Xgig Load Tester

Version 8.1

User's Guide

Xgig Load Tester

Version 8.1

User's Guide

Viavi Solutions
1-844-GO-VIAVI
www.viavisolutions.com

Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and Viavi reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright/Trademarks

Copyright release

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to Viavi’s standard terms and conditions, available at www.viavisolutions.com/en/terms-and-conditions.

Contents

About this Guide

Congratulations on your purchase of this Xgig Maestro software which, depending on the licenses you obtain, includes Xgig BERT, Xgig Jammer, Xgig Generator, Xgig Target Emulator, Delay Emulator, and Xgig Load Tester.

Who Should Read this Guide

This guide is intended for networking professionals in research and development who need to monitor and test network performance. It is assumed that users of this guide have an engineering background.

What this Guide Contains

This user guide contains the following chapters:

Chapter 1, “Introducing Xgig Load Tester" describes the Load Tester features and capabilities.

Chapter 2, “Using the Load Tester Tab" describes function tab interface and provides procedures to use it.

Chapter 3, “Configuring Ports" provides procedures in configuring ports for use in Load Tester.

Chapter 4, “Creating Tags" provides procedures in creating tags.

Chapter 5, “Creating and Managing Traffic Patterns" describes procedures in using the Traffic Pattern Editor tab to manage traffic patterns used by Load Tester.

Chapter 6, “Editing Triggers" provides procedures in editing triggers.

Chapter 7, “Managing Multiple Link Services" describes the Link Service tab and the different link service options you can set for the ports locked to Load Tester.

Chapter 8, “Configuring Test Summary Reports" describes procedures in using the creating test summary reports in Load Tester.

Appendix A, “Getting Started with Xgig Load Tester" contains instructions to help you get started in Xgig Load Tester.

Appendix B, “Simplifying Detection and Resolution of Missing Frames" describes how to simplify the detection and resolution of missing frames.

Appendix C, “Load Tester Login State Machine Troubleshooting" describes how to simplify the detection and resolution of missing frames.

Conventions

The following conventions are used in this guide.

Message Formats

This guide uses the following format to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Caution: This format is used to highlight information that will help you prevent equipment failure or loss of data.

Typographical Conventions

This guide uses the following typographical conventions:

bold sans serif	Commands and software button, for example, the **Apply** button
italics	Directory names, book titles, named hard keys, for example, the *Enter* key
courier font	Screen text, user-typed command-line entries

Technical Assistance

If you require technical assistance, call 1-844-GO-VIAVI (1-844-468-4284) or email Techsupport-snt@viavisolutions.com.

For the latest TAC information, go to http://www.viavisolutions.com/en/services-and-support/support/technical-assistance.

Chapter 1

Introducing Xgig Load Tester

In this chapter:

- Xgig Load Tester Overview
- New Features
- Features
- Capabilities
- Components

Xgig Load Tester Overview

The Xgig Load Tester is a new generation product on the Xgig platform for the Fibre Channel (FC) protocol and Fibre Channel over Ethernet (FCoE) protocol. The Xgig Load Tester is a powerful data stream generator at full line rate and is used for data performance tests of FC and FCoE networking equipment and components. Load Tester supports FC line rates of 1G (1.0625 Gbps), 2G (2.1250 Gbps), 4G (4.2500 Gbps), 8G (8.5000 Gbps), 16G (14.0250 Gbps) and FCoE line rates of 10G (10.3125 Gbps).

Xgig Load Tester is compatible with Xgig 4G, 8G, 16G and 10G multi-functional blades. Xgig blades are available with two, four, or eight ports and are capable of triggering the Xgig Analyzer.

Using Load Tester in conjunction with other Xgig products like the Xgig Analyzer creates a complete test setup for your Fibre Channel configuration.

Note: The Xgig Load Tester only supports the Xgig chassis and Xgig blades. Depending on licensing, each port pair has the ability to support Load Tester functions as well as other Xgig functions with the same sync group.

New Features

The following new features have been released in this version of Xgig Load Tester.

- Xgig Load Tester provides 64-bit Dynamic and Static API libraries for the Load Tester Software Development Kit (SDK) library for use in 64-bit environments.
- Xgig Load Tester 32-bit client software is supported on both 32-bit and 64-bit versions of the Windows operating systems. Refer to the *Xgig Maestro Software Installation Guide* for the complete list of supported operating systems.
- Xgig Load Tester supports control from a computer (host) to either an Xgig 1000 chassis or an Xgig 5000 chassis (device) directly via a USB cable. Refer to the *Xgig Maestro Introduction Guide* for information.

Features

Xgig Load Tester has the following features:

Link Service

Link initialization (LR,OLS,NOS)

Login (Fabric, NPIV, N_Port)

FC and FCoE data traffic generation

- 1024 data streams per physical port with multi- S_ID, D_ID and OX_ID
- Continuous and burst traffic profile with fixed or variable payload size
- > 100% theoretical line rate (minimum Inter-Frame Gap of 3 IDLES, unidirectional traffic only)
- 4, 6, or 8 uniquely configurable traffic profiles per Physical N_Port. The number of profiles depends on the specific blade hardware. Refer to the *Traffic Profile Engines per Physical N_Port* table in “Traffic Profile Engines” on page 10.

  Each profile includes the following configurable parameters:

  - continuous and burst traffic profiles
  - fixed or variable payload sizes
  - user selectable payloads
- Tx streams per physical N-Port:
  - 4G FC provides 512 streams
  - 8G FC, 16G FC, and 10G FCoE provides 1024 streams
- VN to VN virtual link support for 10G FCoE
- Editable port configuration parameters in states other than Laser Off and Offline

- The Xgig1000 4 Port and 8 Port 10G/16G systems support the Load Tester function at 10.3125 Gbps in the 10 Gigabit Ethernet protocol in Analog Passthrough or Digital Retime. These systems also support the Load Tester function at 4G, 8G, or 16G (4.2500, 8.5000, or 14.0250 Gbps) in the Fibre Channel protocol in Analog Passthrough or Digital Retime.
- Connectivity status bar that monitors the Load Tester connection status

Tx/Rx Stream monitoring and reporting

- 1024 Tx streams per physical N_Port
- Throughput reports
- Error counters
- Latency
- Statistics reports in spreadsheet format

Triggering

You can trigger Analyzers with a TTL output via a connector when an erroneous event occurs.

Error Injection

You can set Load Tester to inject CRC errors in the generated traffic.

The errors for FC/FCoE(SAN) traffic are "FC/FCoE CRC", "Ethernet CRC", "FC/FCoE SOF" (None and Invalid) and "FC/FCoE EOF" (None and Invalid).

The errors for LAN traffic is "Ethernet CRC" only.

Capabilities

The Xgig Load tester is capable of performing the following types of tests:

Subsystem design and debug

- ASIC physical layer test
- Hardware robustness test

Functional test

- Switch performance test
- Switch regression test
- Switch stress test
- System conformance test (with Medusa Labs Test Tools (MLTT))

Interoperability test

- Network data integrity test
- Fabric stress test
- Fabric scalability test

Manufacturing test

Xgig Load Tester is capable of hardware verification.

Components

This section defines the components central to the Load Tester process. These components are discussed in context in the subsequent chapters.

The load tester process involves the following primary components:

- Physical N_Ports
- tags
- data streams
- traffic profile engines
- traffic patterns
- topology

Each Load Tester port transmits and receives data through a Physical N_Port. The Load Tester port manages credits, performs Link Service operations, as well as blasts data streams at line rate in complex topologies, with stressful payload patterns, to challenge the performance capabilities of the switch and the entire SAN.

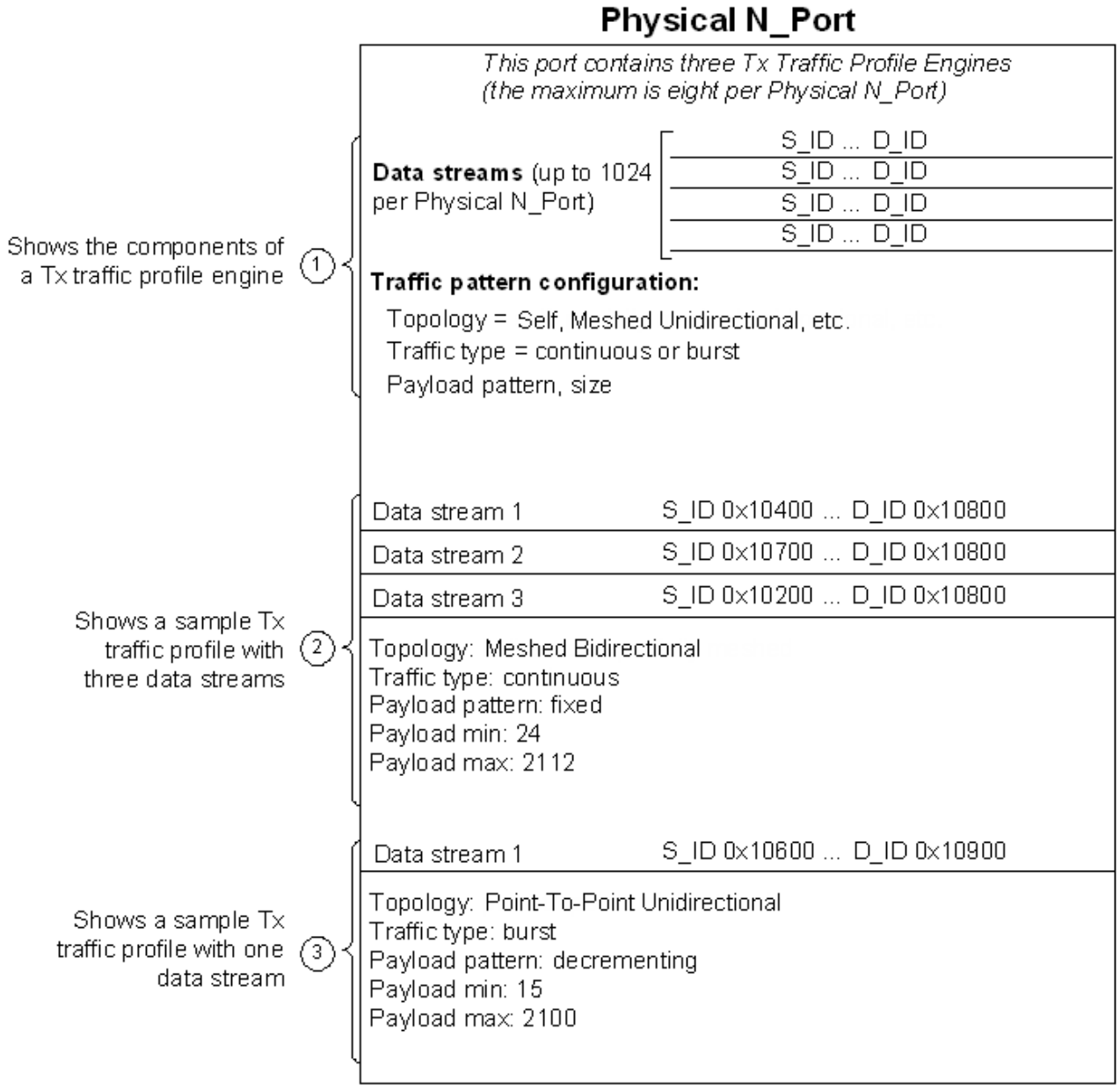
Physical N_Port

Due to hardware constraints, the following resources are available for each Physical N_Port:

- 4, 6, or 8 Traffic Profile Engines (depending on the blade type)
- 1024 TX Data Streams shared among the 8 Traffic Profile Engines
- 1024 Rx Data Streams shared among the 8 Traffic Profile Engines

The following diagram illustrates the configuration of a Physical N_Port.

Figure 1: Example: Physical N_Port Configuration



Tags

Tags are an organizational tool for ports in Load Tester. A tag contains a name, a description, and a list of ports to which the tag is applied. You can apply a tag to any number of ports. When you select a tag, the available ports are listed. When configuring ports, configuring traffic patterns, or setting up multi port link service, you can use tags to quickly find a pre-defined set of ports that you want to perform an action on. When a tag uses an API command as a parameter, the API command will apply to all the ports associated with the tag.

Data Streams

A data stream is defined to be a unique entity within a Load Tester port, defined by its S_ID and D_ID. More than one data stream with the same S_ID and D_ID may coexist with a single Load Tester port; however, they will be monitored for errors independently.

Note: The terms *data stream* and *stream* have the same meaning and are used interchangeably in this guide.

Traffic Profile Engines

Depending on the blade, they can have up to a maximum of eight uniquely configurable Traffic Profile Engines per Physical N_Port.

Blade Description	4G	8G	16G	10G 2 Port	10G IO Blade Regular Mode	10G IO Blade Extended Mode
Available Traffic Profile Engines	6	6	8	4	4	8

Traffic Profile Engines are used to transmit one or more data streams. A Physical N_Port can receive up to 1024 data streams, and Traffic Profile Engines are not required for the receive logic.

Each Traffic Profile Engine has the following uniquely configurable parameters:

- One or more data streams
- Traffic type - continuous or burst
- Payload Pattern/Type
- Payload Size - fixed or random
- Port Topology: the group of ports and the way in which these ports shall be organized to transfer data to each other. (partially meshed, fully meshed, and others)

Traffic Patterns

The term traffic pattern applies to a traffic profile engine. Each Physical N_Port can have up to eight traffic profile engines. Each traffic profile engine contains a traffic pattern configuration, which is a combination of Physical N_Port traffic topologies and traffic configuration settings such as traffic type and payload type, payload size, and seed information.

The Traffic Pattern concept allows a group of ports that share a port topology to also share all the configurations related to the traffic profile engines. When you create a traffic pattern, each port that transmits in the traffic pattern will allocate a single Traffic Profile Engine. In the case where the Port Topology is bi-directional, all ports will allocate a single Traffic Profile Engine.

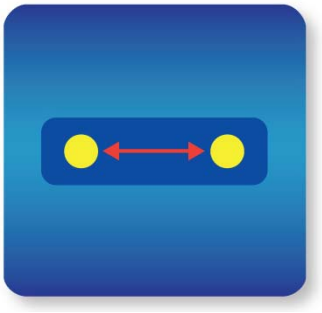
Creating and saving traffic patterns is a good way to preserve test configurations so that you can reuse them.

Topology

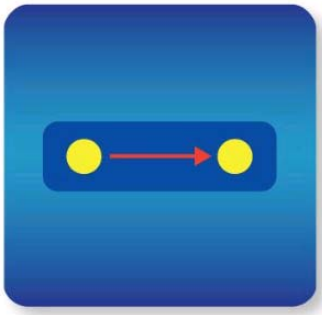
The term topology applies to an individual test. Tests run on a Physical N_Port are defined by a traffic pattern configuration. One aspect of the traffic pattern is the topology, which defines the direction and flow of the link traffic between ports. For each test in Load Tester, the ports can have any of the following logical link topologies:

- **Self** - defines a configuration where data traffic is sent back to the transmitter

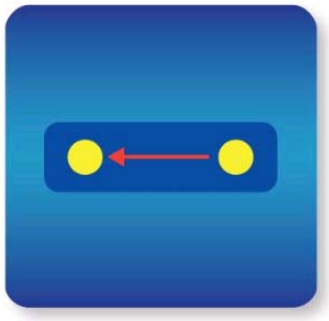
- **Pair Port**- defines a source port sends data to the corresponding port in a port pair on a blade



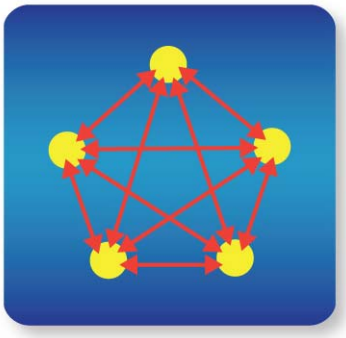
- **Pair Port Tx Odd** - defines a configuration where each selected port exchanges traffic with its pair unidirectionally, for example port 1 to 2 and port 3 to 4.



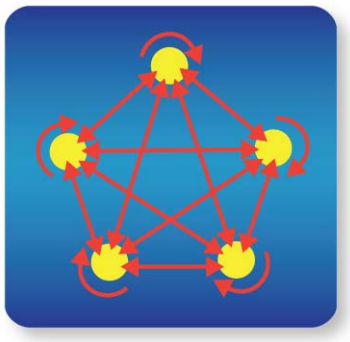
- **Pair Port Tx Even** - Each selected port exchanges traffic with its pair unidirectionally, for example port 2 to 1 and port 4 to 3.



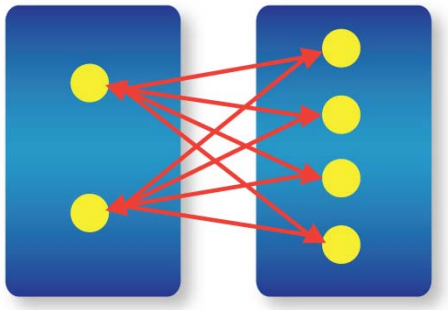
- **Fully Meshed Exclude Self**- defines a configuration where traffic is sent to all ports except to the transmitter



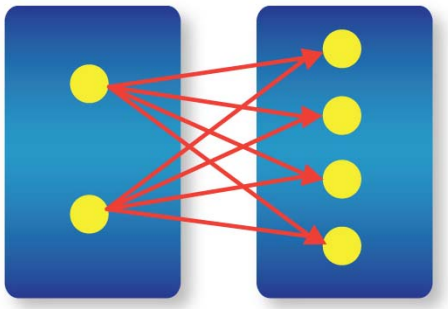
- **Fully Meshed Include Self**- Super set of partially meshed topology. It defines that each port in one test sends and receives the data traffic to and from the rest of the ports. Each port in the list transmits to all the other ports in the list including itself.



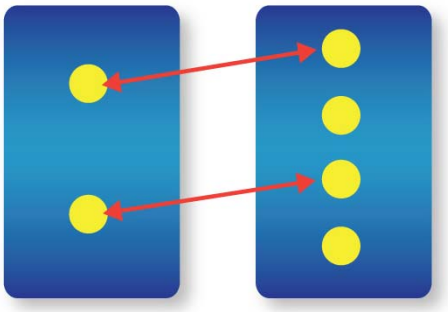
- **Meshed Bidirectional** - defines the specific port(s) send(s)/receive(s) data traffics to/from the other ports that are configured for one test



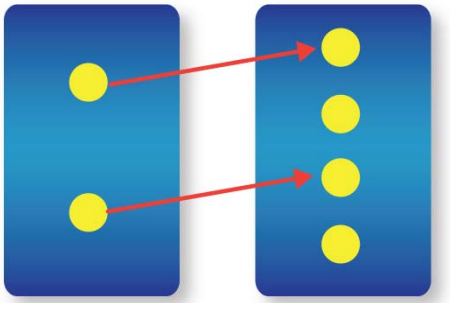
- **Meshed Unidirectional** - defines the specific port(s) send(s) data traffics to the other ports that are configured for one test.



- **Point-to-Point Bidirectional** - defines the source and destination ports send data traffic to ports with the same numbered tag.

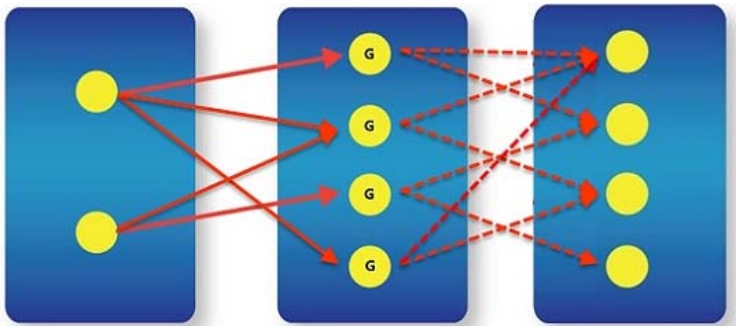


- **Point-to-Point Unidirectional** - defines the source ports send data traffic to destination ports with same numbered tag.

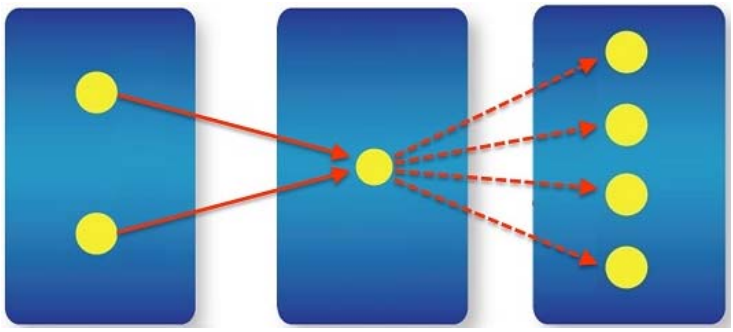


Note: For the Partially Meshed topography, a user provides a set of source ports and destination ports. Each of the source ports sends traffic to each of the destination ports.

- **Multicast** - defines the source ports sending data traffic to the destination groups before forwarding the data traffic to the destination ports associated with the destination groups.



- **Broadcast** - defines the source ports sending data traffic to the switch before forwarding the data traffic to the destination ports connected to switch.



