

# Black Book



---

Edition 10

## Quality of Service Validation



## QUALITY OF SERVICE VALIDATION

### **Your feedback is welcome**

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

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

Your feedback is greatly appreciated!

Copyright © 2014 Ixia. All rights reserved.

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

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

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



## Contents

How to Read This Book .....	vii
Dear Reader .....	viii
Quality of Service (QoS) Validation .....	1
Introduction to L2 QoS .....	9
Test Case: Layer 2 Quality of Service .....	11
Test Case: Layer 3 Quality of Service .....	31
Test Case: Impairment Testing For Layer 3 QoS Mechanisms .....	47
Test Case: Automating Layer 3 Quality of Service .....	59
Contact Ixia .....	73



## How to Read This Book

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

Each test case has the following organization structure:

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

## Typographic Conventions

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

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

## 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

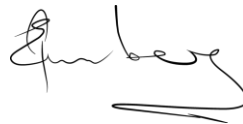
**Volume 20** – SDN/OpenFlow

**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



# Quality of Service Validation

## Test Methodologies

This booklet provides baseline test execution plans for running common QoS testing scenarios. It offers a comprehensive set of recommendations and guidelines for running test cases against various QoS policy implementations.

## Quality of Service (QoS) Validation

Quality of service (QoS) is a network's ability to prioritize end-to-end traffic delivery based on traffic type, specific user, or service type, over various underlying technologies such as:

- Frame relay
- ATM
- Ethernet and 802.1
- SONET
- IP-routed networks

The increasing volumes and types of traffic flowing through today's networks require prioritization. Network managers use QoS to maintain high network performance for delivering time-sensitive traffic – such as high-quality video and real-time voice -- during periods of network congestion. QoS assists in traffic prioritization by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network, and provides improved traffic delivery and more predictable network service.

QoS can be implemented at layer 2 and/or layer 3. QoS methods are varied and include such techniques as VLAN priority (802.1p), IP Precedence (TOS), and differentiated services code points (DSCP).

Some typical methods for implementing QoS are:

- Classification – typically the function of edge routers that organize traffic into classes based on specified criteria.
- Congestion management – operates to control congestion once it occurs. One method for handling traffic is using a queuing algorithm to sort the traffic and determine priority to the output link. Each queuing algorithm solves a specific network traffic problem and affects network performance in a specific way.
- Congestion avoidance – monitors network traffic loads to anticipate and avoid congestion at common network bottlenecks before they become a problem. These techniques are designed to provide preferential treatment for premium (priority) class traffic under congestion situations. Congestion avoidance concurrently maximizes network throughput and capacity while minimizing packet loss and delay.
- Policing and shaping – regulates network traffic based on committed access rate (CAR) and peak rate. Once a service exceeds its SLA, out-of-profile traffic is marked down or dropped. Shaping regulates network traffic by delaying excess traffic, smoothing bursts, and preventing unnecessary drops.

## QUALITY OF SERVICE VALIDATION

- Signaling – provides a way for an end station or network node to request special handling of specified traffic from its neighbors. QoS signaling can coordinate the traffic-handling techniques provided by other QoS features. It plays a key role in configuring successful overall end-to-end QoS service across a network.

QoS provides the preferential delivery of application traffic by ensuring sufficient bandwidth, controlling latency and jitter, and reducing data loss. The following table describes QoS network characteristics.

Table 1. Network Characteristics managed by QoS

Network Characteristic	Description
Bandwidth	The rate at which traffic is carried by the network.
Latency	The delay in data transmission from source to destination.
Jitter	The variation in latency.
Reliability	The percentage of packets discarded by a router.

The Internet Engineering Task Force (IETF) defines two major models for QoS on IP-based networks: integrated services (Intserv) and differentiated services (Diffserv). Each model includes mechanisms that provide preferential treatment to specified traffic. Table 2 lists the two general categories of QoS mechanisms.

## QUALITY OF SERVICE VALIDATION

**Table 2. QoS mechanisms on IP-based networks**

Category of QoS mechanism	Description
Admission Control	Determines which applications and users are entitled to network resources, by specifying how, when, and by whom network resources on a network segment (subnet) can be used.
Traffic Control	Shapes traffic using rate-of-flow limits, and regulates data flows by classifying, scheduling, and marking packets based on priority. Traffic control mechanisms police delivery to the network by segregating traffic into service classes. The assigned traffic flow service class determines the received QoS treatment.

The Intserv model uses both resource reservation and traffic control mechanisms to enact special handling of individual traffic flows. The Diffserv model uses traffic control to enact special handling of aggregated traffic flows.

### QoS Benefits

The two most common approaches used to satisfy the service requirements of applications are:

- Over provisioning
- Managing and controlling

Over provisioning allows for allocating resources to meet or exceed peak load requirements. Over provisioning is only effective if it requires upgrading to faster local area network (LAN) switches, faster network interface cards (NICs), adding memory, adding CPU, or adding disk space. Over provisioning is not viable when dealing with expensive long-haul wide area network (WAN) links, under-used resources, or congestion during short peak periods.

A managing and controlling strategy focuses on allocating network and computing resources. Resource management tries to optimize resource usage by limiting bandwidth, CPU cycles, and network switch buffer memory.

Load management and network design versus implementing QoS is a common debate. In reality, QoS policies are often needed even in a well-designed and well-provisioned network. QoS policies can:

- Delay or reduce the need for expansion and upgrades by using existing resources efficiently

## QUALITY OF SERVICE VALIDATION

- Prevent bandwidth needs from growing faster than the resources of any good network designer
- Allow administrators to manage the network from a business perspective (rather than a technical one) by giving them control over network resources
- Ensure that time-sensitive and mission-critical applications have the resources they require
- Give service providers an added revenue stream by allowing different Service Level Agreements (SLAs) to be sold at different rates (gold, silver, or bronze) based on QoS classifications
- Improve user experience.

There are many ways to implement QoS. Different domains, which may or may not use different technologies and resources, can employ separate QoS implementations to monitor specific portions of the end-to-end path. Two particular domains of implementation are:

- **Enterprises.** Enterprises can control their own networks and systems using IEEE 801.p to mark frames according to priorities. 801.p marking allows the switch to offer preferential treatment to certain flows across virtual local area networks (VLANs). Process computing can obtain differentiated services by using QoS services to mark specific traffic to run at higher priorities.
- **Network Service Provider (NSP).** NSPs aggregate and forward traffic within their network, or hand it off to another NSP. The NSP use technologies such as DiffServ or IntServ to prioritize the traffic handling. NSPs must use QoS policies to enforce SLAs for transit traffic.

### QoS Test Challenges

#### Network convergence

Quality of service (QoS) and maximum throughput are essential for delivering data, voice, and video on Ethernet networks, but traditional testing methods often fall short in their ability to monitor, analyze, and identify critical problems. VLAN, MPLS, and IP service turn-ups require a multi-stream, multi-port, and multi-service testing model. Such testing helps the provider keep service quality and revenues up.

Proper network pre-qualification and monitoring is imperative to ensure that service quality is maintained throughout the network. The commercial services offered range from LAN extension, Internet access, voice, video, and data storage. Since these services all reside on the same network and consume a portion of the shared bandwidth, they must be qualified at the same time. These types of traffic have very different requirements, and stress the network in a unique manner.

In a converged network, service availability is absolutely critical. As mission-critical applications are converged onto a single infrastructure, network fault-tolerance and resiliency become increasingly important. Since a one-minute network outage affecting 100 customers could cost a service provider several hundred thousand dollars, it's obviously why their top concerns are network reliability and availability. In short, high-availability converged networks are a prerequisite for service providers interested in offering reliable and profitable carrier-class services. A QoS provisioned, well-designed network facilitates a highly available network that reduces the CAPEX and OPEX associated with redundant network infrastructures.

#### Ethernet Everywhere

Ethernet services have typically run point-to-point -- from one business campus to another or from one data center to another. These early Ethernet services were straightforward to turn-up, monitor and maintain. Testing was isolated to a single dark fiber, a single wavelength on a DWDM network, or a single channel in an Ethernet over SONET/SDH network. Performance was verified by completing hard loopback tests running at data rates of 10 Mbps, 100 Mbps, or 1 Gbps, based on the bandwidth sold.

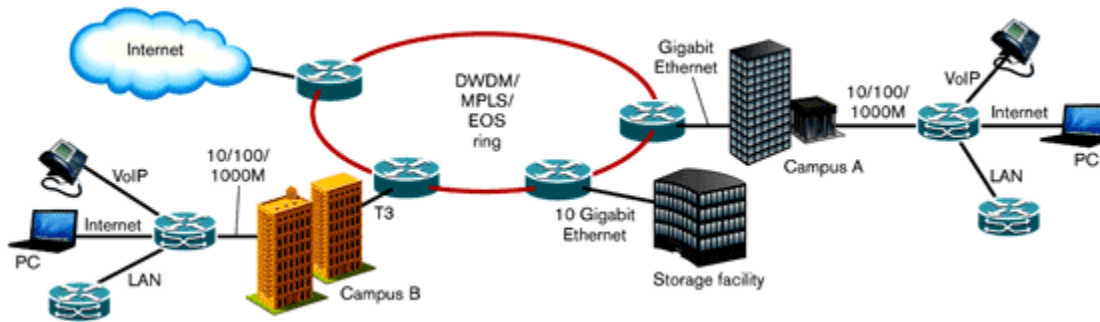
Performance verification of Ethernet services was a simple task under those circumstances. Many services were sold as a fixed bandwidth without any QoS designation -- a promise of non-guaranteed bandwidth was sufficient.

Service providers did not provide traffic grooming or policing to ensure the QoS -- they simply installed the network, verified end-to-end throughput, made a note of the roundtrip delay, and performed troubleshooting when customers complained. Now, however, network providers must conform to standards established by the ITU and Metro Ethernet Forum (MEF) as the demand for Ethernet services and bandwidth continues to increase. This means adding more capacity without impacting existing services.

## QUALITY OF SERVICE VALIDATION

Today's providers must offer the option of multiple services tiers based on QoS levels when selling commercial Ethernet services. Today, providers have significantly more flexibility in offering Ethernet services by grooming networks to handle differentiated services. In addition, Ethernet-over-copper solutions provide much greater bandwidth control and cost savings when using existing T1 and T3 infrastructures.

## Complexity



**Figure 91. Tests must generate traffic streams in the same format used by the network architecture (e.g., VLAN, MPLS, IP) for each of the service types in order to verify differentiated services.**

Traditional test sets focused on stressing one piece of the puzzle at a time, by testing each service type separately. Such tests no longer provide adequate coverage for networks that provide triple play services and multiple types of traffic simultaneously. Differentiated services existing side-by-side on the network must be tested simultaneously.

To verify differentiated services, tests must generate traffic streams in the same format (VLAN, MPLS, IP) used by the network architecture for each service type. Testing the priority and/or TOS for each traffic stream must be specified based on the appropriate class of service.

At the far end, tests must separate and perform QoS measurements on each traffic stream (see Figure 1). Though each service may individually meet QoS standards, multiple services can negatively impact performance by increasing the traffic load. Services must be tested at higher than the maximum subscribed rate to verify network's ability to handle future policing and load management.

A network device must be tested on all ports, not just a single port, to confirm its effectiveness in the network. Network deployments must be overstressed to determine their potential – the ability of a network to handle future QoS provisioned traffic is just as important as its current level of efficacy.





## Introduction to L2 QoS

L2QoS provides best-effort quality of service (QoS) or class of service (CoS) at layer 2 without requiring reservation setup. User priority as defined by the 802.1p specification (also called class of service) is used to prioritize network traffic at the data link/MAC sub-layer.

The 802.1p field is a three bits field in the 802.1Q header of an Ethernet tagged frame. It defines eight different classes of service using a priority value between 0 and 7 (inclusive). It identifies the class of the incoming traffic and transmits it based on class when the switch or network is congested. Figure 1 shows the format of a VLAN header.

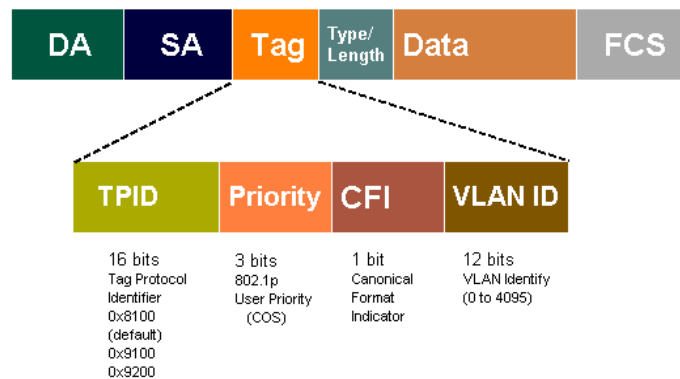


Figure 92. VLAN header information

Network administrators can setup the queues to match various business requirements and priority levels. The IEEE recommendation for QoS classifications is shown in Table 3.

Table 3. IEEE classifications

User Priority	Traffic Type
1	Background
2	Spare
0	Best Effort
3	Excellent Effort
4	Controlled Load
5	"Video" < 100 ms latency and jitter
6	"Voice" < 10 ms latency and jitter
7	Network Control

L2QoS is an important component when implementing end-to-end QoS across service provider or enterprise networks. Implementing combined QoS functionality at multiple network locations guarantees that end-to-end service level agreements (SLA) can transmit real-time or mission-critical application traffic (such as video and voice traffic) as desired.



## Test Case: Layer 2 Quality of Service

### Overview

Ethernet services such as commercial triple play and mobile backhaul must comply with strict SLAs. As end-users increase their demands for high quality of experience (QoE), meeting agreements to deliver mixed data, voice, and video traffic over an IP network is increasingly important. New and complex QoS features have grown significantly, requiring more comprehensive test methodologies.

Router and switch vendors must validate that their devices can handle QoS features such as classification, queue scheduling, and buffer management under different traffic loads. They must confirm that the various queuing mechanisms such as a weighted round robin (WRR) and weighted early random detect (WRED) are implemented correctly so as to prevent high priority traffic being dropped. Enterprise network administrators need to validate QoS settings to verify bandwidth for mission critical applications. Service providers need to validate network design and configuration to provide and monitor customer SLAs.

L2QoS is typically implemented in access and metro Ethernet networks where packets are switched instead of routed. It enables bridges/switches to reduce processing time by inspecting layer 2 headers for QoS information, without looking at layer 3 content.

The following key measurements need to be collected in order to test a device's L2 QoS implementation:

- Throughput
- Frame loss
- Latency
- Jitter

These metrics are inspected for each traffic class at various traffic loads and frame sizes in order to validate the DUT or network's conformity to configured QoS policy.

### Objective

Most of the routing/switching vendors implement a complex queuing and scheduling mechanism to process packets with different priorities. Different VLAN priorities are mapped to different queues. The objective of this test is to verify the scheduling function of the DUT's output queue. In the test, IxNetwork's advanced traffic wizard builds traffic with various CoS values, and defines flow tracking per CoS value. Congestion is created at the DUT output port, and

## TEST CASE: LAYER 2 QUALITY OF SERVICE

IxNetwork aggregated and multi-level drill-down statistics are used to monitor frame loss, latency and, jitter at each CoS level.

By monitoring frame loss, latency, and jitter at each CoS level, the scheduling function of the DUT's output queue can be validated against various QoS configurations.

### Setup

In this test, three Ixia ports are connected to the Gigabit Ethernet interfaces of a DUT switch. The DUT interfaces are configured as trunk ports.

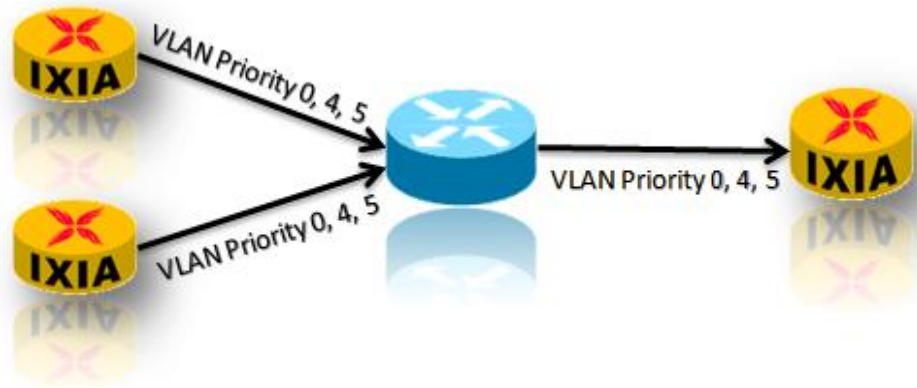


Figure 93. L2QoS test topology


There is one priority queue and two WRR queues on the line card of the DUT interfaces. The values for CoS value-to-queue mapping and bandwidth allocation between queues are listed below.

Table 4. DUT output queue configuration

Queue	Bandwidth	VLAN Priority
1 - WRR low	30%	0, 1, 2, 3
2 - WRR high	70%	4, 6, 7
3 – Priority queue		5

Layer 2 traffic is sent from two Tx ports to one Rx port. The traffic is configured with three VLAN priority values (0, 4, and 5) and three frame sizes (512, 1280 and 68) to emulate data, video, and voice traffic. To monitor frame loss, latency, and jitter for each VLAN priority, traffic tracking is configured by VLAN priority (three flows for the different VLAN priority values). Initially, traffic is sent at a low rate so that the Rx port is not oversubscribed and all frames are received. Then the traffic rate is increased to create oversubscription at the Rx port. The DUT congestion management feature will kick in and drop low priority traffic.

## Step by Step Instructions

1. Configure the DUT interfaces connected to the three Ixia ports as trunk ports, to pass traffic for VLAN 121 to VLAN 130. Enable QoS features at a global level.
2. After reserving ports, go to the **Protocol Configuration > Static** window. Click **LANs** tab, and then click  **Add LANs**. The **Add Static LANS** dialog box appears.

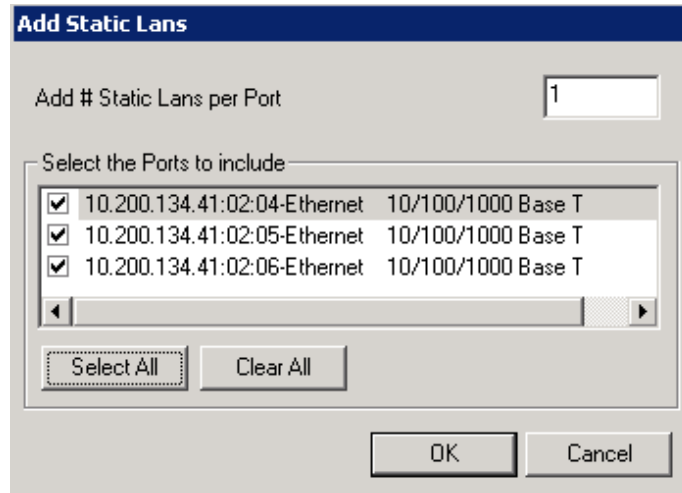


Figure 94. Configure static MAC ranges

3. Click **Select All** in the **Add Static LANS** dialog box to select all three ports, and then add one static LAN per port.
4. Click **OK** to close the **Add Static LANS** dialog box.
5. In the LANs tab add the **MAC Address** and **Count Per LAN Range**.

Diagram   IP   <b>LANs</b>   FR   ATM   Interface Groups   Interfaces In Groups								
Static								
	Port	Enable	MAC Address	Increment MAC	Count	Enable VLAN	VLAN Count	VLAN ID
1	10.200.134.41:02:0	<input checked="" type="checkbox"/>	00 00 00 01 00 01	<input checked="" type="checkbox"/>	100	<input type="checkbox"/>	1	1
2	10.200.134.41:02:0	<input checked="" type="checkbox"/>	00 00 00 02 00 01	<input checked="" type="checkbox"/>	100	<input type="checkbox"/>	1	1
3	10.200.134.41:02:0	<input checked="" type="checkbox"/>	00 00 00 03 00 01	<input checked="" type="checkbox"/>	100	<input type="checkbox"/>	1	1

Figure 95. Customized static MAC ranges

6. Go to **Traffic Configuration** and click **Advanced Traffic Wizard** to start the advanced traffic wizard.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

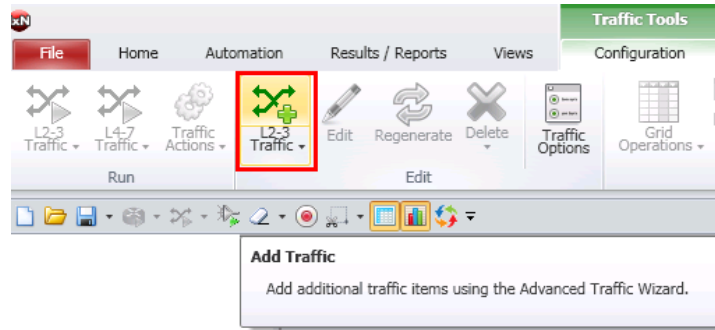



Figure 96. Launching Advanced Traffic Wizard

7. In the **Endpoint** selection window, select **Ethernet/VLAN** as the **Type of Traffic**. Then select the MAC range on port 1 and 2 in the **Source** window and select MAC range on port 3 in the **Destination** window.
8. Click the **Add** button  to add selected endpoints.

