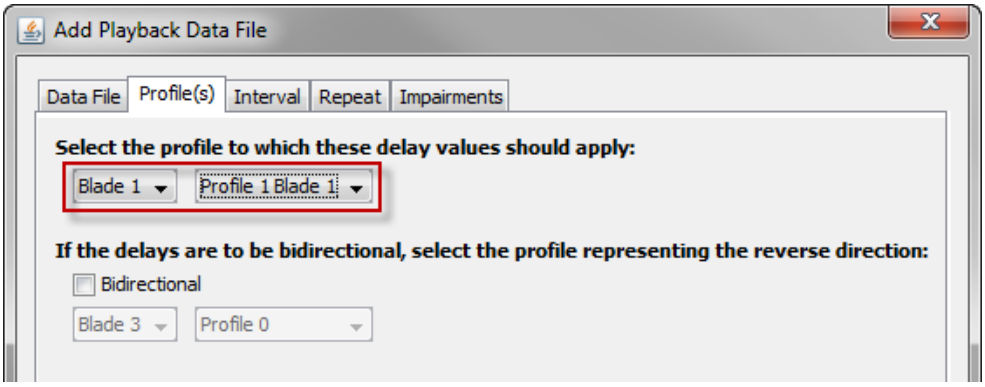
7. Select the .anr log file created in the Interpreting and Saving Profiler Data section of this document. Then click **Open**.



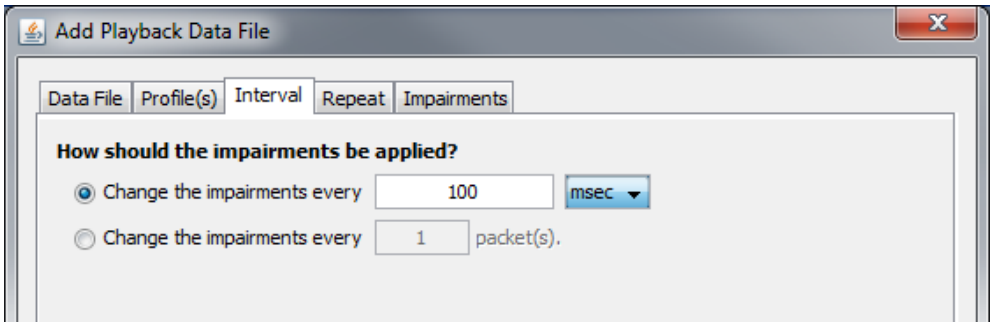
8. Click the **Profile(s)** tab.



9. Select the Network Profile configured in Step 4 (Profile #1).



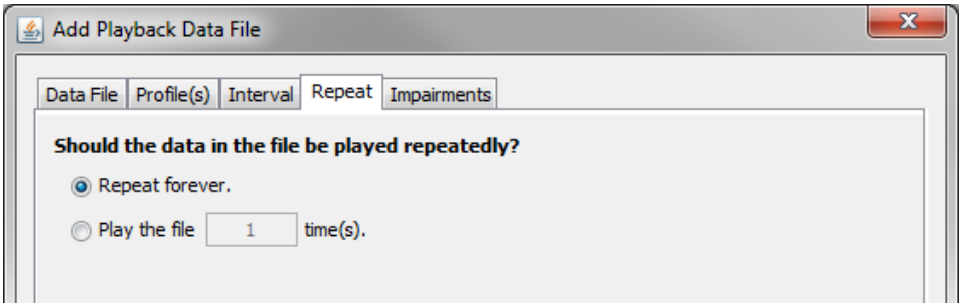
10. Click the **Interval** tab.



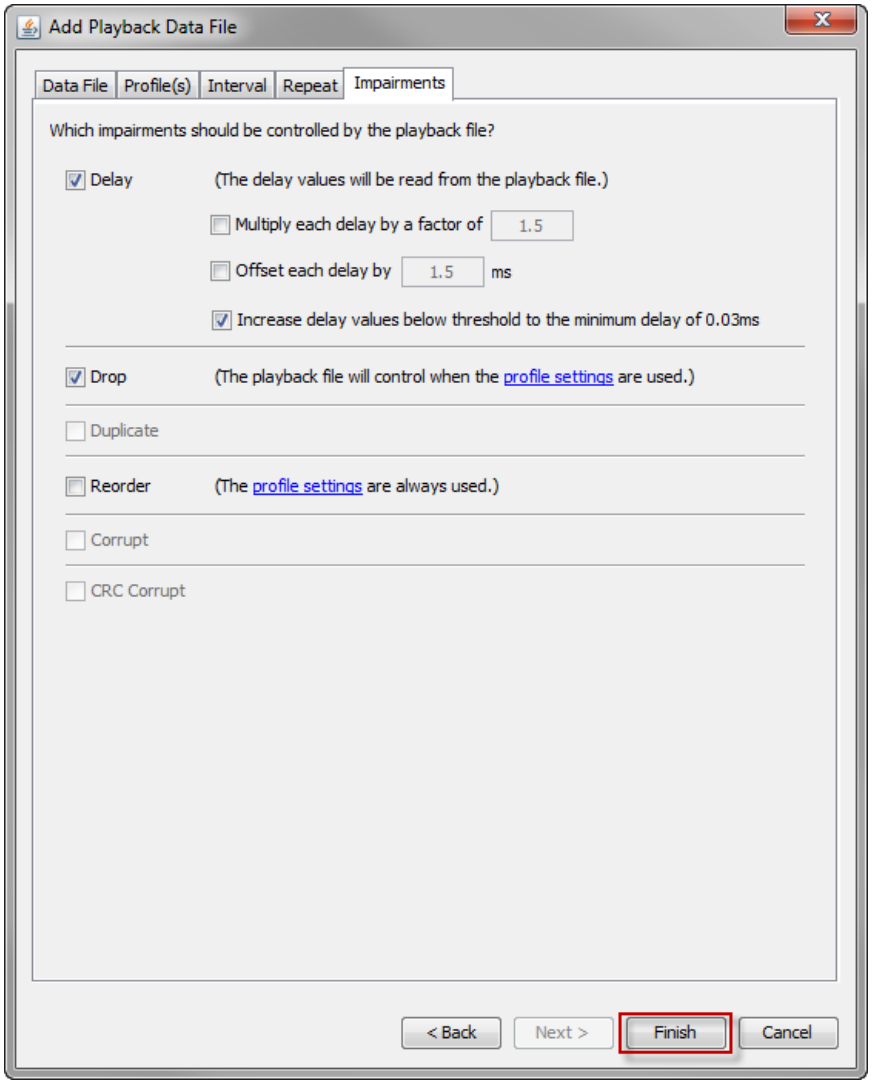
Configure the **Change the impairments every** setting to 100 msec, because the ping interval for Anue Profiler was also 100 msec.