Chapter 2

Using the Load Tester Tab

In this chapter:

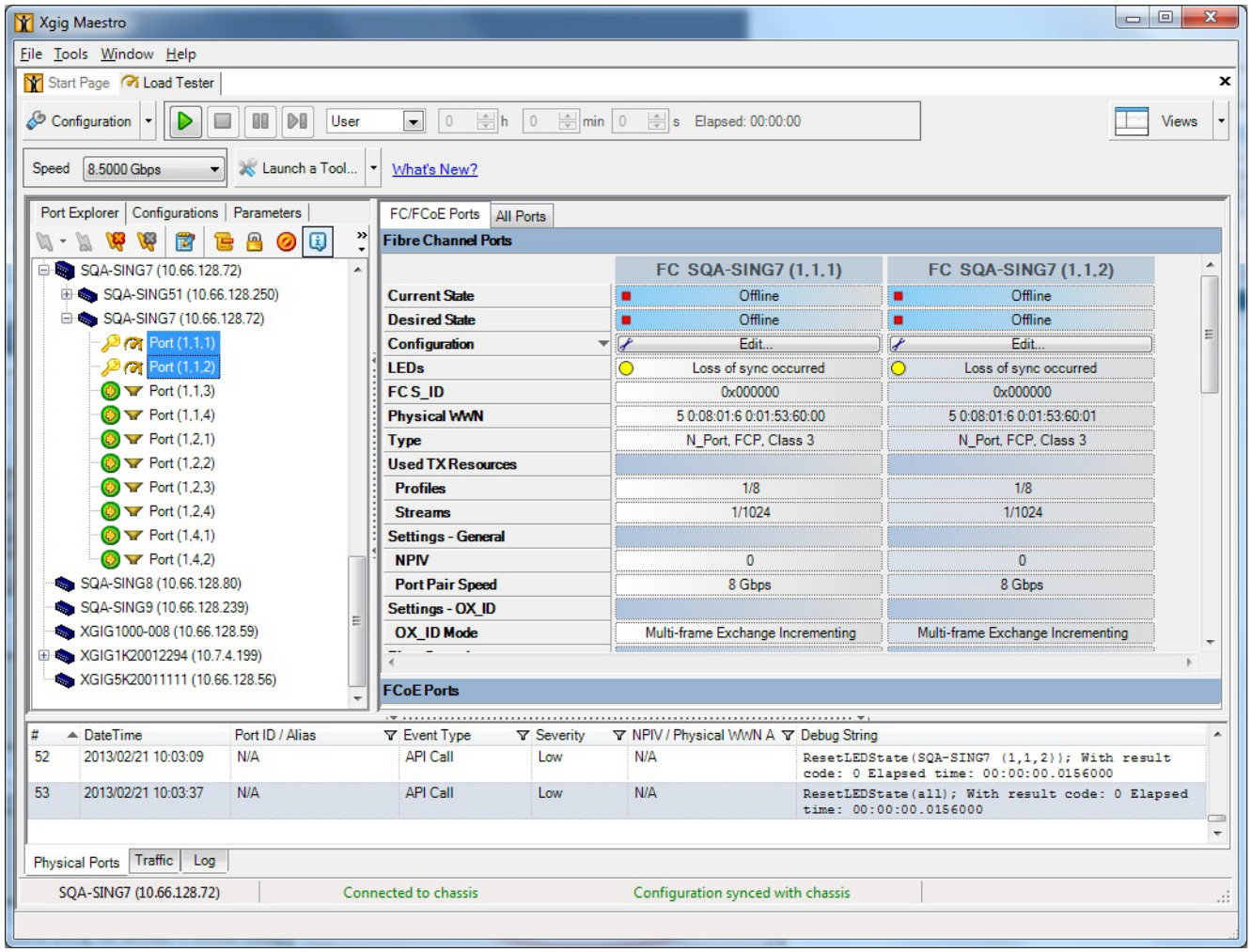
In order to use Load Tester, you must lock one or more port pairs on the blades within your Xgig chassis for use as Load Testers as described in the *Xgig Maestro Introduction Guide*. In order to use ports as Load Testers, the multi-function blade they reside in must be licensed for this functionality.

You should have launched Xgig Maestro and locked at least one pair port.

After you have discovered and locked the Load Tester ports that you plan to use and have set up your capturing and monitoring applications (such as Xgig Analyzer), you are ready to run the Xgig Load Tester application. This chapter provides an overview of the Load Tester tab on the Xgig Maestro main window, and its functions.

Clicking the Load Tester tab in the Maestro main window displays the Xgig Load Tester window, shown below. This tab is where you operate the Load Testers you have locked.

Figure 2: Xgig Load Tester Window

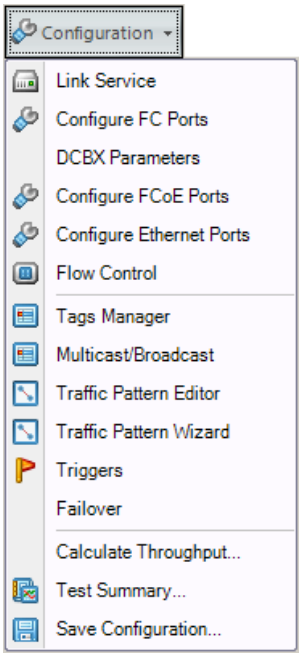


Load Tester Domain Operations

On the upper part of the Load Tester window are the domain operations buttons and options that you can use to configure and run your tests. These are:

Configuration Button - Opens the Load Tester multi-tab Device Window.

Figure 3: Configuration Button Option List



You can click the drop-down arrow to see more configuration option listed below:

Link Service - Opens the **Link Service** tab in the Load Tester Device Window that displays all the ports locked as Load Testers and also the different Link Service options you can set for the ports.

Configure FC Ports - Opens the **FC Ports Configuration** tab in the Load Tester Device Window where you can configure individual or multiple FC ports locked to Load Tester.

DCBX Parameters - Opens the **DCBX** sub-tab under the 10G Ports Configurations tab in the Load Tester Device Window where you manage the DCBX settings for a selected FCoE port.

Configure FCoE Ports - Opens the **FCoE** sub-tab under the 10G Ports Configuration tab in the Load Tester Device Window where you can configure individual or multiple FCoE ports locked to Load Tester.

Configure Ethernet Ports - Opens the **Ethernet** sub-tab under the 10G Ports Configuration tab in the Load Tester Device Window where you can configure individual or multiple ethernet ports locked to Load Tester.

Flow Control - Opens the **Flow Control** tab in the Load Tester Device Window where you can configure the traffic flows for individual or multiple FC or FCoE ports locked to Load Tester.

Tags Manager - Opens the **Tags Manager** tab in the Load Tester Device Window where you can create, edit, and delete tags used in Load Tester.

Multicast/Broadcast - Launches the **Multicast Broadcast Configuration** tab. This option is only applicable when Load Tester is connected to one or more FC port pairs on a legacy 8G blade.

Traffic Pattern Editor - Opens **Traffic Pattern Configuration** tab in the Load Tester Device Window where you can create, edit, or delete traffic patterns used in the tests.

Traffic Pattern Wizard - Launches the Traffic Pattern Wizard.

Triggers - Opens the **Triggers** tab in the Load Tester Device Window where you can turn on and pause triggers.

Failover - Opens the **Failover** tab in the Load Tester Device Window where you can configure the failover settings for Fibre Channel ports.

Calculate Throughput - Opens the **Calculate Throughput** dialog box where you can select which portions of the frame will be used in the calculation of the throughput.

Test Summary - Opens the **Test Summary Report Options** dialog box displays all the options for the test summary reports.

Save Configuration - Opens the **Save Load Tester Configuration As** dialog box where you may save the current test configuration under the folder and name of your choice. The configuration cannot be saved and the **Save Configuration...** option is inactive when Load Tester is in the offline state because the corresponding API "get_ConfigurationAsTCL" cannot be used in offline mode. You can only save after the connection is restored.

Start test - Starts the test by sending requests to the ports to log into the Fabric. Also, if you have not done so, it also initialize the hardware with the selected configuration and begins the test.

Stop test - Stops the current test in progress and requests the ports go to a logged in state.

Pause test - Pauses the current test in progress. It makes no changes to the user's selected configuration and the flow control sending status.

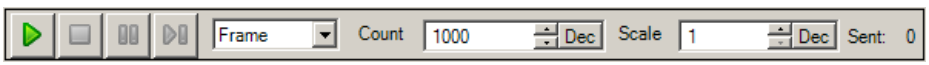
Resume test - Resumes the test in progress.

Sending Mode - There are three modes to run a test:

- **User** – Allows you to start the test anytime you want. Once you start the test in this mode, it will continue running until you pause or stop it manually. This is the default mode.

- **Time** – Allows you to configure a time period for the test to run. When the **Start test** button is selected, the test runs for the specified duration.

- **Frame** – Allows you to configure the number of frames to send per port. The total frame count per port is calculated value of the **Count** × **Scale** values. When the **Start test** button is selected, the test runs for the specified number of frames.



When you choose to pause the test using the **Pause test** button (described above), the time or frames sent counter stops incrementing for all ports.

However, if you want to pause only some of the ports, select the **Pause** button described in Traffic tab -> TX Port based view (see Table 5 on page 71).

Note: If the first port is excluded from the selected ports to be paused, the **Time** or **Frame Sent** counter will continue to increment.

Test Length - Sets the amount time or number of frames that the test will run.

Speed - Sets the speed of the ports to use during the test. Changing the Speed settings is only applicable for FC ports.

Launch a Tool... - Provides a drop-down list that allows you to access the following tools:**Single Frame Tx/Rx**, **Port Capture**, **Configuration Summary**, **API Shell - Load Tester**, and **Clock Sync Ordered Set**. For complete information on each of these tools, refer to "Launch a Tool" on page 19.

What's New? - Provides a quick way to see what new features Load Tester has added since the previous release of the software. Click on Next Update or Last Update to navigate between the new features.

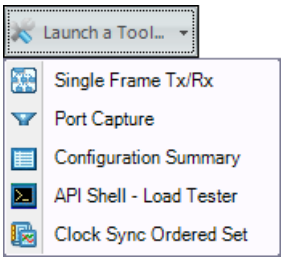
Views - Shows the options for displaying the different sections of the Load Tester Graphical User Interface (GUI). The available options would be dependent on the current tab presented in the Load Tester GUI.

The Load Tester window is further divided into three tabs: the Physical Ports, Traffic, and Log. These tabs are discussed in the following sections.

Launch a Tool

Launch a Tool... - Provides a drop-down list that allows you to access the following tools:

- **Single Frame Tx/Rx** (see page 19)
- **Port Capture** (see page 22)
- **Configuration Summary** (see page 23)
- **API Shell - Load Tester** (see page 23)
- **Clock Sync Ordered Set** (see page 25)



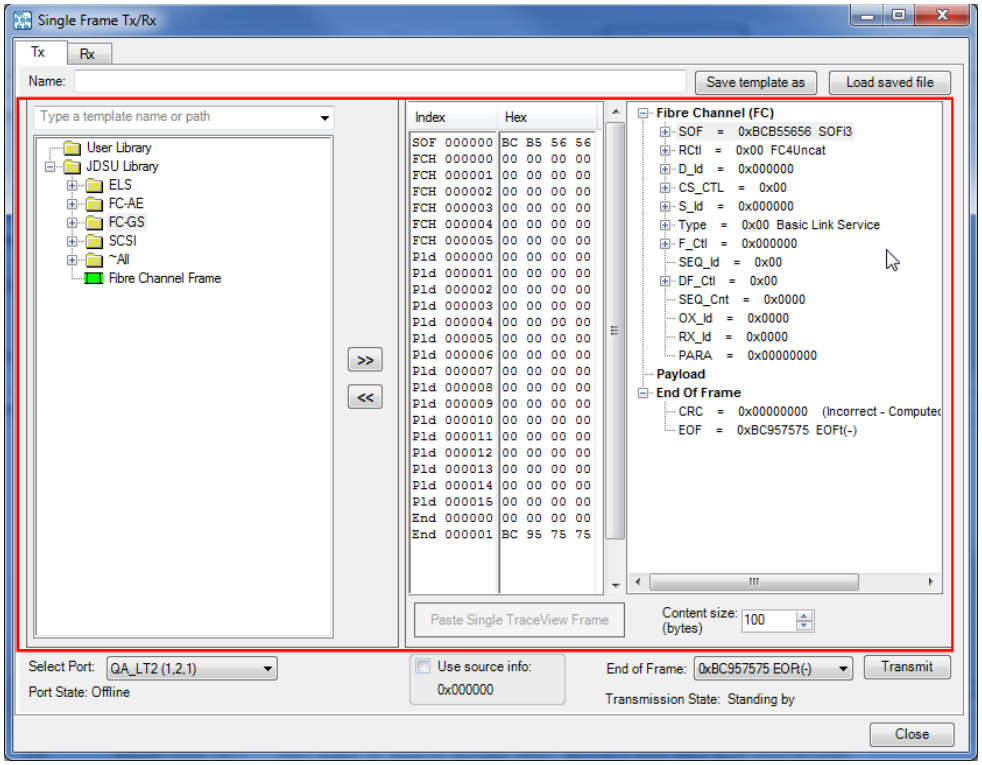
Single Frame Tx/Rx

Opens the Single Frame Tx/Rx window. The Single Frame Tx/Rx window is used to send and examine frames, one at a time.
The **Tx tab** allows you to open a new or saved frame, modify the frame's data as desired, and transmit it. Single Frame Tx can be used to transmit any frames in the library templates .
The **Rx tab** is used to examine the received frame (response). Single Frame Rx is designed to receive login frames only.

While appearing very similar at first glance, the two tabs are slightly different. The following describes both tabs:

The Tx Tab

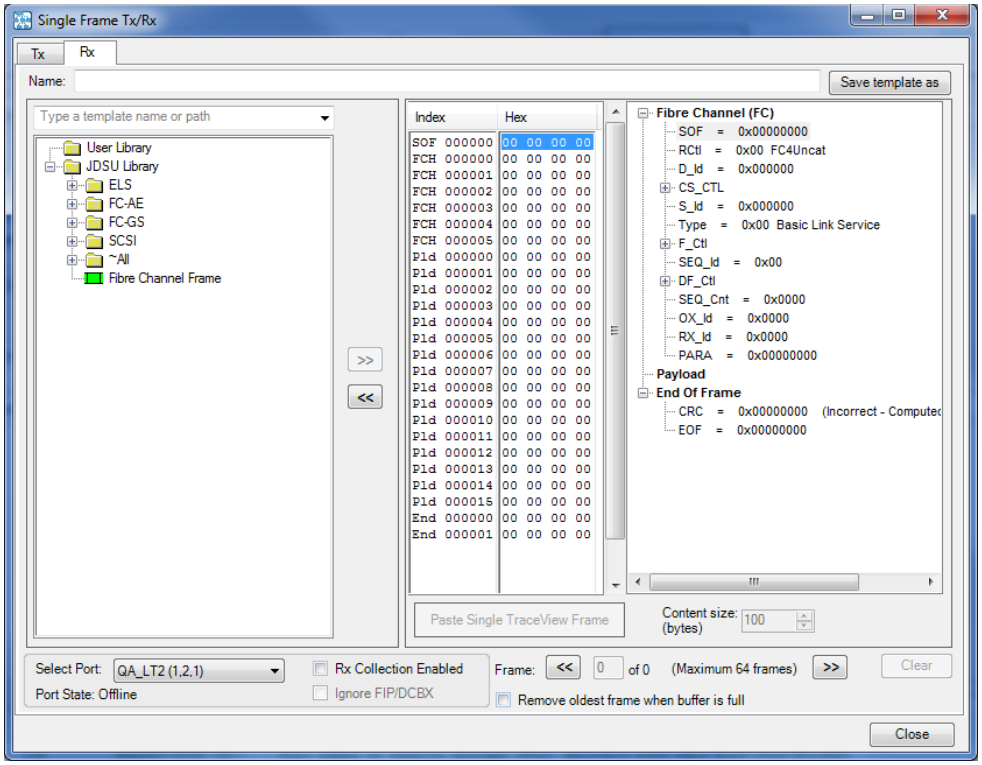
Figure 4: Single Frame Tx/Rx Window - Tx Tab



- **Name:** field - Displays the name of the file used or the name of the template being saved.
- **Save template as** button - Saves a custom frame as a template.
- **Load saved file** button - Loads a saved frame template.
- The **Frame Customization** editor - Also shown in Figure 52 on page 136 and is described briefly in that section. This area is outlined in red in Figure 4 above.
- **Select Port:** field - Selects which port will be used to transmit the frame.
- **Port State:** message - Displays the current state of the port. Refer to the Current State section on page 42 for a list of port states.
- **Use source info:** check box - Where applicable, automatically inserts the Load Tester's source ID as the source ID (S_Id) in the frame information. (Displayed on Tx tab only). It inserts the MAC Address for FCoE ports.
- **End of Frame:** drop-down list - Selects the end of frame string that you want to use: EOFt (End of Frame Terminate), EOFa (End of Frame Abort), EOFn (End of Frame Normal), EOFni (End of Frame Invalid), or another End of Frame type (User-defined EOF) that you can define. (Displayed for FC ports only).
- **Transmission State:** message - Lists the status of the transmission.
- **Transmit** button - Transmits the frame.

The Rx Tab

Figure 5: Single Frame Tx/Rx Window - Rx Tab



- **Name:** field - Identifies the name of the template to be saved.
- **Save template as** button - Saves the response for future analysis or to save the received response to be transmitted.
- The **Frame Customization** editor - Also shown in Figure 52 on page 136 and is described briefly in that section. This area is outlined in red in Figure 4 above.
- **Select Port:** field - Allows you to select which port will receive the transmitted frame.
- **Port State:** message - Displays the current state of the port. Refer to the "Current State" on page 42 for a list of port states.
- **Rx Collection Enabled** check box - Enables the selected receive port to receive transmitted frames. When this option is enabled, the selected port will not process incoming frames. Also when enabled, an informational dialog box is displayed stating "Enabling Rx collection intercepts received frames on the affected port, making it unresponsive and unable to participate in a login process. Keep in mind that if you experience a login problem, check to make sure the Rx collection option has been turned off."
- **Ignore FIP/DCBX** check box - Ignores the FIP and DCBX Keep Alive events. (Active for 10G FCoE only.)
- Frame selection area, includes:
- << button - Decrements the frame number being viewed.
- **X of X** counter - Identifies the frame being viewed and the number of frames received. A maximum of 64 frames are kept in the buffer.
- >> button - Increments the frame number being viewed.

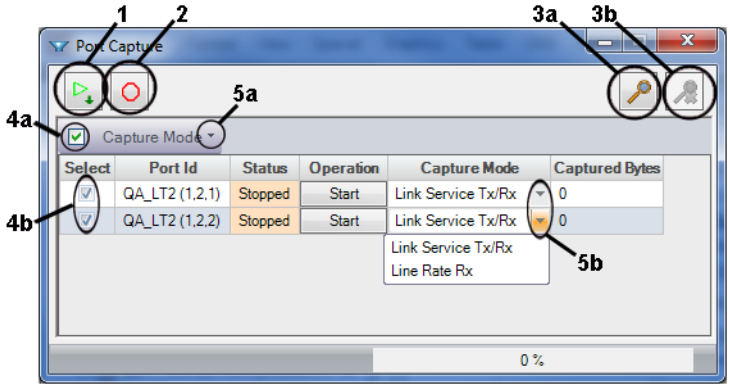
- **Remove oldest frame when buffer is full** button - Deletes the oldest frame once the buffer becomes full.
- **Clear** button - Removes all of the received frames from the buffer.

Port Capture

- Activates the Port Capture feature of Load Tester, displaying the Port Capture dialog box, which is used to capture and create trace files for the following data that are sent and received by Load Tester:

- 4G/8G/16G Blades: Fibre Channel Login Frames, RSCN Messages, and Data Frames
- 10G Blades: LLDP Frames, FIP Frames, FCoE Login Frames, RSCN Messages, and Data Frames (Extended Mode)

Figure 6: Port Capture Dialog Box



The start capture (1) and stop capture (2) buttons are available for these functions.

The TraceView button (3a) is used to invoke TraceView to view the captured traffic of a port pair or an individual port. Refer to the Xgig Analyzer User Guide for information on using TraceView. The Cancel Port Processing button (3b) can be used to cancel the processing of the capture before the trace is launched.

The ports can be selected individually using the check boxes in the Select column (4b) or you can select all of the ports using the check box located above the Select column (4a).

Login Frames would include Extended Link Service Requests and Replies, and Generic Service Requests and Replies.

Data Frames can be captured but only on the Rx Side.

The port Capture Mode settings can be set as:

- **Link Service Tx/Rx**-> Captures sent and received Link Service frames.
- **Line Rate Rx** -> Captures both Link Service and data frames but only those received.

The Capture Mode settings can be set by selecting the appropriate setting (Link Service Tx/Rx or Line Rate Rx) for:

- Individual ports from the Capture Mode cell for that specific port (5b).
- All of the selected ports from the Capture Mode drop-down list at the top of the port table (5a).

Refer to the bitfile matrix since line rate is not applicable to all blades.

To perform a capture:

1. Select the port(s) to capture.
2. Select the desired capture mode.
3. Select the Start Capture button.

Configuration Summary

Opens the **Configuration Summary** window where you can view and save the configuration information from the Port tab, the Traffic tab, and the Miscellaneous tab. Select Save configuration as Spreadsheet... from the File menu to save the configuration information.

API Shell - Load Tester

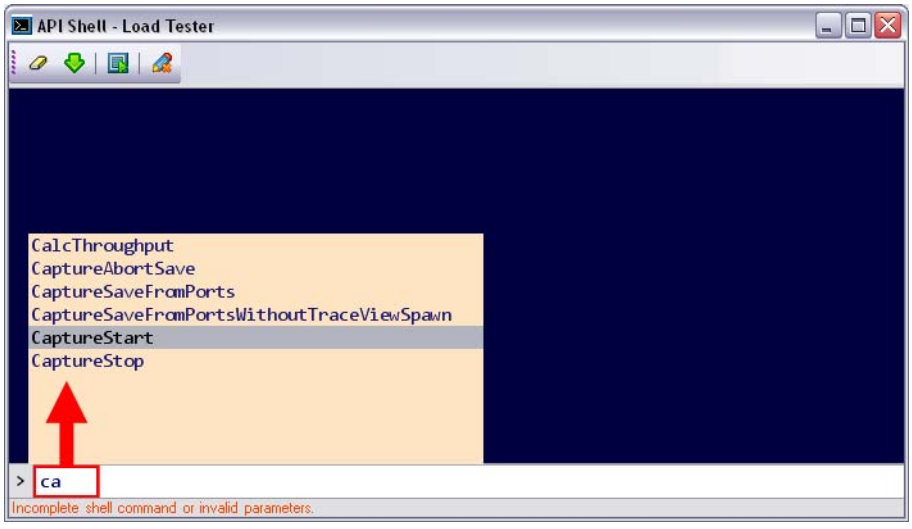
Opens the **API Shell - Load Tester** window which allows you to run API commands directly from the text box at the bottom of the window and view the results in the large display area at the center of the window. This is useful as a quick alternative if you want to control Load Tester from the GUI with an API command. It is also useful if you are a user who is writing a script and wants to experiment with various API functions to observe what an API command does prior to incorporating the command into a script. The command lines can be copied from the display window and pasted into a text editor.

1. To enter an API command, start typing the command name in the text area. As you begin entering the command name, a list of the command matching the entry is displayed as shown in Figure 7.

   As you can see in this example, the first two letters of “capture” were entered in the text area and all commands matching the entered value are displayed.

2. Using the up (↑) and down (↓) arrow keys on the keyboard, move so the desired command is highlighted.

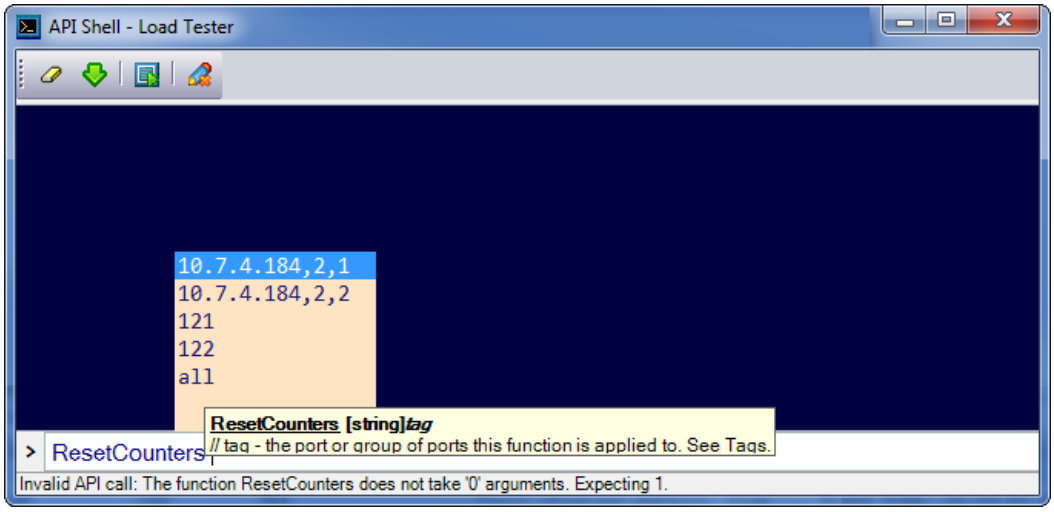
Figure 7: API Shell Command Selection



3. Select the *Enter* key to select the command and then enter a *space* using the spacebar.

4 Type in an additional command parameters preceded and followed by a space character (parameters containing spaces must be double quoted).