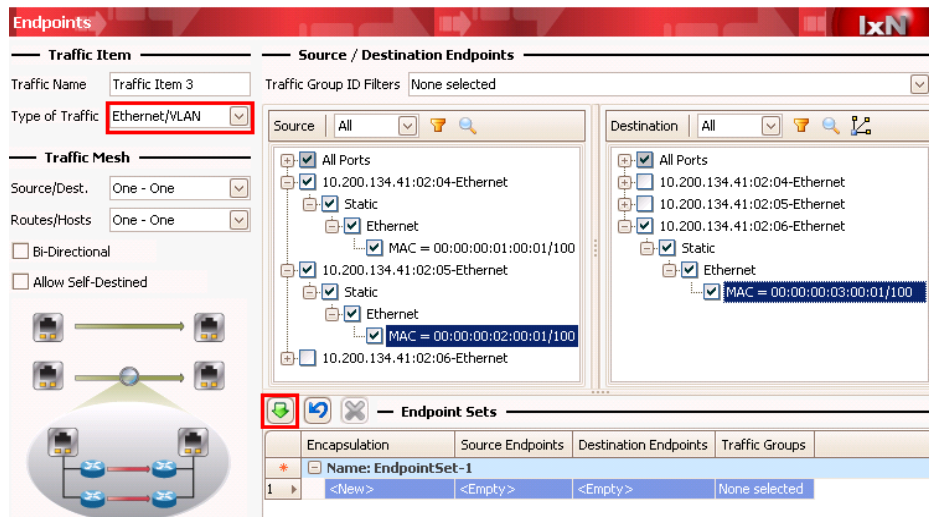




Figure 97. Advanced traffic wizard – endpoint

9. Click **Next** to goto the **Packet/QoS** window., Optionally, click the **Packet/QoS** tab in the left panel. The **Packet/QoS** window presents the packet view and QoS grid. The available QoS fields are populated dynamically based on packet content.
10. In the **Packet/QoS** page click the **VLAN** button  to append the VLAN header. Then, Highlight the VLAN header and click the **Expand** button  to expand the VLAN header. From the VLAN-ID option list, select the value to configure VLAN 121 through 130 with an increment pattern.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

The 10 VLAN IDs is distributed across the 100 MAC addressed per Tx port. VLAN ID 121 is used with Mac1, Mac11, Mac21, and so on. VLAN ID 122 is used with Mac2, Mac12, Mac22, and so on.

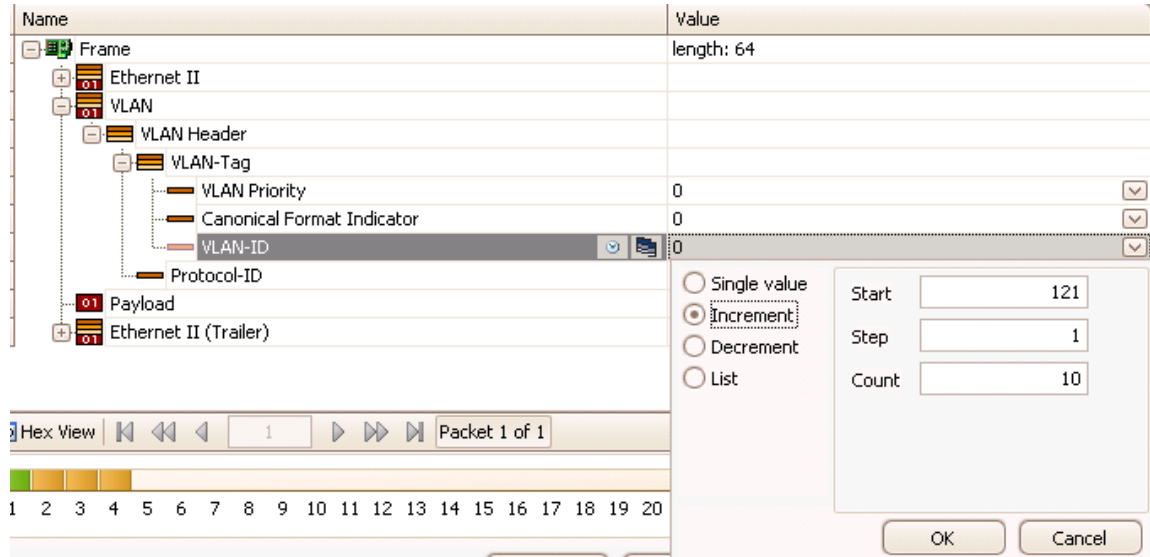


Figure 98. Advanced traffic wizard - Packet/QoS (Packet Editor)



## TEST CASE: LAYER 2 QUALITY OF SERVICE

- Click the **VLAN** priority option list to configure a list pattern with the values of 0, 4, and 5. Click Fully Meshed button to fully mesh the QoS values with the existing number of MAC Addresses.

This creates 100 flows, each with three QoS values, for a total of 300 unique flows per Tx Port.

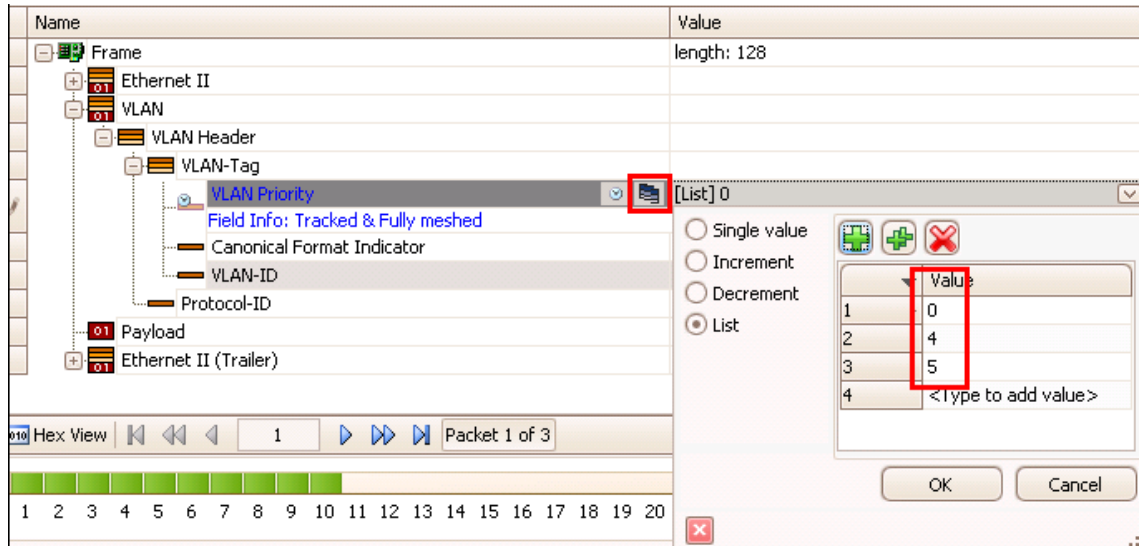


Figure 99. Advanced traffic wizard - Packet/QoS (Packet Editor)

- In the **Flow Group Setup** window, select **VLAN Priority**. This will group together all flows with the same VLAN priority so that you can configure a different traffic profile for flow groups with different VLAN priority. Three flow groups are created in this test.

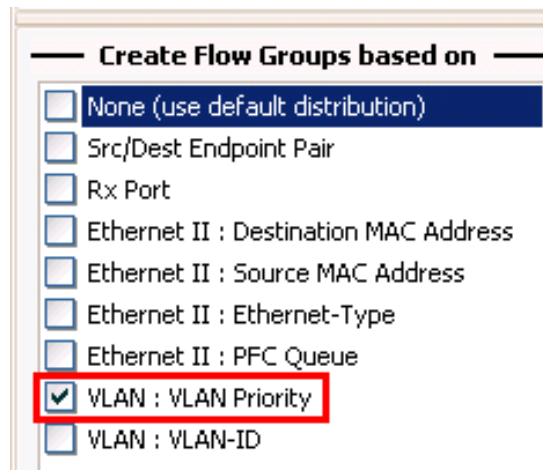
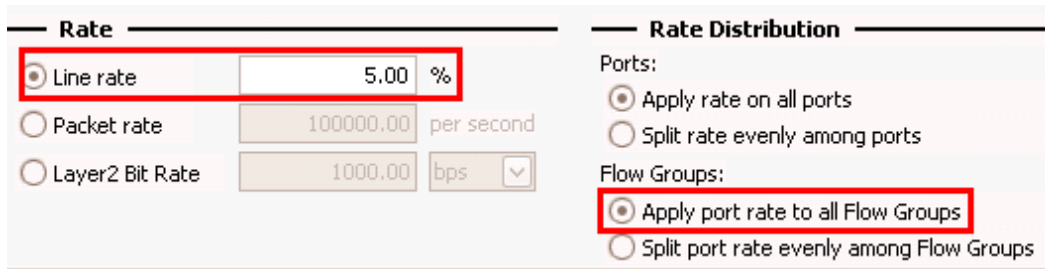


Figure 100. Advanced traffic wizard – flow group setup

- In the **Frame Setup** window, leave all parameters at their default value.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

14. In the **Rate Setup** window, configure the frame rate to be 5 percent of line rate. For rate distribution, select **Apply port rate to all Flow Groups**. Each VLAN priority flow group will get a 5 percent line rate.



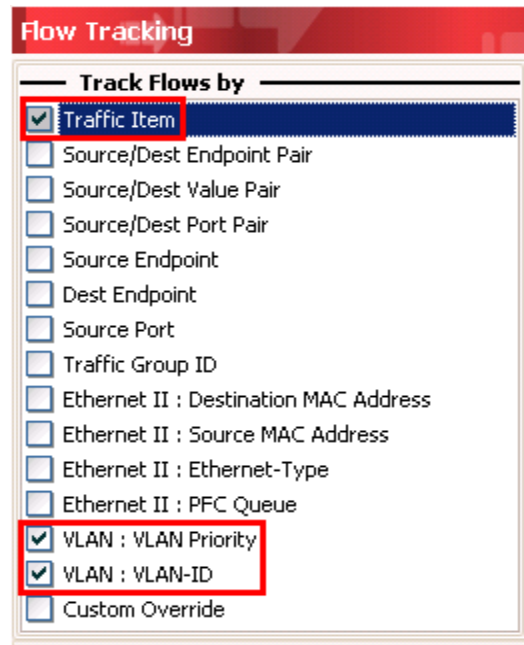
The screenshot shows the 'Rate Setup' window. On the left, under the 'Rate' tab, 'Line rate' is selected with a value of 5.00 %. Below it, 'Packet rate' is set to 100000.00 per second, and 'Layer2 Bit Rate' is set to 1000.00 bps. On the right, under the 'Rate Distribution' tab, 'Apply rate on all ports' is selected. Below that, 'Apply port rate to all Flow Groups' is selected, and 'Split port rate evenly among Flow Groups' is unselected.

Figure 101. Advanced traffic wizard – rate setup

15. In the **Flow Tracking** page, select **VLAN Priority** and **VLAN-ID** as tracking options. The traffic item option is automatically selected as long as there is one other tracking option selected.

**Note:** By Tracking only on VLAN ID and VLAN Priority, IxNetwork only tracks a total of 30 flows in the test, even though there are 300 unique packets created per Tx Port. This is because there are only 10 VLAN IDs multiplied by three VLAN Priorities.

To track all 600 flows across both Tx Ports, select either **EthernetII:Destination MAC Address**, **EthernetII:Destination MAC Address**, or **Source/Dest Value Pair**.



The screenshot shows the 'Flow Tracking' window. Under the 'Track Flows by' section, 'Traffic Item' is selected. Below it, 'VLAN : VLAN Priority' and 'VLAN : VLAN-ID' are selected. Other options like 'Source/Dest Endpoint Pair', 'Source/Dest Value Pair', 'Source/Dest Port Pair', 'Source Endpoint', 'Dest Endpoint', 'Source Port', 'Traffic Group ID', 'Ethernet II : Destination MAC Address', 'Ethernet II : Source MAC Address', 'Ethernet II : Ethernet-Type', 'Ethernet II : PFC Queue', and 'Custom Override' are unselected.

Figure 102. Advanced traffic wizard - Flow Tracking

16. Select **Egress Tracking** on the VLAN priority to verify the VLAN priority of received packets.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

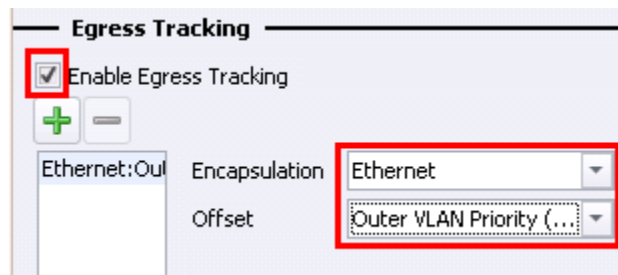


Figure 103. Advanced Traffic Wizard – (Egress) Flow Tracking

17. In the **Preview** window, click **View Flow Groups/Packets** to preview the generated packets. You can preview the current traffic item packets or all traffic items packets.

As shown in the following figures, three Flow Groups are created per port. Each Flow Group has a unique QoS value, but each has the same MAC and VLAN IDs. There is a total of 300 Flows per Tx Port.

Preview

Flow Groups/Packets

Current Traffic Item

All Traffic Items

View

	Flow Group	Traffic Item
	▼ Port: P1	
1 ▶	L2QoS-EndpointSet-1 - Flow Group 0001	L2QoS
2	L2QoS-EndpointSet-1 - Flow Group 0002	L2QoS
3	L2QoS-EndpointSet-1 - Flow Group 0003	L2QoS
	▼ Port: P2	
4	L2QoS-EndpointSet-1 - Flow Group 0004	L2QoS
5	L2QoS-EndpointSet-1 - Flow Group 0005	L2QoS
6	L2QoS-EndpointSet-1 - Flow Group 0006	L2QoS

100 Packets for flow group: L2QoS-EndpointSet-1 - Flow Group 0001

Packet #	Destination MAC Address	Source MAC Address	Ethernet-Type	PFC Queue	VLAN Priority	VLAN-ID
1	00:00:00:03:00:01	00:00:00:01:00:01	8100	0	0	121
2	00:00:00:03:00:02	00:00:00:01:00:02	8100	0	0	122
3	00:00:00:03:00:03	00:00:00:01:00:03	8100	0	0	123
4	00:00:00:03:00:04	00:00:00:01:00:04	8100	0	0	124
5	00:00:00:03:00:05	00:00:00:01:00:05	8100	0	0	125
6	00:00:00:03:00:06	00:00:00:01:00:06	8100	0	0	126
7	00:00:00:03:00:07	00:00:00:01:00:07	8100	0	0	127
8	00:00:00:03:00:08	00:00:00:01:00:08	8100	0	0	128
9	00:00:00:03:00:09	00:00:00:01:00:09	8100	0	0	129
10	00:00:00:03:00:0a	00:00:00:01:00:0a	8100	0	0	130
11	00:00:00:03:00:0b	00:00:00:01:00:0b	8100	0	0	121
12	00:00:00:03:00:0c	00:00:00:01:00:0c	8100	0	0	122
13	00:00:00:03:00:0d	00:00:00:01:00:0d	8100	0	0	123

1

Figure 104. Advanced traffic wizard – preview

18. In the **Validate** window, validate the traffic item before actually generating it. The validation process confirms configuration, packets, flow groups, and flows for either the

## TEST CASE: LAYER 2 QUALITY OF SERVICE

current traffic item or all traffic items. If there is any problem, it will display an error/warning message and correction suggestions.

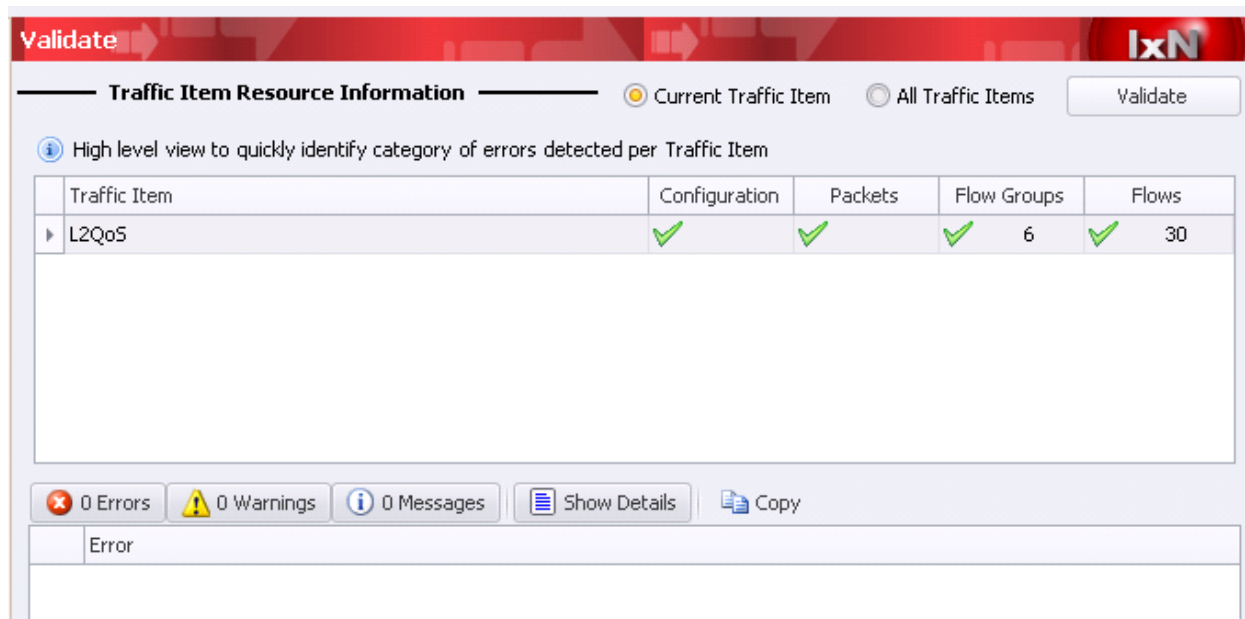


Figure 105. Advanced traffic wizard – validate

- Click **Finish**. A traffic item is created under the **L2-3 Traffic Items** tab in the left panel. Also click **L2-3 Flow groups** to make them appear in the right panel.

Optionally, customize **Frame Size**, **Frame Rate**, **Flow group name**, and so on , for each flow group using the grid operation as well as control the start, stop, suspend, or resume traffic at per flow group level.

Traffic Configuration > L2-3 Flow Groups								
	Transmit State	Suspend	Tx Port	Encapsulation Name	Endpoint Set	VLAN:VLAN Priority	Traffic Item Name	Rx Ports
1		<input type="checkbox"/>	P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 0	L2QoS	P3;
2		<input type="checkbox"/>	P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 4	L2QoS	P3;
3		<input type="checkbox"/>	P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 5	L2QoS	P3;
4		<input type="checkbox"/>	P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 0	L2QoS	P3;
5		<input type="checkbox"/>	P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 4	L2QoS	P3;
6		<input type="checkbox"/>	P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 5	L2QoS	P3;

Figure 106. Traffic grid

## TEST CASE: LAYER 2 QUALITY OF SERVICE

20. **Group** the flow groups by **VLAN priority**. Change the Frame Size of the Flow groups in the traffic grid as shown below:

- VLAN priority 0 – 512
- VLAN priority 4 – 1280
- VLAN priority 5 – 68

The screenshot shows the IxNetwork traffic grid interface. The 'Traffic Tools' tab is active, and the 'Configuration' view is selected. The 'Grid/Column Profiles' dropdown is set to '0%'. The 'Rate Control' section shows 'P2' at 90.00% and '5.00%'. The 'Traffic Configuration' pane shows 'L2-3 Flow Groups'. The main grid has columns: Transmit State, Suspend, Tx Port, Encapsulation, Item Name, Rx Ports, Configured Frame Size, and Frame Rate. The rows are grouped by VLAN priority: 0, 4, and 5. The 'Configured Frame Size' column shows values of 512, 1280, and 68 respectively. A context menu is open over the 'Group Rows By' button, with 'VLAN:VLAN Priority' selected.

Transmit State	Suspend	Tx Port	Encapsulation	Item Name	Rx Ports	Configured Frame Size	Frame Rate
VLAN:VLAN Priority: VLAN:VLAN Priority- 0							
1		P1	Ethernet II		P3;	Fixed: 512	5% Line Rate
2		P2	Ethernet II		P3;	Fixed: 512	5% Line Rate
VLAN:VLAN Priority: VLAN:VLAN Priority- 4							
3		P1	Ethernet II		P3;	Fixed: 1280	5% Line Rate
4		P2	Ethernet II		P3;	Fixed: 1280	5% Line Rate
VLAN:VLAN Priority: VLAN:VLAN Priority- 5							
5		P1	Ethernet II	EndpointSet-1 L2QoS	P3;	Fixed: 68	5% Line Rate
6		P2	Ethernet II	EndpointSet-1 L2QoS	P3;	Fixed: 68	5% Line Rate

Figure 107. Traffic grid – grouping

## TEST CASE: LAYER 2 QUALITY OF SERVICE

21. On the top toolbar, click the **Traffic Options** button to view the **Statistics Measurements** tab. Clear **Latency** and then select **Latency and Delay Variation (Jitter)**. Select **Latency Mode** and **Statistics Mode** as shown in the figure below. Other modes can be selected based on the test requirement.