11. Click the **Repeat** tab.

Configure the file playback to **Repeat Forever** (playback the impairments repetitively until stopped).



12. Click the **Impairments** tab.

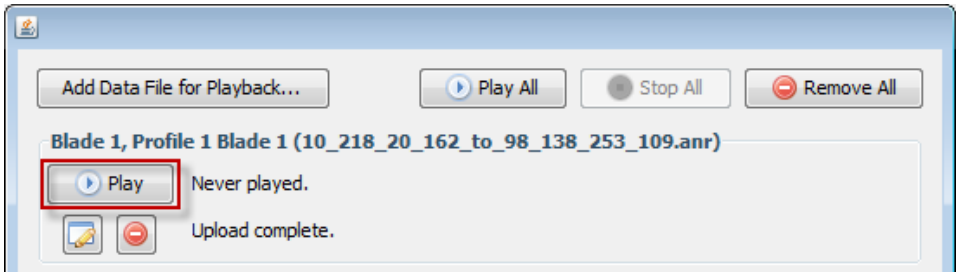


The Impairment settings can be left at the defaults.

Click **Finish**.

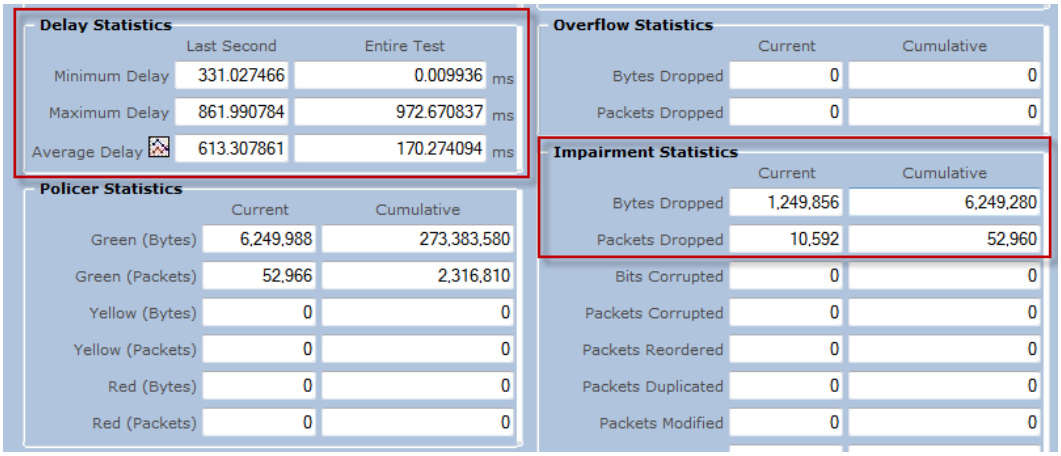
The **Playback Manager** appears.

13. Click **Play** to start impairment playback.



14. Application performance can now be observed as the impairment characteristics that were captured from the live network will be replayed and applied to traffic associated with Network Profile 1. Recall that Network Profile 1 has been configured to classify traffic that originates from the application under test that is destined for the application server (DUT1 to DUT2).

    Note: Applied delay can be observed in the **Delay Statistics** section of the **Profiler Stats** page and packet drop can be observed in the **Impairment Statistics** section of the **Profiler Stats** page. Note that the application of delay and packet drop can only occur when there is traffic present at the time of impairment application, that is, if the traffic is bursty, packets can only be delayed or dropped at the time when packets are being transmitted.



Test Variables

You can use the following variables in separate test cases in order to focus on solutions for specific network scenarios.

Performance Variable	Description
Record network characteristics from several PCs	You can run Profiler on several PCs (for example one from each dept. that utilize drastically different applications) and then load the recorded log files into a single GEM unit. Allowing you test several real network impairment scenarios simultaneously.
Add additional impairments	Impairments from the Delay/impairments page can be applied to a stream of traffic in addition to the impairments being applied based on the recorded network characteristics.
Focus on high traffic time periods	You can select and save high traffic time periods from Profiler and replay them continuously to stress DUTs.
Modify impairment playback	The Network Playback configuration tabs allow the replay interval of impairments and delay values to be modified in order to create new impairment scenarios that are based on the recorded network characteristics.
Customize the playback file for granular delay/drift scenarios	The Profiler log file (.anr) is saved in ASCII text format. The values in the file can be modified per the instructions in the GEM User Guide. Delay can be increased or decreased at very granular levels (drift) in order to validate performance in this scenario.
Apply impairments in both link directions	The Network Playback configuration tabs allow to you configure impairment and delay playback in both link directions.

Results Analysis

The Profiler application produces a graphical view of network performance. This information alone can provide valuable information about the network characteristics and patterns of network usage by users.

Loading the log files into the Anue Network Emulator allows the captured live network characteristics to be replayed in the lab subjecting the DUTs to the most realistic, real world, network impairments and delay.

Troubleshooting Tips

Issue	Troubleshooting Solution
Profiler fails to reach the client on all attempts	Ensure that a firewall is not blocking ICMP packets.
An error is displayed when the Profiler **Start** button is clicked	If your PC has more than one NIC card installed, follow the directions in the Profiler User guide to indicate which NIC card has access to network you wish to characterize.
No traffic is flowing through the Network Profile	Ensure that the classifier (Configure Classifier option in the GEM GUI) is configured correctly. Verify that traffic is flowing on the Blade Overview page. All traffic flows on Network Profile 0 until it is correctly classified by a network profile.
I do not see the network impairments being applied when I view the network profile statistics page	Note that the application of delay and impairments can only occur when there is traffic present at the time of impairment application, in other words, if the traffic is bursty, packets can only be delayed or dropped at the time when packets are burst.

Conclusions

This test demonstrates how real world network characteristics can be captured and replayed in a lab in order to provide the most relevant test scenario for application performance testing.

Test Case: Verify Application Performance Using TIA-921/G.1050 Network Models

Overview

After understanding the importance of network emulation testing before deployment, the first question that customers usually ask is, “what impairments should I use to validate application, device or service performance?” The Anue Network Emulator provides two answers, 1) Profiler and 2) ITU-T G.1050/TIA-921 IP network models. This section will discuss the GEM TIA-921 feature.

The network models, published by the Telecommunications Industry Association as TI A-921 and the International Telecommunications Union as ITU-T G.1050, are based on actual network data provided by anonymous IP service providers and IP network equipment manufacturers. They are designed to facilitate testing of any IP-based service, including voice, video, data, or combinations as found in triple-play services.

The models define time-varying values for packet delay, loss, and reorder for 133 typical end-to-end network configurations with eight levels of impairment severity, resulting in 1064 network/impairment combinations or test cases.

Severity tests are the tests within a test case that have parameters that simulate severity levels of the test case objective. Severity tests are labeled A-H with ‘A’ being the least severe scenario and ‘H’ being the most severe scenario.