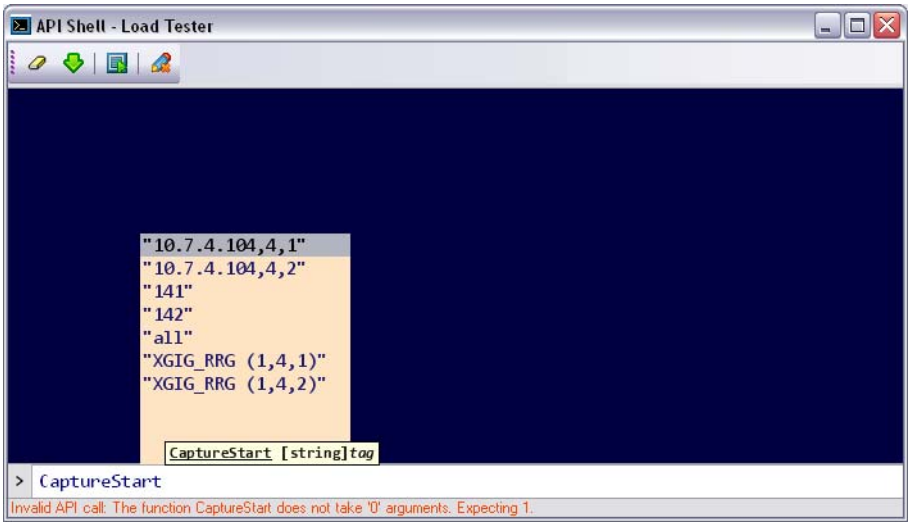
Note: When you enter a command in the API Shell - Load Tester tool, a pop-up box appears showing the description information for the API command. When a space is entered to input the API command parameters, a description of the parameters is displayed in the pop-up box. Occasionally, the name of the parameter and description may not match exactly, but the meaning will be similar.



If a list of candidates for the current parameter is available (such as port, tag, and traffic pattern names), they will be displayed as shown in Figure 8. Using the up (↑) and down (↓) arrow keys, move to highlight the desired parameter and press the *Enter* key to select the parameter.

Skip to step 6 if the command is complete.

Figure 8: API Shell Parameter Selection



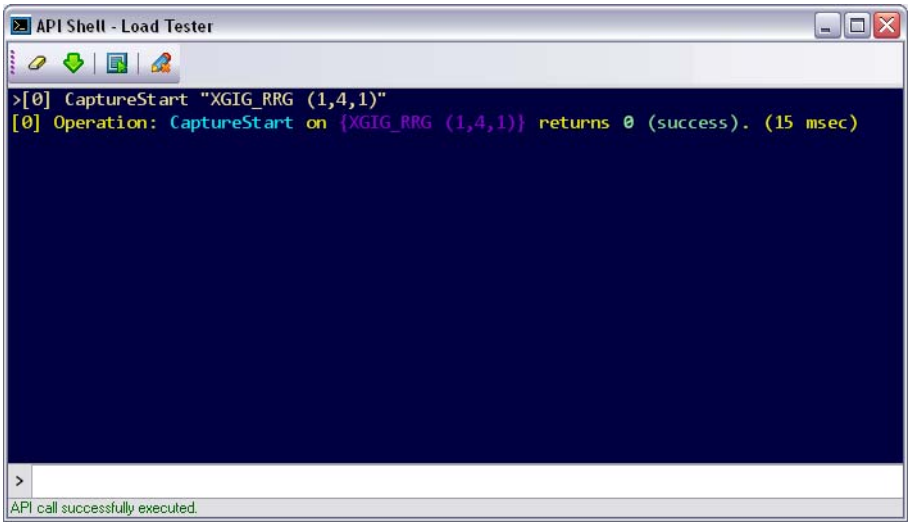
5 Enter a *space* using the spacebar. If additional parameters are displayed, repeat step 4.

6 Select the *Enter* key to run the API command.

The results of the command are shown in the display area as shown in Figure 9.

Note the results are color-coded based on the command name, port ID, and the results value.

Figure 9: API Shell Results Display



There are four buttons in the top left corner of the window:

Clear Shell View button clears the results from the display area.

Auto-scroll Enabled/Auto-scroll Disabled button toggles the auto-scroll function on and off.
- When enabled, the results filling the display area are scrolled up, allowing the output into the display area to refresh and show the most recent results in the visible display area. The older results can be accessed by scrolling up.
- When disabled, the results filling the display area are scrolled down, allowing only the older output results to be shown in the visible display area. The newer results can be accessed by scrolling down.

Load Tcl Script button opens a dialog box to choose a saved script. This will allow you to run it in the API Shell window and display the results in the display area.

To avoid confusion, it is not recommended that you load scripts that perform port management from inside in API Shell. If a loaded script includes port locking, this may fail because ports are already locked by the GUI before API Shell is launched. If the script is locking different ports from GUI, the script will run on all ports locked by both the GUI and the script.

Logging Enabled/Logging Disabled button toggles the logging function on or off. When enabled, logging is allowed to occur in the main Load Tester window on the Physical Ports, Traffic, and Log tabs.

Clock Sync Ordered Set

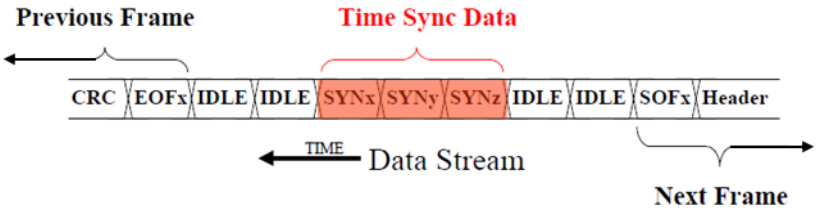
Selecting Clock Sync Ordered Set from the Launch a Tool... dropdown list opens the Clock Sync Ordered Set dialog box for FC ports on legacy 8G blades. This dialog box is described in “Using the Clock Sync Ordered Set Dialog Box” on page 27, however using this dialog box is not the first step in using this clock synchronization feature. A complete process is described in “Clock Synchronization Ordered Set Process” on page 26.

There are two definitions that are important in understanding the Clock Synchronization for Load Tester:

Clock Synchronization Ordered Set (SYN)

The Clock Synchronization Server periodically generates a synchronization event. The synchronization event causes the transfer of clock synchronization symbols (SYN primitives) to Clients. (The period between synchronization events are controlled by the Clock Synchronization Server.) Embedded within the clock synchronization symbols is the necessary data to update the Clients real-time clock.

The clock synchronization server generates the synchronization event by substituting three synchronization symbols for a sequence of three IDLEs in the intra Frame interval (between the frames). The three synchronization symbols for a sequence consist of a Clock Synchronization Ordered Set (SYN).



Real-Time Clock (RTC)

The Clock Synchronization Server and the Client both have their own Real-Time Clock (RTC). The Client will use the embedded time data within the clock synchronization symbols to update its RTC to complete the synchronization.

Clock Synchronization Ordered Set Process

Follow the process below to set up the Clock Synchronization Ordered Set:

1. Configure Clock Synchronization Ordered Set in Port Configuration tab.

   Refer to “Clock Synchronization Ordered Set (SYN)” on page 95.

2. Enable SYN and View SYN statistics (Rx and Tx).

   a. Make sure SYN server and client ports are all in “Link Active” status. If not, go to Link Service tab and click “Link Initialization” to switch the status of those ports to “Link Active”. Refer to “Managing the Link Service Operations” on page 161 if you need help with this.

   b. Click “Launch a Tool…” -> “Clock Sync Ordered Set” to open the Clock Sync Ordered Set dialog box. See “Launch a Tool” on page 19.

   c. Verify the Synchronization Resolution (Granularity) setting and enable or disable the Server and Client Ports as appropriate which is described in “Using the Clock Sync Ordered Set Dialog Box” on page 27.

3. Generate the SYN report.

   Set the report options on the Clock Sync Ordered Set dialog box. Refer to “Selecting Report Options” on page 28.

Using the Clock Sync Ordered Set Dialog Box

Selecting Clock Sync Ordered Set from the Launch a Tool... dropdown list opens the Clock Sync Ordered Set dialog box shown in Figure 10. This dialog box is used to enter general settings such as setting the synchronization resolution and enabling the Server and Client ports for Clock Synchronization Ordered Set (SYN). It is also used to set options for reporting.

Enable SYN and View SYN Statistics (Rx and Tx)

Synchronization Resolution (Granularity) – defines the granularity of SYN for both Synchronization Clock Server and Client. You can set the resolution from 100ns to 20µs to configure any value with the 100ns step size. The default value is 100ns.

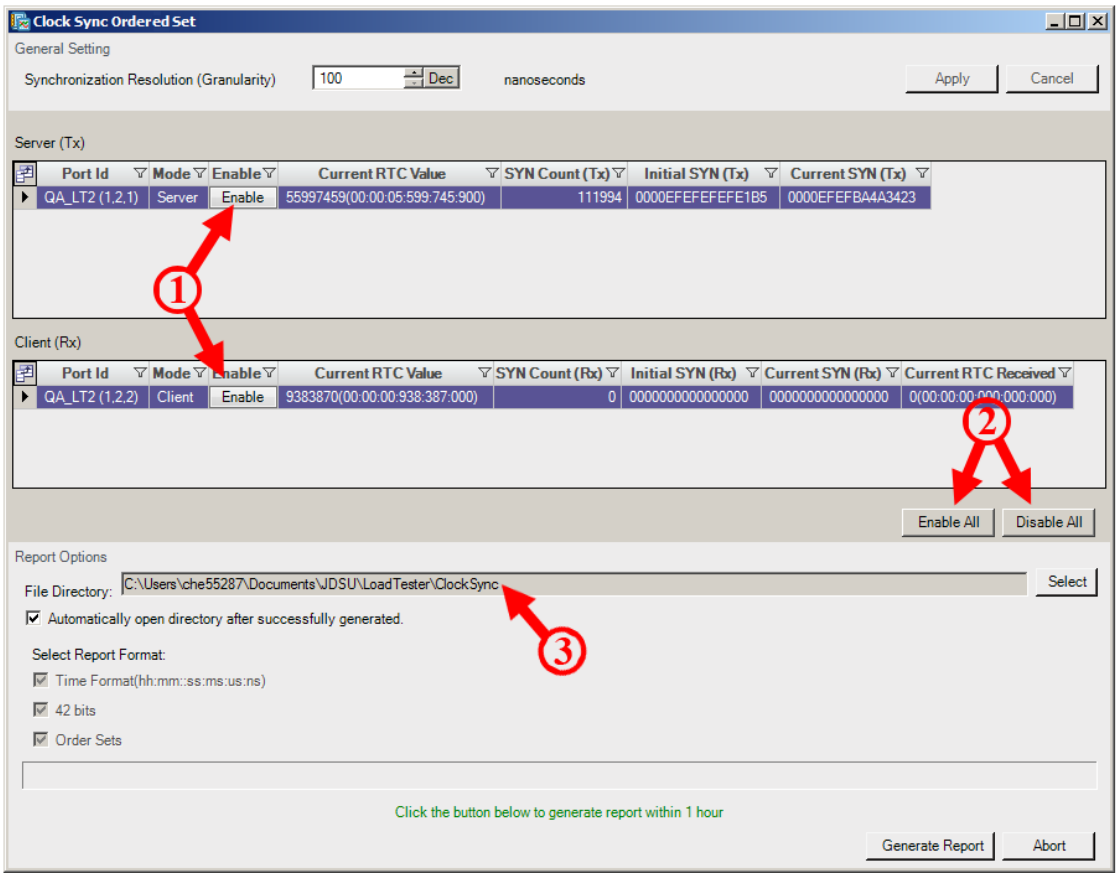
Enable/Disable Server and Client Ports – You will need to enable the Server and Client ports to utilize the SYN.

Click **Enable** button (1 on Figure 10)for each port to enable the Clock Sync function. (Enabling the Server starts to send SYN; enabling the Client starts to receive the SYN.)

Click **Disable** button (1 on Figure 10) for each port to disable Clock Sync function for each port. The statistic value will still be shown but will be reset for next enable. Note that the **Disable** button is displayed only when the port is already enabled.

Click the **Enable All** or the **Disable All** button (2 on Figure 10) to enable or disable the Clock Sync function for all the ports above.

Figure 10: Clock Sync Ordered Set Dialog Box



Selecting Report Options

All of the statistical reports of the selected ports are saved into a user-defined directory. You can configure the directory path before generating the report, and check the automatically open directory after successfully generated if desired. By default, the three report formats are all selected.

The **File Directory** (3 on Figure 10) allows you to define the folder where you want to save the statistical reports of the selected ports. Clicking the **Select** button opens the **Browse for Folder** dialog box that allows you to choose the desired folder.

Selecting the **Automatically open directory after successfully generated** check box will automatically open the directory where the reports are being saved when the **Generate Report** button is clicked.

In the **Select Report Format:** area, the following formats are included in the report. These are default formats that are included in every report.

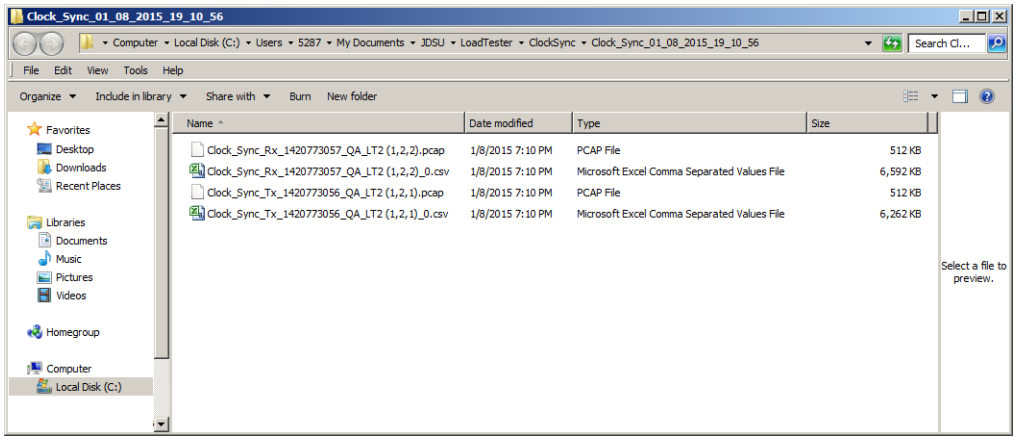
- **Time Format(hh:mm:ss:ms:us:ns)**
- **42 bits**
- **Ordered Sets**

Clicking the **Generate Report** button disables the ports and generates a report for the last hour that the ports where enabled. If the ports were not enabled for an hour or longer, a report is generated for the entire period. The generated report includes two parts: report transmission from chassis (server) and format conversion in client. The label below the progress bar shows the status. Clicking the **Abort** button will cancel the generation of current report.

Opening the Generated Report

When you view the directory that contains the reports, you will see that it contains files for the Tx (server) port(s) and files for the Rx (client) port(s). Each port will have one or more .csv files that contain the report data for the port (and one .pcap file that is merely used as a temporary file). The Report file will be split into multiple .csv files if the size of the report file exceeds the 10 MB limit or if the maximum number of records in each file exceeds 100,000. Up to 360 files for each port can be generated if the Interval of SYN is set to the minimum value (100µs).

Figure 11: Generated Reports Directory

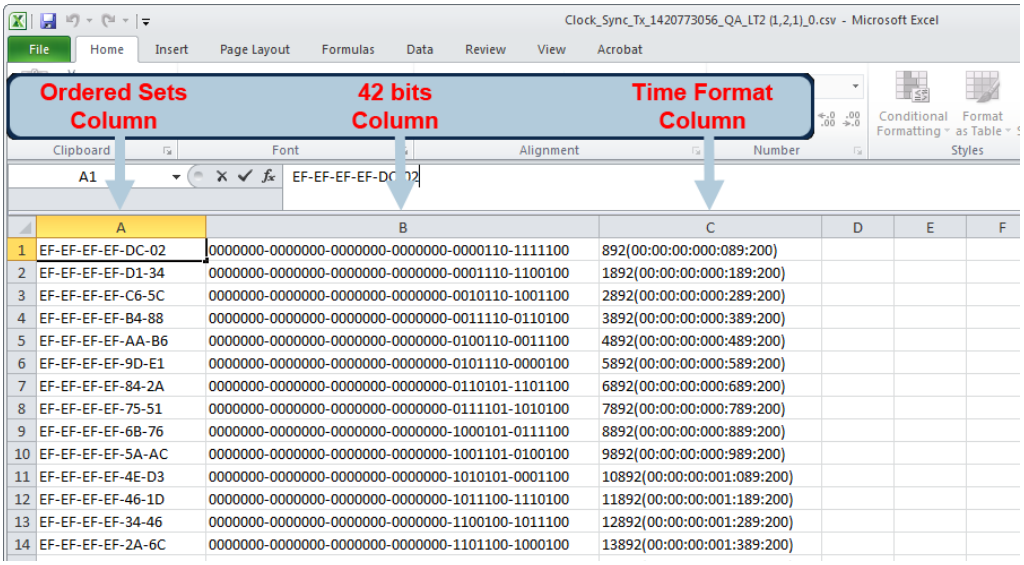


When you open a .csv file, you will see that the report data is displayed in three columns that match the three formats specified in the Clock Sync Ordered Set dialog box.

Column A is Ordered Sets data
Column B is 42 bits data
Column C is Time Format data

Column C contains the count followed by the time in hours “hh”, minutes “mm”, seconds “ss”, milliseconds “mmm”, microseconds “uuu”, and nanoseconds “nnn”. Each of these time units is separated by a colon “:” The time counts are described in the “Primitive signal Service” section of the “Clock synchronization service” chapter in the *Fibre Channel Framing and Signaling (FC-FS)* standard.

Figure 12: Generated Report File



	A	B	C
1	EF-EF-EF-EF-DC-02	0000000-0000000-0000000-0000000-0000110-1111100	892(00:00:00:000:089:200)
2	EF-EF-EF-EF-D1-34	0000000-0000000-0000000-0000000-0001110-1100100	1892(00:00:00:000:189:200)
3	EF-EF-EF-EF-C6-5C	0000000-0000000-0000000-0000000-0010110-1001100	2892(00:00:00:000:289:200)
4	EF-EF-EF-EF-B4-88	0000000-0000000-0000000-0000000-0011110-0110100	3892(00:00:00:000:389:200)
5	EF-EF-EF-EF-AA-B6	0000000-0000000-0000000-0000000-0100110-0011100	4892(00:00:00:000:489:200)
6	EF-EF-EF-EF-9D-E1	0000000-0000000-0000000-0000000-0101110-0000100	5892(00:00:00:000:589:200)
7	EF-EF-EF-EF-84-2A	0000000-0000000-0000000-0000000-0110101-1101100	6892(00:00:00:000:689:200)
8	EF-EF-EF-EF-75-51	0000000-0000000-0000000-0000000-0111101-1010100	7892(00:00:00:000:789:200)
9	EF-EF-EF-EF-6B-76	0000000-0000000-0000000-0000000-1000101-0111100	8892(00:00:00:000:889:200)
10	EF-EF-EF-EF-5A-AC	0000000-0000000-0000000-0000000-1001101-0100100	9892(00:00:00:000:989:200)
11	EF-EF-EF-EF-4E-D3	0000000-0000000-0000000-0000000-1010101-0001100	10892(00:00:00:001:089:200)
12	EF-EF-EF-EF-46-1D	0000000-0000000-0000000-0000000-1011100-1110100	11892(00:00:00:001:189:200)
13	EF-EF-EF-EF-34-46	0000000-0000000-0000000-0000000-1100100-1011100	12892(00:00:00:001:289:200)
14	EF-EF-EF-EF-2A-6C	0000000-0000000-0000000-0000000-1101100-1000100	13892(00:00:00:001:389:200)

The hours unit is required since the time may not start from 0 if the initial RTC value is set to non-0 value, which could cause the time to exceed one hour. This scenario could also occur if the test has been running for an extended period (over an hour), and the report contains only the last hour of date. As an example, if the test has been running 2 hours, the report will contain the last hour’s data, so the data should be 1hour – 2hour, in this case hh needs to be displayed. Once the RTC value reaches its maximum value (4398046511103 or $2^{42}-1$), it will restart from 0.

Physical Ports Tab

The Physical Ports tab is the default display of the Load Tester form after the function is launched.

The following section describes the different parts of the tab.

Parameters Status Table

The Parameters Status table shows the ports you have locked. The locked tabs are organized by Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) ports. The locked ports can be divided in a sorted manner in the **FC/FCoE Ports** tab or displayed unsorted in the **All Ports** tab.

To configure how to display the ports in the Parameters Status Table, click on the **View** button and do the following:

Select or unselect **Configuration** to display or hide the Port Explorer tab, Configurations tab and Parameters tab where you manage ports locked to Load Tester, manage Load Tester configuration files, and select the Parameters to display, respectively.

Select or unselect **Log** to display or hide the Configurations tab and Parameters tab where you manage Load Tester configuration files and select the Parameters to display, respectively.

Click **Ports** to display the ports in the viewing option that you prefer in the Parameters Status Table.

Tile Horizontally - Select this option to display the Fibre Channel Ports pane before the FCoE Ports pane

Tile Vertically - Select this option to display the Fibre Channel Ports pane beside the FCoE Ports pane

Tabs - Select this option to display the Fibre Channel Ports pane and FCoE Ports as tabs.

Each Load Tester port is displayed by a column on the Parameters Status table (Figure 13). At the top of each column is the protocol, the chassis name, and in parenthesis the chassis number, the slot number and port number(s).