Global Settings		Statistics Configuration
<b>Available Sets of Statistics</b>		
Statistics Set	Settings	
<input type="checkbox"/> Latency		
<input checked="" type="checkbox"/> Latency and Delay Variation (Jitter)		
	Threshold for large sequence number e... 1	
	Latency Mode	<input checked="" type="radio"/> Store and Forward Latency <input type="radio"/> Cut Through Latency <input type="radio"/> MEF Frame Delay <input type="radio"/> Forwarding Delay
	Statistics Mode	<input type="radio"/> Rx Delay Variation with Sequence Errors and Rx Rate <input type="radio"/> Rx Delay Variation with Latency Ave/Min/Max <input checked="" type="radio"/> Rx Delay Variation with Latency Min/Max and Rx Rate

Figure 108. Traffic options – statistics configuration

## TEST CASE: LAYER 2 QUALITY OF SERVICE

22. On the **L2-3 Traffic Items** option in the left pane, select the Traffic Item and then **Traffic Actions -> Send Learning Frames**. This sends learning frames for all of the Rx ports on this Traffic Item.

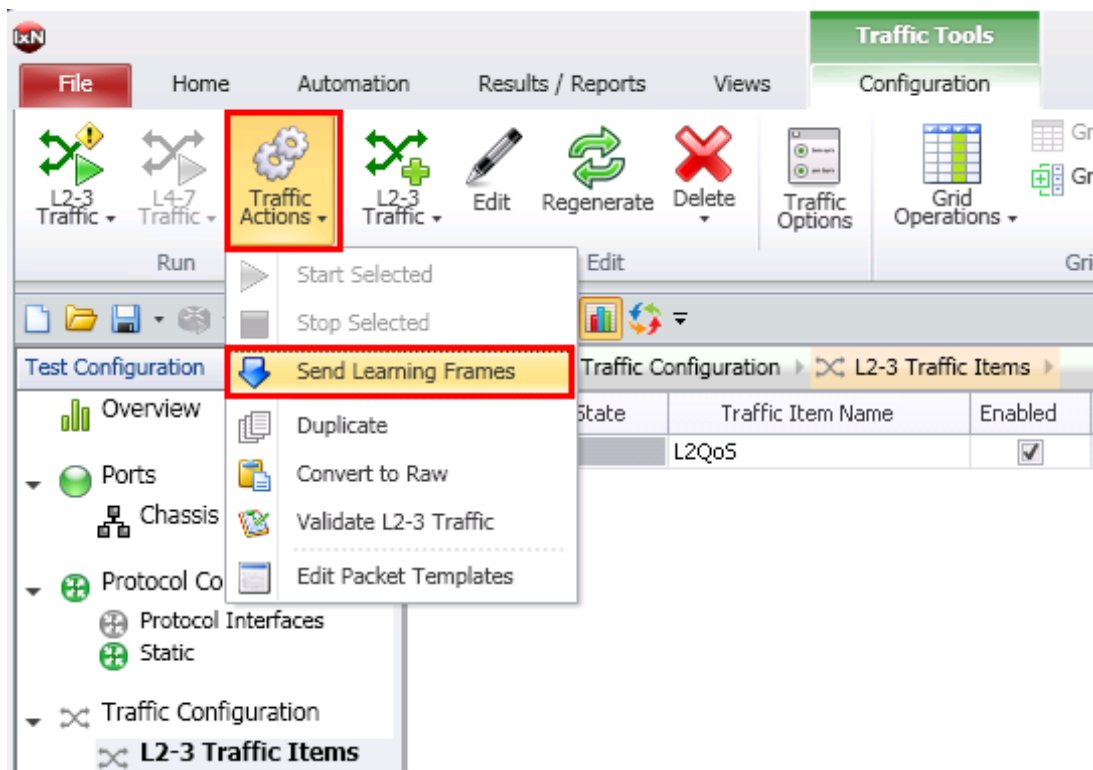


Figure 109. Send L2 Learning frames

23. **Apply** and **Start** traffic.



Figure 110. Apply and start traffic

24. In the **Statistics** window click **Traffic Item Statistics** tab.

Traffic Statistics		Traffic Item Statistics			Global Protocol Statistics		Flow Detecti
	Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1	L2QoS	9,374,082	9,374,068	14	0.000	175,157.000	175,153.000

Figure 111. Traffic item statistics

## TEST CASE: LAYER 2 QUALITY OF SERVICE

25. Select the **Drill Down** icon in the top toolbar, and select **Drill Down per VLAN:VLAN Priority** option. This will drill down within this Traffic Item and display the aggregate statistics for each ingress VLAN Priority.

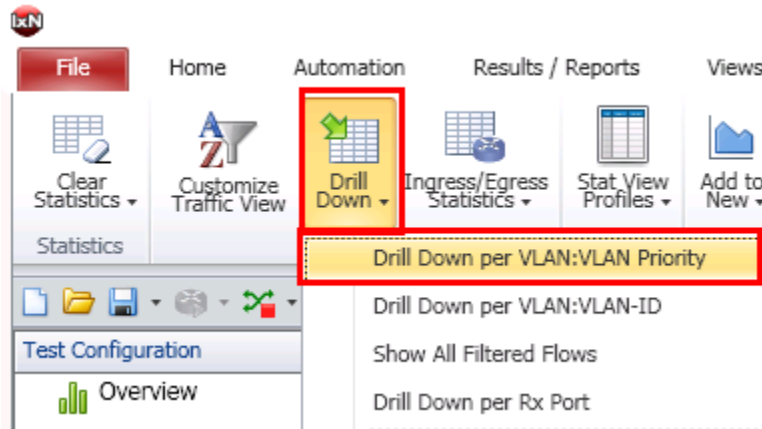


Figure 112. Traffic item drill down options

The traffic rate is 15 percent per Tx port. The Rx port receives about 30 percent of the line rate traffic. There is no congestion and therefore no frame loss at each VLAN priority level. Verify latency and delay variation (jitter). VLAN priority flow statistics provide all the necessary information, as shown below.

Traffic Statistics

Traffic Item Statistics

User Defined Statistics

Global Protocol Statistics

Back

Traffic Item

VLAN:VLAN Priority

	VLAN:VLAN Priority	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1	0	62,629,656	62,629,656	0	0.000	23,496.000	23,497.000
2	4	25,629,982	25,629,982	0	0.000	9,615.000	9,616.000
3	5	378,624,736	378,624,734	2	0.000	142,046.000	142,050.000

	VLAN:VLAN Priority	Store-Forward Min Latency (ns)	Store-Forward Max Latency (ns)	Min Delay Variation (ns)
1	0	25,240	79,080	0
2	4	54,620	70,120	0
3	5	8,140	72,420	0

Max Delay Variation (ns)	Avg Delay Variation (ns)	Short Term Avg Delay Variation (ns)
51,220	7,799	7,794
15,380	1,046	1,045
64,160	28,659	28,654

Figure 113. VLAN priority flow statistics



## TEST CASE: LAYER 2 QUALITY OF SERVICE

26. Highlight the main header row for the flow groups for VLAN priority 0 (simulate data traffic) and 4 (simulate video traffic). Slide the rate bar to about 46 percent of line rate. This generates about 46 percent simulated data and video traffic per Tx port. With the 5 percent voice traffic per port, this creates congestion at the Rx port.

The screenshot shows the IxNetwork configuration interface. The 'Rate Control' section is highlighted, showing a slider for 'Multiple Ports Selected' set to 46.71%. Below this, the 'L2-3 Flow Groups' table is visible, showing two flow groups for VLAN priority 0, both with a frame rate of 46.7104%.

Transmit State	Suspend	Tx Port	Encapsulation Name	Endpoint Set	Traffic Item Name	Rx Ports	Configured Frame Size	Frame Rate
<b>VLAN:VLAN Priority: VLAN:VLAN Priority- 0</b>								
1		P1	Ethernet II	EndpointSet-1	L2QoS	P3;	Fixed: 512	46.7104% Lin...
2		P2	Ethernet II	EndpointSet-1	L2QoS	P3;	Fixed: 512	46.7104% Lin...

Figure 114. Rate change sliding bar

27. Monitor the three flows with different VLAN priorities. VLAN priority 5 flow has the most frame loss and VLAN priority 4 flow has least frame loss. Apparently, high priority flow is not treated differently from low priority flows.

Traffic Statistics

Traffic Item Statistics

User Defined Statistics

Global Protocol Statistics

Back

Traffic Item

VLAN:VLAN Priority

VLAN:VLAN Priority	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1 0	1,993,530	1,976,195	17,335	0.870	197,368.000	195,741.000
2 4	97,122	97,072	50	0.051	9,616.000	9,615.000
3 5	1,434,736	966,180	468,556	32.658	142,045.000	95,064.500

VLAN:VLAN Priority	Store-Forward Min Latency (ns)	Store-Forward Max Latency (ns)	Avg Delay Variation (ns)
0	25,300	4,670,640	9,224
4	54,680	4,657,680	3,744
5	28,440	4,668,460	7,737

	Min Delay Variation (ns)	Max Delay Variation (ns)	Short Term Avg Delay Variation (ns)
0	0	53,280	9,234
0	0	94,100	3,607
0	0	47,960	7,737

Figure 115. VLAN priority flow statistics

## TEST CASE: LAYER 2 QUALITY OF SERVICE

28. Select any cell within the stat view from the previous Step. Click the **Ingress/Egress Statistics** icon on the top toolbar, and then select **Ethernet: Outer VLAN Priority (3 bits) at offset 112**.

This clearly shows both the Ingress and Egress traffic statistics for this Traffic Item based upon the TOS values going in and coming out of the DUT. This view is useful for QoS Remarking tests.

This view shows sent traffic with VLAN priority 0, 4, and 5, while receiving traffic with VLAN priority 0 for all flows. This explains the statistics in step 22 with high frame loss for high priority traffic. The VLAN priority for all packets is marked at the DUT, given the same priority, and placed in same queue. Smaller voice packets are dropped the most.

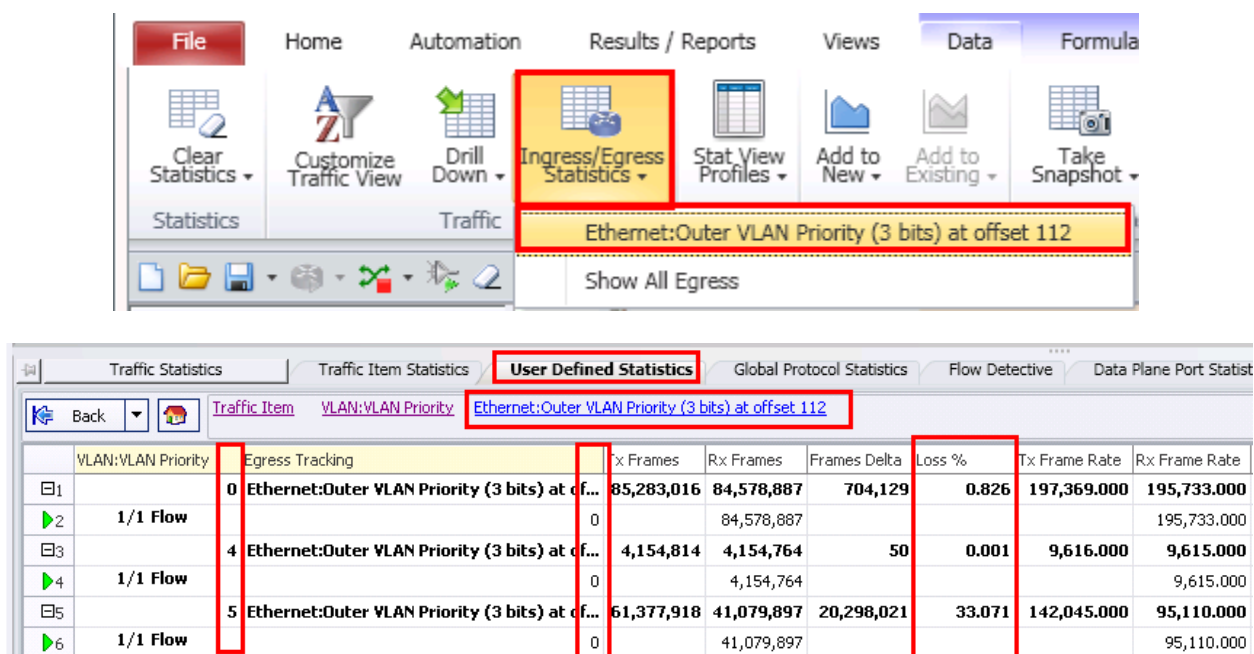


Figure 116. VLAN priority flow statistics ingress/egress view

29. Configure all three DUT interfaces to view the COS value of incoming packets, and schedule the packets based on the original priority at the congestion point.
30. Restart the traffic with the same traffic load as in step 21. The flow with VLAN priority 0 now starts dropping frames, while the other two flows do not (there may be a small frame delta on these two flows, but this is due to packets on-wire and not real frame loss).

L2QoS functionality continues working on the DUT, and incoming packets are differentiated based on their VLAN priority. High priority traffic is given more bandwidth during congestion.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

Compare the latency and delay variation (jitter) with normal conditions – both latency and jitter have increased. However, the high priority flow has increased less while the low priority flow has increased more.

Convert the statistics view above to ingress/egress view by right-clicking the view. This view shows that the received packets of a specific flow have the same VLAN priority the value with which they were sent.

Traffic Statistics

Traffic Item Statistics

User Defined Statistics

Global Protocol Statistics

Flow Detective

Data Plane Port Statistics

Back

Traffic Item

VLAN:VLAN Priority

Ethernet:Outer VLAN Priority (3 bits) at offset 112

	VLAN:VLAN Priority	Egress Tracking	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
0	1/1 Flow	Ethernet:Outer VLAN Priority (3 bits) at offset 12	3,635,308	3,462,178	173,130	4.762	197,368.000	187,969.500
4	1/1 Flow	Ethernet:Outer VLAN Priority (3 bits) at offset 12	177,106	177,100	6	0.003	9,616.000	9,615.000
5	1/1 Flow	Ethernet:Outer VLAN Priority (3 bits) at offset 12	2,616,318	2,616,260	58	0.002	142,045.000	142,045.000

VLAN:VLAN Priority	Egress Tracking	Store-Forward Min Latency (ns)	Store-Forward Max Latency (ns)
0	Ethernet:Outer VLAN Priority (3 bits) at offs...	25,300	5,834,560
1/1 Flow	0	25,300	5,834,560
4	Ethernet:Outer VLAN Priority (3 bits) at offs...	54,660	494,540
1/1 Flow	4	54,660	494,540
5	Ethernet:Outer VLAN Priority (3 bits) at offs...	28,480	440,460
1/1 Flow	5	28,480	440,460

Min Delay Variation (ns)	Max Delay Variation (ns)	Avg Delay Variation (ns)	Short Term Avg Delay Variation (ns)
0	53,300	13,052	13,062
0	53,300	13,052	13,062
0	121,360	21,804	21,714
0	121,360	21,804	21,714
0	47,880	7,959	7,944
0	47,880	7,959	7,944

Figure 117. VLAN priority flow statistics ingress/egress view

## TEST CASE: LAYER 2 QUALITY OF SERVICE

31. Continue increasing the rate to about 49 percent for the flow groups with VLAN priorities 0 and 4 (25 percent and 24 percent respectively). Including the 5 percent traffic for VLAN priority 5, each Tx port sends about 54 percent of the line rate. This increases the congestion at the DUT. Now packets from the flow with VLAN priority 4 start getting dropped. Compare the latency and delay variation (jitter) with previous congestion conditions. Both latency and jitter increased with the congestion increase, but the high priority flow always has the least latency and jitter.

Traffic Statistics							
Traffic Item Statistics							
User Defined Statistics							
Global Protocol Statistics							
Back		Traffic Item VLAN:VLAN Priority					
	VLAN:VLAN Priority	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1	0	1,007,552	846,375	161,177	15.997	117,482.000	98,682.000
2	4	395,826	395,804	22	0.006	46,154.000	46,154.000
3	5	1,218,220	1,218,156	64	0.005	142,046.000	142,044.000
VLAN:VLAN Priority		Store-Forward Min Latency (ns)		Store-Forward Max Latency (ns)			
0		25,340		10,774,760			
4		54,680		505,120			
5		24,800		447,000			
Avg Delay Variation (ns)		Min Delay Variation (ns)		Max Delay Variation (ns)		Short Term Avg Delay Variation (ns)	
28,763		0		127,480		28,691	
20,359		0		87,380		20,354	
6,440		0		58,380		6,462	

Figure 28. VLAN priority flow statistics

32. Drill down further to the VLAN ID level by right-clicking on any VLAN priority and selecting the **Drill Down per VLAN:VLAN-ID** option.

Traffic Statistics							
Traffic Item Statistics							
User Defined Statistics							
Global Protocol Statistics							
Back		Traffic Item VLAN:VLAN Priority					
	VLAN:VLAN Priority	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1	0	102,276,348	85,910,797	16,365,551	16.001	117,481.000	98,680.000
2	4	Drill down per VLAN:VLAN-ID			21	0.000	46,154.500
3	5	Show All Filtered Flows			62	0.000	142,045.000

Figure 29. Drill down VLAN ID (2nd level)

## TEST CASE: LAYER 2 QUALITY OF SERVICE

33. This brings up per VLAN ID flow statistics for a specific VLAN priority level. There is no specific ordering for drill down options. You can drill down from the top aggregated traffic item statistics view with any available drill down option and drill down further with any desired order to suit the test requirement.

Back		Traffic Item VLAN:VLAN Priority VLAN:VLAN-ID					
	VLAN:VLAN-ID	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
▶ 1	121	9,710,718	8,146,373	1,564,345	16.109	11,748.000	9,875.500
2	122	9,710,718	8,184,903	1,525,815	15.713	11,748.000	9,879.000
3	123	9,710,718	8,126,297	1,584,421	16.316	11,748.000	9,794.000
4	124	9,710,718	8,157,939	1,552,779	15.990	11,748.000	9,854.500
5	125	9,710,718	8,165,862	1,544,856	15.909	11,748.000	9,897.500
6	126	9,710,718	8,155,577	1,555,141	16.015	11,748.000	9,868.500
7	127	9,710,718	8,135,681	1,575,037	16.220	11,749.000	9,847.500
8	128	9,710,718	8,189,230	1,521,488	15.668	11,749.000	9,917.000
9	129	9,710,716	8,160,321	1,550,395	15.966	11,748.000	9,885.500
10	130	9,710,716	8,146,589	1,564,127	16.107	11,748.000	9,864.000

Figure 30. VLAN ID flow statistics

## Result Analysis

Without QoS, the CoS value of incoming packets is marked to 0 at the DUT and all flows are treated equally. When congestion occurs, all flows suffer a similar percentage of packet loss, latency, and jitter.

With QoS, flows with different CoS values are treated differently at the DUT. When congestion occurs, flows with higher priority are given more bandwidth and are served at a higher frequency, and suffer less latency and jitter. This can be verified with frame loss and latency/jitter values measured using per-CoS flow statistics.

## Troubleshooting and Diagnostics

Issue	Troubleshooting Tip
All CoS flows suffer similar frame loss	Check the DUT's configuration to make sure QoS is enabled at global level, and CoS values are trusted on the incoming port. Alternatively, use Ixia's ingress/egress view to find out receiving packet's QoS value
DUT does not pass any traffic	Verify that the VLANs used in Ixia traffic are created at DUT and the ports are in forwarding state for the spanning tree instance they belong to.

## TEST CASE: LAYER 2 QUALITY OF SERVICE

### Test Variables

Test Variables	Description
# of test ports	Increase # of Tx and Rx ports to validate DUT's capability to perform QoS function concurrently across multiple ports and line cards.
# of Mac address	Increase # of source and destination MAC addresses to validate DUT's capability to perform QoS function on a large # of MAC addresses.
VLAN ID	Increase # of VLAN IDs to validate DUT's capability to perform QoS function for multiple broadcast domains.
Frame Rate	Test DUT's capability to perform QoS function under various traffic loads.
Frame Size	Test DUT's capability to perform QoS function under various frame sizes.
Integrated Test	Use Integrated Test to find out throughput/latency, frame loss, etc. for traffic with various CoS levels.
Event Scheduler program	Create an event scheduler program to iterate frame rates and frame sizes, and snapshot the per-CoS flow statistics view for post analysis.
Change encapsulation	Add layer 3 and/or layer 4 encapsulations to the packet and validate QoS function.
MPLS Exp bits	Perform similar test for MPLS label-switched traffic by setting various MPLS Exp bits. MPLS is a layer between layer 2 and layer 3.
DUT queue bandwidth ratio	Perform similar test with a different queue bandwidth ratio.
DUT queue buffer allocation	Perform similar test with a different buffer allocation.