For example, Test Case 1A has a small amount of delay and jitter and no packet loss, test Case 1H produces a delay of approximately 1 second, a large amount of jitter and packet loss.

Note: A thorough understanding of ITU-T G.1050/TIA-921 can be acquired by reading the standard. GEM allows you to gain a basic understanding of the test methodology. Select the best test for their scenario, and then point and click to begin testing.

Objective
In this scenario, an application service provider needs to validate network application performance over a network being proposed in a Service Level Agreement (SLA).

An SLA typically has a technical definition in terms of mean time between failures (MTBF), mean time to repair or mean time to recovery (MTTR); various data rates; throughput; jitter; or similar measurable details. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties and often includes details about the financial penalties that occur when these objectives are not met.

This test case allows the service provider to test application performance, experiment with various equipment settings and fixes and make proactive suggestions in regards to the SLA **before deployment**. Testing these scenarios in the lab results in a higher quality of experience

for the customer at the time of deployment and save the application service provider time and money (by preventing SLA penalties).

Setup

The Anue Network Emulator is installed inline between the DUTs as shown in the figure below.

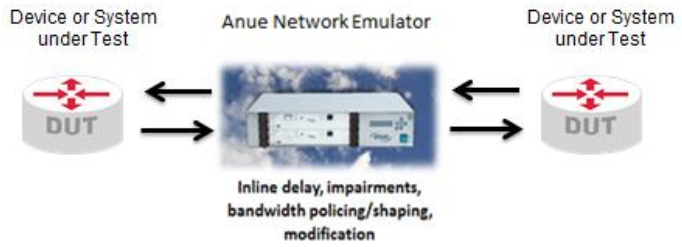


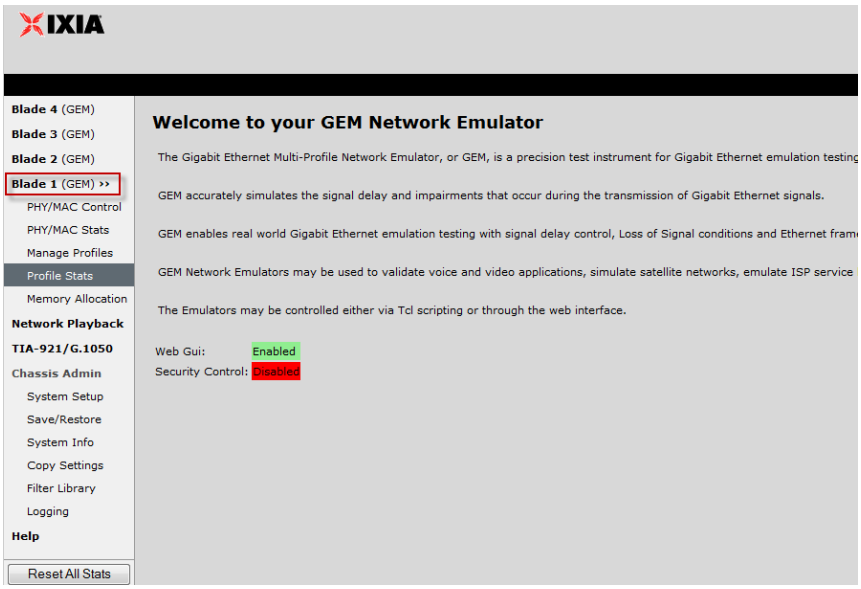
Figure 133. Anue Network Emulator Installed Inline Between DUTs

Step-by-step Instructions

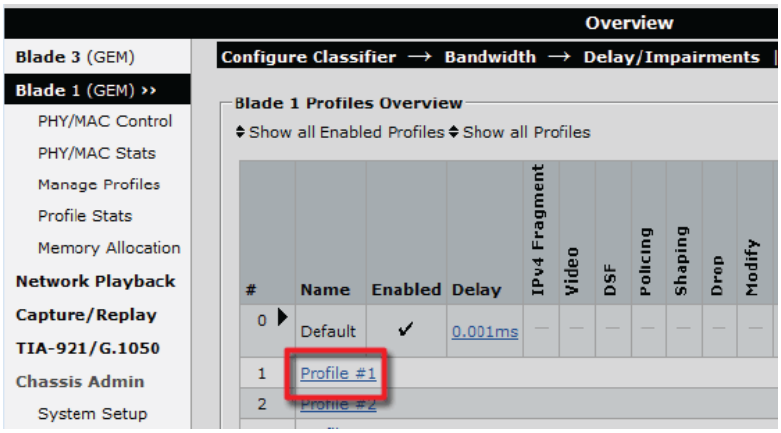
1. Enter the IP address of the GEM Network Emulator IP address into the URL field of your IE or Firefox HTML browser.

   The GEM Welcome page appears.

2. Select **Blade 1** (GEM).



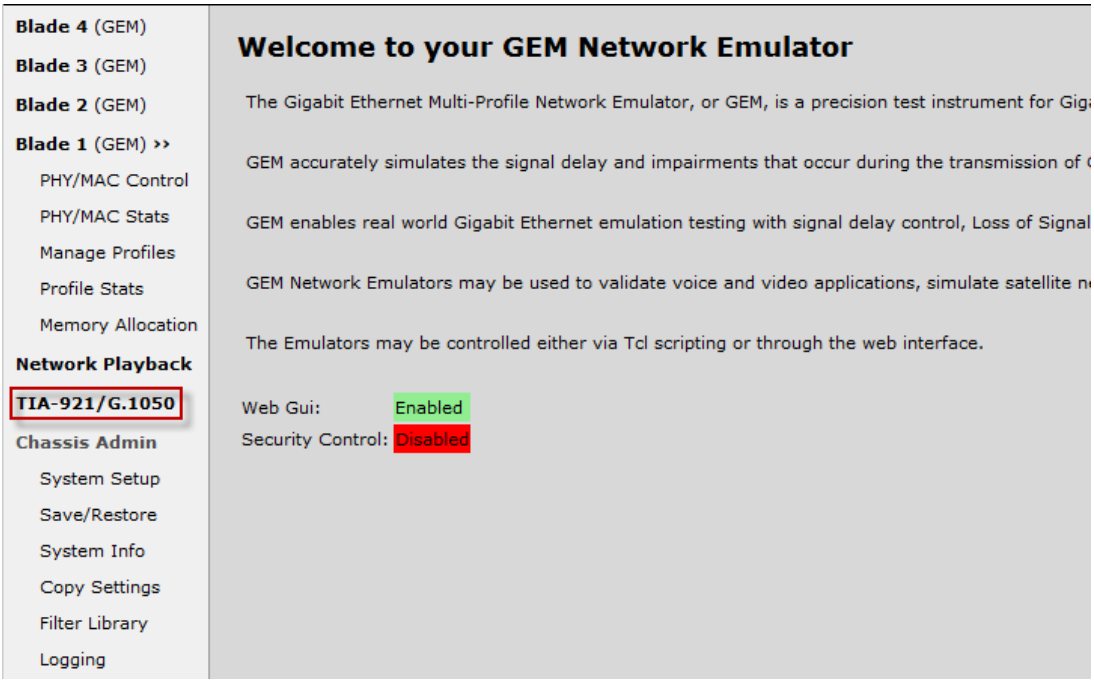
3. The Blade **Overview** page appears. Select **Profile #1**.