Figure 13: Parameters Status Table

	10 GE QA_5000_GEN3 (1,4,7)	10 GE QA_5000_GEN3 (1,4,8)
Current State	Offline	Offline
Desired State	Offline	Offline
Configuration	Edit...	Edit...
Feature Set	Regular	Regular
LEDs	Loss of sync occurred	Loss of sync occurred
E_Node Source MAC	00:80:16:90:31:F2	00:80:16:90:31:F3
VN_Port MAC Addresses...	View...	View...
MAC/IP View...	View...	View...
FCF MAC Addresses	00:01:01:29:11:98	00:01:01:29:11:98
FC S_ID	0x000000	0x000000
Physical WWN	5 0:08:01:6 0:01:58:76:36	5 0:08:01:6 0:01:58:76:37
Type	10G (SAN/LAN)	10G (SAN/LAN)
Used TX Resources		
Profiles	1/4	1/4
Streams	1/1024	1/1024
Settings - General		
NPIV	0	0
Login/FIP		
Login VLAN Tag	Enabled	Enabled
VLAN Class Of Service	3	3
VLAN VID	0x002	0x002
Max RX FCoE Payload	2112	2112
DCBX		
Enable	True	True
FCoE Logical Link	Disabled	Disabled
Ethernet Logical Link	Disabled	Disabled
Parameters...	View...	View...
Settings - OX_ID		
OX_ID Mode	Multi-frame Exchange Incrementing	Multi-frame Exchange Incrementing
Flow Control		
PFC Override	True	True
RX Pause Detect Delay	0	0
RX Pause Detect Mask	0	0
Errors Counters		
FC CRC Errors	0	0
Ethernet CRC Errors	0	0

The first column on the Parameters Status table lists the legends of rows, which are user configurable. The following are the parameter categories that are available depending on the type of port:

For Fibre Channel Band	For Fibre Channel over Ethernet Band
• Current State • Desired State • Configuration... • LEDs • FC S_ID • Physical WWN • Type • Port Group Tag List • Used TX Resources • Settings - General • Settings - OX_ID • RSCN • Flow Control • SFP Status • Error Counters	• Current State • Desired State • Configuration... • Feature Set • LEDs • E_Node Source MAC • VN_Port MAC Addresses... • MAC/IP View... • FCF MAC Addresses • FC S_ID • Physical WWN • Type • Port Group Tag List • Used TX Resources • Settings - General • Login/FIP • DCBX • Settings - OX_ID • RSCN • Flow Control • SFP Status • Error Counters

You can select the parameters that will appear on the Parameters Status Table by selecting the parameters from the Parameters panel on the left of the Parameters Status Table.

Parameters Category Descriptions for Fibre Channel Ports

Current State

This row shows the following current status of the Load Tester:

- Laser Off
- Offline
- Port Failure
- Link Initializing
- Link Active
- Logout in Progress
- Fabric Login in Progress
- Logged in to Fabric
- NPIV Login in Progress
- NPIVs Logged In
- N-Port Login in Progress
- Logged In
- Test Preparation
- Test in Progress
- Transmit Complete
- Test Complete
- Blast Fabric Login
- Ignored in Test
- Unknown State

Refer to the `get_State()` function in the API Help for more information.

Desired State

This row shows the target state of the Load Tester ports: Laser Off, Offline, Link Active, Logged in to Fabric, NPIVs Logged In, Logged In, Test in Progress. Refer to the `get_DesiredState` function in the API Help for more information.

Configuration

This row contains the **Edit...** button that launches the **FC Ports Configuration** window for the selected port.

LEDs

This indicator changes color (green, red, yellow, or black) depending on the link status. The indicator corresponds to the Link status LEDs on the blade in the Xgig chassis. Refer to the `get_LEDState` function in the API Help for more information.

The LEDs on the blade's front panel provide status about each port on the blade. See Table 1.

Table 1: Xgig Fibre Channel Blade Link Status LED

Port column LED color	Description
Black	Loss of signal
Red	Loss of synchronization
Green	Synchronized
Yellow	Loss of synchronization has occurred

Once sync has been resolved, a red LED turns to yellow. To reset the LED indicator to green, you need to reset the LED.

To reset the blade LEDs:

1. Right-click in the Parameters Status table to open the Parameters context menu.
2. Select **Reset LED** or **Reset LEDs for all ports**.

FC S_ID

This row shows the Source ID. This is the initial address given to this Load Tester by the switch during Fabric Login.

Physical WWN

This row shows the World Wide Name (WWN) of the port. Refer to the `get_WwnByNpiv` function in the API Help for more information.

Type

This row indicates the port type, for example, N_Port, FCP, Class 3.

Used TX Resources

This category displays the number of traffic profiles used or data streams used. Refer to the `get_TrafficUsedStreams` function in the API Help for more information.

Profiles

Indicates the number of continuous or burst traffic profiles used by the Physical N_Port.

Streams

Indicates the number of data streams being used by the Physical N_Port. Each physical Load Tester transmission path supports a maximum of 1024 data streams.

Settings - General

This category indicates the current physical setup of the Load Tester port. You can change the settings in this category by using the Parameters context menu for each port you have locked.

When changing the line rate from 8.5000 Gbps to any other speed, Scrambling is automatically set to Disabled. When changing to 8.5000 Gbps, it is automatically set to Enabled. You may then manually override this setting by selecting **Configure Port** from the Parameters context menu.

Alias

Indicates the current alias or label assigned to the port. Refer to the `Alias` function in the API Help for more information.

NPIV

Indicates the number of virtual S_IDs that will be requested during the NPIV Login by using FDISC command(s). The Physical S_ID is not included in this number.

N_Port ID Virtualization is a Fibre Channel standard that allows a single Physical N_Port to acquire more than one S_ID. The Load Tester supports NPIV during Login. For example, a unique stream could be created for each NPIV S_ID, destined to a single D_ID.

Port Pair Speed

This indicates the link rate for the port. In Fibre Channel, the link rate can be 1.0625 Gbps, 2.1250 Gbps, 4.2500 Gbps, 8.5000 Gbps, or 14.025 Gbps (16G).

When the speed of a port is changed, the speed for the corresponding port in the port pair is changed automatically. In addition, if the scrambling and idle primitive settings are changed automatically in response to a speed change for a port, the scrambling and idle primitive settings for the corresponding port are changed automatically.

Note: Xgig Load Tester does not support speed auto-negotiation. To change the speed for a port, select **Configure port** from the Parameters context menu. To change the speed of multiple ports, select **Configure multiple ports** from the Parameters context menu.

Scramble

The 8G blades give the option of enabling Fibre Channel Frame Scrambling, which is the mandatory requirement for 8G Fibre Channel (8GFC) Specification. Xgig Load Tester offers the options to enable/disable the scrambling feature at 1.0625 Gbps, 2.1250 Gbps, 4.2500 Gbps, 8.5000 Gbps, or 16Gbps.

To enable Scrambling:

1. Right-click on the port to open the Parameters context menu.
2. Select **Configure port**.
3. Select the **Scramble** check box and select **YES** from the list.
4. Click **Ok**.

When Scrambling is enabled, Fibre Channel Frame Scrambling is performed in the Configuration pattern starting after any SOF indicator template and continues until the next word with a K character (usually EOF). Scrambling is enabled by default for line rate 8.5000 Gbps and 16Gbs. Scrambling is disabled by default for line rates 1.0625 Gbps, 2.1250 Gbps, and 4.2500 Gbps. See `ScramblingMode` in the API Help.

Idle Primitive

Indicates the idle primitive setting. Per 8GFC specification, the available options are **Idle** and **ARB(FF)**. The idle primitive setting is **ARB(FF)** by default for line rate 8.5000 Gbps. The idle primitive setting is **Idle** by default for line rates 1.0625 Gbps, 2.1250 Gbps, and 4.2500 Gbps. Refer to the `IdleIsARBff` function in the API Help system located on the product USB drive for more information.

Minimum IFG

Displays the Minimum Inter-Frame Gap (IFG). It is the guaranteed minimum number of idles between consecutive frames. Refer to the `MinimumInterPacketGap` function in the API Help for more information.

RX Buffer Size

Displays the buffer-to-buffer credits that will be advertised by the Load Tester port to the switch in Fabric Login (FLOGi) command. Refer to the `RxCredits` function in the API Help for more information.

Login Retry Limit

Displays the Login Retry Limit set for this port. If the login fails, then it will automatically retry after an elapsed time defined by login retry delay. See the `LoginRetryCountLimit` and `LoginRetryDelay` functions for more information.

Login Retry Delay

Displays the amount of time before a login retry is executed. See the `LoginRetryCountLimit` and `LoginRetryDelay` functions for more information.

Settings - OX_ID

This category indicates the current OX_ID of the Load Tester port. You can change the settings in this category by using the Parameters context menu for each port you have locked.

OX_ID Mode

The OX_ID is a field in the header of the Fibre Channel frame whose value is inserted by the Load Tester. The OX_ID value chosen depends on the mode selected. Possible modes include: **Multi-frame Exchange Incrementing**, **Single-frame Exchange Incrementing**, and **Single-frame Exchange Random**.

Refer to the `OxidMode` function in the API Help for more information.

OX_ID has the following modes:

- **Multi-frame Exchange Incrementing**
  The **Multi-frame Exchange Incrementing** mode assigns the OX_ID similar to the manner hosts assign OX_IDs. When sending Fibre Channel frames, this mode assigns each exchange and all frames within the exchange a unique OX_ID. This mode will correctly report sequence errors, unaccounted frames and out-of-order frames in both S_ID / D_ID and S_ID / D_ID / OX_ID routing environments. When testing ISLs or SAN equipment where routing policies are based on S_ID / D_ID / OX_ID, the **Multi-frame Exchange Incrementing** mode is the only configuration that will provide valid test results specifically for out of sequence or unaccounted frames analysis.

  Refer to `TrafficOxidBase` and `TrafficOxidStep` functions for more information on user configuration of these values.

- **Single-frame Exchange Incrementing**
  For a given Physical N_Port, the value of the OX_ID increases by one for each consecutive frame transmitted by the Load Tester. The lower and upper bounds can be specified by the user.

  Refer to `OxidMin` and `OxidMax` functions in the API Help for more information.

- **Single-frame Exchange Random**
  For a given Physical N_Port, the value of the OX_ID will be random between a lower and upper bound. The OX_ID value varies in a pseudo random manner, changing for each consecutive frame transmitted. The lower and upper bounds can be specified by the user. Refer to `OxidMin` and `OxidMax` functions in the API Help for more information.

Additional Clarification

The **Single-frame Exchange Incrementing** and **Single-frame Exchange Random** OX_ID test modes send test frames that vary the OX_ID of each successive frame sent. Incrementing or Random OX_ID modes can be used to test for single-frame exchanges that are received in an order different than how they were transmitted. When testing in this configuration, the Unaccounted Frames and Sequence Errors counters will be set to 0 and should be ignored. Because the Fibre Channel specification does not explicitly define in-order or out-of-order exchanges the column heading “Out of Order Frames” should be interpreted as “single-frame exchanges received in an order other than the order transmitted.”

OX_ID Minimum

Displays the minimum value to be used for OX_ID when the OX_ID mode is set to **Single-frame Exchange Incrementing** or **Single-frame Exchange Random**.

Refer to the `OxidMin` function in the API Help for more information.

OX_ID Maximum

Displays the maximum value to be used for OX_ID when the OX_ID mode is set to **Single-frame Exchange Incrementing** or **Single-frame Exchange Random**.

Refer to the `OxidMax` function in the API Help for more information.

OX_ID Seed

Indicates the seed value for the OX_ID in random mode

A seed is a number used to initialize a random number generator. The random generator is initialized once using the seed and the subsequent patterns will be generated automatically in a random manner. Refer to **Single-frame Exchange Random** OX_ID Mode discussed above.

You can also refer to the `OxidSeed` function in the API Help system on the product USB drive for more information.

RSCN

Indicates whether or not this port register to receive Registered State Change Notifications (RSCN) from the Fabric.

Flow Control

Max TX Credits

Indicates the phys current count of remaining credits. When this value reaches 0, the phy must receive an Rrdy prior to transmitting another frame.

TX Credits Available

Indicates the phys transmit credit count that was received from the login target. This value will be 1 during login. Post login this will contain an integer value returned from the switch. It represents the maximum depth of the targets receive buffer.

ns @Zero Credits

When Current TX Credit count reaches Maximum TX Credit Value an underlying counter starts incrementing. When a credit is received, and the Current TX Credit count drops, the number of nanoseconds is stored.

SFP Status

Indicates the status of the Small Form-factor Pluggable (SFP) optical transceiver

SFP Rx Power

Indicates the SFP Rx power of the port

See get_SFPRxPower in the API Help.

SFP Tx Power

Indicates the SFP Tx power of the port

See get_SFPTxPower in the API Help.

SFP Make

Indicates the SFP Make number of the port

See get_SFPMake in the API Help.

SFP Model

Indicates the SFP Model of the port

See get_SFPModel in the API Help.

Error Counters

Contains all the errors reported back to Load Tester when statistics are updated

FC CRC Errors

Displays number of CRC Errors

See `get_CRCErrors` in the API Help.

Code Violations

Indicates number of Code Violations

See `get_CodeViolationErrors` in the API Help.

Disparity Errors

Displays number of Disparity Errors

See `get_DisparityErrors` in the API Help.

Sequence Errors

Displays number of Sequence Errors. This counter does not apply for LAN traffic so they are all 0 for LAN data streams.

See `get_FrameSequenceErrors` in the API Help.

Out Of Order

Indicates number of Out of Order Frame Errors. An Out of Order error occurs when a frame arrives that is not the expected successor (increased by one). This counter does not apply for LAN traffic so they are all 0 for LAN data streams.

Refer to the `get_FrameOutOfOrderErrors` function in the API Help for more information.

Unaccounted Frames

Displays number of Unaccounted Frames. An unaccounted frame occurs when then one or more frames have not arrived when the final frame of the sequence arrives. For LAN traffic "Unaccounted Frames" are derived from FCoE algorithm that applies to every 32 frames. Although this may not be true packet loss, it often reflects packet drop or extreme delay.

Refer to the `get_FrameDroppedErrors` function in the API Help for more information.

Misdirected

Displays the number of Misdirected Errors. A misdirected error occurs when a frame arrives that was not destined for the selected load tester port.

A misdirected error occurs when a frame arrives that was not destined for the selected load tester port. Misdirected frames are Load Tester Data frames (for SAN that means SCSI Data frames, for LAN this could mean TCP/UDP frames) with meta data that were sent to the wrong Load Tester port. In the meta data there is a field that specifies the destination load tester port. If this field doesn't match the receiving port, then the misdirected frame counter increments by 1.

Refer to the `get_FrameMisdirectedErrors` function in the API Help for more information.

Error Recovery Count

If the Load Tester has zero credits for longer than E_D_TOV (Default is 2 seconds) then the Load Tester issues a LR to the switch, implicitly causing credits available to the value achieved at login, and the Error Recovery Count increments. If a test was running at the time of the error recovery event, it will resume after LISM completes. Refer to the `get_ErrorRecoveryCount` function in the API Help for more information.

Additional Information on Error Counters

The following error counters are tracked by the Load Tester receiver on a PER STREAM basis. The Load Tester can track 512/1024 streams per receiver.

Sequence Errors

Displays the number of sequence errors. The sequence error counter increments anytime the SEQ_CNT of the current frame is not equal to the last frame's SEQ_CNT+1.

Note: Unaccounted frames, out of order frames, CRC errors, Disparity errors, and Code Violations will all lead to Sequence errors.

Unaccounted Frames

Displays the number of unaccounted frames. Each stream is similar to a unidirectional exchange consisting of a single sequence of 32 frames. The Load Tester remembers the SEQ_CNT of all the frames in the current pending exchange. When the final frame of the exchange arrives, indicated by SEQ_CNT=31, a 32-bit memory is evaluated and the unaccounted frame counter is incremented for each missing frame.

Note: Due to a limitation of the Load Tester if the frame with SEQ_CNT=31 is dropped by the switch, the unaccounted frame counter will NOT increment, but the SEQUENCE error count will increment. Frames dropped by switch with SEQ_CNT=0-30 will all increment the unaccounted frame counter. This is assuming Exchange Length is equal to 32.

Warning: All frames with CRC errors will be discarded by the Load Tester receiver "prior" to doing unaccounted frame evaluation. This is by design, since the data integrity of all fields in a frame with a CRC error is uncertain. For example, if a frame arrives with SEQ_CNT=30 AND also has a CRC Error, then it is discarded by the Load Tester, and when the final frame with SEQ_CNT=31 for the exchange arrives, a 32-bit memory will be evaluated and it will show that the frame with SEQ_CNT=30 did not arrive and the unaccounted frame counter will be incremented. In general, frames with code violations or running disparity errors will also lead to a CRC error.

Out of Order

An out of order frame counter increases if the SEQ_CNT of the current frame is less than the SEQ_CNT of the last frame.

Error Counter Example:

The following example assumes Exchange Length equal to 32.

If for a particular stream, frames arrive with the following SEQ_CNT's:

```
0,1,3,2,4,5,6,8,9,...,31
```

Error Counter Summary for this stream:

Number of Sequence errors: 3

Out of order errors: 1

Unaccounted Frames: 1
(evaluated when frame with SEQ_CNT=31 arrives to allow immediate trigger)

Parameters Category Descriptions for FCoE Ports

Current State

This row shows the following current status of the Load Tester:

- Laser Off
- Offline
- Port Failure
- Link Initializing
- Link Active
- Logout in Progress
- Fabric Login in Progress
- Logged in to Fabric
- NPIV Login in Progress
- NPIVs Logged In
- N-Port Login in Progress
- Logged In
- Test in Progress
- Unknown State
- Ignored in Test

Refer to the `get_State()` function in the API Help for more information.

Desired State

This row shows the target state of the Load Tester ports: Laser Off, Offline, Link Active, Logged in to Fabric, NPIVs Logged In, Logged In, Test in Progress. Refer to the `get_DesiredState` function in the API Help for more information.

Configuration

This row contains the **Edit...** button that launches the **10G Ports Configuration** window for the selected port.

Feature Set

This row shows whether the port is using regular feature set or the extended feature set. To enable extended features set, right-click on the port and select Enable Extended Features. When the **Feature Set** row is disabled for a blade, it means the blade does not support the Extended Feature Set.

This is currently applicable to ports 1,2,5, and 6 of the 10G IO Blade. To Enable this feature, four ports (1-4, 5-8,) or all eight of them must be locked in.

LEDs

This indicator changes color (green, red, yellow, or black) depending on the link status. The indicator corresponds to the Link status LEDs on the blade in the Xgig chassis. Refer to the `get_LEDState` function in the API Help for more information.

The LEDs on the blade's front panel provide status about each port on the blade. See Table 2.

Table 2: Xgig FCoE Blade Link Status LED

Port column LED color	Description
Black	Loss of signal
Red	Loss of synchronization
Green	Synchronized
Yellow	Loss of synchronization has occurred

Once sync has been resolved, a red LED turns to yellow. To reset the LED indicator to green, you need to reset the LED.

To reset the blade LEDs:

1. Right-click in the Parameters Status table to open the Parameters context menu.
2. Select **Reset LED** or **Reset LEDs for all ports**.

E_Node Source MAC

This row shows the E_Node Ethernet address for the FCoE port.

VN_Port MAC Addresses

This row shows the **View** button that opens the VN_Port Addresses window that lists the VN_Port Addresses and details.

As the Load Tester VN_Ports are being acquired during NPIV Login, the user can click the **View VN_Port MAC Addresses...** button from the Physical Ports grid. This will open port's **VN_Port Addresses** window displaying the Source and Destination MAC addresses, Fibre Channel Source Id and World Wide Name, and the status for each VN_Port (Online - Green, Offline - Red).

If the user clicks the **Advanced** button, the Enode and VN_Port Keep Alive timer values will be displayed.

One or multiple VN_Ports can be selected and right-clicked to bring up the option to change the Enode or VN_Port Keep Alive timer value. Setting the value to zero will disable the transmission of Keep Alives for that VN_Port. If the Keep Alive settings for a VN_Port are set to an incorrect interval or disabled, the switch will eventually send a Clear Virtual Links to the Load Tester. Upon receipt of the Clear Virtual Links, the status of the VN_Port will be changed to Offline, and the contents of the Clear Virtual Links will be added to the log.

MAC/IP View...

This row shows the **View** button that opens the MAC/IP View window that lists the MAC and IP details of the selected support.

FCF MAC Addresses

Indicates the MAC address for the FCF discovered during the FCoE login process.

FC S_ID

This row shows the Source ID. This is the initial address given to this Load Tester by the switch during Fabric Login.

Physical WWN

This row shows the World Wide Name (WWN) of the port. Refer to the `get_WwnByNpiv` function in the API Help for more information.

Type

This row indicates the port type.

Port Group Tag List

Indicates the tags that are applied to the port. You can also view the port's tags by selecting **Port Tags** from the Parameters context menu. In addition, you can add a tag to or remove a tag from a port by selecting **Add Tag** or **Remove Tag** from the Parameters context menu. Refer to the `get_TagList` function in the API Help for more information.

Used TX Resources

This category displays the number of traffic profiles used or data streams used. Refer to the `get_TrafficUsedStreams` function in the API Help for more information.

Profiles

Indicates the number of continuous or burst traffic profiles used by the Physical N_Port.

Streams

Indicates the number of data streams being used by the Physical N_Port. Each physical Load Tester transmission path supports a maximum of 1024 data streams.

Settings - General

This category indicates the current physical setup of the Load Tester port. You can change the settings in this category by using the Parameters context menu for each port you have locked.

When changing the line rate from 8.5000 Gbps to any other speed, Scrambling is automatically set to Disabled. When changing to 8.5000 Gbps, it is automatically set to Enabled. You may then manually override this setting by selecting **Configure Port** from the Parameters context menu.

Alias

Indicates the current alias or label assigned to the port. Refer to the `Alias` function in the API Help for more information.

NPIV

Indicates the number of virtual S_IDs that will be requested during the NPIV Login by using FDISC command(s). The Physical S_ID it not included in this number.

N_Port ID Virtualization is a Fibre Channel standard that allows a single Physical N_Port to acquire more than one S_ID. The Load Tester supports NPIV during Login. For example, a unique stream could be created for each NPIV S_ID, destined to a single D_ID.

Minimum IFG

Displays the Minimum Inter-Frame Gap (IFG). It is the guaranteed minimum number of idles between consecutive frames. Refer to the `MinimumInterPacketGap` function in the API Help for more information.

Login/FIP

This category indicates the current Login/FIP

Login VLAN Tag

Indicates the Ethernet value that this FCoE port will use for all frames during the FCoE login process.

VLAN Class Of Service

Indicates the enable vector that will be sent in a PFC pause frame. The bits set in the bit mask correspond to the classes that will be paused in the receive data path.

VLAN VID

Indicates the VLAN VID assigned to the port.

Login Retry Limit

Displays the Login Retry Limit set for this port. If the login fails, then it will automatically retry after an elapsed time defined by login retry delay. See the `LoginRetryCountLimit` and `LoginRetryDelay` functions for more information.

Login Retry Delay

Displays the amount of time before a login retry is executed. See the `LoginRetryCountLimit` and `LoginRetryDelay` functions for more information.

Max RX FCoE Payload

Indicates the maximum size to be used by the **trafficId**.

FIP Keep Alive

Indicates whether the enable/disable FIP frames/timers (Tx and Rx) for the port(s) are enabled. It will display **True** if they are enabled.

DCBX

This category indicates the current DCBX settings of the Load Tester port.

Enable

Indicates whether DCBX operation for the port is enabled or disabled.

FCoE Logical Link

Indicates the DCBX Logical Link Down FCoE Logical Link Status (LLS) flag value. Please note this DCBX feature may not be present.

Ethernet Logical Link

Indicates the DCBX Logical Link Down FCoE Logical Link Status (LLS) flag value for LAN traffic. Please note this DCBX feature may not be present.