### Conclusions

This test proves that a DUT properly implemented the mapping of packets with different CoS values to different queues, and properly implemented transmit scheduling among different queues.

This test also shows that IxNetwork's advanced traffic wizard can build highly flexible QoS traffic. The aggregated statistics view provides many important benchmarks, such as frame loss, Rx rate (bytes, bits, Mbps, etc), latency, jitter, and sequence error at the traffic-item level, as well as various user-defined levels. The multi-field drill down view helps identify issues quickly by only looking at interesting flows out of large numbers of flow statistics. The egress tracking can track any field of receiving packets. With combined ingress/egress view, real-time statistics are used to identify DUT QoS marking.

IxNetwork's numerous capabilities make QoS testing very easy.



## Test Case: Layer 3 Quality of Service

Layer 3 quality of service (QoS) classifies traffic at layer 3 to differentiate between different traffic types. Layer 3 QoS enables the network to improve delivery-sensitive application services and results in predictable network behavior.

### Layer 3 QoS Benefits

Layer 3 QoS implementations often improve network functionality, resulting in:

- **True end-to-end QoS layer 3** -- QoS allows network administrators to configure QoS from source to destination endpoints.
- **Optimum efficiency** -- A properly configured layer 3 QoS system creates better network resource management for the various application traffic requirements.
- **Assured scalability and performance** -- Correctly planned networks – ones that include QoS provisioning -- allow for performance improvements that don't require a design overhaul.
- **Customized services** -- Fine tuning QoS policies allows service providers to provide customized services, such as low latency Citrix traffic.

### Layer 3 QoS Challenges

Layer 3 QoS must provide customers with the expected service quality and reliability for their latency- and bandwidth-sensitive applications.

#### Correct queue size configuration

Different types of traffic must be handled differently to achieve optimal network performance. In order to ensure differentiated handling of traffic classes, network switches must support enough queues to accommodate the various traffic classes.

Predictable network performance requires that different traffic types have different queue specifications. Latency-sensitive applications such as video and voice must have priority queuing, while general data applications only need some form of round-robin queuing.

#### Consistent Policy Across Devices

Traffic path devices must adhere to the same configured QoS policy. Predictable network performance results from classifying packets as close to their source as possible, and enforcing the classification along the entire network path.



## TEST CASE: LAYER 3 QUALITY OF SERVICE

### Packet Loss

Packet loss is one of the most common factors affecting application traffic. For example, even though voice CODECs can accept some packet loss without dramatically degrading speech quality, the loss of many consecutive packets dramatically affects the end result even if the total loss percentage is low. Even in data transfer traffic scenarios, excessive packet loss causes unnecessary network resource allocation from data retransmissions.

Since voice and data use the same resources in converged networks, voice traffic must have priority treatment over data traffic, which is less affected by delay, jitter, and packet loss.

### Effect of Delay on Traffic

It is well known that network delay leads to two-way traffic difficulties. For example, Alice and Bob enact a VoIP call using an IP network with a high round-trip delay (for example, 500 ms). If Alice interrupts Bob, he will continue to speak until the interruption is perceived. It takes a moment to sort out the conversation. To meet quality requirements the one-way delay must be kept below 150 ms.

VoIP calls are just one example of the importance of limiting delay in time-sensitive applications.

### Jitter

Jitter is the measurement of receiver delay. Many devices implement a jitter buffer that accounts for the jitter effect. A jitter buffer minimizes delay variations by temporarily storing packets and discarding packets that arrive too late. If a jitter buffer is too small, then an excessive number of packets may be discarded, which can lead to degradation of service.

The most common causes of jitter are network congestion and router/switch queuing methods.

## Layer 3 QoS Mechanisms

There are multiple layer 3 QoS mechanisms to satisfy network needs. However, IntServ and DiffServ are the most common methods of implementing layer 3 QoS.

### Intserv

IntServ is a rich and granular QoS solution by using RSVP for end-to-end signaling, state maintenance, and admission control. IntServ requires that network elements keep track of each individual traffic flow on the network. This requires that core network routers and switches maintain a soft state by setting aside resources.

### Diffserv

Diffserv, while coarser, offers a simpler QoS method by categorizing traffic into different classes and then providing each class a different QoS service. This method sidesteps the issues of cost, complexity, and scalability associated with Intserv.

Diffserv uses the type of service (TOS) byte in IP (both IPv4 and IPv6) headers. There are two Diffserv implementations developed by vendors in the field:

### A. TOS/IP Precedence

The TOS byte in the IP header is sub-divided into three different fields. Bits 0-2 give the packet one of the eight possible IP precedence values. Higher precedence packets are dropped less than those with lower precedence. In addition, the TOS field provides different delay, throughput, and reliability to the packet.

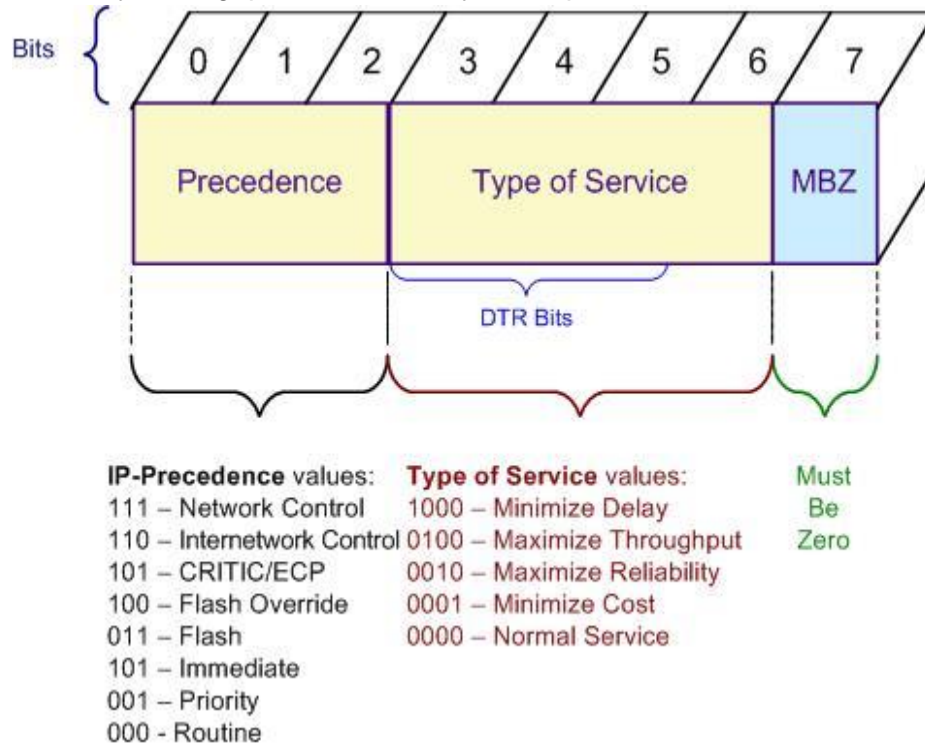


Figure 31. Precedence values in the packet header

The TOS/IP precedence method not only defines the relative priority of a packet, but also assigns an no-drop precedence to packets belonging to the same class. For example, FTP and Telnet traffic may belong to the same precedence class. During network congestion, however, a network operator might assign higher drop probability to FTP traffic.

Three bits in the header for precedence only allows eight possible priority classes.

### B. Differentiated Services

Differentiated services have two main components: packet marking and per-hop behavior (PHB).

**Packet Marking:** The TOS byte in the IP header has been completely redefined. The first 6 bits are set aside for differentiated services code point (DSCP) values. DSCP values are used to support up to 64 different aggregates/classes of traffic.

## TEST CASE: LAYER 3 QUALITY OF SERVICE

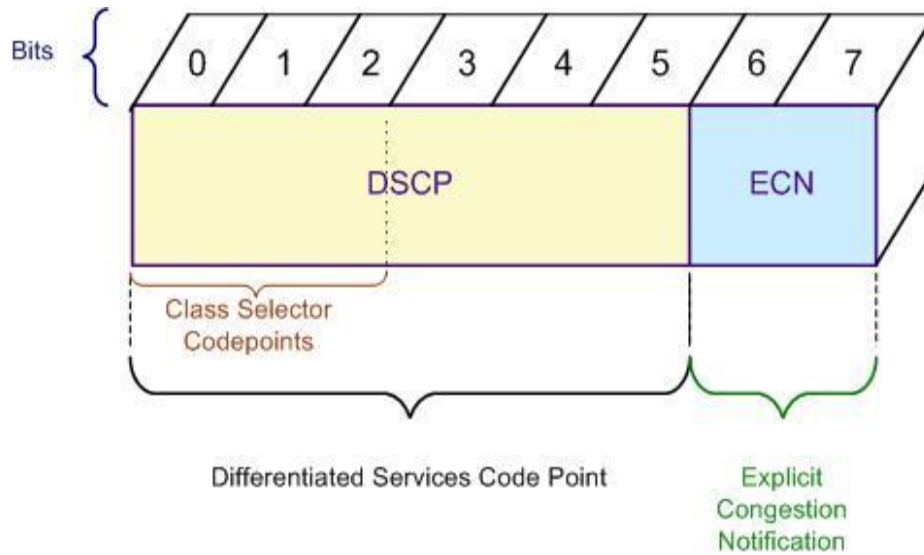


Figure 32. DSCP values

All packets sharing the same DSCP value and direction are called a behavior aggregate (BA).

**Per Hop Behavior (PHB):** PHB is the packet scheduling, queuing, policing, and shaping performed by a network node on packets belonging to any particular BA. The network operator can configure different policies for different BAs.

The following PHBs are widely used to implement a Diffserv-enabled network:

- Default PHB – the PHB defined for packets marked with DSCP value of 000000. Packets marked with this DSCP value get the best effort service.
- Class-Selector PHB – the PHB used to ensure compatibility with TOS/IP precedence and is associated with packets marked with DSCP values of the form “xxx000,” where xxx correspond to IP-Precedence values.
- Expedited Forwarding PHB – the PHB for applications with low-loss, low-latency, low-jitter, and guaranteed bandwidth service, such as VoIP and IPTV.
- Assured Forwarding PHB – the PHB that defines which BAs can be assigned priority as well as drop precedence values. This allows for more granular QoS control of packets that share the same class but have different drop precedence (low, medium, and high).

### Objective

The objective of this test is to show the DUT QoS performance under different load conditions.

Ixia ports will send traffic with three different TOS values, and the DUT will give different priority to the traffic based on the TOS Precedence field value. Traffic is initially sent below the link threshold on the DUT egress port, and then is increased to cross the DUT egress port link

## TEST CASE: LAYER 3 QUALITY OF SERVICE

bandwidth threshold. The DUT is configured to mark the TOS precedence when the bandwidth goes over the configured threshold.

This test demonstrates IxNetwork's QoS test capabilities. The methodology includes automation of DUT configuration via CLI as well as sequencing of IxNetwork traffic events using Test Composer.

### 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. Ixia Port 1 is running at 1000M, and Ixia Port 2 is running at 100M Full Duplex. The DUT processes the packets based upon the TOS precedence values in the IPv4 headers.

The DUT should prioritize TOS values 7, 4 and 0 (in that order).

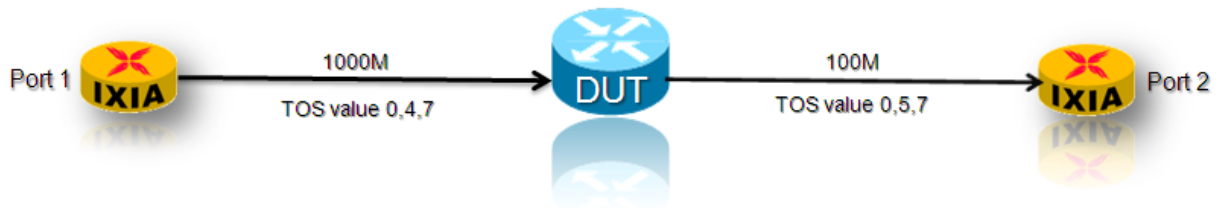


Figure 33. Network diagram of 'Layer 3 Quality of Service' Test Case

## TEST CASE: LAYER 3 QUALITY OF SERVICE

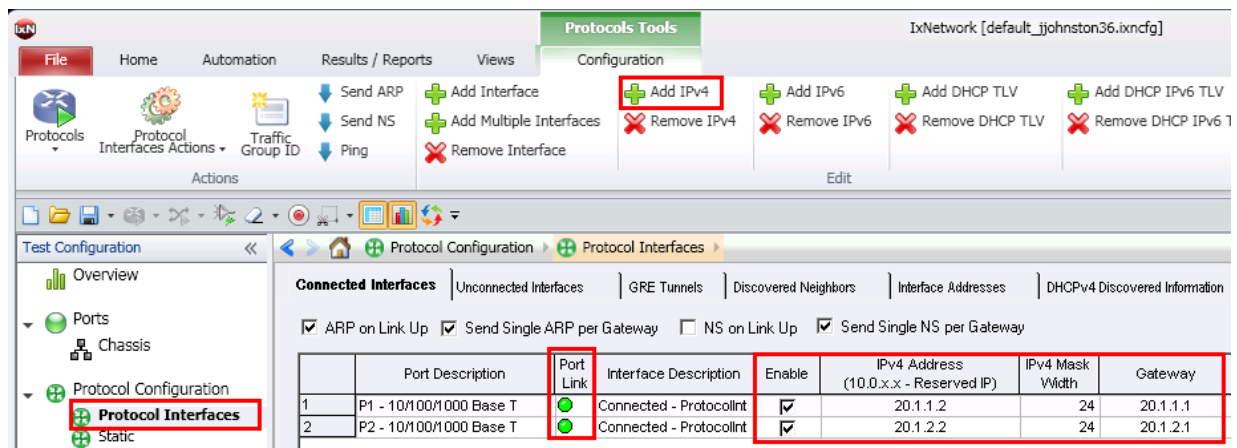
### Step by Step Instructions

The following step-by-step instructions highlight how to set the essential IxNetwork parameters, and explain additional options that can modify the test behavior.

1. Open the IxNetwork GUI, and add two physical ports to the configuration.
2. Under **Protocol Interfaces**, configure two connected protocol interfaces with the following parameters:

**Table 5. Summary of protocol interface parameters**

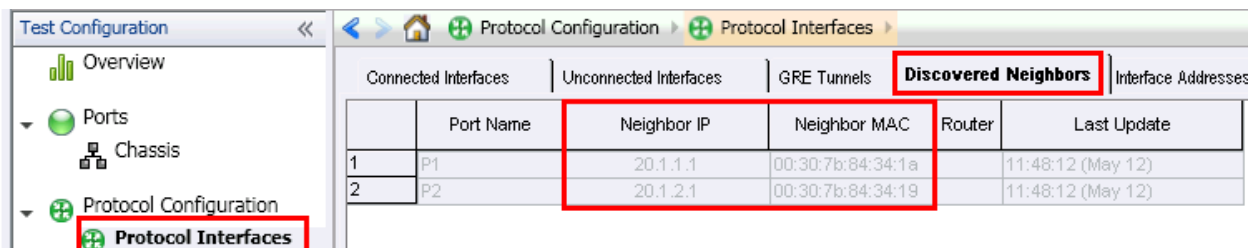
IP Type	First IP / Subnet	Mask Width	Gateway	MTU
IPv4	20.1.1.2	24	20.1.1.1	1500
IPv4	20.1.2.2	24	20.1.2.1	1500



**Figure 34. Configuring IP addresses in IxNetwork**

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

1. 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 35. Verifying IP connectivity**

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

## TEST CASE: LAYER 3 QUALITY OF SERVICE

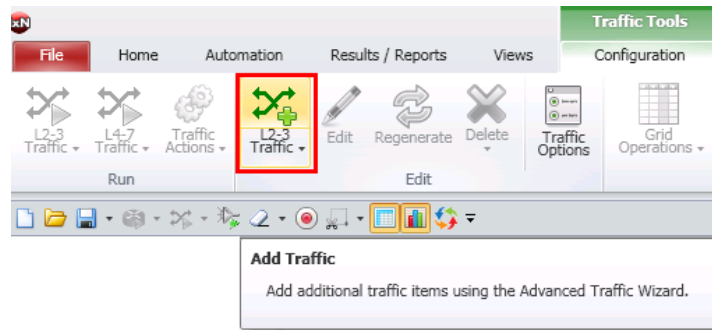



Figure 36. Starting Advance Traffic Wizard

3. 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.
4. Configure the IP priority TOS values of 0, 4, and 7 in the **Packet/QoS** screen.

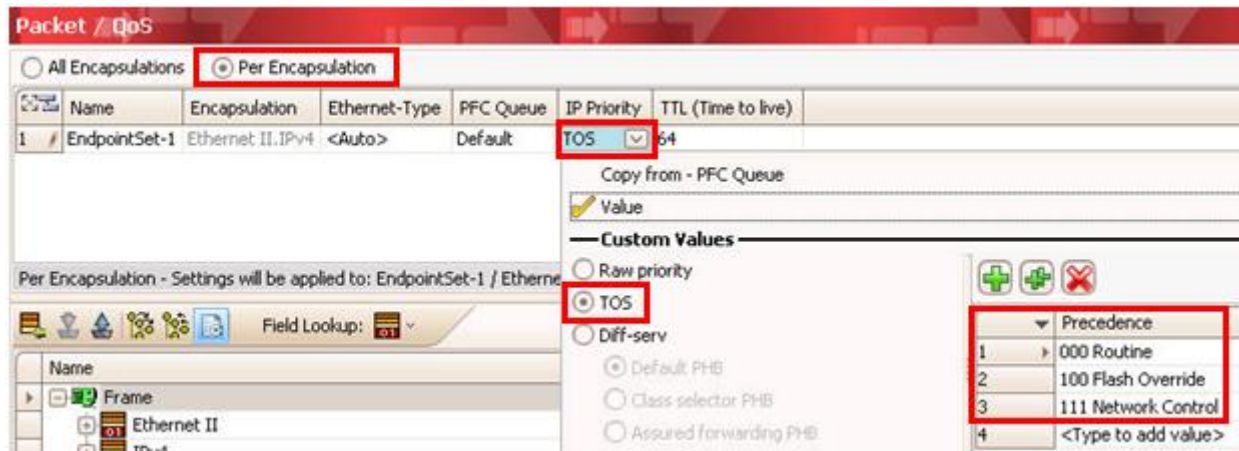


Figure 37. TOS values

## TEST CASE: LAYER 3 QUALITY OF SERVICE

- After configuring the TOS values, create the flow groups. In the **Flow Group Setup** step, configure flow groups for each TOS precedence value. Select the **IPv4: Precedence** option.

**Note:** See the description and diagram on the right explaining how IxNetwork creates Flow Groups based on the type of Flow Grouping selected.

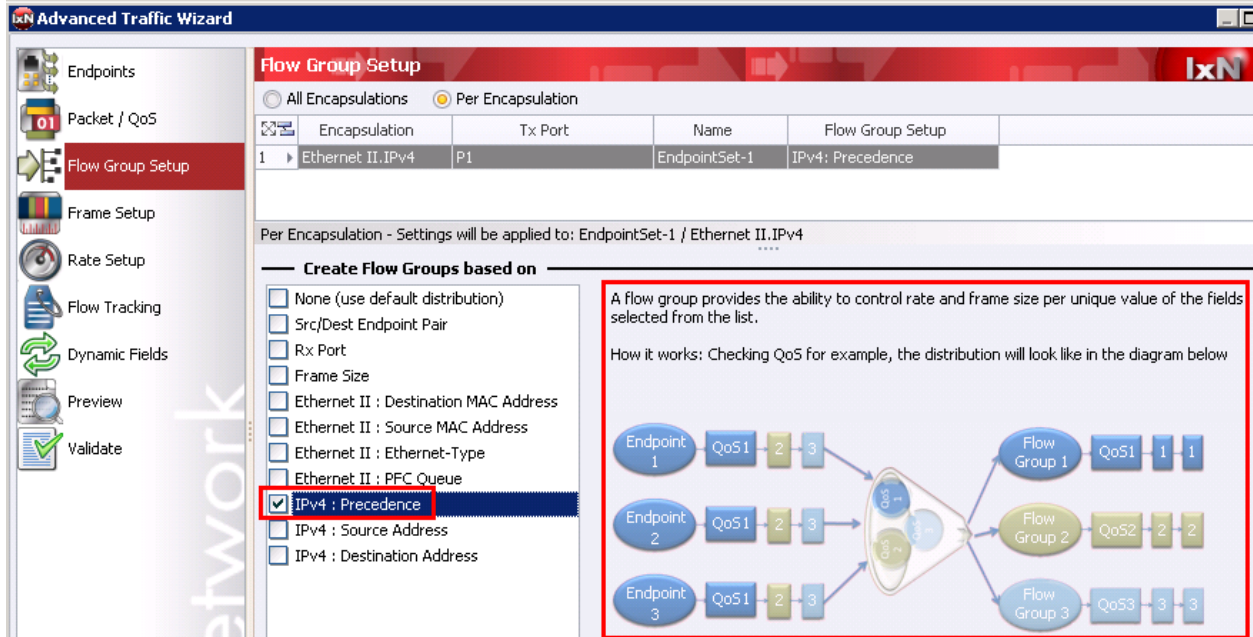


Figure 38. Flow Grouping based on IPv4 precedence

- 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**.