4. The **Network Profile Classifier** page appears.

   Configure the Network Profile Classifier to impair traffic destined for the application server and click **Apply**. The example below uses the destination IP address of the application server.

5. In the GEM GUI, select the **TIA-921/G.1050** option.

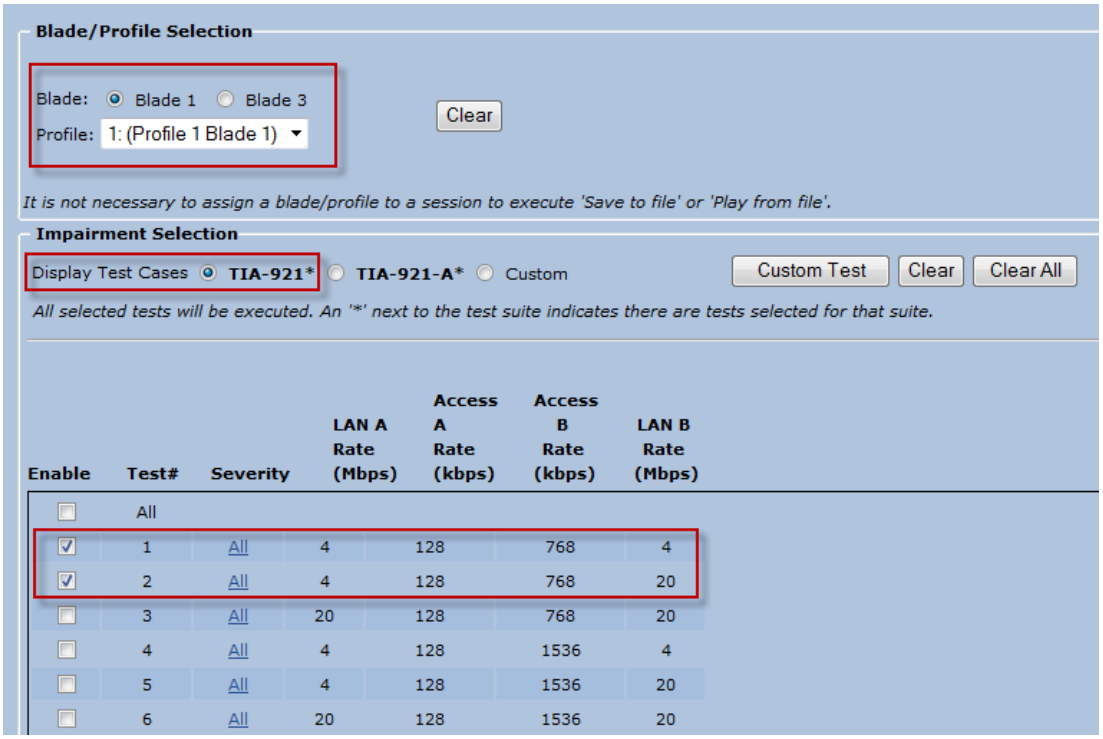


The **TIA-921/G.1050** dialog appears.

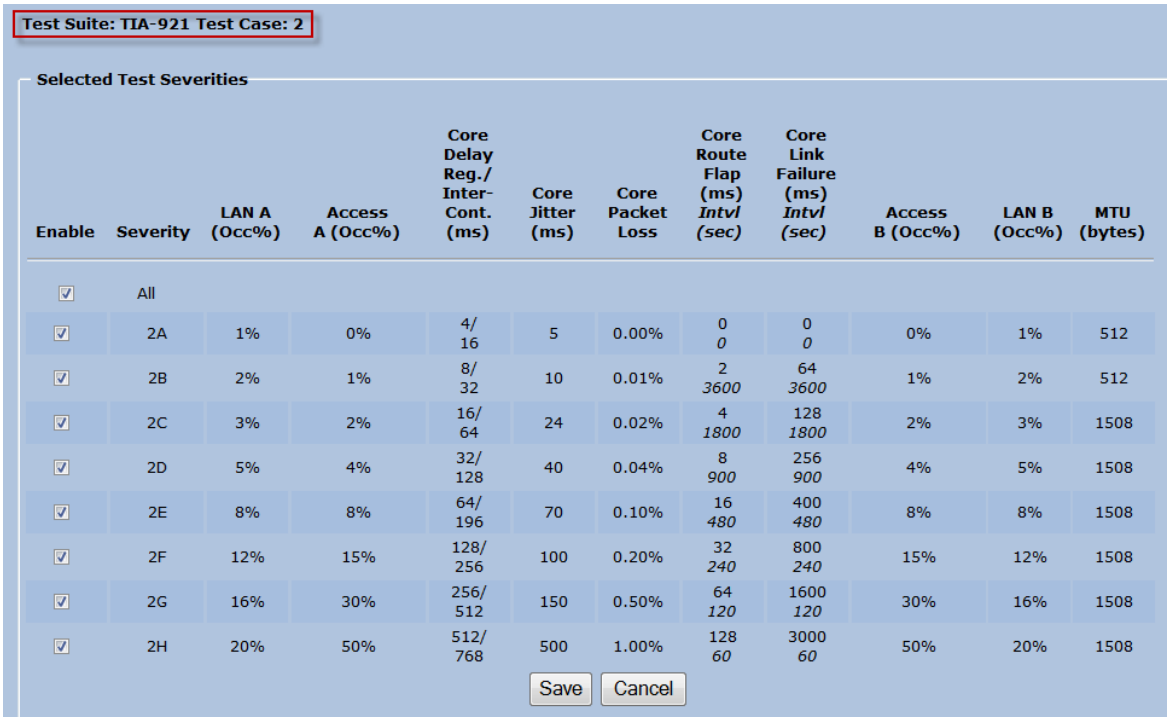
6. Select **Blade 1** and **Profile 1**.

   a. Select **Display Test Cases TIA-921***.