Parameters...

This row contains the **Parameters...** that will launch the **DCBX Parameters** window for the selected port.

Settings - OX_ID

This category indicates the current OX_ID of the Load Tester port. You can change the settings in this category by using the Parameters context menu for each port you have locked.

OX_ID Mode

The OX_ID is a field in the header of the Fibre Channel frame whose value is inserted by the Load Tester. The OX_ID value chosen depends on the mode selected. Possible modes include: **Multi-frame Exchange Incrementing**, **Single-frame Exchange Incrementing**, and **Single-frame Exchange Random**.

Refer to the `OxidMode` function in the API Help for more information.

OX_ID has the following modes:

- **Multi-frame Exchange Incrementing**
  The **Multi-frame Exchange Incrementing** mode assigns the OX_ID similar to the manner hosts assign OX_IDs. When sending Fibre Channel frames, this mode assigns each exchange and all frames within the exchange a unique OX_ID. This mode will correctly report sequence errors, unaccounted frames and out-of-order frames in both S_ID / D_ID and S_ID / D_ID / OX_ID routing environments.

When testing ISLs or SAN equipment where routing policies are based on S_ID / D_ID / OX_ID, the **Multi-frame Exchange Incrementing** mode is the only configuration that will provide valid test results specifically for out of sequence or unaccounted frames analysis.

Refer to `TrafficOxidBase` and `TrafficOxidStep` functions for more information on user configuration of these values.

- **Single-frame Exchange Incrementing**
  For a given Physical N_Port, the value of the OX_ID increases by one for each consecutive frame transmitted by the Load Tester. The lower and upper bounds can be specified by the user.

  Refer to `OxidMin` and `OxidMax` functions in the API Help for more information.

- **Single-frame Exchange Random**
  For a given Physical N_Port, the value of the OX_ID will be random between a lower and upper bound. The OX_ID value varies in a pseudo random manner, changing for each consecutive frame transmitted. The lower and upper bounds can be specified by the user. Refer to `OxidMin` and `OxidMax` functions in the API Help for more information.

Additional Clarification

The **Single-frame Exchange Incrementing** and **Single-frame Exchange Random** OX_ID test modes send test frames that vary the OX_ID of each successive frame sent. Incrementing or Random OX_ID modes can be used to test for single-frame exchanges that are received in an order different than how they were transmitted. When testing in this configuration, the Unaccounted Frames and Sequence Errors counters will be set to 0 and should be ignored. Because the Fibre Channel specification does not explicitly define in-order or out-of-order exchanges the column heading “Out of Order Frames” should be interpreted as “single-frame exchanges received in an order other than the order transmitted.”

OX_ID Minimum

Displays the minimum value to be used for OX_ID when the OX_ID mode is set to **Single-frame Exchange Incrementing** or **Single-frame Exchange Random**.

Refer to the `OxidMin` function in the API Help for more information.

OX_ID Maximum

Displays the maximum value to be used for OX_ID when the OX_ID mode is set to **Single-frame Exchange Incrementing** or **Single-frame Exchange Random**.

Refer to the `OxidMax` function in the API Help for more information.

OX_ID Seed

Indicates the seed value for the OX_ID in random mode

A seed is a number used to initialize a random number generator. The random generator is initialized once using the seed and then the subsequent patterns will be generated automatically in a random manner. Refer to **Single-frame Exchange Random** OX_ID Mode discussed above.

You can also refer to the `OxidSeed` function in the API Help system on the product USB drive for more information.

RSCN

Indicates whether or not this port register to receive Registered State Change Notifications (RSCN) from the Fabric

Flow Control

This category displays the flow control settings of the port.

PFC Override

Indicates whether the PFC Pause frames are enabled. If enabled PFC Pause frames are detected and transmitted, otherwise non-PFC Pause frames are detected and transmitted.

RX Pause Detect Delay

Indicates the delay for the detection of frames. The step-size for this value is 51.2 ns (1 quanta).

RX Pause Detect Mask

Indicates the specified classes of service that will be lossy based on a bitmask. Lossy channels ignore received pause frames.

SFP Status

Indicates the status of the Small Form-factor Pluggable (SFP) optical transceiver

SFP Rx Power

Indicates the SFP Rx power of the port

See `get_SFPRxPower` in the API Help.

SFP Tx Power

Indicates the SFP Tx power of the port

See `get_SFPTxPower` in the API Help.

SFP Make

Indicates the SFP Make number of the port

See `get_SFPMake` in the API Help.

SFP Model

Indicates the SFP Model of the port

See `get_SFPModel` in the API Help.

Errors Counters

Contains all the errors reported back to Load Tester when statistics are updated

FC CRC Errors

Displays number of CRC Errors

See `get_CRCErrors` in the API Help.

Ethernet CRC Errors

Displays number of Ethernet CRC Errors

See `get_CRCErrorsEthernet` in the API Help.

Alignment Errors

Indicates the number of times the FCoE **portid** has left the Aligned/Locked state

See `get_RxLostAlignmentCountEthernet` in the API Help.

Sequence Errors

Displays number of Sequence Errors

See `get_FrameSequenceErrors` in the API Help.

Out Of Order

Indicates number of Out of Order Frame Errors. An Out Of Order error occurs when a frame arrives that is not the expected successor (increased by one). Refer to the `get_FrameOutOfOrderErrors` function in the API Help for more information.

Unaccounted Frames

Displays number of unaccounted frames. An unaccounted frame occurs when then one or more frames have not arrived when the final frame of the sequence arrives. Refer to the `get_FrameDroppedErrors` function in the API Help for more information.

Misdirected

Displays the number of Misdirected Errors. A misdirected error occurs when a frame arrives that was not destined for the selected load tester port. Misdirected frames are Load Tester Data frames (for SAN that means SCSI Data frames, for LAN this could mean TCP/UDP frames) with meta data that were sent to the wrong Load Tester port. In the meta data there is a field that specifies the destination load tester port. If this field doesn't match the receiving port, then the misdirected frame counter increments by 1.

Refer to the `get_FrameMisdirectedErrors` function in the API Help for more information.

Frame Flooded Errors

Displays the number of flooded frames received by the port. All unicast frames that are received are compared against the list of addresses. If the incoming frame's destination MAC address doesn't match then the flooded frame counter increments by 1.

Additional Information on Error Counters

The following error counters are tracked by the Load Tester receiver on a PER STREAM basis. The Load Tester can track 512/1024 streams per receiver. The following descriptions assume Exchange Length equal to 32.

Sequence Errors

Displays the number of sequence errors. The sequence error counter increments anytime the SEQ_CNT of the current frame is not equal to the last frame's SEQ_CNT+1.

Note: Unaccounted frames, out of order frames, CRC errors, Disparity errors, and Code Violations will all lead to Sequence errors.

Unaccounted Frames

Displays the number of unaccounted frame. Each stream is similar to a unidirectional exchange consisting of a single sequence of 32 frames. The Load Tester remembers the SEQ_CNT of all the frames in the current pending exchange. When the final frame of the exchange arrives, a 32-bit memory is evaluated and the unaccounted frame counter is incremented for each missing frame.

Note: Due to a limitation of the Load Tester if the frame with SEQ_CNT=31 is dropped by the switch, the unaccounted frames counter will NOT increment, but the SEQUENCE error count will increment. Frames dropped by switch with SEQ_CNT=0-30 will all increment the unaccounted frame counter. This is assuming Exchange Length is equal to 32.

Warning: All frames with CRC errors will be discarded by the Load Tester receiver "prior" to doing unaccounted frame evaluation. This is by design, since the data integrity of all fields in a frame with a CRC error is uncertain. For example, if a frame arrives with SEQ_CNT=30 AND also has a CRC Error, then it is discarded by the Load Tester, and when the final frame with SEQ_CNT=31 for the exchange arrives, a 32-bit memory will be evaluated and it will show that the frame with SEQ_CNT=30 did not arrive and the unaccounted frame counter will be incremented. In general, frames with code violations or running disparity errors will also lead to a CRC error.

Out of Order

An out of order frame counter increases if the SEQ_CNT of the current frame is less than the SEQ_CNT of the last frame.

Error Counter Example:

The following example assumes Exchange Length equal to 32.

If for a particular stream, frames arrive with the following SEQ_CNT's:

```
0,1,3,2,4,5,6,8,9,...,31
```

Error Counter Summary for this stream:

Number of Sequence errors: 3

Out of order errors: 1

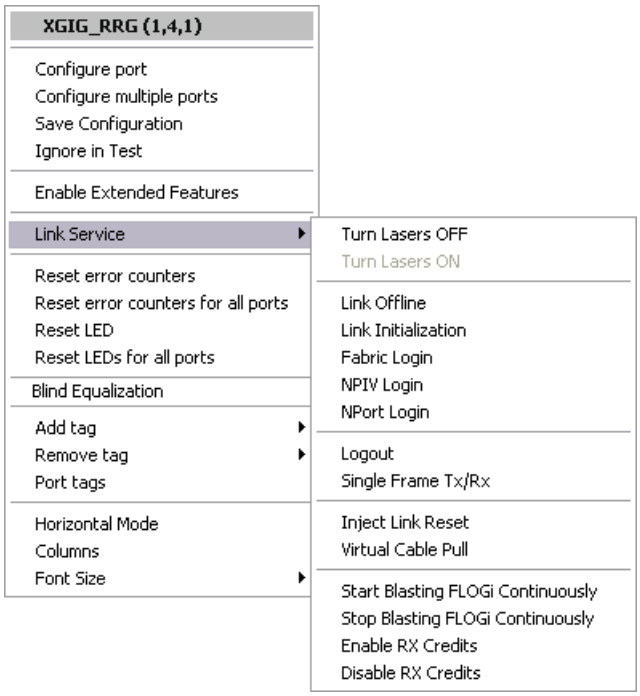
Unaccounted frames: 1

(evaluated when frame with SEQ_CNT=31 arrives to allow immediate trigger)

Using the Parameters Context Menu for Fibre Channel Ports

Right-click anywhere in the port column to display the context menu for that port. This menu is shown in Figure 14.

Figure 14: Load Tester Parameters context menu



The Parameters context menu contains the following options:

Configure port

Directs to **FC Ports Configuration** tab in the Load Tester Device Window.

For more information on the options in the **FC Ports Configuration** tab, refer to Using the Ports Configuration Tabs.

Configure multiple ports

Directs to FC Ports Configuration tab in the Load Tester Device window. For more information, refer to Using the Ports Configuration Tabs.

Save Configuration

Directs to the **Save Load Tester Configuration As** dialog where you may save the configuration under the folder and name of your choice. The configuration cannot be saved and the **Save Configuration...** option is inactive when Load Tester is in the offline state because the corresponding API "get_ConfigurationAsTCL" cannot be used in offline mode. You can only save after the connection is restored.

Ignore in Test

Directs the port to be ignored during testing and the port state is identified as **Ignored in Test**. When activated and the port is ignored, this selection is replaced with **Reactivate in Test**.

Link Service

Opens the sub-menu for link service options listed below:

Turn laser OFF

Turns the laser off

Turn laser ON

Turns the laser on

Link Offline

Takes the port(s) offline, and sets the Desired State of the port(s) to "Offline".

Link Initialization

Enables the hardware LISM engine for the port(s), and set the Desired State of the port(s) to "Link Active". If successful, the hardware LISM engine will enter the Active state and transmit the IDLE primitive. This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Fabric login

Logs into and registers with the Fabric with the port(s) specified, and sets the Desired State of the port(s) to "Logged in to Fabric".

The port(s) will send Fabric Login (FLOGI) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI), Register FC Types (RFT_ID), and State Change Registration (SCR) to the Directory Server (Well Known Address 0xFFFFFC).

This function will operate in accordance with the settings of the login retry count and login retry delay values. If the Fabric login is unsuccessful, the state of the port(s) will be "Port Failure".

NPIV login

Logs the port to the switch and will attempt to acquire Virtual Ports from the Fabric, and set the Desired State of the port(s) to "NPIVs Logged In". The number of Virtual Ports to acquire per port is set via the `NPIVports()` function.

The port(s) will send Fabric Discover (FDISC) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI) and Register FC Types (RFT_ID) to the Directory Server (Well Known Address 0xFFFFFC) if a Virtual ID (NPIV) was successfully acquired.

This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

NPort login

Send Port Login (PLOGI) frames to all Load Tester ports present in the Fabric, and set the Desired State of the port(s) to "Logged In". The port(s) will send a Get Port Identifiers (GID_PT) to the Directory Server, to discover the available Load Tester ports in the Fabric zone. It will then send PLOGI frames to the available Load Tester ports.

This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Load Tester is able to discover the Port IDs in the zone by issuing NPort Login and bypassing Fabric Login. If Fabric Login was issued first, NPort Login will use the Port IDs issued by the Fabric.

Logout

Sends a Port Logout to the Fabric for the port(s) specified, and set the Desired State of the port(s) to "Link Active". This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Inject Link Reset

Resets the credit count for the port(s) by entering the LR1 State, and following the Link Reset protocol.

Virtual Cable Pull

Turns the port(s) laser off and then back on to simulate a cable pull while a test is running. The port(s) will automatically attempt to Login, and if successful, will resume running the test.

Start Blasting FLOGi Continuously

Initiates a continuous Blast FLOGI test.

Blast FLOGI is a special error mode for testing Switch recovery. The Load Tester ports blasts a canned FLOGI frame at the switch continuously.

Stop Blasting FLOGi Continuously

Stops the continuous FLOGi blast.

Enable RX Credits

Instantly adjusts the Rx buffer-to-buffer credits of the physical port, which will be used in the Fabric Login and Port Login frames.

Disable RX Credits

Turns off the Rx buffer-to-buffer credits adjustment of the physical port

Reset error counters

Resets all the error counters of the Port

Reset error counters for all ports

Resets all the error counters of all locked ports

Reset LED

Resets the status LED for the port on the Xgig blade and the Parameters Status table

Reset LEDs for all ports

Reset the status LEDs for all the locked ports on the Xgig blade and the Parameters Status table

Blind Equalization

Resets the SERDES to help synchronize to wire data. This option is only visible when the ports are 8G.

Add tag

Lets you add a tag alias to a port

To add a tag using the context menu:

1. Right-click on the port to open the Parameters context menu.
2. Click on **Add tag**.
3. Select the tag to add to the port (Figure 15).

Figure 15: Add tag

To create a new tag and add it to the port:

1. Select **[New Tag]**. This will open the **Create New Tag** dialog box.
2. Enter a name for the new tag.
3. Click **Ok** to save the new tag and add it to the port.

Remove tag

Lets you remove a tag from the port

To remove a tag using the context menu:

1. Right-click on the port to open the Parameters context menu.
2. Click on **Remove tag**.

3 Select the tag to remove from the port (Figure 16).

Figure 16: Remove tag

Port tags

Displays a list of all tags that have been applied to the port

For more information about creating or editing tags, refer to Chapter 4: "Creating Tags".

Horizontal Mode

Displays the port as rows and the parameters as columns.

To return to default layout for the ports:

1 Right-click on the port to open the Parameters context menu.

2 Click on **Vertical Mode**.

Columns

Opens the **Customize Band** dialog box where you can select which parameters to show in the Parameters Status Table when the display is in Horizontal Mode.

To select or unselect the parameters to show as columns:

1 Select the **Visibility** radio button.

2 Click on the check boxes of the parameters to display or hide.

3 Click **OK** when you are done.

To arrange the sequence of columns displayed:

1 Select the **Sorting** radio button.

2 Click and drag the parameter names according to your preferred sequence.

3 Click **OK** when you are done.

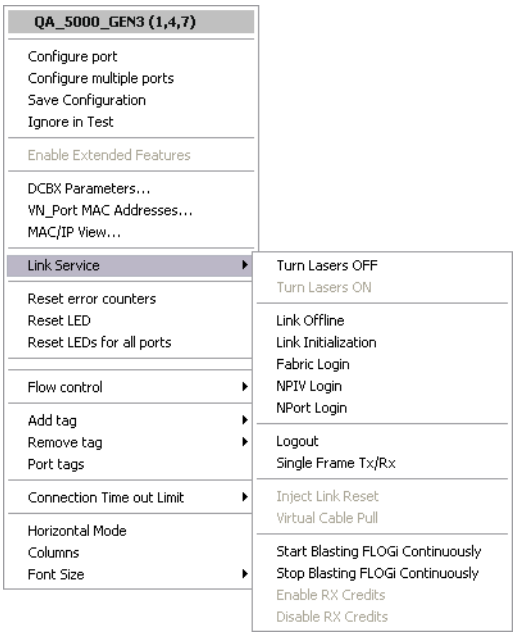
Font Size

Lets you select the size of the text used in the Parameters Status Table.

Using the Parameters Context Menu for FCoE Ports

Right-click anywhere in the port column to display the context menu for that port. This menu is shown in Figure 17.

Figure 17: Load Tester Parameters Context Menu



The Parameters context menu contains the following options:

Configure port

Directs to **10G Ports Configuration** tab in the Load Tester Device Window.

For more information on the options in the **10G Ports Configuration** tab, refer to Using the Ports Configuration Tabs.

Configure multiple ports

Directs to 10G Ports Configuration tab in the Load Tester Device window. For more information, refer to Using the Ports Configuration Tabs.

Save Configuration

Directs to the S**ave Load Tester Configuration As** dialog where you may save the configuration under the folder and name of your choice.

The configuration cannot be saved and the **Save Configuration...** option is inactive when Load Tester is in the offline state because the corresponding API "get_ConfigurationAsTCL" cannot be used in offline mode. You can only save after the connection is restored.

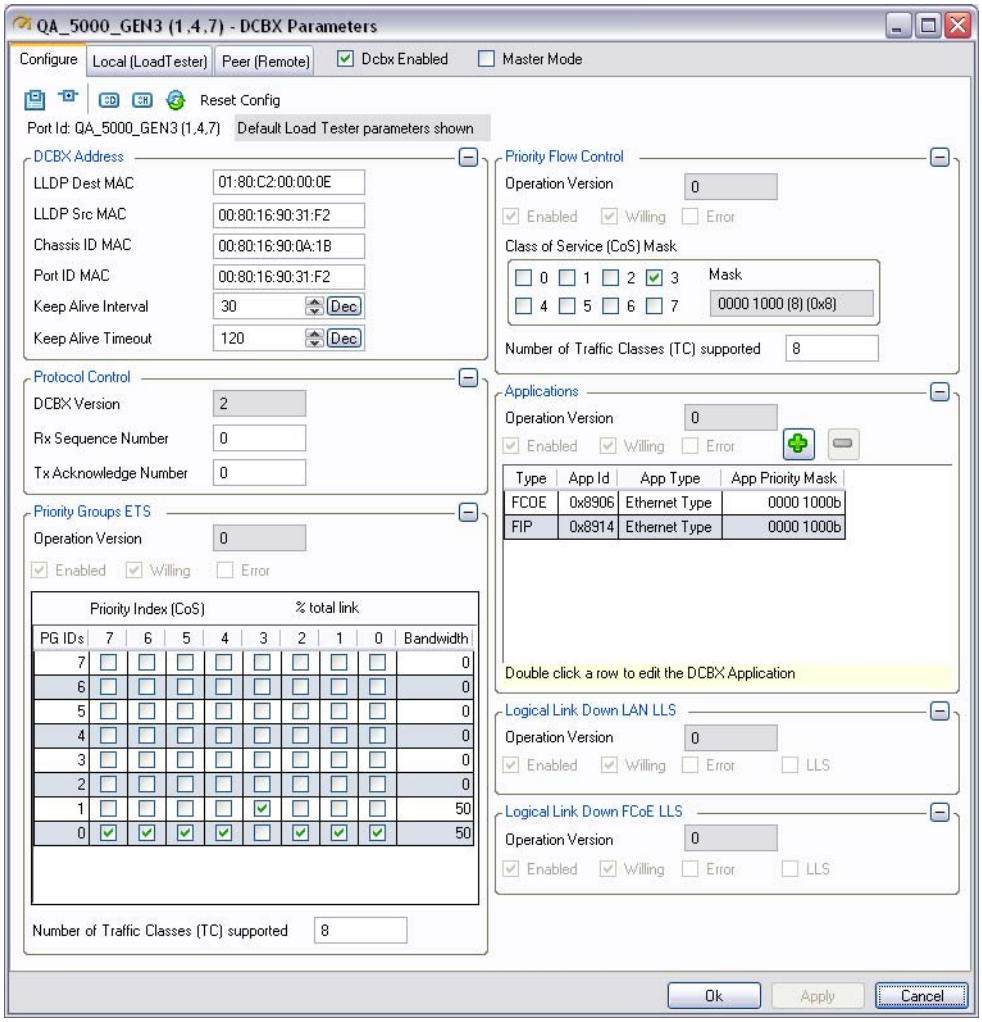
Enable Extended Features

Enables and disables the supported extended feature set for the port. As part of this process other extended feature set member ports WILL also be enabled or disabled. This function is only allowed while the port is in the LaserDisabled or OffLine state. A disabled port that is in an "Ignored in Test" will not block this option.

DCBX Parameters

Opens the **DCBX Parameters** window (Figure 18) where you can view the Load Tester port's DCBX settings.

Figure 18: DCBX Parameters Window



VN_Port MAC Addresses

Opens the VN_Port Addresses window that lists the VN_Port Addresses and details.

MAC/IP View

Opens the MAC/IP View window that lists the IP and Ethernet Addresses and details.

Link Service

Opens the sub-menu for link service options listed below:

Turn laser OFF

Turns the laser off

Turn laser ON

Turns the laser on

Link Offline

Takes the port(s) offline, and sets the Desired State of the port(s) to "Offline".

Link Initialization

Enables the hardware LISM engine for the port(s), and set the Desired State of the port(s) to "Link Active". If successful, the hardware LISM engine will enter the Active state and transmit the IDLE primitive. This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Fabric login

Logs into and registers with the Fabric with the port(s) specified, and sets the Desired State of the port(s) to "Logged in to Fabric".

The port(s) will send Fabric Login (FLOGI) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI), Register FC Types (RFT_ID), and State Change Registration (SCR) to the Directory Server (Well Known Address 0xFFFFFC).

This function will operate in accordance with the settings of the login retry count and login retry delay values. If the Fabric login is unsuccessful, the state of the port(s) will be "Port Failure".

NPIV login

Logs the port to the switch and will attempt to acquire Virtual Ports from the Fabric, and set the Desired State of the port(s) to "NPIVs Logged In". The number of Virtual Ports to acquire per port is set via the `NPIVports()` function.

The port(s) will send Fabric Discover (FDISC) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI) and Register FC Types (RFT_ID) to the Directory Server (Well Known Address 0xFFFFFC) if a Virtual ID (NPIV) was successfully acquired.

This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

NPort login

Send Port Login (PLOGI) frames to all Load Tester ports present in the Fabric, and set the Desired State of the port(s) to "Logged In". The port(s) will send a Get Port Identifiers (GID_PT) to the Directory Server, to discover the available Load Tester ports in the Fabric zone. It will then send PLOGI frames to the available Load Tester ports.