- In the **Rate Setup**, configure a line rate of 3 percent.

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



## TEST CASE: LAYER 3 QUALITY OF SERVICE

8. 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 will track the IP Precedence (TOS) field from the DUT ingress and egress side. In some cases the DUT will change the TOS value as traffic flows through the DUT. This usually occurs 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 which are oversubscribing the DUT Egress port.

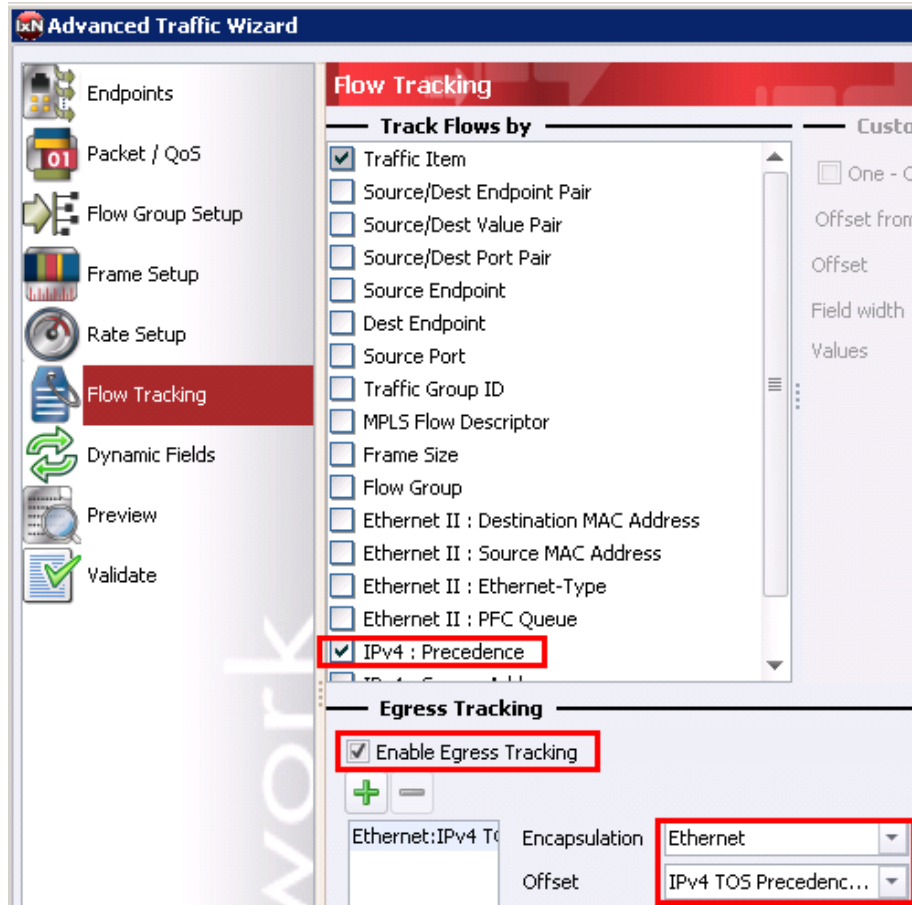


Figure 39. Flow tracking

9. Do not configure or select anything on the **Dynamic Fields** screen.
10. In the preview step, click **View Flow Groups/Packets** to verify that the flow groups are created.
11. The final **Validate** screen is optional. This screen allows the user to validate if the settings used in this run of the traffic wizard, and gives other useful information such as number of Flow Groups and Flows.
12. Click **FINISH**



## TEST CASE: LAYER 3 QUALITY OF SERVICE

13. Apply and start the traffic.

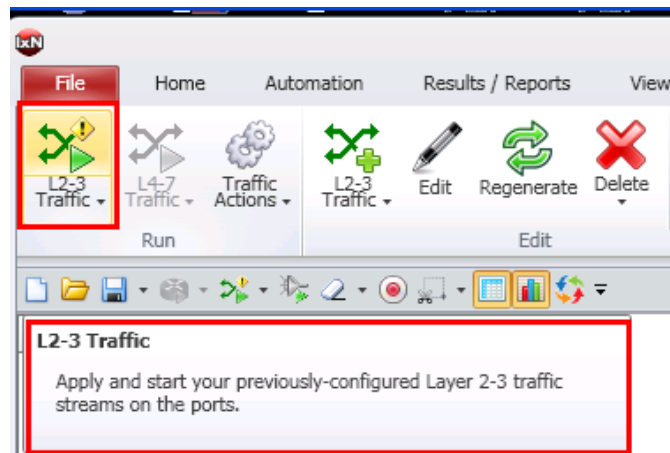


Figure 40. Apply and Start traffic

14. In the Statistics pane in the lower pane of the window, click **Traffic Item Statistics** Tab. The aggregate statistics for the traffic item, including the statistics for all flow groups and flows created within the traffic item appears.

Traffic Statistics		Traffic Item Statistics			User Defined Statistics		Port CPU Statistics	
	Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate	Rx B
▶ 1	Traffic Item 1	236,389	234,959	1,430	0.605	7,049.000	7,049.000	120

Figure 41. Traffic Item Statistics view

## TEST CASE: LAYER 3 QUALITY OF SERVICE

15. Select the **Drill Down** icon in the top toolbar, and select **Drill Down per IPv4: Precedence** option. This will drill down within this Traffic Item and display the aggregate statistics for each ingress TOS precedence value.

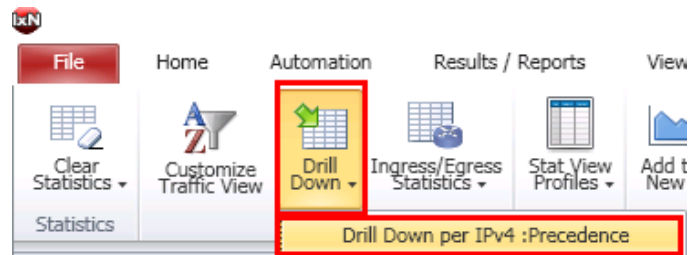
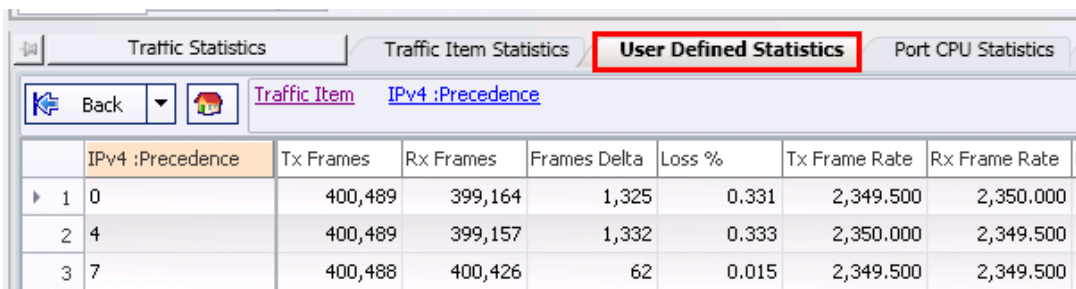


Figure 42. Drill Down



	IPv4 :Precedence	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1	0	400,489	399,164	1,325	0.331	2,349.500	2,350.000
2	4	400,489	399,157	1,332	0.333	2,350.000	2,349.500
3	7	400,488	400,426	62	0.015	2,349.500	2,349.500

Figure 43. Ingress Tracking - TOS precedence values

## TEST CASE: LAYER 3 QUALITY OF SERVICE

16. Select any cell within the stat view from Step 15. Click the **Ingress/Egress Statistics** icon in the top toolbar, and then select **Ethernet: IPv4 TOS Precedence (3 bits) at offset 120**. This will show both the Ingress and Egress traffic statistics for this Traffic Item based upon the TOS values going in and coming out of the DUT. This view is useful for QOS Remarking tests.

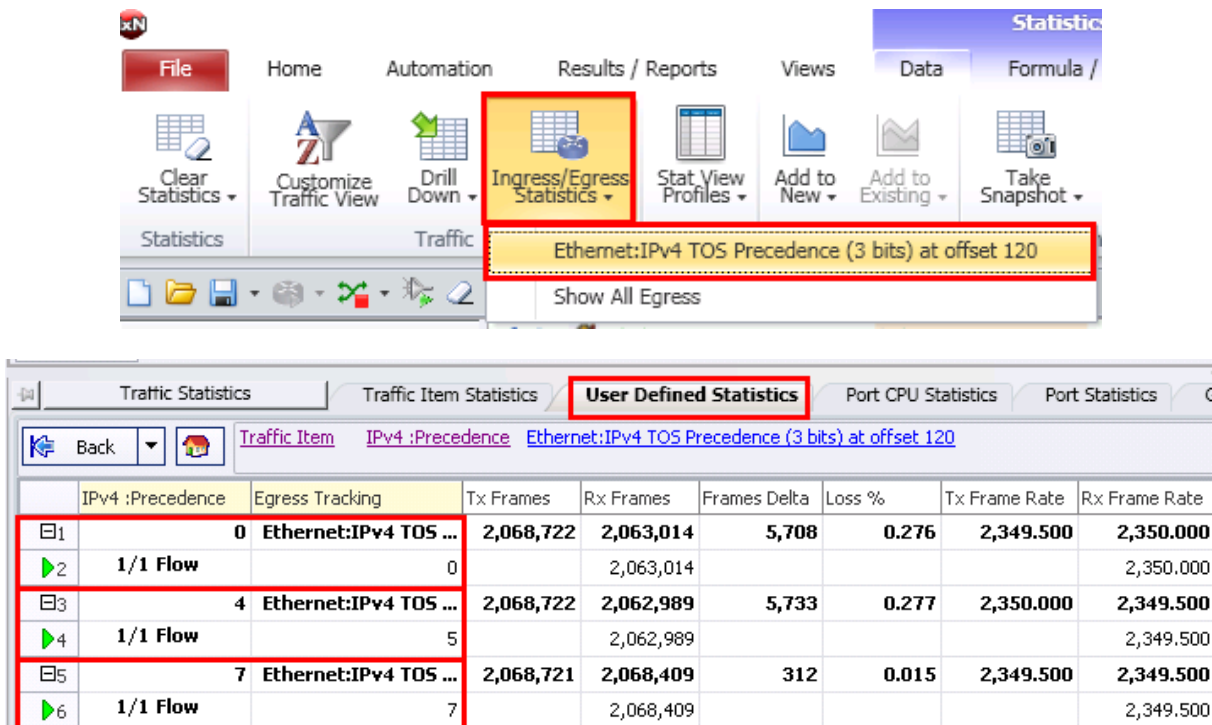


Figure 44. Ingress and Egress Tracking - TOS precedence values

17. Increase the throughput of each of the flow groups by entering a value of 5% in the frame rate column for all groups. This will oversubscribe the DUT Egress port.

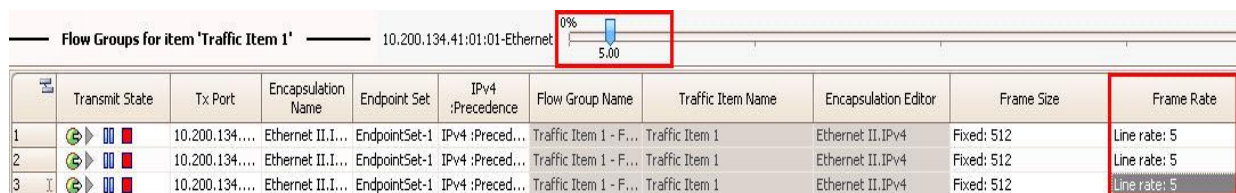


Figure 45. Frame rate column

## TEST CASE: LAYER 3 QUALITY OF SERVICE

18. Verify the DUT's behavior by checking the traffic statistics again.

**Note:** The DUT prioritizes the high priority TOS value of 7 while discarding the lower priority traffic in this oversubscription environment.

Traffic Item IPv4 :Precedence Ethernet:IPv4 TOS Precedence (3 bits) at offset 120						
	IPv4 :Precedence	Egress Tracking	Tx Frames	Rx Frames	Frames Delta	Loss %
1	0	Ethernet:IPv4 TOS ...	133,192	18,439	114,753	86.156
2	1/1 Flow	0		18,439		
3	4	Ethernet:IPv4 TOS ...	177,587	65,694	111,893	63.007
4	1/1 Flow	5		65,694		
5	7	Ethernet:IPv4 TOS ...	221,982	221,595	387	0.174
6	1/1 Flow	7		221,595		

Figure 46. Traffic statistics

19. By default, the generated traffic only has latency enabled. However, you can select the performance statistics to display in the **Traffic Options**.

Options		
Global Settings Statistics Configuration		
<b>Available Sets of Statistics</b>		
Statistics Set	Settings	Description
<input type="checkbox"/> Latency		One-way per packet delay measurement (over time) reported as Ave, Min, and Max
<input checked="" type="checkbox"/> Latency and Delay Variation (Jitter)		One-way per packet delay measurement and delay variation measurement from output port to input port
Threshold for large sequence number error	2	The user-configurable threshold value - used to determine error levels for out-of-sequence, received packets
	Latency Mode <input checked="" type="radio"/> Store and Forward Latency <input type="radio"/> Cut Through Latency <input type="radio"/> MEF Frame Delay <input type="radio"/> Forwarding Delay	Standard: RFC 1242 Method: The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port (LIFO)
	Statistics Mode <input checked="" type="radio"/> Rx Delay Variation with Sequence Errors <input type="radio"/> Rx Delay Variation with Latency Ave/Mir <input type="radio"/> Rx Delay Variation with Latency Min/Max	Delay Variation reported as Ave/Min/Max and Short Term with Sequence Errors reported as Small, Big and Reverse, all Rx Rate measurements

Figure 47. Traffic options

## Results Analysis

The following questions provide guidelines on how to recognize specific problems during or after test execution:

1. Has the test objective been achieved? Check the **IP Precedence** values in the **User Defined Statistics**.

**Table 6. TOS Precedence statistics**

Statistic Name	Value	Questions
IPv4: Precedence		Are the ingress and egress IPv4 precedence values the same?
Egress Tracking: IPv4 TOS Precedence		Is the DUT correctly remarking TOS precedence values under different traffic conditions?

2. Is the traffic being processed by the DUT correctly?

**Table 7. Traffic behavior statistics**

Statistic Name	Behavior
Loss %	Is the loss % experienced by flow groups the expected behavior? Compare the Loss % with ingress and egress TOS precedence values
Tx Frames	
Rx Frames	
Tx Frame Rate	
Rx Frame Rate	

3. How much Jitter (Delay Variation) is the DUT introducing to traffic as it processes the IP Precedence values in the header?

**Table 8. Statistics highlighting the pass/fail result based on call flow execution**

Statistic Name	Behavior
Average Delay Variation	Are the successful loops and total loops values equal?  Have any failed loops, aborted loops, or warning loops been reported?
Min. Delay Variation	
Max. Delay Variation	
Small Error	
Big Error	

## Troubleshooting and Diagnostics

The following table summarizes some common issues that occur when running a layer 3 QoS test.

## TEST CASE: LAYER 3 QUALITY OF SERVICE

**Table 9. Common testing issues**

Issue	Solution
Can't ping to/from the DUT	Check the <b>Protocol Interface</b> tab and look for red exclamation marks (!). If found, there is likely an IP address or gateway mismatch. Ensure that the <b>Discovered Neighbors</b> tab has the correct information.
DUT starts to drop packets	Check the DUT configuration to verify that: <ul style="list-style-type: none"> <li>▪ The traffic transmit rate does not exceed the DUT egress port's capability.</li> <li>▪ The DUT's configuration is set to drop packets when they cross a certain threshold.</li> </ul>
The TOS precedence bits are not remarked	Verify that the policy on the DUT is setup to correctly identify and mark the packets.

### Test Variables

IxNetwork offers flexible and comprehensive coverage of layer 3 QoS test use cases. The values configured in the above test can be modified to test different layer 3 QoS test scenarios.

**Table 10. Test tool parameters employed**

Parameter Name	Options
<b>Step 1.</b> Number of Ports used	In this test we used two ports. However IxNetwork can be used to scale to large number of ports that can emulate real-life networks.
<b>Step 2.</b> Number of Endpoints	Traffic endpoints.
<b>Step 3.</b> TOS Precedence values	Any value from 000 (Routine) to 111 (network control).
<b>Step 3.</b> DSCP Values	DiffServ values for default, class-selector, assured and expedited forwarding can also be configured.
<b>Step 4.</b> Flow Group creation	Based upon IPv4 precedence value. However you can create flow groups based upon other criteria.
<b>Step 5.</b> Frame Size	This test used fixed frame size. IxNetwork also allows for other frame size mechanisms: Increment, random, IMIX, quad gaussian, or auto.
<b>Step 6.</b> Rate	3% and 5% of line rate. These rates can be changed on the fly from the traffic grid.
<b>Step 7.</b> Flow Tracking	IPv4 precedence. There are many other flow tracking elements available depending on your requirements.
<b>Step 7.</b> Flow Tracking: Egress Tracking	IPv4 TOS precedence. There are many other egress tracking elements available for tracking.

**Table 11. DUT test variables**

Parameter Name	Current Value/Behavior
TOS Precedence	7,4 and 0

## TEST CASE: LAYER 3 QUALITY OF SERVICE

Action to perform when egress bandwidth is overloaded	Apply Layer 3 QoS policy configured to remark IP Precedence values from 4 to 5. IxNetwork can be used to verify that the DUT is performing the TOS header remarking correctly
Traffic Shaping	DUT can be configured to provide different traffic treatment to different QoS classes. IxNetwork statistics can be used to verify the traffic shaping results

### Conclusions

This test methodology demonstrated how to configure the parameters of a layer 3 QoS test, using practical examples and varying traffic loads. The DUT was configured to process TOS classes, resulting in different traffic behavior as the load was progressively increased.

## 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

The setup is similar to the setup of Test Case: Layer 3 Quality of Service Layer 3 QoS Mechanisms. The only difference is that an ImpairNet module is inserted between the Ixia test port (acting as source) and DUT.



Figure 48. Impairment testing – Layer 3 QoS Mechanism

### Step by Step Instructions

These instructions will result in Delay, Jitter and Drop Impairment test for Layer 3 QoS topology shown in Figure 48. The steps below will guide you to build other Impairment test scenarios.



## TEST CASE: LAYER 3 QUALITY OF SERVICE

1. Follow the steps in the Test Case: Layer 3 Quality of Service to configure Layer 3 QoS Topology. Open the traffic item and clear the Precedence check box. This creates one traffic flow instead of three traffic flows. In the following steps, the traffic from the same flow will be impaired based on precedence value.

The traffic rate is configured as 2% in this test setup. If the traffic rate is different in your setup, then impairment statistics will vary.