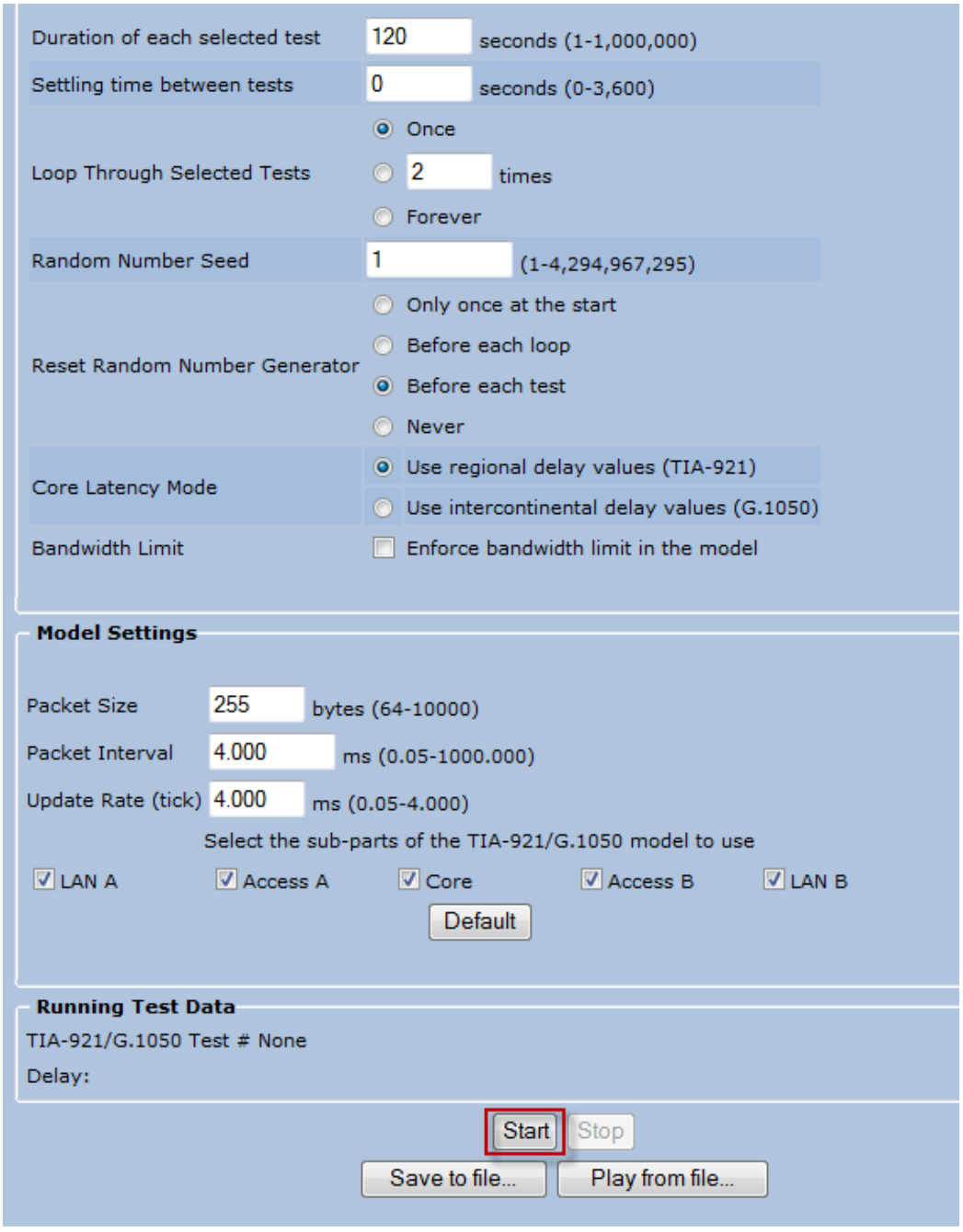
   b. Select test cases 1 and 2, because these tests correlate best to the proposed network Service Level Agreement.



Note: By clicking the **All** hyperlink in the **Severity** heading (shown in the figure above)**,** you can view a detailed description of the severity settings for the test cases as defined per TIA-921/G.1050 (shown in the figure below). Also note that individual severity levels can be disabled (by clearing the **Enable** checkbox).



7. The options at the bottom of the **TIA-921/G.1050** page (shown in the figure below) can be left at the defaults until you become more familiar with the network models and wish to customize the playback of the test scenarios. The options are described in detail in the *TIA-921/G.1050 Settings Appendix*.



8. Click **Start** to begin the playback of the configured network scenarios.

   GEM begins to apply the network impairments as defined in the configured TIA-921 test cases to the Network Profile traffic. You can now validate the application performance under these real world network conditions.

   Note: The application of delay and impairments can be observed in the **Profile Stats** page in the GEM GUI. Note that the application of delay and impairments can only occur when there is traffic present at the time of impairment application, in other words, if the traffic is bursty, packets can only be delayed or dropped at the time when packets are burst.

Test Variables

You can use the following variables in separate test cases.

Performance Variable	Description
Validate performance against all of the test case severity levels	For a more comprehensive evaluation, configure the test case severity levels outside of the known SLA parameters in order to gain a better understanding of performance in non-ideal scenarios. You could possibly discover that the SLA is over-provisioned (resulting in unnecessary additional monthly costs).
Modify the TIA-921 options and parameters	See Appendix B for details about the TIA-921 parameters and options such as Bandwidth Limit. (Bandwidth Limit restricts the network profile bandwidth to the speed of the slowest link or rate specified in the test case that is running. Note that this feature is not required by TIA-921 or G.1050. It has been provided to make testing more realistic.)

Troubleshooting Tips

Issue	Troubleshooting Solution
The Network Profile statistics indicates that there is no traffic	Ensure that the classifier (Configure Classifier option in the GEM GUI) is configured correctly. Verify that traffic is flowing in the Blade **Overview** page. All traffic flows on Network Profile 0 until is correctly classified by a network profile.
I do not see the network impairments being applied when I view the network profile statistics page	Note that the application of delay and impairments can only occur when there is traffic present at the time of impairment application, in other words if the traffic is bursty, packets can only be delayed or dropped at the time when packets are burst.

Results Analysis

The configured TIA-921 test cases demonstrate the ability of the application to operate as designed in the presence of common network impairments like drop, delay, and jitter. You may also want to experiment with various application configuration settings to see if application performance can be improved under these network conditions.

Conclusions

This test demonstrates how real world network characteristics can be reproduced in the lab by using the industry standard network impairment scenarios defined in ITU-T G.1050/TIA-921. This test allowed for the validation of application performance and the test variables also provide a method to validate the proposed SLA.

Test Case: Verify Storage Disaster Recovery Fail Over

Overview

For many large companies, verifying remote data center disaster recovery represents an important business and regulatory requirement. This is because the delays and impairments experienced on an optical network can have a devastating effect on software applications and storage. Day-to-day operations can be disrupted as decreased throughput and response times lead to applications that crash or become effectively unusable.

This test case helps the customers to validate their failover mechanism and application performance once failover has occurred, giving them confidence that their solution is in compliance with their business and regulatory requirements.

The customer's primary data center is1km away from the company campus. The secondary (backup) data center is 6km away from the company campus.