This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Logout

Sends a Port Logout to the Fabric for the port(s) specified, and set the Desired State of the port(s) to "Link Active". This function will operate in accordance with the settings of the login retry count and login retry delay values. If unsuccessful, the state of the port(s) will be "Port Failure".

Inject Link Reset

Resets the credit count for the port(s) by entering the LR1 State, and following the Link Reset protocol.

Virtual Cable Pull

Turns the port(s) laser off and then back on to simulate a cable pull while a test is running. The port(s) will automatically attempt to Login, and if successful, will resume running the test.

Start Blasting FLOGi Continuously

Initiates a continuous Blast FLOGI test.

Blast FLOGI is a special error mode for testing Switch recovery. The Load Tester ports blasts a canned FLOGI frame at the switch continuously.

Stop Blasting FLOGi Continuously

Stops the continuous FLOGi blast.

Reset error counters

Resets all the error counters of the Port

Reset error counters for all ports

Resets all the error counters of all locked ports

Reset LED

Resets the status LED for the port on the Xgig blade and the Parameters Status table

Reset LEDs for all ports

Reset the status LEDs for all the locked ports on the Xgig blade and the Parameters Status table

Flow Control

Opens the sub-menu for the following flow control options:

Start sending pause frames

Starts sending pause frames continuously based on mode. This function invokes all ports to start sending pause frames continuously based on the mode.

Note: For 10G 2-port blades, pause frames generation is only available for odd ports.

Stop sending pause frames

Stops sending pause frames on the ports specified.

Send one pause frame

This function invokes all ports to send a single pause frame.

Note: For 10G 2-port blades, pause frames generation is only available for odd ports.

Add tag

Lets you add a tag alias to a port

To add a tag using the context menu:

1. Right-click on the port to open the Parameters context menu.
2. Click on **Add tag**.
3. Select the tag to add to the port (Figure 19).

Figure 19: Add Tag

To create a new tag and add it to the port:

1. Select **[New Tag]**. This will open the **Create New Tag** dialog box.
2. Enter a name for the new tag.
3. Click **Ok** to save the new tag and add it to the port.

Remove tag

Lets you remove a tag from the port.

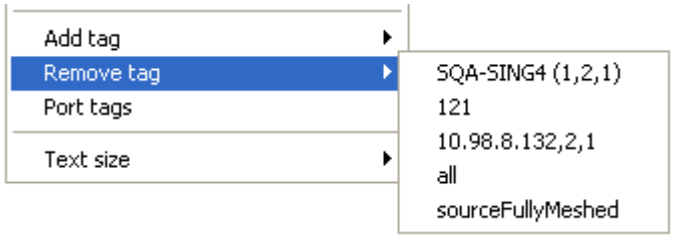
To remove a tag using the context menu:

1 Right-click on the port to open the Parameters context menu.

2 Click on **Remove tag**.

3 Select the tag to remove from the port (Figure 20).

Figure 20: Remove tag



Port tags

Displays a list of all tags that have been applied to the port

For more information about creating or editing tags, refer to Chapter 4: "Creating Tags".

Horizontal Mode

Displays the port as rows and the parameters as columns.

To return to default layout for the ports:

1 Right-click on the port to open the Parameters context menu.

2 Click on **Vertical Mode**.

Columns

Opens the **Customize Band** dialog box where you can select which parameters to show in the Parameters Status Table when the display is in Horizontal Mode.

To select or unselect the parameters to show as columns:

1 Select the **Visibility** radio button.

2 Click on the check boxes of the parameters to display or hide.

3 Click **OK** when you are done.

To arrange the sequence of columns displayed:

1 Select the **Sorting** radio button.

2 Click and drag the parameter names according to your preferred sequence.

3 Click **OK** when you are done.

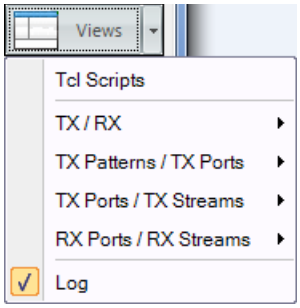
Font Size

Lets you select the size of the text used in the Parameters Status Table.

Traffic Tab

The Traffic tab contains live traffic statistics information about the Load Tester ports' TX and RX data paths. The Traffic tab is divided into sub-tabs, the TX tab (refer to Figure 24 on page 67) and the Rx tab (refer to Figure 27 on page 74).

Figure 21: Traffic Tab Views Drop-down List

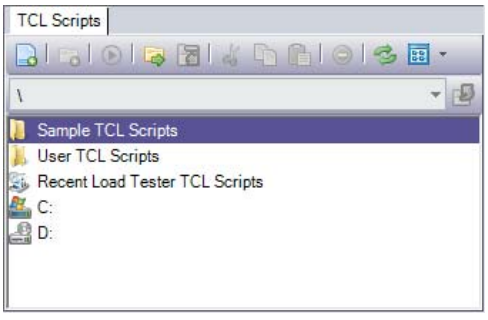


- Under the TX tab, there are two additional sub-tabs:
  - TX Pattern Based View tab
  - TX Port Based View tab
- Under the RX tab, there are two spreadsheet pane views:
  - RX Physical Ports pane
  - RX Streams pane
- A Tcl scripts manager (Figure 22) is also found in the Traffic tab by selecting Tcl Scripts from the Views drop-down list

  The Tcl Scripts Manager allows you to create, edit and manage Tcl script files.

Using the TCL Scripts Manager

Figure 22: Tcl Scripts Manager



Create a New Tcl Script

To create a new Tcl script file:

1 Click **New TCL Script** button. The **New TCL Script - Script Viewer** appears. See Figure 23.

2 Enter the Tcl script.

3 Click on **Save**. The **Save TCL Script** as window appears.

4 Double-click the folder where you want to save the Tcl Script file.

To save the Tcl script file to a different folder, or to map a new folder, click **Map Folder**. In the **Map Folder** dialog box, enter the name for the folder to map in the **Mapped Folder Name** text box.

Enter the path of the folder to map, or click **Browse** to locate it.

Click **Ok**. The new folder will be added to the list of mapped folders.

5 Enter the name of the file in the **File name** text box.

6 Click **Save**.

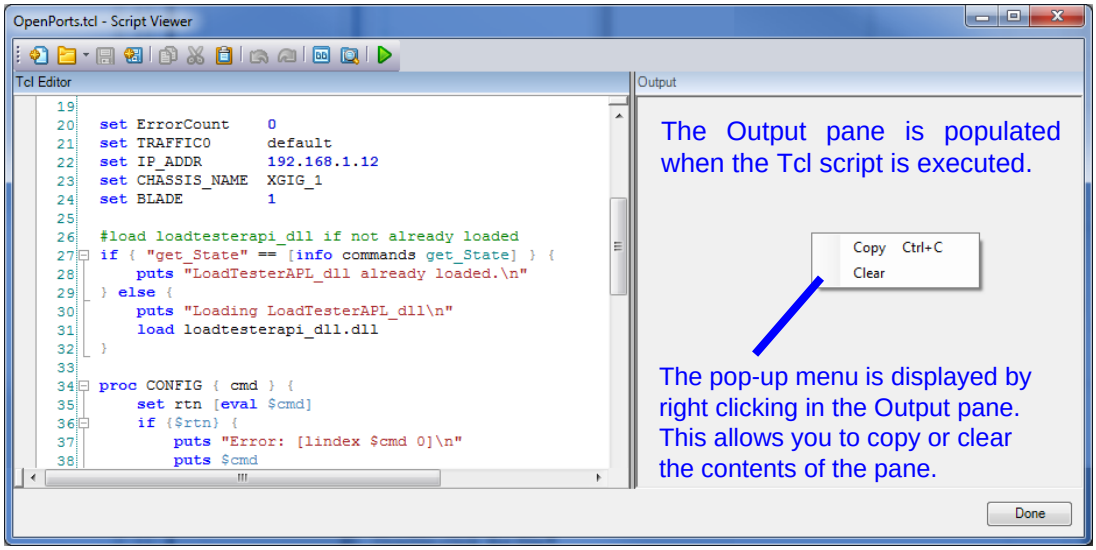
Open a Saved Tcl Script

To open a saved Tcl script:

1 Double-click the folder where the file is located.

2 Double-click the file.

Figure 23: Tcl Script - Script Viewer



The script editor is IDE-like. Each type of text has a unique color associated with it.

Color	Text Type	Color	Text Type
Blue	Keywords	Green	Comments
Brown	Strings	Gray	Operator
Steel Blue	Variable	Teal	API
Black	All other		

Run a Saved Tcl Script

To run a saved Tcl script:

1 Open the script file.

2 From the script viewer, click **Run**.

TX Pattern Based View

The Pattern Based View tab lists all configured traffic patterns and the participating ports of each traffic pattern. From this tab you can create, copy, edit and delete traffic patterns. Additionally, you can adjust the average load of each port in the selected traffic patterns in real time using the incremental load adjuster or pause and resume the selected traffic pattern. You can also reset the load to the default value.

The details for each traffic pattern are displayed in columns. Each column represents a particular property of that traffic pattern. You may need to scroll horizontally to see all the columns.

By default, you have a sample traffic pattern in the Pattern Based View named “default”. You can edit this traffic pattern for your needs.

On top of the list of traffic patterns there are several buttons for editing the traffic patterns. Below is a table with the descriptions of the buttons.

Table 3: Traffic Pattern operation buttons

Icon	Description
	**Create new Traffic Pattern** - click to create a new traffic pattern. The **Traffic Pattern Editor** tab in the Load Tester Device Window will open.
	**Copy Traffic Pattern** - click to copy the selected traffic pattern. The **Traffic Pattern Editor** tab in the Load Tester Device Window will open with the name of the selected traffic pattern appended with the suffix “(Copy)”. You can also rename the traffic pattern Label.
	**Edit selected Traffic Pattern** - click to edit the selected traffic pattern. The **Traffic Pattern Editor** tab in the Load Tester Device Window box will open.
	**Delete selected Traffic Pattern** - click to edit the selected traffic pattern. The **Traffic Pattern Editor** tab in the Load Tester Device Window box will open.
	**View** - Opens the **Traffic Pattern View** for the selected traffic pattern where the traffic configuration details are displayed.
	**% Increment Average Load** - Increases the average load of the traffic pattern by the specified delta.
	**% Decrement Average Load** - Decreases the average load of the traffic pattern by the specified delta.
	**Return loads to default value** - Returns the load to the value set in the Traffic Pattern configuration.
	**Pause** - Pauses all enabled profiles on the specified port(s). This function does not change the enabled/disabled state of the individual profiles and the flow control sending status.
	**Resume** - Resumes all paused profiles on the specified port(s). This function does not change the enabled/disabled state of the individual profiles and the flow control sending status.
	**Clear Filter** - Removes all the filters that have been applied.
	**Display % PFC Paused Tx Bandwidth for port** - Opens the **Percentage of PFC Paused Tx Bandwidth** window.

To inject errors during a test (this only applies to FC ports):

1. Click **Inject Errors**.
2. Select **Inject One Code Violation Error** to inject a coding violation on Byte 0 to the ports. The illegal character that is sent is composed of a 6-bit part and a 4-bit part. This selection is active only on 4G and 8G ports
3. Select **Inject One Disparity Error** to inject a disparity error on Byte 3 to the ports. It will flip the disparity on Byte 3. This selection is active only on 4G and 8G ports
4. Select **Inject One Bit Error** to inject one bit error in the 64-bit frame data. This selection is active only on 16G ports that are set at a 16G speed.

Note: When Load Tester receives a frame with EOFni (End of Frame Normal, Frame Contents Invalid), that frame is flagged with a CRC error (even if the frame had no actual CRC error.) This is done to increase the visibility of abnormal frames.

An EOFni could be caused when an error is injected (as in the previous procedure) or for a variety of other instances that would cause the frame to be recognized as having an error.

To send pause frames (available only for FCoE ports):

1. Click **Flow Control**.
2. Select **Start sending pause frames** to start sending pause frames continuously based on mode.
3. Select **Stop sending pause frames** to stop sending pause frames on ports specified.
4. Select **Send one pause frame** to invoke all ports to send a single pause frame.

To show or hide traffic values:

Click **Static** to show or hide static traffic values.

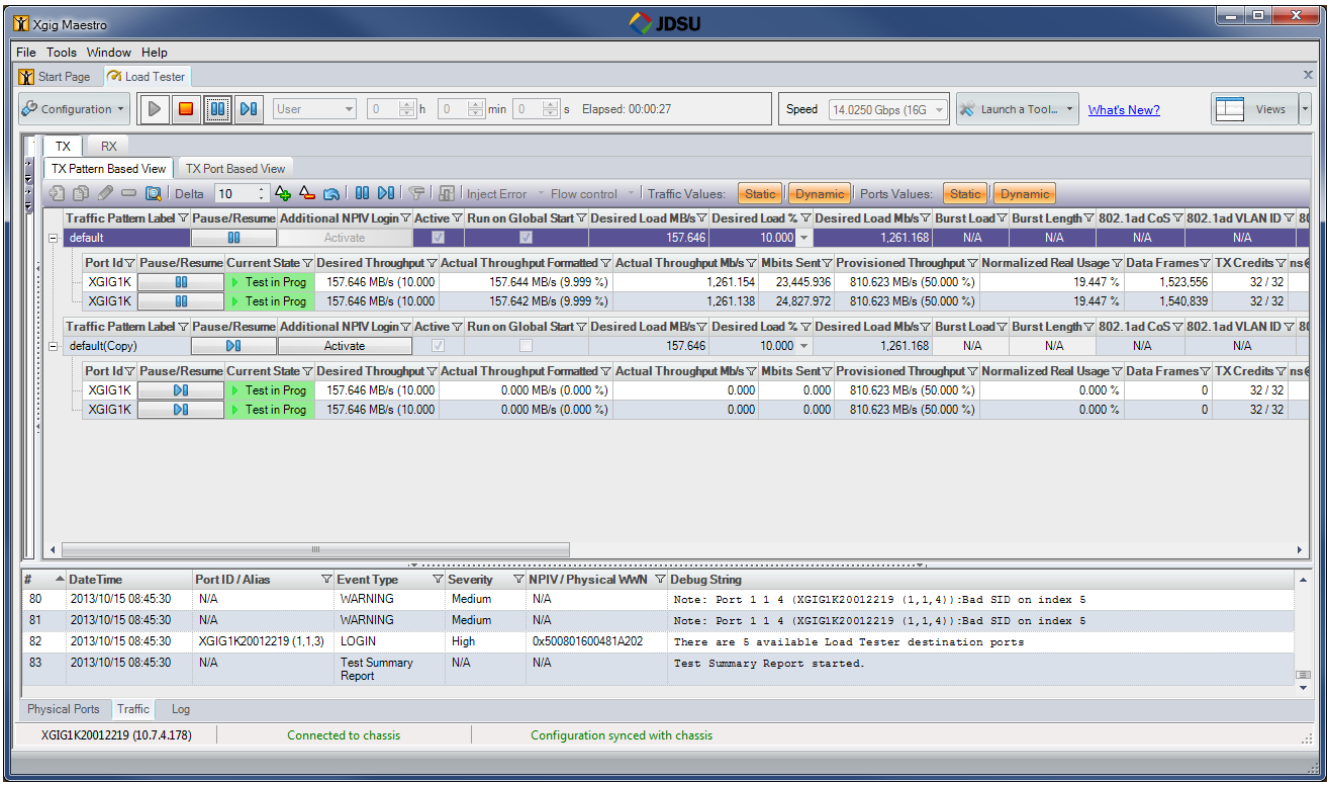
Click **Dynamic** to show or hide dynamic traffic values.

To show or hide ports values:

Click **Static** to show or hide static ports values.

Click **Dynamic** to show or hide dynamic ports values.

Figure 24: TX Pattern Based View Tab



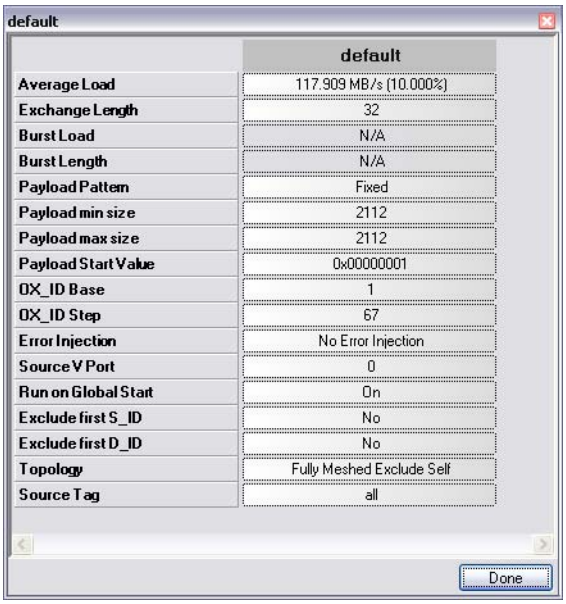
The main or top level bands represent the traffic patterns. Clicking on the expand button (represented by the cross icon) will expand the band and show the ports used in that traffic pattern.

Right-clicking on the TX window will bring up the context menu. Depending on where you right-click in the TX window, different options will appear in the context menu.

If you right-click on the Traffic Pattern band or row, the following options will be displayed:

- **Add new Traffic Pattern** - Opens the **Traffic Pattern Editor** tab in the Load Tester Device Window to allow the user to create a new traffic pattern
- **Copy Traffic Pattern** - Opens the **Traffic Pattern Editor** tab in the Load Tester Device Window to allow the user to create a new traffic pattern using the same settings as the selected traffic pattern
- **Edit Traffic Pattern** - Opens the **Traffic Pattern Editor** tab in the Load Tester Device Window to allow the user to edit the selected traffic pattern
- **Delete Traffic Pattern** - Deletes the selected traffic pattern
- **View Traffic Pattern** - Opens the **Traffic Pattern View** window (Figure 25) that displays configuration settings of the selected traffic pattern

Figure 25: Traffic Pattern View



- **Pause** - Pauses the current test.
- **Resume** - Resumes the current test.
- **Reset Counters for all ports** - Resets all counters of the ports in the traffic pattern.
- **Columns** - Opens the Columns dialog box where you can select which columns to display.
- **Collapse All** - Collapse all expanded bands.
- **Expand All** - Expands all collapsed bands.
- **Hide Filters** - Hides the filter icons.
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern.
- **Font Size** -Selects the size of the text used for the traffic pattern table.

If you right-click on the port band or row, the following will be the options:

- **Add Traffic Pattern** - Opens the Traffic Pattern Configuration Dialog Box to allow the user to create a new traffic pattern.
- **Pause** - Pauses the traffic on the selected port of the traffic pattern.
- **Resume** - Resumes the traffic on the selected port of the traffic pattern.
- **Reset Counters** - Resets all counters of the port.
- **Reset Counters for all ports** - Resets all counters of the ports in the traffic pattern.
- **Port Properties** - Opens a message box that list the properties of the port.
- **Port Tags** - Opens a message box that displays the tags.
- **Flow Control** - Displays additional options to **Start sending pause frames**, **Stop sending pause frames**, and **Send one pause frame** (available only for FCoE ports).
- **Inject Error** - Lets you **Inject One Code Violation Error** or **Inject One Disparity Error** (available only for FC ports).

- **Columns -** Opens the Columns dialog box where you can select which columns to display.
- **Hide Filters -** Hides the filter icons.
- **Clear Filter -** Removes all applied filters for the selected Traffic Pattern.
- **Font Size -** Lets you select the size of the text used for the traffic pattern table.

TX Port Based View

The TX Port Based View sub-tab is divided into two panels: the Port Based View and the TX Streams panel.

Port Based View

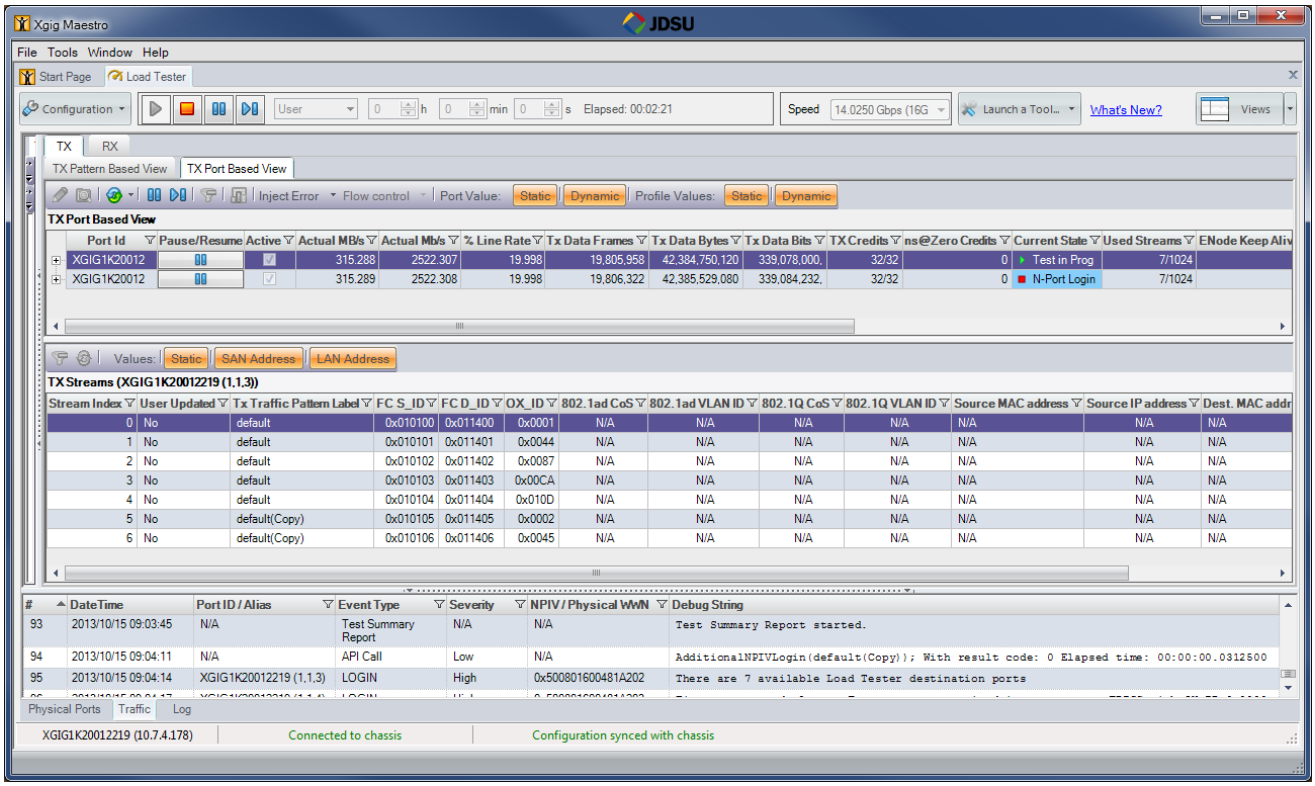
The Port Based View shows all reserved (locked) ports and their profiles (refer to Figure 26). Each port can have up to n profiles, numbered from 0 to n-1, where n is 4, 6, or 8 depending on the specific blade hardware. Each profile is associated with one traffic pattern. A single physical port can allocate up to n traffic profile engines each representing a traffic pattern.