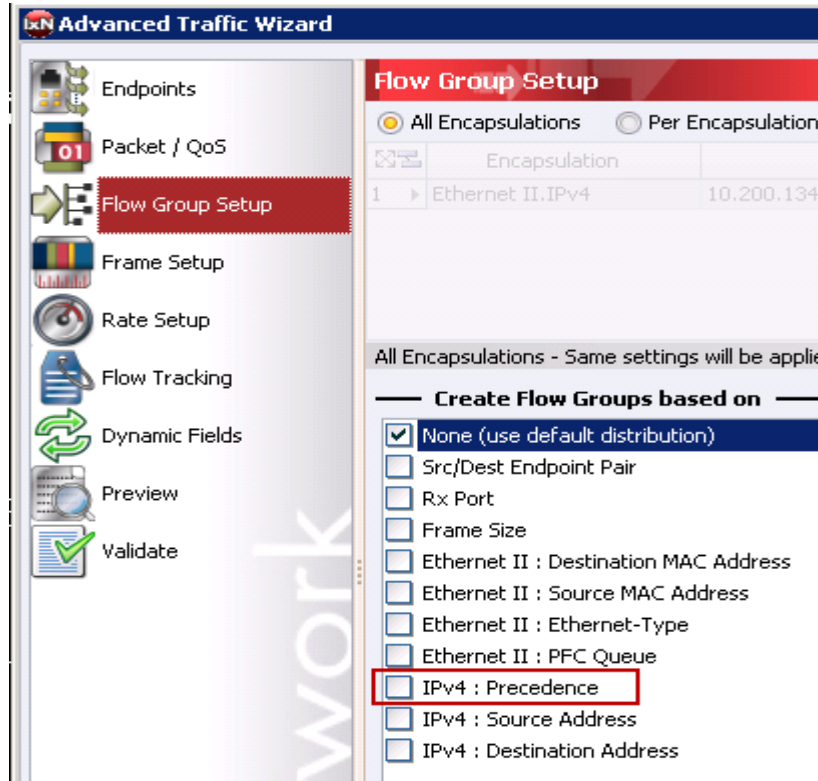


Figure 49. Impairment Port Selection

## TEST CASE: LAYER 3 QUALITY OF SERVICE

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

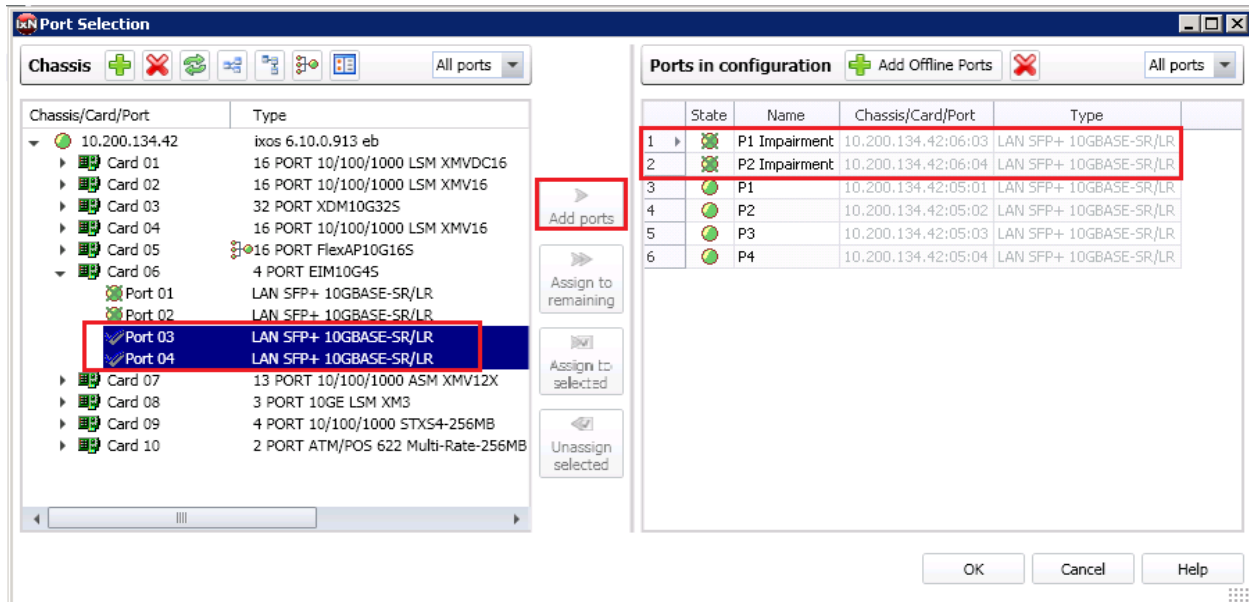


Figure 50. Impairment Port Selection

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

- 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 the desired flow group in **L2-3 Flow Groups** view and choose **Create Impairment Profile** from the menu.

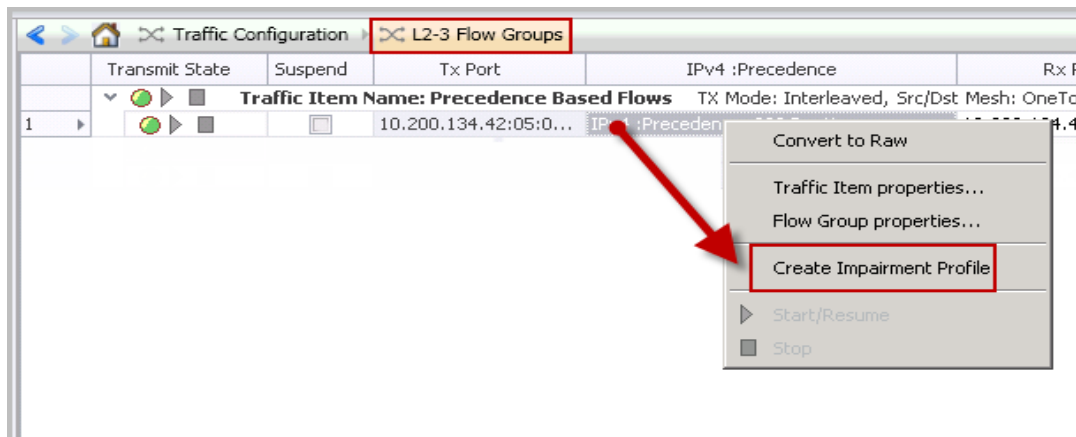


Figure 51. Impairment Profile Creation

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

## TEST CASE: LAYER 3 QUALITY OF SERVICE

- The Network Impairment view has three tabs: Diagram, Profiles and Links. The Diagram tab is chosen by default. Select the **Profiles** tab to see the list of all the impairment profiles. This view has multiple tabs at bottom for different impairments.

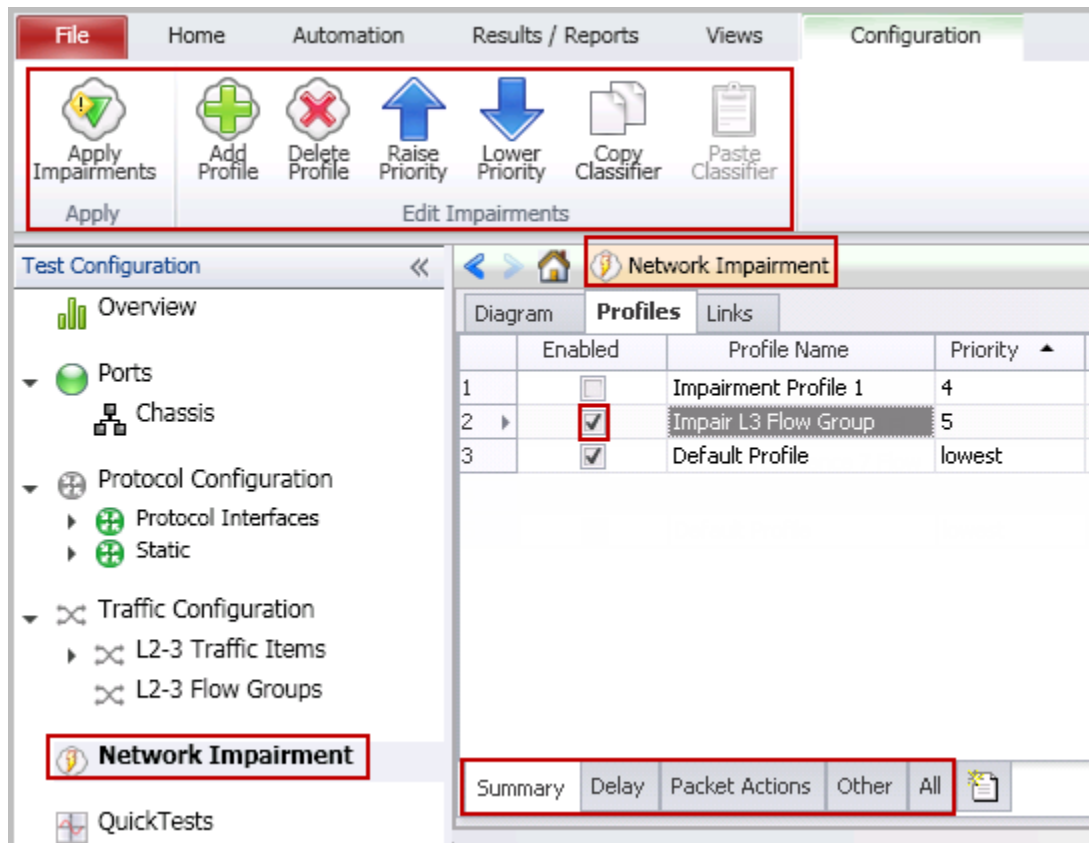


Figure 52. Network Impairment view

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

### Note:

- The Network Impairment 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.
- Click the **Classifier** grid in the Network Impairment -> Profiles tab. The **Packet Classifier** dialogue opens.

## TEST CASE: LAYER 3 QUALITY OF SERVICE

Classifier						
all packets						
Packet Classifier # Matchers Used: 0/8						
<div> <div>+</div> Add           <div>✗</div> Delete           <div>≡</div> Edit         </div>						
Enabled	Pattern Name	Offset	Value	Mask	Field Size (bits)	
<input type="checkbox"/>	Ethernet.Destination M...	0	00:00:00:1A:A6:7B	FF:FF:FF:FF:FF:FF	48	
<input type="checkbox"/>	Ethernet.Source MAC A...	6	00:00:00:1A:64:DA	FF:FF:FF:FF:FF:FF	48	
<input type="checkbox"/>	Ethernet.Ethernet-Type	12	08 00	FF FF	16	
<input type="checkbox"/>	IPv4.Protocol	23	3D	FF	8	
<input type="checkbox"/>	IPv4.Source Address	26	20.1.1.1	255.255.255.255	32	
<input type="checkbox"/>	IPv4.Destination Address	30	20.1.1.2	255.255.255.255	32	

Figure 53. Open Traffic classifiers

- 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 the unused classifier patterns.

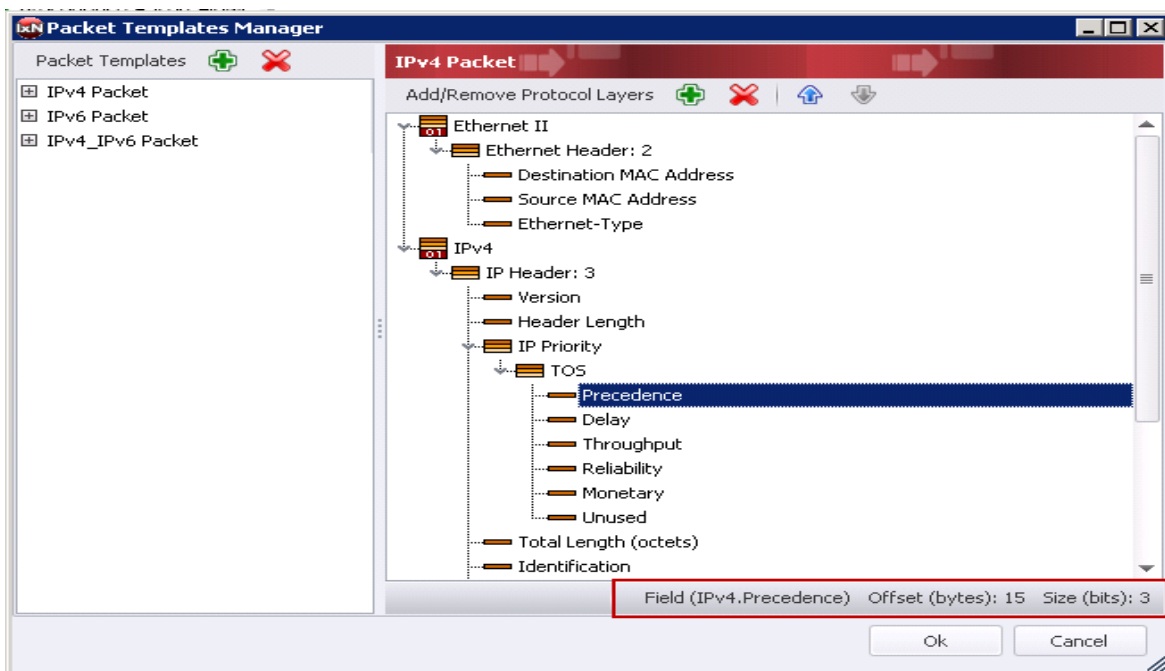


Figure 54. Packet Templates Manager

## TEST CASE: LAYER 3 QUALITY OF SERVICE

- 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.

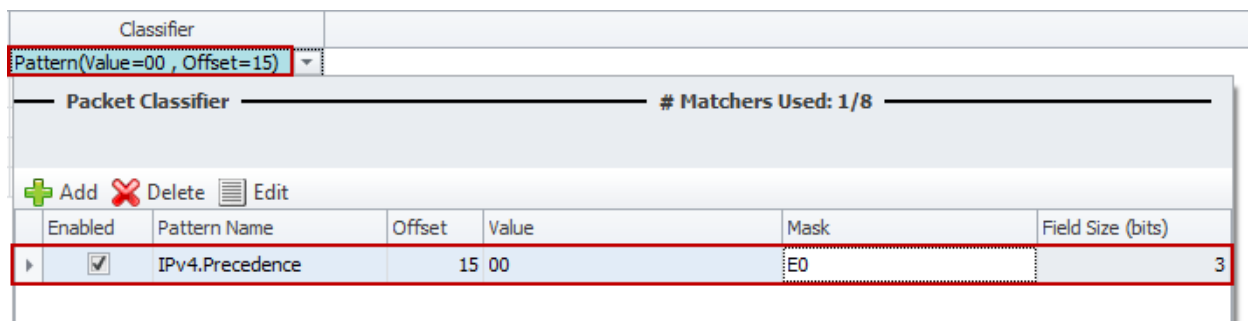


Figure 55. Configure Traffic classifiers

- Click **Add Profile** icon twice to create two profiles in Network Impairment Configuration ribbon. Optionally, name the profiles.
- 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.
- Edit the classifier to impair traffic for Precedence values 4 and 7. Only the value should be changed in the classifier.

Network Impairment								
Diagram		Profiles	Links					
	Enabled	Profile Name	Priority ▲	Rate Limit	Delay	Drop	Links	Classifier
1	<input checked="" type="checkbox"/>	Impair Precedence 0 Traffic	1	disabled	disabled	disabled	all links	Pattern(Value=00, Offset=15)
2	<input checked="" type="checkbox"/>	Impair Precedence 4 Traffic	2	disabled	disabled	disabled	all links	Pattern(Value=80, Offset=15)
3	<input checked="" type="checkbox"/>	Impair Precedence 7 Traffic	3	disabled	disabled	disabled	all links	Pattern(Value=E0, Offset=15)
4	<input checked="" type="checkbox"/>	Impairment Profile 4	4	disabled	disabled	disabled	all links	all packets
5	<input checked="" type="checkbox"/>	Default Profile	lowest	disabled	disabled	disabled	all links	all packets

Figure 56. Copying Traffic Classifiers across impairment profiles

- 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.

## TEST CASE: LAYER 3 QUALITY OF SERVICE

Select the link so that the traffic flowing through the DUT is impaired. Configure the links for the other two profiles.

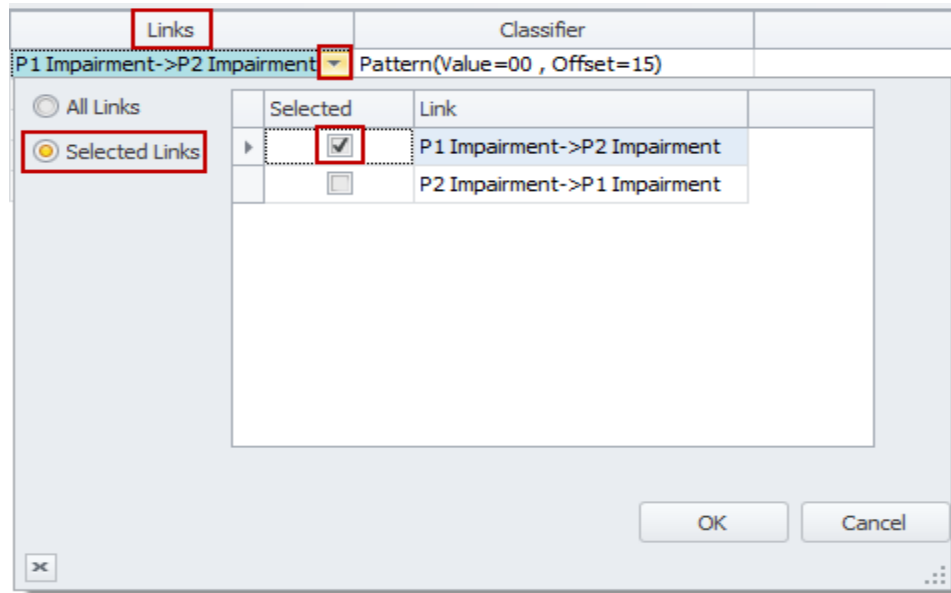


Figure 57. Network Impairment Link Selection

- 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.

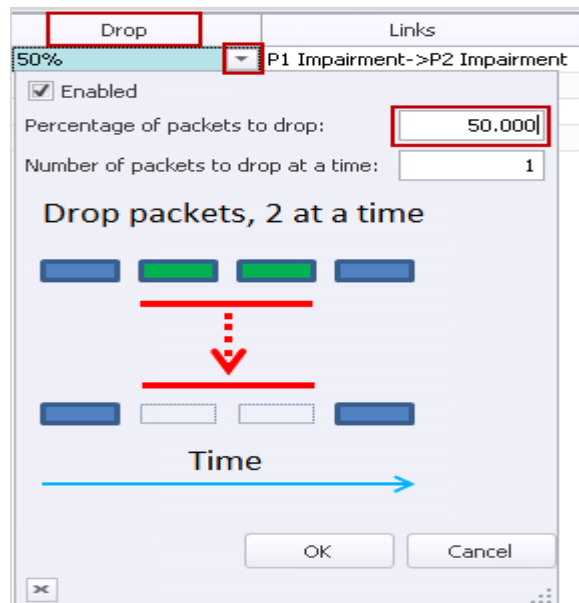


Figure 58. Drop Impairment Configuration

- To configure delay and jitter impairments, Change the bottom tab to Delay, to configure delay and jitter impairments, in Network Impairment -> Profiles tab. Select the

## TEST CASE: LAYER 3 QUALITY OF SERVICE

impairment profile and right click the **Delay** grid. Select the **Enabled** checkbox and enter the delay as *300 microseconds*. Configure delay for the second and third profiles.

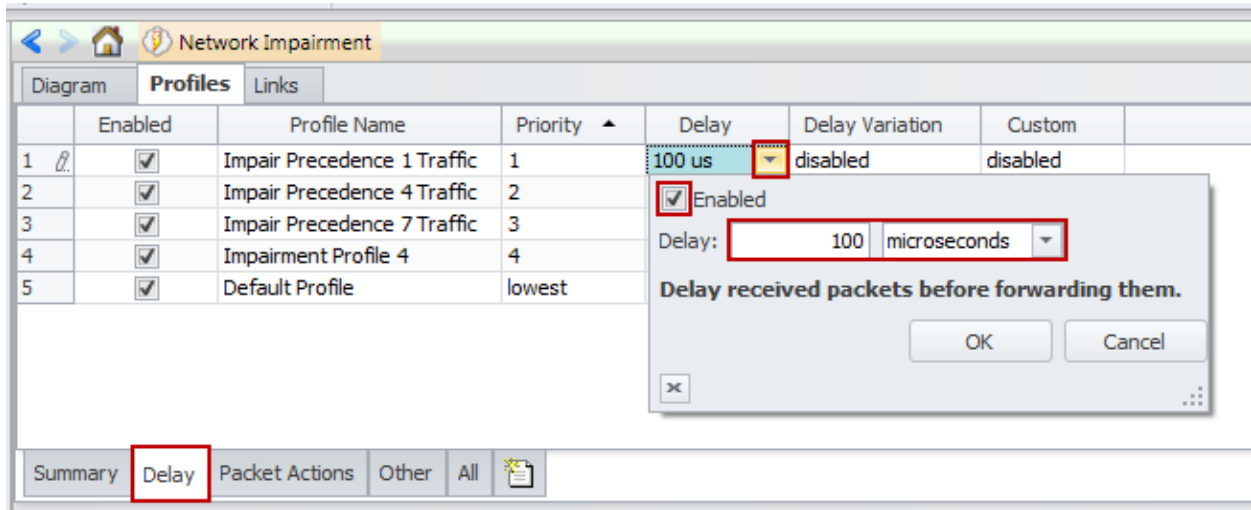


Figure 59. Delay Impairment Configuration

14. Select the impairment profile and right 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 Figure 60. Configure delay variation for the second and third profiles.

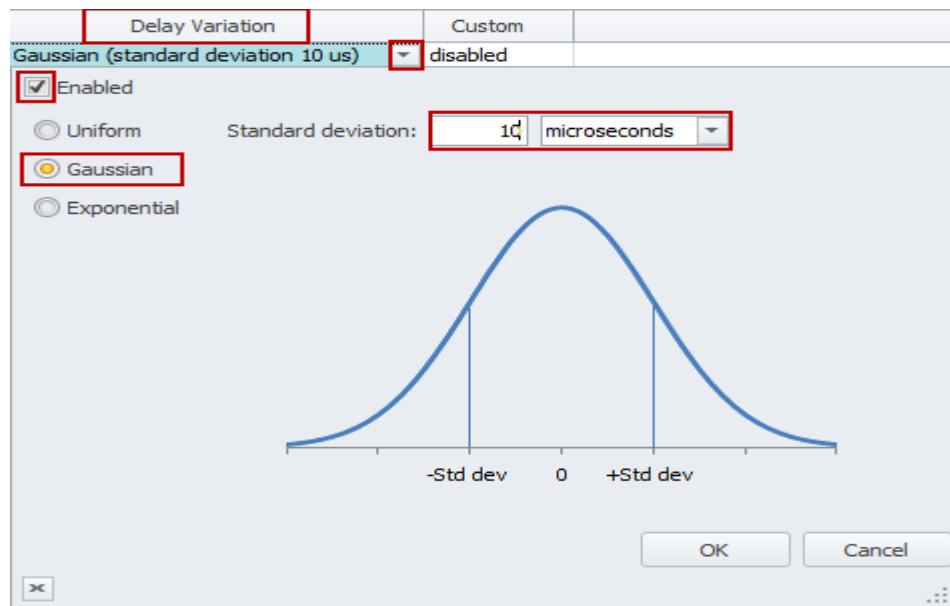


Figure 60. Jitter Impairment Configuration

15. To apply the impairment profile in the hardware, click on Apply Impairment icon in the configuration ribbon as shown in Figure 61. Only the enabled profiles are applied to the hardware. If applying impairment profile changes is successful, then the exclamation mark on the Apply Impairment icon will disappear.