Objective

The objective of this test is to:

1. Emulate the network between the clients and the primary data center.
2. Observe client application performance and throughput to establish a baseline.
3. Emulate the network between the clients and the secondary data center.
4. Introduce Loss of Signal between the client and secondary data center, which results in a failover to the secondary data center.
5. Observe the client application performance and throughput.

Setup

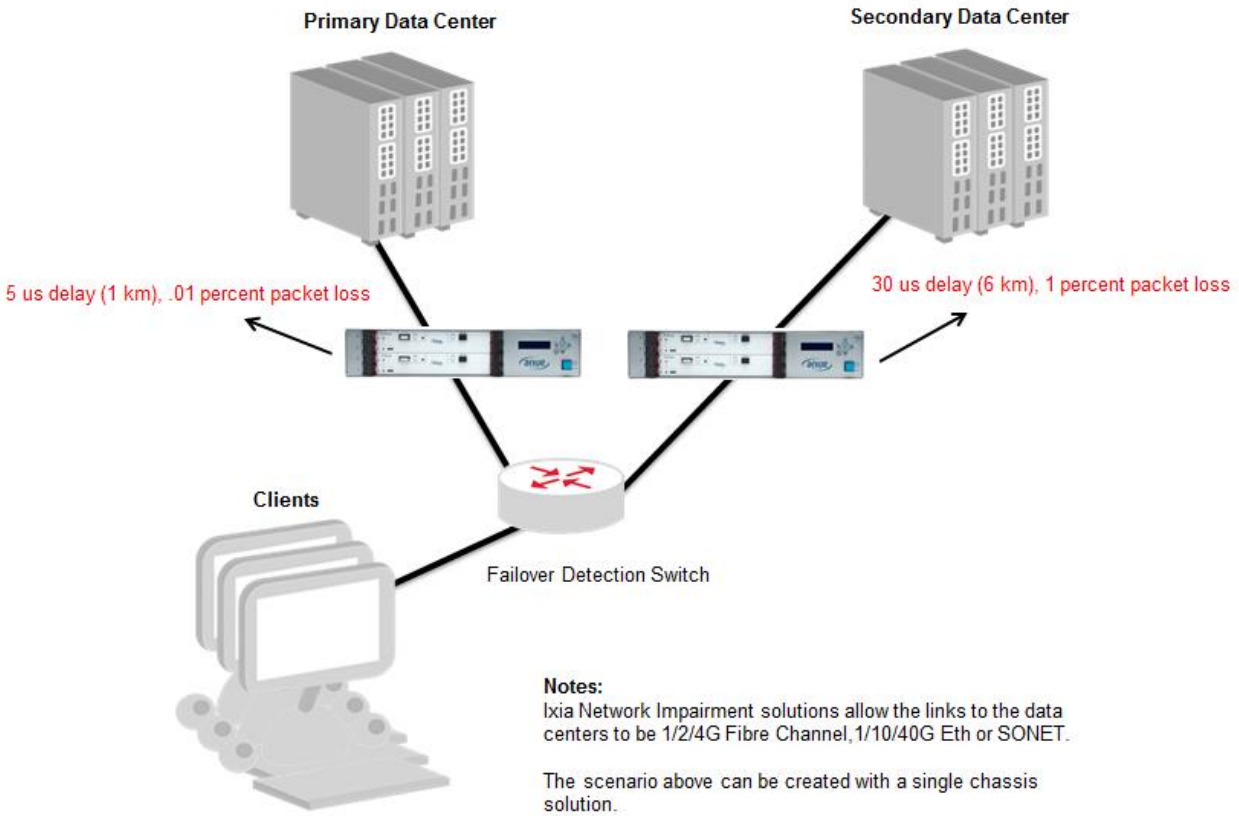
Hardware Setup

FC-4 (Fibre channel 4) network emulator load running on the Hawaii network emulator is required.

Make the connections between the clients, switch, network emulators, and data center servers as shown in the figure below.

Notes: Ixia Network Impairment solutions allow the links to the data centers to be 1/2/4G Fibre Channel, 1/10/40G Ethernet or various SONET/SDH rates. The scenario shown in the figure below can also be created with an Ixia single chassis network impairment solution. For example,

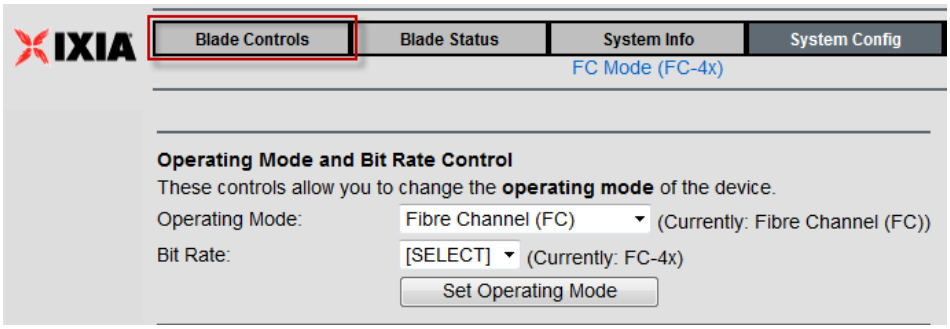
a 4 blade Anue Maui chassis could support both the primary and secondary network links as shown in the figure below.



Network Emulator GUI Setup – Primary Data Center

This section describes the steps required in the network emulator GUI to emulate the Primary Data Center network displayed on the left side of the network diagram above.

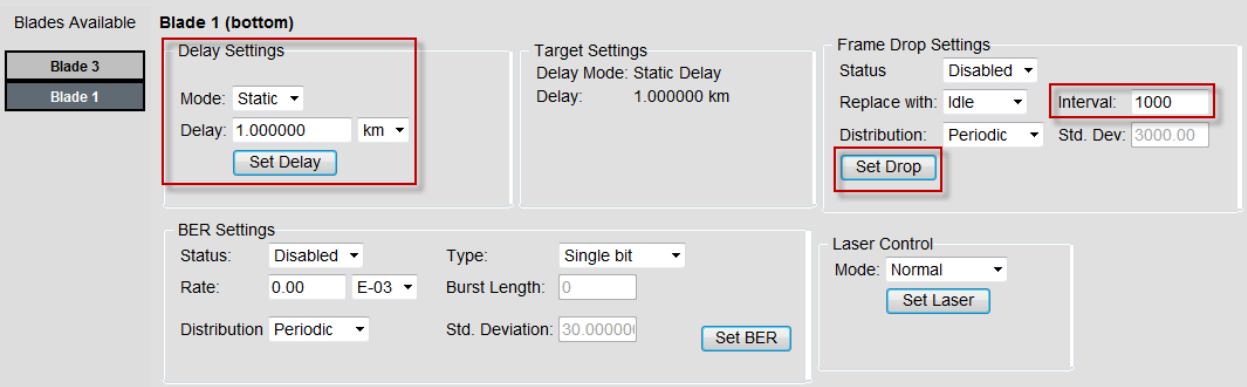
1. In the **Primary** Anue FC-4 network emulator GUI, click **Blade Controls,** and then select Blade 1.