Table 4: Number of Profiles by Blade Type

FC Port Blades	FCoE Port Blades
FC 16G - 8 profiles FC 8G - 6 profiles FC 4G - 6 profiles	2-port 10G - 4 profiles 8-port 10G blade (8 ports enabled) - 4 profiles 8-port 10G blade (4 ports enabled) - 8 profiles

Note: There is no limit on the number of engines a port can receive from, as long as the configuration does not exceed 1024 RX data streams (1024 = 10 Gig and 16Gig/8 Gig, 512 = 4 Gig).

Figure 26: Tx Port Based View Tab



On top of the list of traffic patterns there are several buttons for editing the traffic patterns. Below is a table with the descriptions of the buttons.

Table 5: TX Port Based View operation buttons

Icon	Description
	**Edit selected Traffic Pattern** - click to edit the selected traffic pattern. The **Traffic Pattern Editor** tab in the Load Tester Device Window will open.
	**View** - Opens the **Traffic Pattern View** for the selected traffic pattern where the traffic configuration details are displayed.
	**Reset Counters**- Clears all counters to 0, not including error counters. The client copy of the counters is updated asynchronously from the server, so a counter refresh interval will have to pass before the client copy of the counters reflect the reset action. Click on the drop-down arrow beside the icon to either reset the Error Counters for a selected port or reset the Error Counters for all ports.
	**Pause** - Pauses all enabled profiles on the specified port(s). This function does not change the enabled/disabled state of the individual profiles and the flow control sending status.
	**Resume** - Resumes all paused profiles on the specified port(s). This function does not change the enabled/disabled state of the individual profiles.
	**Clear Filter** - Removes all the filters that have been applied.
	**Display % PFC Paused Tx Bandwidth for port** - Opens the **Percentage of PFC Paused Tx Bandwidth** window.

To inject errors during a test (available only for FC ports):

1. Click **Inject Errors**.
2. Select **Inject One Code Violation Error** to inject a coding violation on Byte 0 to the ports. The illegal character that is sent is composed of a 6-bit part and a 4-bit part.
3. Select **Inject One Disparity Error** to inject a disparity error on Byte 3 to the ports. It will flip the disparity on Byte 3.

Note: When Load Tester receives a frame with EOFni (End of Frame Normal, Frame Contents Invalid), that frame is flagged with a CRC error (even if the frame had no actual CRC error.) This is done to increase the visibility of abnormal frames.

An EOFni could be caused when an error is injected (as in the previous procedure) or for a variety of other instances that would cause the frame to be recognized as having an error.

To send pause frames (available only for FCoE ports):

1. Click **Flow Control**.
2. Select **Start sending pause frames** to start sending pause frames continuously based on mode.
3. Select **Stop sending pause frames** to stop sending pause frames on ports specified.
4. Select **Send one pause frame** to invoke all ports to send a single pause frame.

To show or hide traffic values:

Click **Static** to show or hide static traffic values.

Click **Dynamic** to show or hide dynamic traffic values.

To show or hide ports values:

Click **Static** to show or hide static ports values.

Click **Dynamic** to show or hide dynamic ports values.

If you right-click on the port band or row, the following options will be available:

- **Reset Counters** - Resets all counters of the port.
- **Reset Counters for all ports** - Resets all counters of the port.
- **Pause** - Pauses the selected port.
- **Resume** - Resumes the selected port.
- **Port Properties** - Opens a message box that lists the properties of the port.
- **Port Tags** - Opens a message box that displays the tags.
- **Flow Control** - Displays additional options to **Start sending pause frames**, **Stop sending pause frames**, and **Send one pause frame** (available only for FCoE ports).
- **Inject Error** - Lets you inject either **One Code Violation Error** or **One Disparity Error** (available only for FC ports).
- **Columns** - Opens the **Columns** dialog box where you can select which columns to display.
- **Hide Filters** - Hides the filter icons.
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern.
- **Font Size** - Lets you select the size of the text used for the traffic pattern table.

If you right-click on the profile band or row, the following options will be available:

- **Edit Traffic Pattern** - Opens the Traffic Pattern Editor to let you edit the selected traffic pattern.
- **View Traffic Pattern** - Opens the Traffic Pattern View window that displays the properties for the selected traffic pattern.
- **Reset Counters for all ports** - Resets all counters of the port.
- **Pause** - Pauses the selected port.
- **Resume** - Resumes the selected port.
- **Columns** - Opens the **Columns** dialog box where you can select which columns to display.
- **Hide Filters** - Hides the filter icons.
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern.
- **Font Size** - Lets you select the size of the text used for the traffic pattern table.

TX Streams

The TX Streams panel lists all the TX Streams for the selected port.

Below is a table with the descriptions of the operation buttons for the TX Streams View.

Table 6: TX Streams View operation buttons

Icon	Description
	**Reset Streams** - Resets all content on TX Streams.
	**Clear Filter** - Removes all the filters that have been applied.

The TX Streams view lists this column (value) by default:

Stream Index

To show or hide port values:

Click **Static** to show or hide the stream's static traffic values.

Click **SAN Address** to show or hide the stream's SAN address values.

Click **LAN Address** to show or hide the stream's LAN address values.

Table 7: The columns (values) associated with each button are:

Static	User Updated TX Traffic Pattern Label 802.1ad CoS 802.1ad VLAN ID 802.1Q CoS 802.1Q VLAN ID Source MAC address Destination MAC address

SAN Address	FC S_ID FC D_ID OX_ID
LAN Address	Source IP address Destination IP address

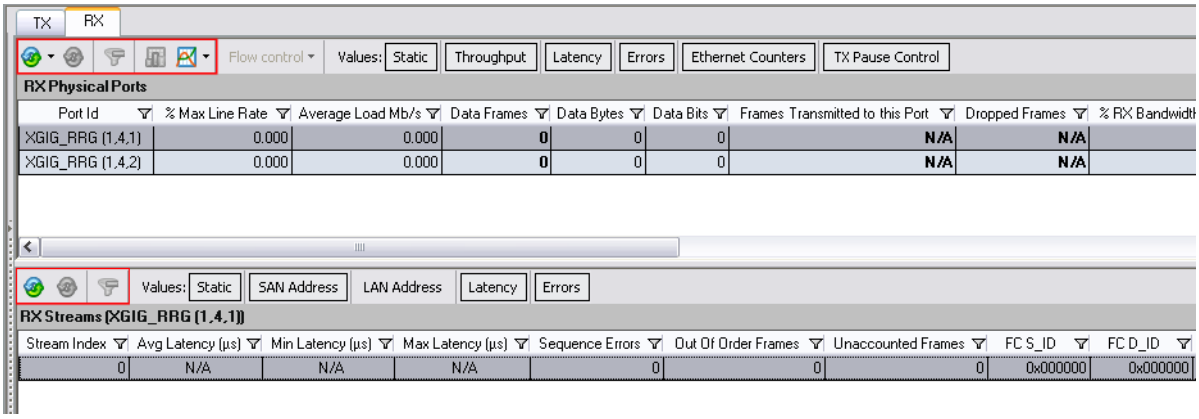
If you right-click on the stream band or row, the following options will be available:

- **Columns** - Opens the **Columns** dialog box where you can select which columns to display
- **Hide Filters** - Hides the filter icons
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern
- **Font Size** - Lets you select the size of the text used for the traffic pattern table.

RX Physical Ports

The **Physical Ports View** under the tab's menu bar lists the physical ports locked by this instance of the Load Tester application and displays the statistics associated with the data streams received and processed by the RX data path.

Figure 27: RX Tab



Below is a table with the descriptions of the operation buttons for the RX Physical Ports View.

Table 8: RX Physical Ports View operation buttons

Icon	Description
	Reset Counters- Clears all counters to 0, not including error counters. The client copy of the counters is updated asynchronously from the server, so a counter refresh interval will have to pass before the client copy of the counters reflect the reset action. Click on the drop-down arrow beside the icon to either reset the Error Counters for a selected port or reset the Error Counters for all ports.
	Reset Triggers - Resets all Triggered Frame Errors and content allowing receipt of new Trigger Frames.
	Clear Filter - Removes all the filters that have been applied.
	Display Throughput per Priority Group- Opens the **Display Throughput per Priority Group** window.
	Latency and % of Max Frame Rate Charts - Gives you the option to display either the chart of percentage of the maximum line rate or the latency for a selected port.

The RX Physical Ports view lists this column (value) by default:

Port Id

To send pause frames (available only for FCoE ports):

1. Click **Flow Control**.
2. Select **Start sending pause frames** to start sending pause frames continuously based on mode.
3. Select **Stop sending pause frames** to stop sending pause frames on ports specified.
4. Select **Send one pause frame** to invoke all ports to send a single pause frame.

To show or hide port values:

Click **Static** to show or hide static traffic values.

Click **Throughput** to show or hide the port's throughput values.

Click **Latency** to show or hide the port's latency values.

Click **Errors** to show or hide the port's error values.

Ethernet Counters to show or hide the port's ethernet counter values.

TX Pause Control to show or hide the port's TX Pause control values.

Table 9: The columns (values) associated with each button are:

Static	Port Alias Current State Trigger Source Traffic Profiles Streams Traffic Patterns	**Errors**	Sequence Errors Out Of Order Frames Out Of Order Errors per Data Byte Unaccounted Frames Misdirected Frame Flooded Errors FC CRC Errors Ethernet CRC Errors Code Violations Running Disparity Errors Alignment Errors FEC Parity Errors
Throughput	Max Line Rate Average Load Mb/s' Rx Data Frames Rx Broadcast Data Frames Rx Data Bytes Rx Data Bits Rx Other Frames Rx Other Bytes Frames Transmitted to this Port Dropped Frames*****	**Ethernet Counters**	Unicast Multicast Broadcast FIP Count FCoE VLAN Pause Frames Received iSCSI Packet Octet/Byte Unsolicited Discovery Advertisements
Latency	Avg Latency (µs) Min Latency (µs) Max Latency (µs)	**TX Pause Control**	% RX Bandwidth Paused TX PFC Class Enable Pause Frames Transmitted Enable Rx Credits Credit Delay (ns)

***** Frames targeted at this port by Tx activity but having not yet arrived in the RX are considered dropped. To achieve an accurate count of dropped frames, allow a few seconds for the counter to settle after pausing or stopping the traffic.

If you right-click on the port band or row, the following options will be available:

- **Reset Counters -** Resets all counters for the selected port
- **Reset Counters for all ports-** Resets all counters for all ports.
- **Reset Error Counters -** Resets all error counters for the selected port.
- **Reset Error Counters for all ports -** Resets all error counters for all ports.
- **Reset Trigger** - Resets the triggers applied to this port.
- **Port Properties** - Opens a message box that lists the properties of the port.
- **Port Tags** - Opens a message box that displays the tags.
- **Columns** - Opens the Columns dialog box where you can select which columns to display.
- **Hide Filters -** Hides the filter icons.
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern.
- **Font Size** - Lets you select the size of the text used for the traffic pattern table.

RX Streams

The RX Streams View lists the details of all the 1024 possible streams. Depending on the configuration of the Traffic Patterns in the Load Tester application, there may be up to 1024 RX Streams shown per Physical N_Port (1024 RX Streams for 10G and 8G blades, 4G blades is 512).

Below is a table with the descriptions of the operation buttons for the RX Streams View.

Table 10: RX Streams View operation buttons

Icon	Description
	**Reset Counters**- Clears all counters to 0, not including error counters. The client copy of the counters is updated asynchronously from the server, so a counter refresh interval will have to pass before the client copy of the counters reflect the reset action. Click on the drop-down arrow beside the icon to either reset the counters for a selected port or reset the counters for all ports.
	**Reset Triggers** - Resets all Triggered Frame Errors and content allowing receipt of new Trigger Frames.
	**Clear Filter** - Removes all the filters that have been applied.

The RX Streams view lists these columns (values) by default:

Stream Index
Data Frames
Data Frames per second

To show or hide port values:

Click **Static** to show or hide the stream's static traffic values.

Click **SAN Address** to show or hide the stream's SAN address values.

Click **LAN Address** to show or hide the stream's LAN address values.

Click **Latency** to show or hide the stream's latency values.

Click **Errors** to show or hide the stream's error values.

Table 11: The columns (values) associated with each button are:

Static	TX Traffic Pattern Label 802.1ad CoS 802.1ad VLAN ID 802.1Q CoS Source MAC address Destination MAC address	**LAN Address**	Source IP address Destination IP address
		Latency	Avg Latency (µs) Min Latency (µs) Max Latency (µs)
SAN Address	FC S_ID Source NPIV/Phy WWN FC D_ID Destination NPIV/Phy WWN OX_ID	**Errors**	Sequence Errors Out Of Order Frames Unaccounted Frames

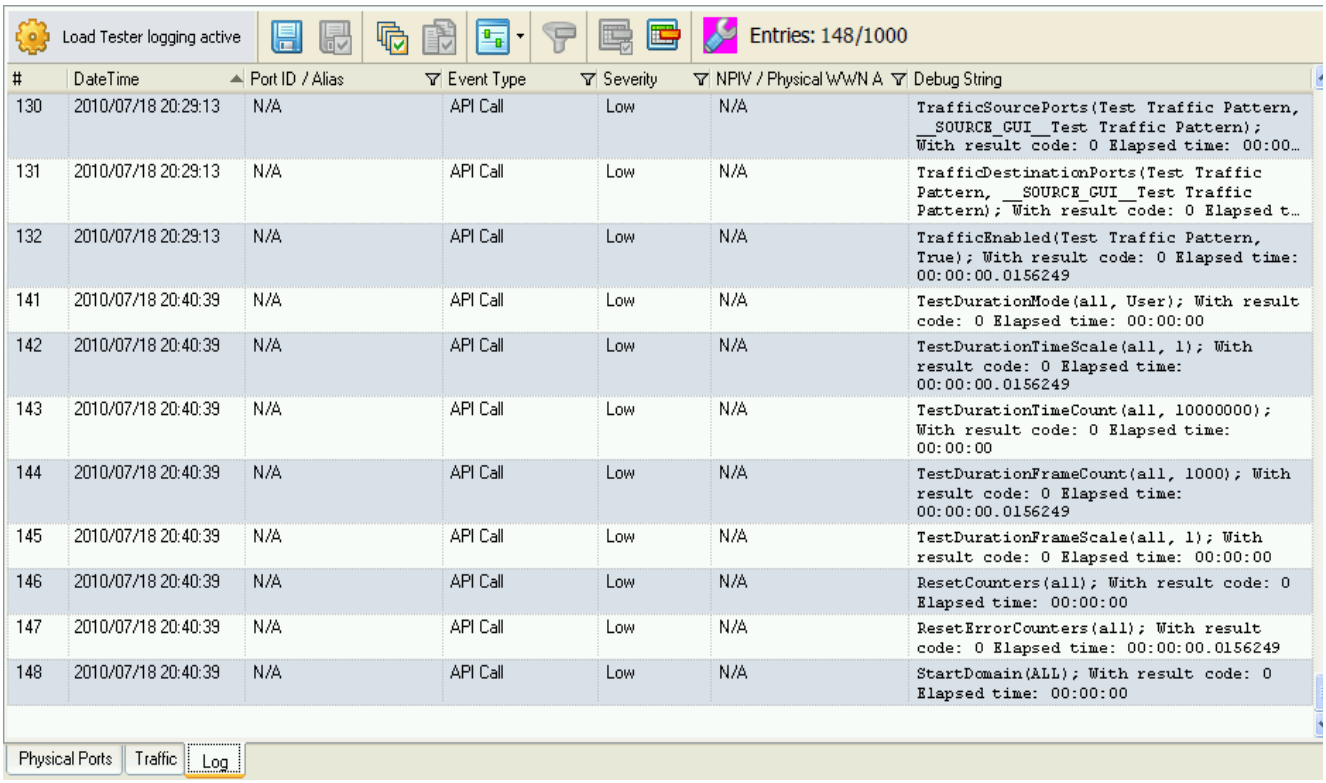
If you right-click on the stream band or row, the following options will be available:

- **Reset Counters** - Resets the counters of the selected stream
- **Reset Trigger** - Resets the triggers for the selected stream
- **Columns** - Opens the **Columns** dialog box where you can select which columns to display
- **Hide Filters** - Hides the filter icons
- **Clear Filter** - Removes all applied filters for the selected Traffic Pattern
- **Font Size** - Lets you select the size of the text used for the traffic pattern table.

Log Tab

The Log tab or Log view (Figure 28) displays the log entries generated for the tests you run. It displays the logs according to the sorting order of the columns. The date and time of the log shows when the log entry was generated.

Figure 28: Log Tab



#	DateTime	Port ID / Alias	Event Type	Severity	NPIV / Physical WWN A	Debug String
130	2010/07/18 20:29:13	N/A	API Call	Low	N/A	TrafficSourcePorts(Test Traffic Pattern, __SOURCE_GUI__Test Traffic Pattern); With result code: 0 Elapsed time: 00:00…
131	2010/07/18 20:29:13	N/A	API Call	Low	N/A	TrafficDestinationPorts(Test Traffic Pattern, __SOURCE_GUI__Test Traffic Pattern); With result code: 0 Elapsed t…
132	2010/07/18 20:29:13	N/A	API Call	Low	N/A	TrafficEnabled(Test Traffic Pattern, True); With result code: 0 Elapsed time: 00:00:00.0156249
141	2010/07/18 20:40:39	N/A	API Call	Low	N/A	TestDurationMode(all, User); With result code: 0 Elapsed time: 00:00:00
142	2010/07/18 20:40:39	N/A	API Call	Low	N/A	TestDurationTimeScale(all, 1); With result code: 0 Elapsed time: 00:00:00.0156249
143	2010/07/18 20:40:39	N/A	API Call	Low	N/A	TestDurationTimeCount(all, 10000000); With result code: 0 Elapsed time: 00:00:00
144	2010/07/18 20:40:39	N/A	API Call	Low	N/A	TestDurationFrameCount(all, 1000); With result code: 0 Elapsed time: 00:00:00.0156249
145	2010/07/18 20:40:39	N/A	API Call	Low	N/A	TestDurationFrameScale(all, 1); With result code: 0 Elapsed time: 00:00:00
146	2010/07/18 20:40:39	N/A	API Call	Low	N/A	ResetCounters(all); With result code: 0 Elapsed time: 00:00:00
147	2010/07/18 20:40:39	N/A	API Call	Low	N/A	ResetErrorCounters(all); With result code: 0 Elapsed time: 00:00:00.0156249
148	2010/07/18 20:40:39	N/A	API Call	Low	N/A	StartDomain(ALL); With result code: 0 Elapsed time: 00:00:00

Viewing a Log

The Load Tester log shows a list of all events that occurred during the duration of the test.

The Log Manager continuously lists the logs and displays them with options you have selected.

You can save the log to a `*.csv` file, `*.txt` file or an HTML file.

To save a log from the Log Manager tab as an HTML file or text file:

1 Highlight the log you want to save.

2 Click the **Save Selected Entries As**... button. The Save Log Manager Contents As window is displayed.

3 Name and save the log as an HTML or text file to the Saved Logs folder or to a location you prefer.

Setting Locations

To set up the locations of Load Tester log files:

1 Click the Log Manager Options icon to open the drop-down menu (Figure 29) and select **Log Manager Options**.

Figure 29: Log Manager Options Menu

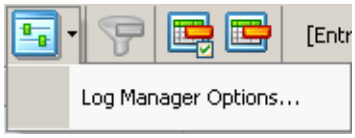
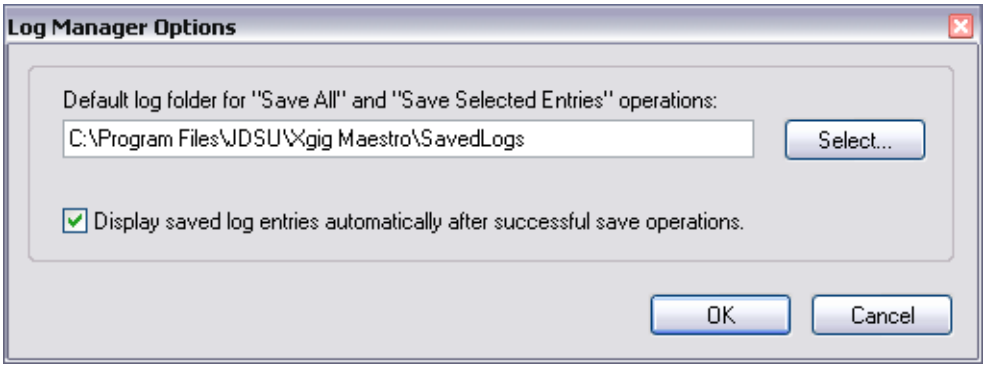


Figure 30: Log Options Dialog



2 Enter the path to the folder where you want to save the log file.

You can browse to where you want to save the log file by clicking the **Select** button.

3 Click **OK**.

Note: These settings apply to all Load Tester logs. Log options are the same for all Load Tester ports.

Multi-filtering Event Types

You can filter the logs using more than one event type by using multi-filtering feature.

To filter the logs using more than one event type:

1 Click the **Filter** icon on the Event column.

2 Select **Multi-filtering**. A dialog box will appear with check boxes for available event types.

3 Check the boxes of the events you want to use.

4 Click **Ok** to apply multi-filtering.

Setting the Number of Log Entries

The current number of log entries and the maximum number of log entries is displayed in the toolbar as shown by the illustration in Figure 31.

Figure 31: Number of Log Entries

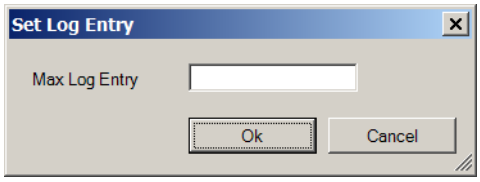
In the case of this illustration, the **Entries: 148/1000** shows that Load Tester currently has 148 log entries and is set to allow a maximum of 1000 log entries. As the maximum amount of log files is reached, the oldest log entries are discarded. (There is no way to recover discarded/truncated logs.)

The maximum number of log entries is set to 1000 as a default. This default maximum value should be sufficient for typical Load Tester use. This maximum value is provided to prevent the logs stored on the client from growing to an excessive number of log files which could use an excessive amount of memory.

However, the maximum value may be adjusted. For example you may want to set the maximum to a larger value to allow for client runs of extended duration of time where the need to examine the logs may be valuable. If you set the maximum value to a number less than the current number of log files, the older current files in excess of the new maximum value will be truncated. (There is no way to recover discarded/truncated logs.)