## TEST CASE: LAYER 3 QUALITY OF SERVICE



Figure 61. Apply Impairment Icon Change

**Note:** If the impairment profile contains configuration errors, then the exclamation mark will not disappear and an error notification pop-up will appear on the right hand side bottom corner of the IxNetwork GUI. For further troubleshooting, follow the instructions in the Troubleshooting Tips section.

16. After applying impairments, the impairment statistics also starts getting updated. Select Impairment Profiles and click on the Dropped tab at the bottom in the impairment statistics view as shown in Figure 62.

Impairment Statistics					
Port CPU Statistics					
Impairment Link Statistics					
Impairment Profile Statistics					
Stat Name	Dropped Frames	Dropped Frame Rate	Dropped Bytes	Dropped Bit Rate	
1 Default Profile	0	0	0	0	
2 Impair Precedence 0 Traffic	23,201,513	49,604	1,484,896,832	25,397,248	
3 Impair Precedence 4 Traffic	23,201,513	49,604	1,484,896,832	25,397,248	
4 Impair Precedence 7 Traffic	23,201,513	49,605	1,484,896,832	25,397,760	
5 Impairment Profile 4	0	0	0	0	

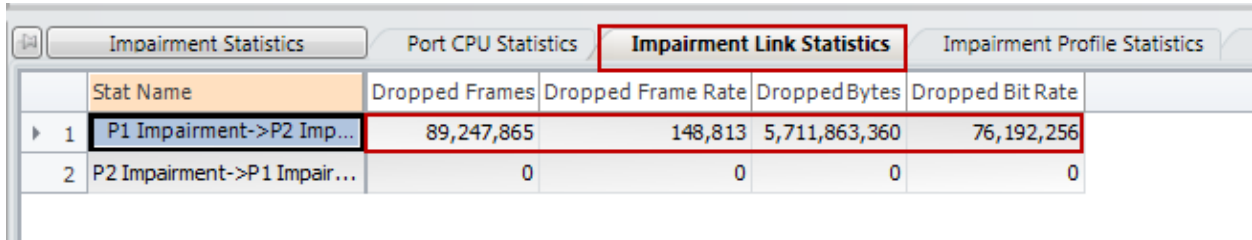
Figure 62. Drop Impairment Profile Statistics

Only the profiles with drop impairment enabled will drop the packets as seen in Figure 622. Check that the packets are dropped as per the configured rate.



## TEST CASE: LAYER 3 QUALITY OF SERVICE

17. To check the dropped packet statistics for each link direction, select Impairment Link Statistics tab in the Impairment Statistics view and select Dropped tab at the bottom as shown in Figure 63. Note that the link drop statistics are aggregate of the profile drop statistics.

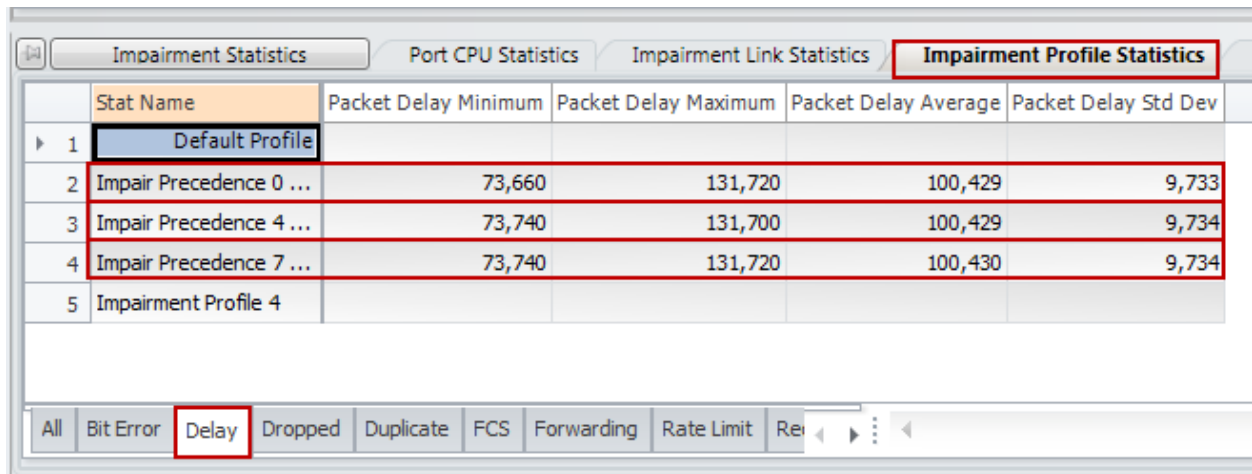


Impairment Statistics					
Port CPU Statistics		Impairment Link Statistics		Impairment Profile Statistics	
Stat Name	Dropped Frames	Dropped Frame Rate	Dropped Bytes	Dropped Bit Rate	
1 P1 Impairment->P2 Imp...	89,247,865	148,813	5,711,863,360	76,192,256	
2 P2 Impairment->P1 Impair...	0	0	0	0	

Figure 63. Drop Impairment Link Statistics

18. 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.



Impairment Statistics					
Port CPU Statistics		Impairment Link Statistics		Impairment Profile Statistics	
Stat Name	Packet Delay Minimum	Packet Delay Maximum	Packet Delay Average	Packet Delay Std Dev	
1 Default Profile					
2 Impair Precedence 0 ...	73,660	131,720	100,429	9,733	
3 Impair Precedence 4 ...	73,740	131,700	100,429	9,734	
4 Impair Precedence 7 ...	73,740	131,720	100,430	9,734	
5 Impairment Profile 4					

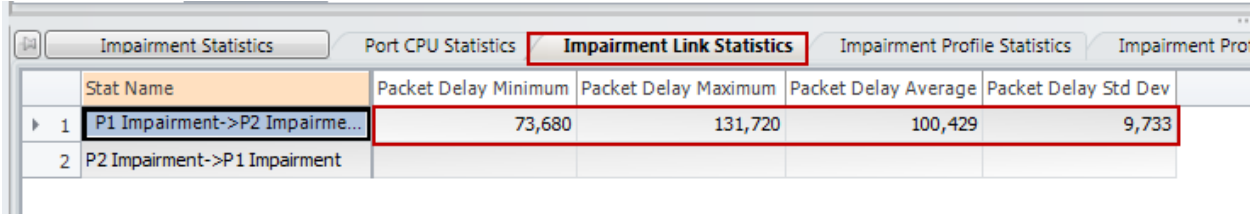
All Bit Error Delay Dropped Duplicate FCS Forwarding Rate Limit Rel

Figure 64. Delay Impairment Profile Statistics

## TEST CASE: LAYER 3 QUALITY OF SERVICE

19. Select Impairment Link Statistics tab, and select 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.



The screenshot shows a software interface with several tabs: 'Impairment Statistics', 'Port CPU Statistics', 'Impairment Link Statistics' (which is selected and highlighted with a red box), 'Impairment Profile Statistics', and 'Impairment Profile'. Below the tabs is a table with the following data:

Stat Name	Packet Delay Minimum	Packet Delay Maximum	Packet Delay Average	Packet Delay Std Dev
1 P1 Impairment->P2 Impairme...	73,680	131,720	100,429	9,733
2 P2 Impairment->P1 Impairment				

Figure 65. Delay Impairment Link Statistics

### Test Variables

Each of the following variables may be used 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 Network Impairment 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	You can create up to 32 bidirectional or 64 unidirectional impairment profiles per impairment port pair.
Use multiple classifiers	You can introduce multiple classifiers in a single impairment profile. Classifiers can also be copied and pasted across impairment profiles by using <b>Copy Classifier</b> and <b>Paste Classifier</b> commands in the <b>Network Impairment Configuration</b> tab. A maximum of 16 classifiers can be added for each link direction.
Apply impairments in both link directions	You can select to impair either one or both the links. See Figure 68.
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 impairment. Reorder and duplicate impairments are present in the <b>Packet Actions</b> tab.
Increase Delay	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	Introduce delay in us, ms or km. 1 km of WAN Link cause a delay of 5 us.
Apply different delay variations	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. The drop and delay measurements can be used to verify the statistics report generated by DUT.

## Troubleshooting Tips

Issue	Troubleshooting Solution
Impairment profiles are enabled but impairment statistics are not updated.	Check that the <b>Apply Impairments</b> icon does not have any error mark. Check that the traffic is flowing and the drop rate is not configured to <i>100%</i> for all the profiles.
No traffic is flowing through the impairment links.	Disable all the impairment profiles except default profile. Make sure that the default profile is not set to <i>100%</i> 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 <b>Links</b> tab, clear the checkbox for <b>Interrupt Forwarding</b> .
An error window pops up in the right hand side bottom when Apply Impairments is clicked.	Check for impairment profile configuration error. Ensure that the impairments are applied within the configuration limits. Check ImpairNet module specifications for the configuration limits.
Traffic is not getting impaired though the Apply Impairment icon is not showing any exclamation mark.	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 <b>Enabled</b> checkbox is selected for the configured impairments.

## Conclusions

The test verifies that the ImpairNet is used as an effective and accurate impairment tool. The focus of this test was to impair traffic based on a particular packet field (precedence). Impairments can be generated for other fields to test the DUT's capability to generate accurate statistics report.

## Test Case: Automating Layer 3 Quality of Service

### Overview

The goal of this section is to show how to automate the above **Layer 3 Quality of Service** Test Case using IxNetwork Test Composer. Test Composer is part of the IxNetwork GUI Application.

This automation sequence will help the user understand how to:

1. **Combine protocol configuration, traffic configuration, and automation sequence into one unified file.**

This is accomplished through using the built-in Test Composer module to add automation to the L3 QoS configuration outlined in this test case. The benefit of using the IxNetwork Test Composer is that there is one IxNetwork file to be shared between teammates.

2. **Reduce the setup and execution time for the DUT configuration.**

This is accomplished through automatic capture of commands as they are entered into the CLI and automated playback on successive runs. The benefit of using the Capture/Replay module in Composer is the ability to create a DUT playback sequence without having the overhead of having to write a scripting language to send and expect the commands.

3. **Configure the tester for traffic generation and control the duration of traffic.**

This is accomplished by selecting Traffic events from the drop-down of command choices built-in to Composer. The benefit of using the built-in command wizard is that you can select the automation events you want from a GUI which shows you all of the events that are available.

4. **Reduce the setup and execution of repeated traffic rate iterations.**

This is accomplished by using a Composer variable to store the list of traffic rate iterations to be applied to a For-loop iterator. The benefit of using variables in an automation script is that you can make changes to the inputs in one place and it will change the execution of the entire sequence.

5. **Collect traffic generator statistics per traffic rate iteration.**

This is accomplished by using the StatQuery command to select statistics, in conjunction with the CSV Analyzer session to write them to a file. The benefit of using the StatQuery command is that you can select a subset of statistics from the GUI list of available statistics directly from the application.

6. **Generate a single summary report using collected statistics in each iteration.**

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

This is accomplished by using the Reporter session in Composer to read in the iteration CSVs and output them to HTML. The benefit of using the Reporter session is that you can customize the collection of statistics to meet the needs and format of your organization.

### **7. Specify pass/fail criteria to declare the overall success or failure of a test case execution.**


This is accomplished by using the basic If expression builder to create a condition that checks for excessive frame loss. The benefit of having a clear pass/fail condition evaluated by the automation is that this yields a repeatable test case whose results can be quickly and easily compared against previous golden results.

In order to develop an end-to-end automation solution, the following sequence will help to organize the automation script into the key components needed to create a repeatable and portable test solution.

The complete automation script is obtained by opening the example IxNetwork Configuration for this methodology and clicking on the Test Composer icon to open the example script.

## Sequence

1. Open the IxNetwork GUI. Load the example configuration file:  
**QoS-L3\_v6.00\_with\_TC.ixncfg.**  
This file can be found on the Black Book Web site.  
Go to <http://www.ixiacom.com/blackbook>.  
Find the 'Quality of Service Validation' Black Book and download the Templates.
2. Click **Test Composer** icon to open Test Composer which has the automation sequence.





















	Command Type	Session	Return Variable	Command String
1	 <b>Comment</b>			Configure the DUT for QoS Marking
2	 <b>StartSession</b>	DUT		Telnet,10.200.134.63,23
3	 <b>Execute</b>	DUT		****
4	 <b>Execute</b>	DUT		enable
5	 <b>Execute</b>	DUT		****
6	 <b>Execute</b>	DUT		configure t
7	 <b>Execute</b>	DUT		class-map match-all tos0
8	 <b>Execute</b>	DUT		match ip precedence 0
9	 <b>Execute</b>	DUT		exit
10	 <b>Execute</b>	DUT		class-map match-all tos4
11	 <b>Execute</b>	DUT		match ip precedence 4
12	 <b>Execute</b>	DUT		exit
13	 <b>Execute</b>	DUT		class-map match-all tos7
14	 <b>Execute</b>	DUT		match ip precedence 7
15	 <b>Execute</b>	DUT		exit
16	 <b>Execute</b>	DUT		policy-map BB-TOS
17	 <b>Execute</b>	DUT		class tos7
18	 <b>Execute</b>	DUT		bandwidth percent 60

Figure 66. Automation Sequence Opened in Test Composer

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

3. Use the Console in Test Composer to Telnet to the DUT CLI. From the Console, enter commands directly to the DUT and they automatically captured as steps in your automation script.

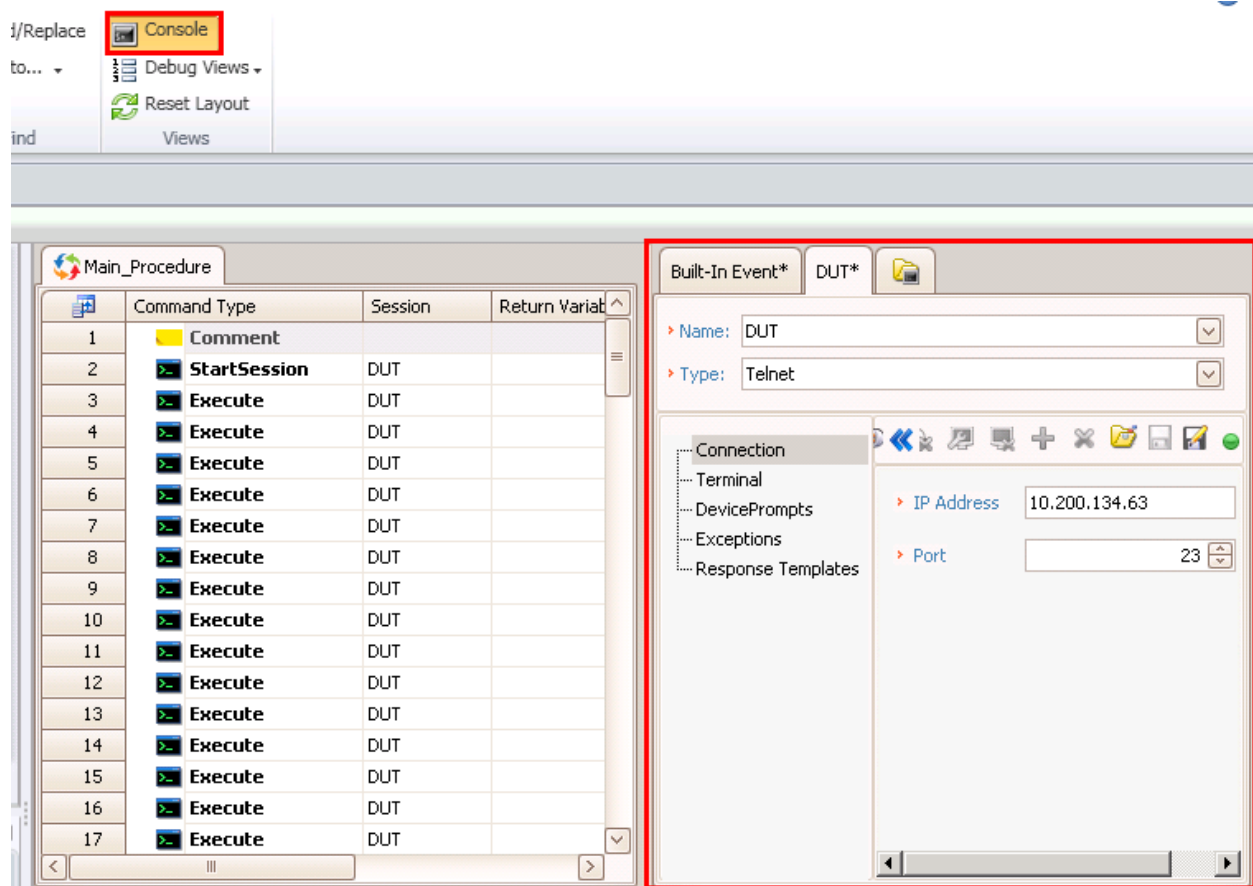


Figure 67. Configuring a Telnet session in Session Manager

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

- Composer is not only used to capture commands issued to a DUT once, but also to replay those commands automatically as part of the end-to-end automated test run by selected the steps you wish to replay in Edit Mode.

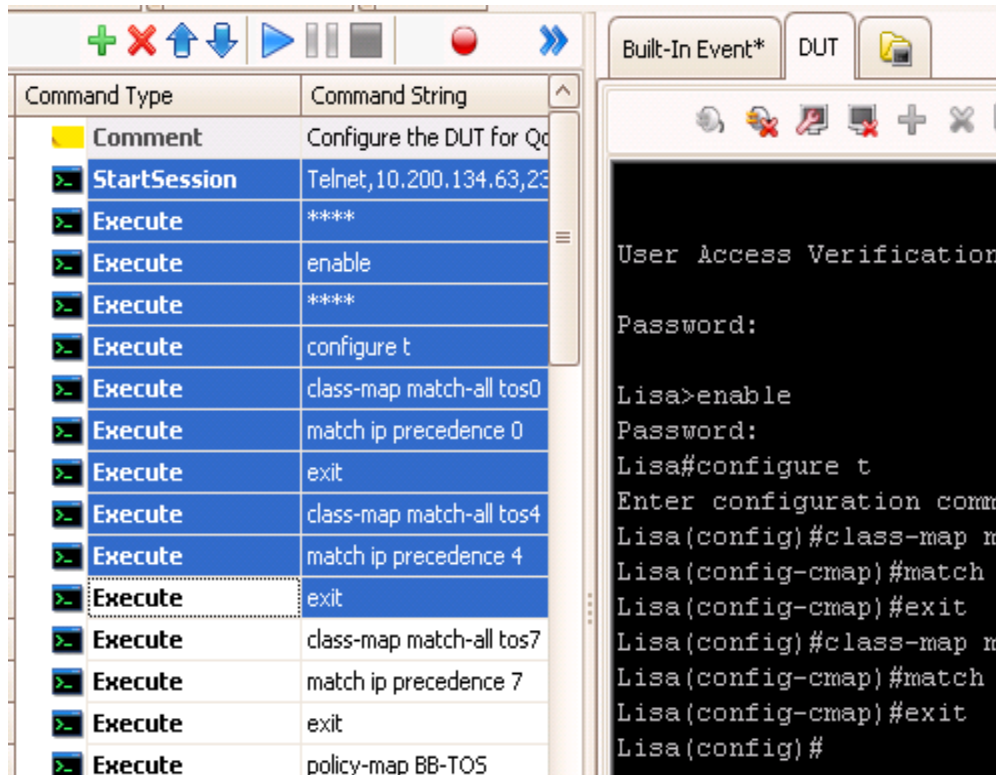


Figure 68. Replaying DUT CLI commands in Edit Mode

For more details on DUT CLI Automation using Test Composer, please refer to the **Getting Started Guide** section of the Automation Blackbook entitled “**Test Automation For IP Systems**”.



## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

- Configure the DUT so that it marks inbound packets with TOS value 4 to have an outbound TOS value 5. In addition, apply match criteria and bandwidth criteria to the QoS policy and bind it to the outbound interface.




