2. Configure the following:

    a. 1 km – then click **Set Delay**

    b. Frame Drop Interval = 1000 (.01 Percent packet loss) – then click **Set Drop**.

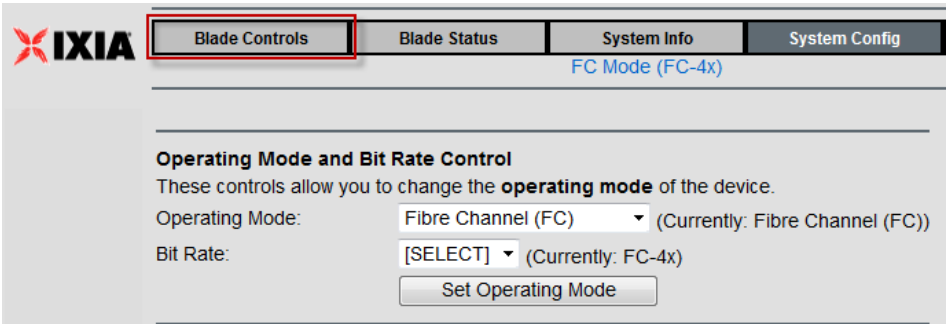


3. Observe client application performance and throughput to establish a baseline.

Network Emulator GUI Setup – Secondary Data Center

This section describes the steps required in the Network Emulator GUI to emulate the Secondary Data Center network displayed on the right side of the network diagram above.

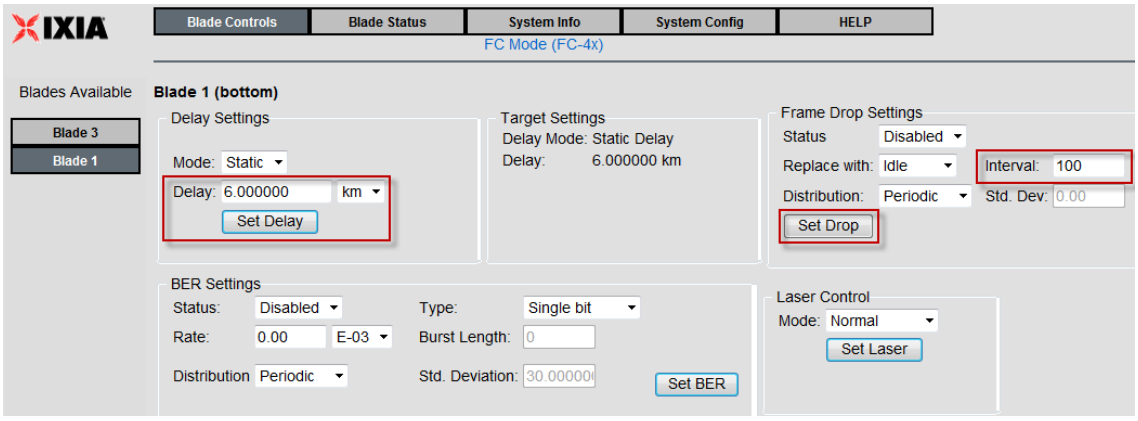
1. In the **Secondary** Anue FC-4 network emulator GUI, click **Blade Controls** and then select Blade 1.



2. Configure the following:

    a. 6 km – then click **Set Delay**

    b. Frame Drop Interval = 100 (1 Percent packet loss) – then click **Set Drop**.



The **Primary** and **Secondary** networks are now configured.

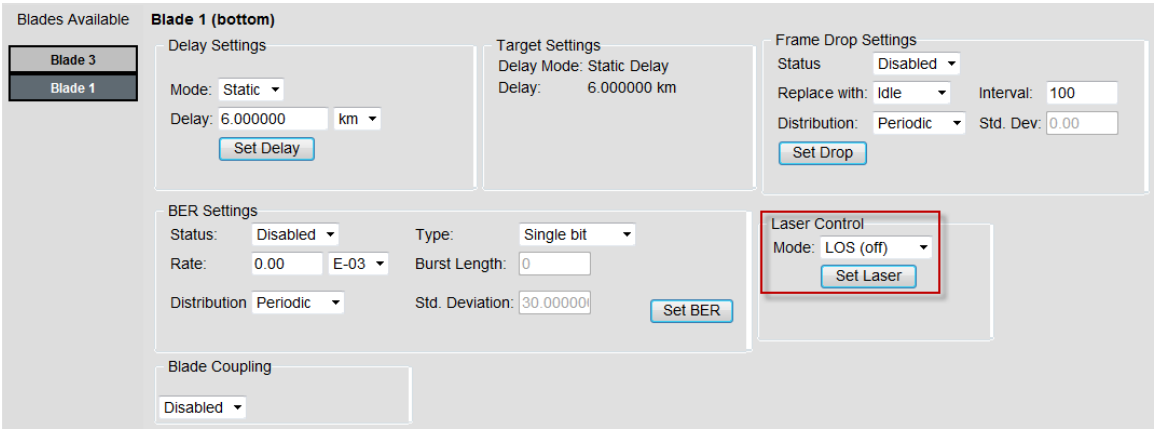
Step-by-step Instructions

Create Network Failover – Then Validate Application Performance

1. In the **Primary** Anue FC-4 network emulator GUI, click **Blade Controls** and then select Blade 1.

2. In the **Laser Control** section, set the **Mode** to: **LOS (off)**.

3. Click **Set Laser**.



4. At this time, the Failover Detection Switch should detect the Loss of Signal and switch the client connection from the Primary Data Center to the Secondary Data Center.

5. Check the console or terminal of the of Failover Detections switch to ensure that the switchover occurred successfully.

6. Observe client application performance to validate that the secondary network (as emulated by the Anue Network Emulator) provides acceptable performance and response time when the clients connect to the backup data center. The criterion for judging application performance is specific to the individual applications being used; for example opening files, saving files, making database updates, rendering drawings,and storing them at the usual network location, and so on.

Test Variables

Performance Variable	Description
Add additional impairments	Add bit errors based on current Primary Data Center network performance or SLA.
Validate performance against similar network delay and drop impairment scenarios	For a more comprehensive evaluation, configure the network impairments outside of the known secondary network parameters in order to gain a better understanding of performance in non-ideal scenarios. You could possibly discover that the SLA is over-provisioned (resulting in unnecessary additional monthly costs).

Troubleshooting Tips

Issue	Troubleshooting Solution
Traffic is not flowing and the DUT may report that its ports are in loopback	Note that the Anue Network Emulation cabling configuration for Fibre Channel is different than the cabling for Ethernet gigabit fiber cabling. Details are provided in the Anue Fibre Channel and GEM User Guides.
Ports on the Anue Network Emulator and the DUT do not synch up	Ensure that you are using supported transceivers for this type of testing. Ensure that the transceivers and mode of fiber cabling match. See troubleshooting tip #1.