1		Comment	Configure the DUT for QoS Marking
2		StartSession	Telnet,10.200.134.63,23
3		Execute	****
4		Execute	enable
5		Execute	****
6		Execute	configure t
7		Execute	class-map match-all tos0
8		Execute	match ip precedence 0
9		Execute	exit
10		Execute	class-map match-all tos4
11		Execute	match ip precedence 4
12		Execute	exit
13		Execute	class-map match-all tos7
14		Execute	match ip precedence 7
15		Execute	exit
16		Execute	policy-map BB-TOS
17		Execute	class tos7
18		Execute	bandwidth percent 60
19		Execute	exit

Figure 69. DUT CLI commands captured via Telnet in Session Manager

- Insert **Execute Steps** for traffic generation. Insert **Traffic Apply** to configure the chassis' ports. Insert **Traffic Set Rate** to set the mode and frequency of the frames.
- Insert **Traffic Start** and **Traffic Stop** to control the tester. Insert a **Sleep** command to pause the automation sequence for the duration of time while the chassis is transmitting frames.











42		Execute	duplex full
43		Execute	no negotiation auto
44		Execute	service-policy output BB-TOS
45		Execute	exit
46		Execute	exit
47		StopSession	
48		Execute	Traffic Apply L2-L3 Traffic
49		Execute	Traffic Start All L2-L3 Traffic
50		Sleep	00:00:10.000
51		Execute	Traffic Stop All L2-L3 Traffic

Figure 70. Configuration and Transmission of IxNetwork Traffic

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

8. Place the traffic events inside a **For** loop control flow statement and use it to select from a set of line rate values that can be stored in a variable called **LineRate** and passed as an argument to **Traffic Set Rate**. This will allow to iterate over multiple scenarios.

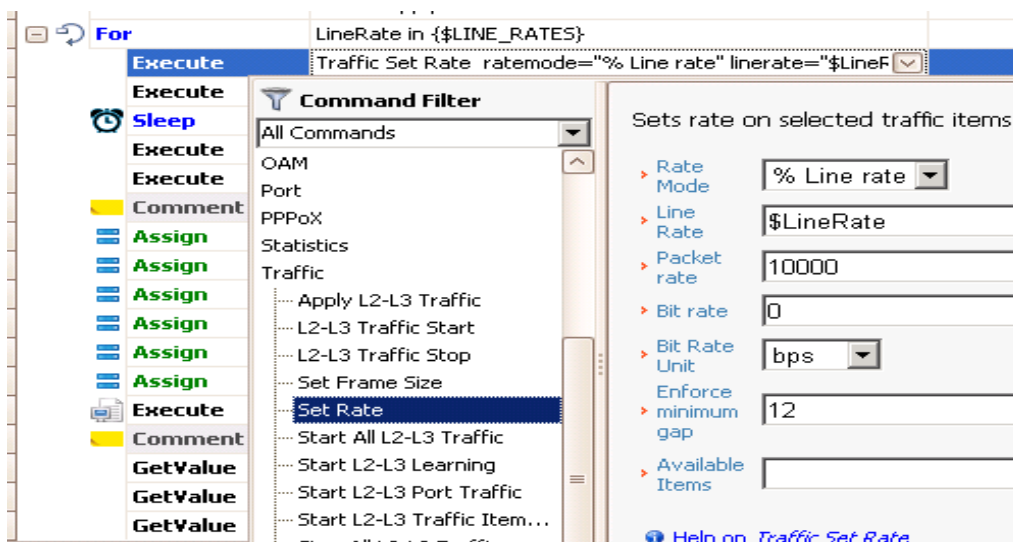


Figure 71. Traffic Set Rate command wizard

9. The dynamic nature of the IxNetwork traffic generation engine allows rates to be changed many times after traffic has been applied once to the port. Additional line rates can be added to the list of rates to scale the testing quickly.

43	Execute	no negotiation auto
44	Execute	service-policy output BB-TOS
45	Execute	exit
46	Execute	exit
47	StopSession	
48	StartSession	CSVAnalyzer, startSession csvFileName="\$CSV1" csvTemplateName
49	StartSession	CSVAnalyzer, startSession csvFileName="\$CSV2" csvTemplateName
50	StartSession	CSVAnalyzer, startSession csvFileName="\$CSV3" csvTemplateName
51	Execute	Traffic Apply L2-L3 Traffic
52	For	LineRate in {\$LINE_RATES}
53	Execute	Traffic Set Rate
54	Execute	Traffic Start All L2-L3 Traffic
55	Sleep	00:00:10.000
56	Execute	Traffic Stop All L2-L3 Traffic
57	Execute	Statistics StatQuery
58	Comment	TOS Precedence statistics
59	Assign	[Index \${StatsTable_1.IPv4_:Precedence} 0]
60	Assign	[Index \${StatsTable_1.IPv4_:Precedence} 2]
61	Assign	[Index \${StatsTable_1.IPv4_:Precedence} 4]

Figure 72. Traffic Generator sequence changing line rate values in a loop

10. For more details on Ixia Traffic Generator Automation using Test Composer, please refer to the Getting Started Guide section of the Automation Blackbook entitled *Test Automation for IP Systems*.

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

A **Statistics StatQuery** command is used to select the traffic statistics from various detail views generated by IxNetwork.

11. Select the **Traffic->Flow Filtering** category.
12. In the **Edit filter**, make sure that **Traffic Item** is **1** and **Rx Port** is any of **All**.
13. In **Sorting Hierarchy**, select **All** to get both **Ingress Tracking** and **Egress Tracking** statistics.

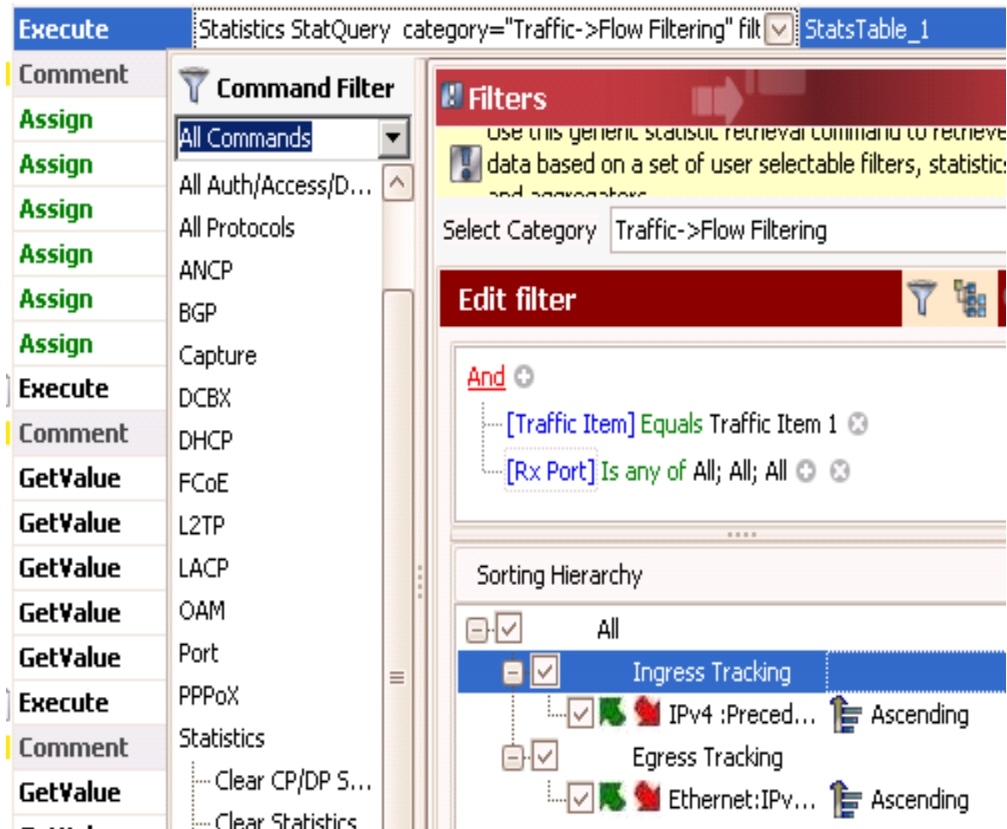


Figure 73. Using Statistics StatQuery to filter Traffic Ingress/Egress

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

14. In **Select Statistics**, select the *Loss %* statistic under the Traffic Statistics **Source Type**.  
When **Statistics StatQuery** is executed, the value of Loss % is automatically returned in a **Return Variable** called StatsTable\_1.

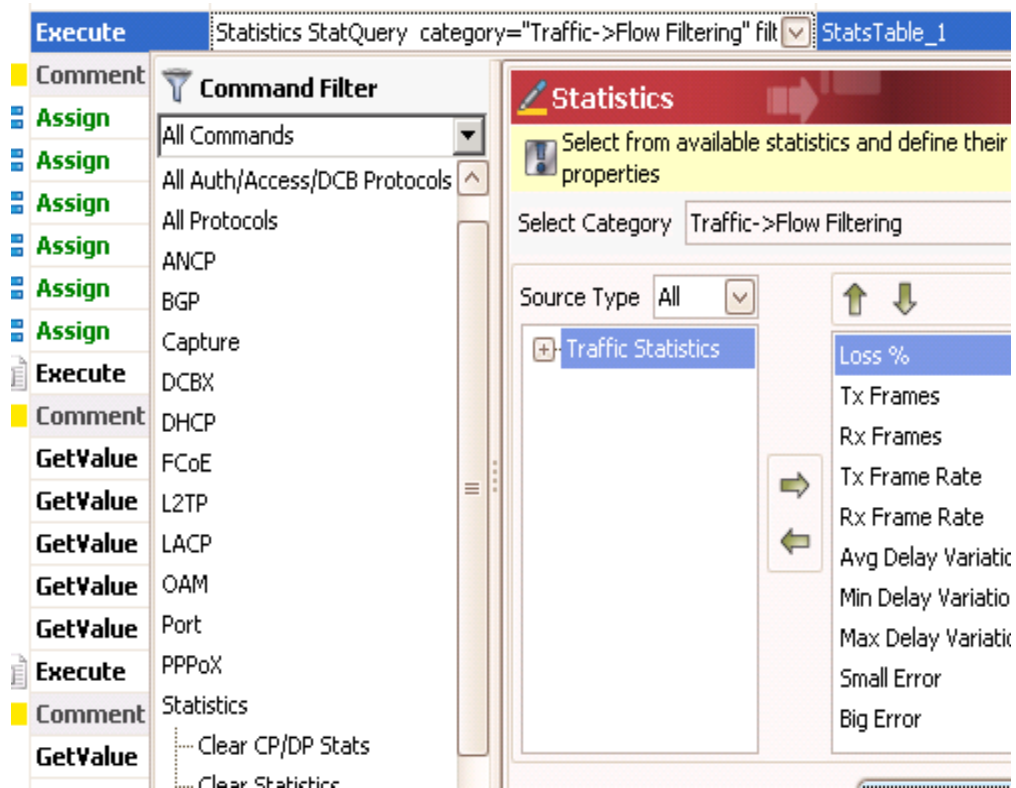


Figure 74. Selecting Loss % statistic to be included in a Return Variable

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

The **GetValue** command is used to determine aggregate values across flows, and ports. such as Min, Max, and Average. This is used for determining the worst frame loss or longest latency for all traffic as an aggregate value in output CSV files.

In addition to the provided CSV reports in IxNetwork, the Session Manager includes a **CSVAnalyzer** session which can be used, for example, to read in automation input from a CSV file.

The **CSVAnalyzer** is also used to output Ixia Traffic Generator and DUT statistics to a CSV file using the **WriteBlock** command.










61		<b>Assign</b>	[Index \${StatsTable_1.IPv4_:Precedence} 4]
62		<b>Assign</b>	[Index \${StatsTable_1.Ethernet:IPv4_TOS_Precedence_(3_bits)_at_
63		<b>Assign</b>	[Index \${StatsTable_1.Ethernet:IPv4_TOS_Precedence_(3_bits)_at_
64		<b>Assign</b>	[Index \${StatsTable_1.Ethernet:IPv4_TOS_Precedence_(3_bits)_at_
65		<b>Execute</b>	WriteBlock
66		<b>Comment</b>	Traffic behavior statistics
67		<b>GetValue</b>	Max StatsTable_1 Min_Delay_Variation_ns
68		<b>GetValue</b>	Max StatsTable_1 Tx_Frames
69		<b>GetValue</b>	Max StatsTable_1 Rx_Frames
70		<b>GetValue</b>	Min StatsTable_1 Tx_Frame_Rate
71		<b>GetValue</b>	Min StatsTable_1 Rx_Frame_Rate
72		<b>Execute</b>	WriteBlock
73		<b>Comment</b>	Statistics highlighting the pass/fail result based on call flow execution
74		<b>GetValue</b>	Avg StatsTable_1 Avg_Delay_Variation_ns
75		<b>GetValue</b>	Min StatsTable_1 Min_Delay_Variation_ns
76		<b>GetValue</b>	Max StatsTable_1 Max_Delay_Variation_ns
77		<b>GetValue</b>	Max StatsTable_1 Small_Error
78		<b>GetValue</b>	Max StatsTable_1 Big_Error
79		<b>Execute</b>	WriteBlock

Figure 75. Generating custom QoS CSV statistics reports using CSVAnalyzer

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

15. Use a **Basic If** Expression Builder to compare egress TOS variables against expected numerical values. Insert new rows and use the drop-downs in each column to select the variables and aggregation to be used in your expression.

Each row can be grouped into an AND expression where all sub-expressions must be true for the entire expression to be true.

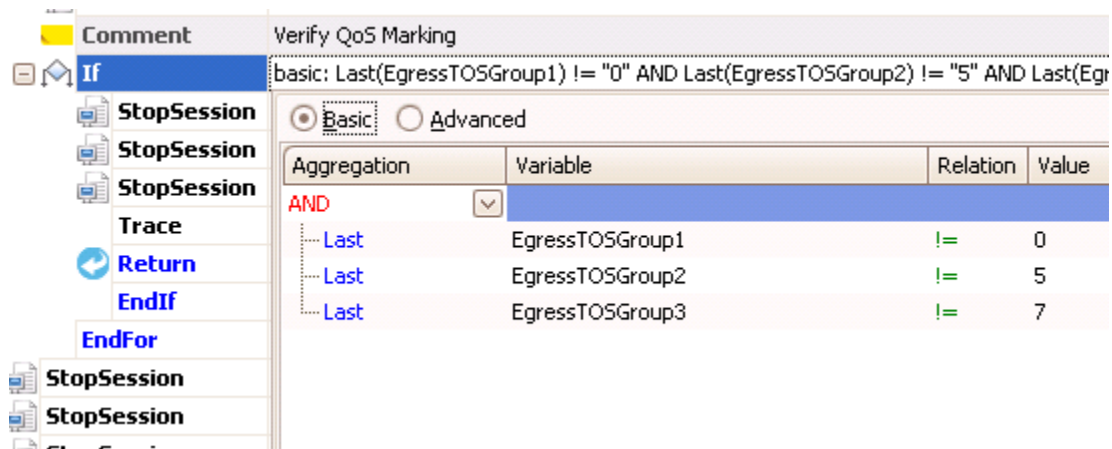


Figure 76. Basic If expression builder TOS values compared to expected values

16. Use an **Advanced If** conditional statement to compare the inbound TOS values to the output TOS values to see if the DUT has marked the outbound packets with the correct values for each of the different line rate conditions.
17. Select the variables to be compared from the **Test Variables** list.

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

19. Use the **Available** operators to compare two variables and also to combine simple expression pairs together into one advanced conditional statement that must evaluate to true in order to yield a passed result.

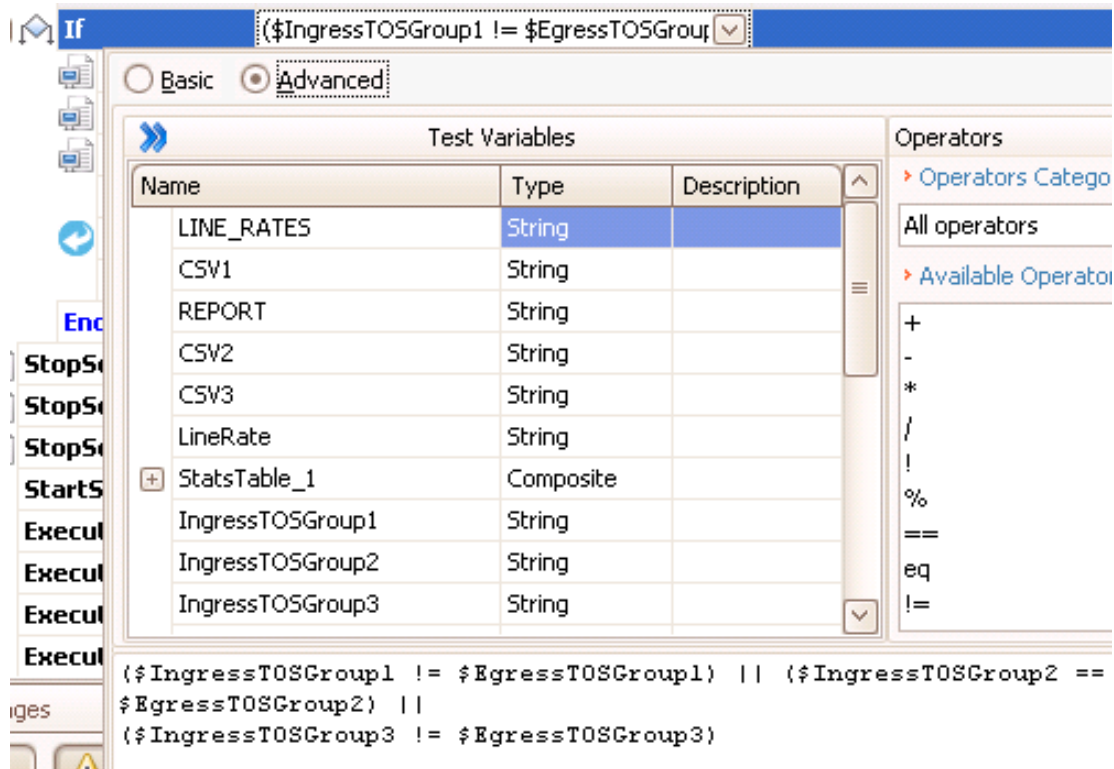


Figure 77. Advanced If Expression Comparing Ingress and Egress variables

## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

Failing this If condition represents failing the Pass/Fail criteria evaluation for the automation script.

On failure, a 0 will be returned when this script is exported into and executed in the Test Conductor unattended automation harness. On success, a 1 will be returned.













73		<b>Comment</b>	Statistics highlighting the pass/fail result based on call flow e
74		<b>GetValue</b>	Avg StatsTable_1 Avg_Delay_Variation_ns
75		<b>GetValue</b>	Min StatsTable_1 Min_Delay_Variation_ns
76		<b>GetValue</b>	Max StatsTable_1 Max_Delay_Variation_ns
77		<b>GetValue</b>	Max StatsTable_1 Small_Error
78		<b>GetValue</b>	Max StatsTable_1 Big_Error
79		<b>Execute</b>	WriteBlock
80		<b>Comment</b>	Verify QoS Marking
81		<b>If</b>	(\$IngressTOSGroup1 != \$EgressTOSGroup1)    (\$IngressTC
82		<b>StopSession</b>	
83		<b>StopSession</b>	
84		<b>StopSession</b>	
 85		<b>Trace</b>	Failed
86		<b>Return</b>	0
87		<b>EndIf</b>	
88		<b>EndFor</b>	
89		<b>StopSession</b>	
90		<b>StopSession</b>	
91		<b>StopSession</b>	

Figure 78. Verifying QoS traffic re-marked using If condition

The Reporter session type generates a custom report in HTML format that contains the aggregated result from our QoS test.



## TEST CASE: AUTOMATING LAYER 3 QUALITY OF SERVICE

20. Use the **AddTableToReport** command to select a CSV file to be read in and formatted for inclusion in the report.












81		<b>If</b>	(\$IngressTOSGroup1 != \$EgressTOSGroup1)    (\$IngressTOS
82		<b>StopSession</b>	
83		<b>StopSession</b>	
84		<b>StopSession</b>	
 85		<b>Trace</b>	Failed
86		<b>Return</b>	0
87		<b>EndIf</b>	
88		<b>EndFor</b>	
89		<b>StopSession</b>	
90		<b>StopSession</b>	
91		<b>StopSession</b>	
92		<b>StartSession</b>	Reporter, Session Start
93		<b>Execute</b>	AddTableToReport
94		<b>Execute</b>	AddTableToReport
95		<b>Execute</b>	AddTableToReport
96		<b>Execute</b>	GenerateReport
97		<b>StopSession</b>	
 98		<b>Trace</b>	Passed
99		<b>Return</b>	1

Figure 79. Generating a custom HTML summary report using a Reporter session

## Contact Ixia

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

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

EMEA  
Ixia 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](mailto:salesemea@ixiacom.com)

Renewals: [renewals-emea@ixiacom.com](mailto:renewals-emea@ixiacom.com)  
Support: [support-emea@ixiacom.com](mailto: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](mailto:Support-Field-Asia-Pacific@ixiacom.com)

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