Results Analysis

This test clearly demonstrates the effect of delay on fibre channel communication links. The test may also allow network equipment settings like buffers to be adjusted on the secondary link to find out, if they can increase the performance.

Conclusions

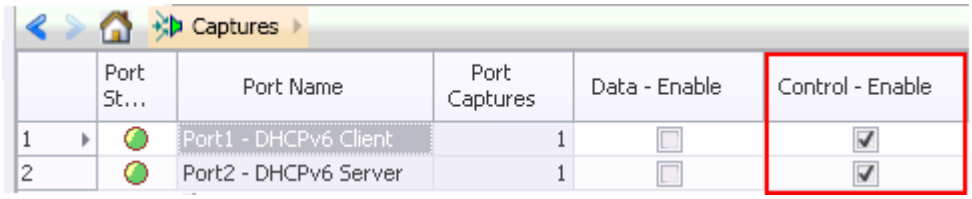
This test demonstrates how to use the Anue Network Emulator to emulate a data center network failover. After the failover condition is emulated, application performance can be validated based on the network characteristics of the secondary network.

Appendix A: Enabling and Analyzing the Packet Captures

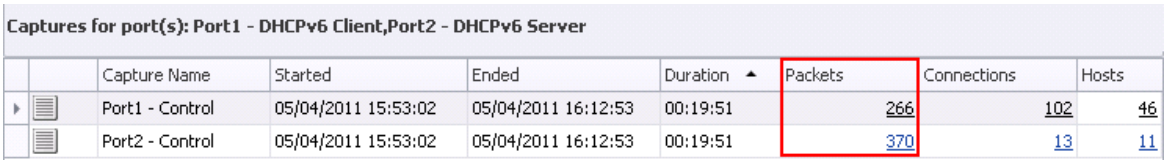
You may enable packet capture when:

- Ixia ports are used for control and/or data plane traffic
- Packet capture and analysis is required to select the packets for impairment
- Classification methodology of packets for impairments is essential

1. In the main IxNetwork navigation window, click Captures and select Control – Enable check box for the required port. This action activates bi-directional packet capture.



2. Click **Packets** column to examine the packets.



3. Double click the Packets column to bring up packet decoding view.

Note: The Data capture is Rx capture which only captures incoming packets, including both control and data packets. The Control capture is a bi-directional PCPU capture which captures control packets only.

Appendix B: Anue Network Emulator TIA-921/G.1050 Settings

This Appendix describes the setting options available when configuring Anue Network Emulator TIA-921/G.1050 tests.

Duration of each selected test: The length of time each selected test case runs, in seconds.

Valid Range: 1 - 1,000,000

Settling time between tests: The amount of time (in seconds) to pause between the execution of each selected test.

Valid Range: 0 - 3,600

Loop Through Selected Tests: Select whether to loop through the selected tests once, twice, or forever. All tests will be run through sequentially and then will run again if indicated.

Random Number Seed: Provides control of the Random Number Seed used when generating random numbers to be used as values for TIA 921 Impairments.

When the same random number seed is used, a session is configured with the same sequence of impairment values.

Valid Range: 1- 4,294,967,295 (The default value = 1)

Reset Random Number Generator: Indicates if the **Random Number Generator** is reset.

- **Only once at the start:** The random number seed is changed to a new value only once at the start of the series of tests that are scheduled to run. For example, if tests 1A, 1C, and 2A were scheduled to run, the random number seed changes before test 1A and not change again during the test cycle.

- **Before each loop:** If the **Loop Through Selected Tests** option is set to a value other than 1, the random number seed is changed to a new value before the start of each loop (sequence of tests).

- **Before each test:** The random number seed is changed to a new value before each individual test. For example, if tests 1A, 1C, and 2A were scheduled to run, the random number seed is changed before each test is run.

- **Never:** Do not change the **Random Number Seed** (do not reset the random number generator).

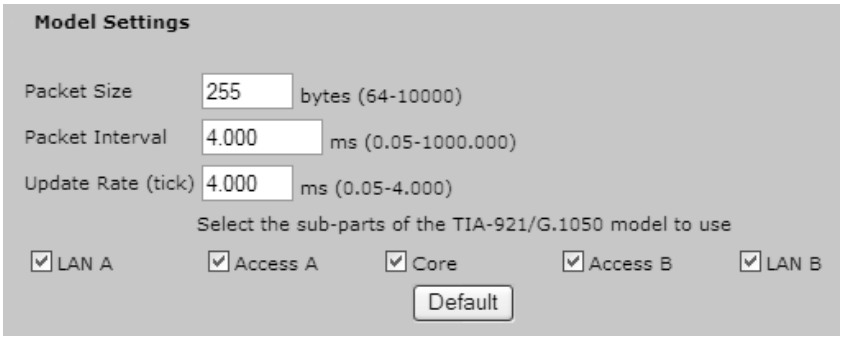
Core Latency Mode: Select whether to use regional delay values (TIA-921) or intercontinental delay values (G.1050).

  - For **TIA-921** compliant testing, this should be set to **regional.**

- For **G.1050** compliant testing, this can be set to either **regional** (same behavior as TIA-921) or **intercontinental** (larger max delays) to model longer links found in international networks.

Bandwidth Limit: Check the box to **Enforce Bandwidth Limit** in the model. This feature restricts the network profile bandwidth to the speed of the slowest link or rate specified in the test case that is running. Note that this feature is not required by TIA-921 or G.1050. It has been provided to make testing more realistic.

Model Settings



Packet Size: Indicates the average packet size of the traffic used for the tests.

Valid Range: 64-10000 bytes

Packet Interval: Indicate the interval between the packets of the traffic used for the tests.

Valid Range: 0.05-1000.000 ms

Note: The **Packet Size** and **Packet Interval** parameters are provided in order to account for serialization delay.

Serialization delay is the time it takes for a unit of data, such as a packet, to be serialized for transmission on a narrow (For example, serial) channel such as a cable. Serialization delay is dependent on size, which means that longer packets experience longer delays over a given network path.

Serialization delay is also dependent on channel capacity (bandwidth), which means that for equal-size packets, the faster the link, the lower the serialization delay.

The Packet Size value is used to adjust the packet delay. Delay is increased for larger packets. The Packet Interval value is used to calculate how much bandwidth is being used.

Update Rate (tick): Specify the interval for playback.

Valid Range: 0.05 – 4.000 ms

Note: The Model Update must be 4.0 ms to run a session locally. To run a session at a faster update rate, use the **Save to File** button to save the session and then use **Play from File** button to load and play the session.

Select the sub-parts of the TIA-921/G.1050 model to use:

LAN A, Access A, Core, Access B, LAN B

Default (button): Clicking this button resets the Model Settings to the defaults.

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/