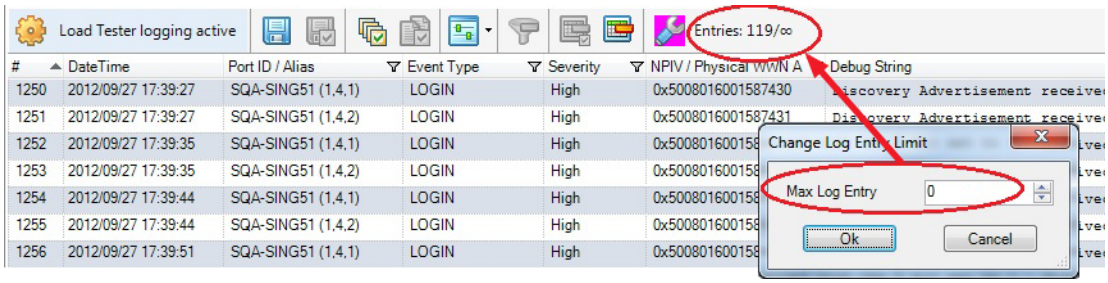
To adjust the maximum number of log files, select the icon button shown in Figure 31. The Set Log Entry dialog box (shown in Figure 32) is displayed. Enter your new maximum value for log entries and click the **Ok** button.

Figure 32: Set Log Entry Dialog Box



No log cap is applied if the Max Log Entry is set to zero and the base displays an infinity symbol (∞) as shown in Figure 33.

Figure 33: Max Log Entry Set to Zero

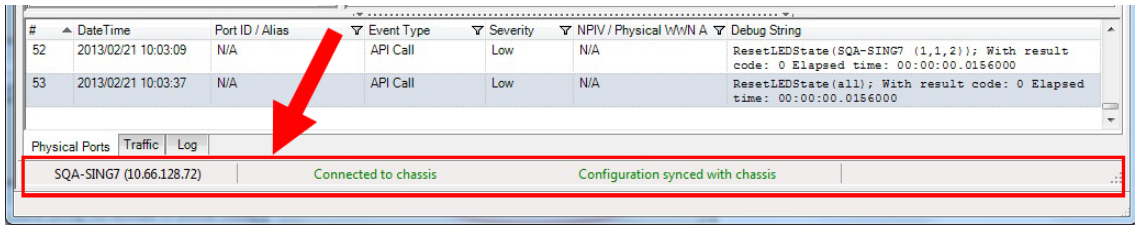


Connectivity Status Bar

The Load Tester connectivity status bar monitors the connection status between the client and the chassis and attempts to mitigate the interruption to users caused by temporary loss of connection. It is a passive feature so you do not need to turn this feature on and there is nothing that needs to be configured.

This new status bar is located near the bottom of the Load Tester window as shown in Figure 34.

Figure 34: Connectivity Status Bar

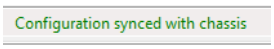


The connectivity status bar has three sections.

- The first section shows the name and IP address of the chassis being connected to. When you hover the mouse over this section, it will provide more details regarding the connection status.
- The second section shows the client's connection status with the chassis. There are three connection states:
  - Connected to chassis - This state is shown in green font when Load Tester is connected to the chassis. Connected to chassis
  - Disconnected from chassis - This state is shown in red font when Load Tester is disconnected from the chassis. Disconnected from chassis The other two sections will display nothing when in this state.
  - Reconnecting to chassis - This state is shown in red font when there is a network interruption during a Load Tester session. This indicator tells users the client is attempting to connect back to the chassis. Reconnecting to chassis (3 secs)...

If you think that the reconnection is not going to be successful (for reasons such as, the chassis has been rebooted or the network condition is too bad to continue), you may stop the process by clicking the yellow X to the right of the **Reconnecting to chassis** message. This opens the **Disconnect from Chassis** dialog box which provides a confirmation prompt to cancel the reconnection attempt.

- The third section shows synchronization information.



or


When Load Tester is attempting to reconnect, you are still allowed to make configuration changes (ports, traffic patterns etc) on the GUI, but as the connection is broken, the connection is queued on the client as pending configuration items. These will be synced to the chassis when the chassis is successfully reconnected. While reconnecting, you can click on the Syncing configuration…" text to show more details or you can click the cancel button to end the syncing process.

Note: When the connectivity status bar displays either of the following messages, it may indicate that there is an unreliable network connection to the chassis and a risk of losing configuration data.

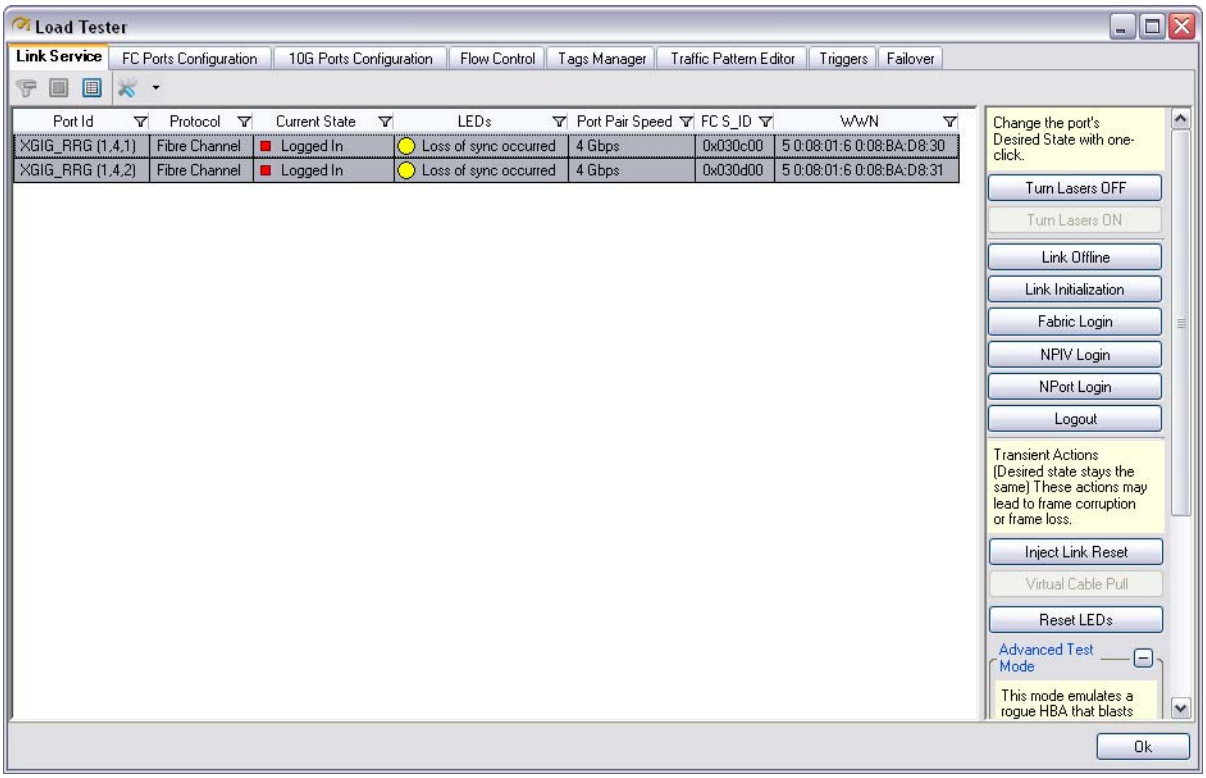
- "Reconnecting to chassis" message frequently or for a prolonged time
- "Syncing configuration… (*X* items pending)" message significantly more slowly than usual

If this occurs, you should check the network connectivity and avoid making changes in the GUI if the problem persists.

Load Tester Device Window

You can configure the Load Tester using the different settings found in the Load Tester Device Window (Figure 35).

Figure 35: Load Tester Device Window



The Load Tester Device Window is divided into the following tabs:

Link Service

The Link Service tab contains options to customize the link service settings for a port or group of ports.

FC Ports Configuration

The FC Ports Configuration tab lets you manage and configure all the Fibre Channel ports that have been locked for use with the Xgig Load Tester. From this tab you can view and access configuration setting for each port, filter ports according to tags or chassis, or select one or more ports for deletion.

10G Ports Configuration

The 10G Ports Configuration tab lets you manage and configure all the FCoE ports that have been locked for use with the Xgig Load Tester. From this tab you can view and access configuration setting for each port, filter ports according to tags or chassis, or select one or more ports for deletion.

Flow Control

The Flow Control tab lets you manage the traffic flow or stream settings for individual ports and group of ports.

Tags Manager

The Tags Manager lets you create, edit, or delete the tags by Load Tester.

Traffic Pattern Editor

The Traffic Pattern Editor tab is where you create or edit a traffic pattern to be used

Triggers

The Triggers tab displays all the available triggers you can set when you run a test in Load Tester. You can turn on and pause triggers through this dialog box.

Failover

The Failover tab lets you set the failover settings for Fibre Channel Load Tester ports.

Chapter 3

Configuring Ports

In this chapter:

After locking the ports for use as a Load Tester, you must configure the selected ports, defining the ports based properties.

You can configure the ports either individually or as a group:

- For FC ports, use the FC Ports Configuration tab in the Load Tester Device Window (refer to Figure 36 on page 87).
- For FCoE ports, use the 10G Ports Configuration tab in the Load Tester Device window (refer to Figure 38 on page 98).

Using the Ports Configuration Tabs

The Load Tester Device Windows have three tabs for configuring the ports locked as Load Testers:

- FC Ports Configuration tab
- 10G Ports Configuration tab
- Multicast/Broadcast Configuration tab

From the FC Ports Configuration and the 10G Ports Configuration tabs, you can view and access configuration settings for each port, filter ports according to tags or chassis, or select one or more ports for deletion.

These ports configuration tabs are each divided into two main panes, the left pane is a ports list and the right pane is the Port Configuration Control.

Operation buttons on the ports configuration tabs are listed below:

Apply - sends the changes in the configuration to the locked ports.

Expand Groupboxes - expands all the configuration group boxes.

Collapse Groupboxes - collapses all the configuration group boxes.

Numeric Editors in Decimal - changes all the numeric editors into decimal format.

Numeric Editors in Hexadecimal - changes all the numeric editors into hexadecimal format.

Clear Filters - removes all filters set for the ports list.

Select all Ports - selects all ports listed in the ports list.

Deselect all Ports - deselects all ports that are selected.

Link Service - lists link service options.

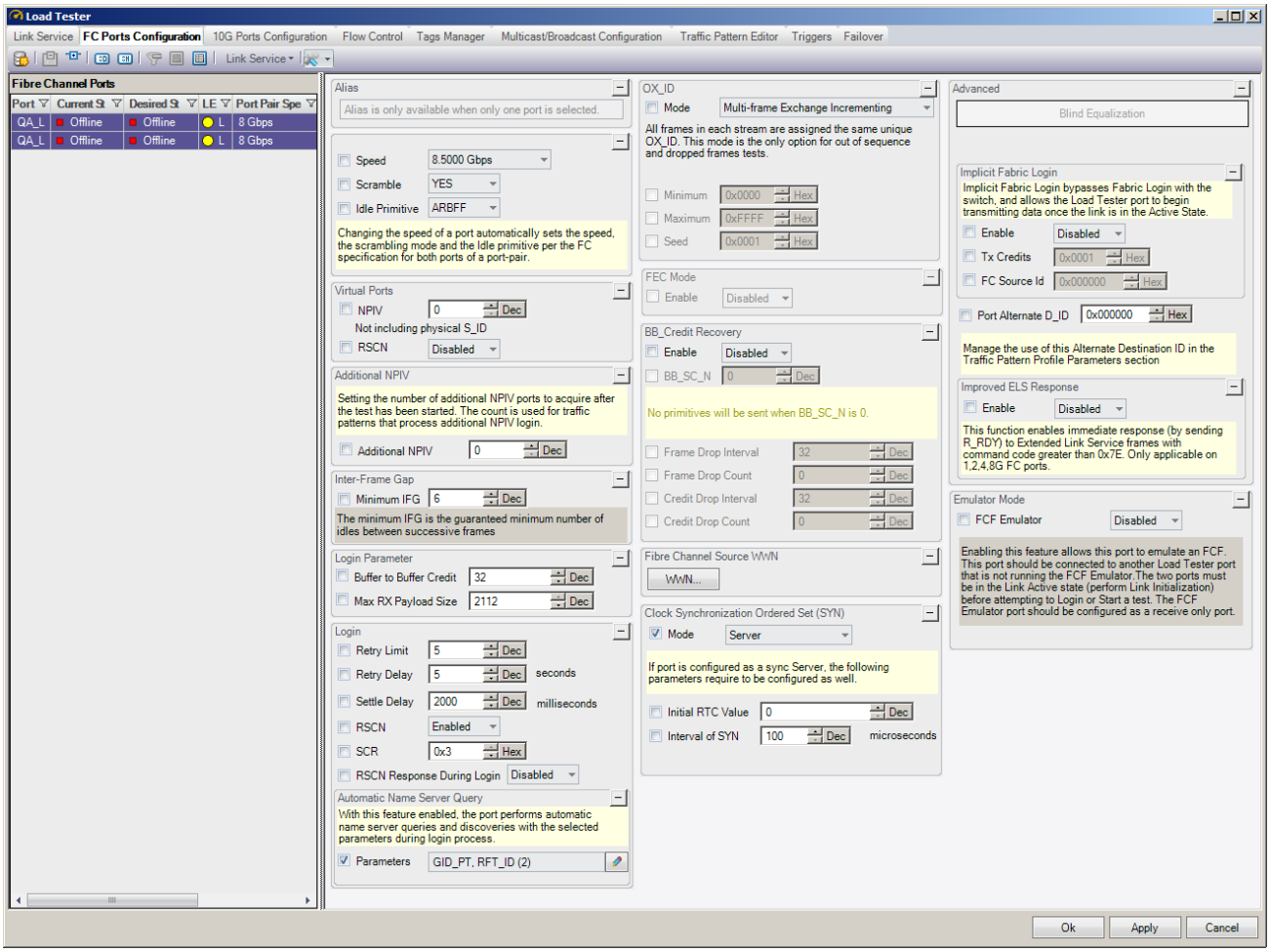
Tools - provides access to the Single Frame Tx/Rx, Port Capture, Configuration Summary, API Shell, and Clock Sync Ordered Set tools. Each of these tools are described in "Launch a Tool" on page 19.

From the Multicast/Broadcast Configuration tab you can configure the available ports for either a Multicast or a Broadcast operation. This tab is only applicable when Load Tester is connected to one or more FC port pairs on a legacy 8G blade as non-8G ports are filtered out from selection in Available Port panel. The left pane/right pane orientation described above does not hold true for the Multicast/Broadcast tab. Operation buttons for this configuration tab include **New** Multicast group and **Delete** Multicast group; **Apply** Multicast settings and **Cancel** Multicast settings; and **Tools** which provides access to the Single Frame Tx/Rx, Port Capture, Configuration Summary, API Shell, and Clock Sync Ordered Set tools, (described in "Launch a Tool" on page 19.)

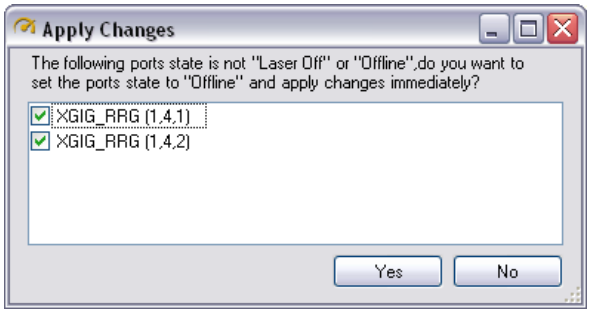
Configuring Fibre Channel Ports

Once you have locked ports for use with Load Tester, you can use the FC Ports Configuration tab to configure the settings for those ports. You can also access a port's configuration setup by right-clicking on the Parameters Status table (described on page 30) and selecting **Configure port** or **Configure multiple ports**.

Figure 36: FC Ports Configuration Tab



Note: The Load Tester **FC Ports Configuration** tab does not allow port configurations to be applied when the selected port(s) are in states other than **Laser Off** and **Offline**. When the selected port(s) are in the other states (**Link initialization**, **Fabric Login**, or **Nport Login** as examples), you can edit the ports configuration tab parameters and select **Apply**. When this is done, the **Apply Changes** dialog box is displayed.



If you select:

Yes, the port states are changed to **Offline** and the configuration changes are applied immediately.

No, the changes are discarded and you are returned to the ports configuration tab.

To configure Fibre Channel ports:

1. Click on the **Configuration** drop-down button on the Xgig Maestro main window.
2. Select **Configure FC Ports**. This will open the **FC Ports Configuration** tab in the Load Tester Device Window. Alternatively, you can right-click on the FC port in the Parameters Status Table and select **Configure port** or **Configure multiple ports**. This will open the **Fibre Channel Port Configuration** dialog box, which is the same as the FC Ports Configuration tab in the Load Tester Device Window.
3. Select the port from the list on the left panel. The configuration panel on the right will update with the settings for the selected port.
4. Set the alias for the selected port. Enter the alias in the **Alias** text field. You can set the alias if only one port is selected.
5. Select the speed of the port from the **Speed** drop-down list. Options are 1.0625 Gbps, 2.1250 Gbps, 4.2500 Gbps, 8.5000 Gbps, and 14.025 Gbps (16G).

Note: When the speed of a port is changed, the speed for the corresponding port in the port pair is changed automatically. In addition, if the scrambling and idle primitive settings are changed automatically in response to a speed change for a port, the scrambling and idle primitive settings for the corresponding port are changed automatically.

6 Set the scrambling feature **ON** or **OFF** from the **Scramble** drop-down list.

Scrambling is enabled by default for line rates 8.5000 Gbps and 14.025 Gbps (16G). Scrambling is disabled by default for line rates 1.0625 Gbps, 2.1250 Gbps, and 4.2500 Gbps.

Note: If the scrambling setting is changed automatically in response to a speed change for a port, the scrambling setting for the corresponding port is changed automatically.

7 Select the idle primitive to use on the port from the **Idle Primitive** drop-down list. Options are **Idle** and **ARB(FF)**. The default is **ARB(FF).**

The idle primitive setting is **Idle** by default for line rates 1.0625 Gbps, 2.1250 Gbps, and 4.2500 Gbps. Refer to the `IdleIsARBff` function in the API Help system located on the product USB drive for more information.

Note: If the idle primitive setting is changed automatically in response to a speed change for a port, the idle primitive setting for the corresponding port is changed automatically.

Virtual Ports

1 Set the number of virtual ports to use on the port in the **NPIV** field. You can set up to 255 virtual ports in addition to the Physical S_ID.

Note: If both the Virtual Ports (NPIV) and Additional NPIV fields are utilized for traffic generation, the total number of these two fields cannot exceed 255 ports.

Note: Once the NPIV is set for port, the configured NPIV will be available in Traffic Port Selection Tab based on topology mode selected.

2 Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the NPIV field.

3 Set the Registered State Change Notification (RSCN) service by selecting the check box and selecting Enabled or Disabled from the drop-down list. By default, this service is disabled.

4 Configuring virtual ports causes Virtual Addresses and Exchange Replication to be updated.

Note: After configuring NPIV or Additional NPIV count, go to Profile Parameters tab and check Virtual Addresses Requested per Port and Exchange Replication value are correct. Please update if needed.
– Virtual Addresses Requested per Port value should be equal to the sum of NPIV and Additional NPIV configured for every Traffic Pattern.
– Exchange Replication value is equal to the sum of NPIV and Additional NPIV values **plus "1"**.
Refer to "Virtual Addresses Requested Per Port (SAN profile) / Virtual End Stations Created Per Port (LAN profile)" and "Exchange Replication" on page 143.

Additional NPIV

Incremental NPIV ports can be enabled to test other test patterns. Up to 255 additional NPIV ports may be added.

Note: If both the Virtual Ports (NPIV) and Additional NPIV fields are utilized for traffic generation, the total number of these two fields cannot exceed 255 ports.

Set the number of additional NPIV to use on the port in the Additional NPIV field.

You can set the number of additional virtual ports using the **up** or **down** button to increase or decrease the value, or enter the new value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the field. Changing the additional NPIV value automatically selects the Additional NPIV check box.

Using Additional NPIV

These are the steps to perform additional NPIV login.

With the FC ports locked and Load Tester plugin launched:

1. If desired, configure NPIV count in the default traffic pattern for each port on Port Configuration tab. See “Virtual Ports” on page 89. (Note: This is not required for Additional NPIV Login).
2. Configure Additional NPIV count for each port in Port Configuration tab. See Additional NPIV above.
3. Configure/Create (Copy recommended) one or more new traffic patterns. See Chapter 5, “Creating and Managing Traffic Patterns on page 127. Copy Traffic Pattern will ensure all the settings in default traffic pattern will be inherited by the new traffic pattern.

   If you are using Create New Traffic Pattern, please be sure to update Virtual Addresses Requested per Port and Exchange Replication values in Profile Parameters tab. See the following note for more information.

Note: After configuring NPIV or Additional NPIV count, please go to Profile Parameters tab and check Virtual Addresses Requested per Port and Exchange Replication value are correct. Please update if needed.
– Virtual Addresses Requested per Port value should be equal to the sum of NPIV and Additional NPIV configured for every Traffic Pattern.
– Exchange Replication value is equal to the sum of NPIV and Additional NPIV values **plus “1”**.
Refer to “Virtual Addresses Requested Per Port (SAN profile) / Virtual End Stations Created Per Port (LAN profile)" and “Exchange Replication” on page 143.

4. For each of these new traffic patterns with Additional NPIV count configured, ensure that they will not run on a global start by unselecting the Run on Global Start check box. See “Run on Global Start” on page 148.

   Refer to the note in step 3 above.

5 Return to the main Load Tester window and view the Traffic Tab at the bottom of the window, ensuring that you are seeing the Tx Pattern Based View. This is shown in Figure 24 on page 67.

6 Start the test using the **Start test** button described on page 18.

- Traffic patterns that are configured as “Run on Global Start” will start running and process Fabric Login and normal NPIV login and generate streams defined within this traffic pattern. All ports will go into the “Test in progress” state.
- Traffic patterns that are not configured to run on global start, they will stay in "paused" state. These paused traffic patterns will not generate any data traffic.

7 Once the test is running, click the **Activate** button on the Additional NPIV Login column for the paused traffic patterns. This is shown in Figure 24 on page 67.

Once the test has started, all ports will process Fabric Login and normal NPIV login. Traffic patterns that are configured as “Run on Global Start” will start running and streams defined within this traffic pattern be generated. Other traffic patterns will stay in the “paused” state. These paused traffic patterns will not generate any data traffic. Then, all ports will go into the “Test in progress” state.

8 You can refer to the Tx Port Based View shown in Figure 26 on page 70 to see the ports that are running. In this illustration, note that the physical port (Stream Index 0) and its four virtual ports (Stream Index 1–4) are running one traffic pattern while the two additional virtual ports (Stream Index 5 and 6) are running another traffic pattern.

Inter-Frame Gap

1 Set the guaranteed minimum number of idles between successive frames in the **Minimum IFG** field. You can set a value from 3 to 65535.

2 Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the Minimum IFG field.

Login Parameter

1 Set the Buffer-To-Buffer Credit in the **Buffer-to-Buffer Credit** field. You can set a value from 0 to 32767. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Buffer-to-Buffer Credit** field.

2 Set the Max RX Payload Size limit in the **Max RX Payload Size** field. You can set a value from 64 to 2112. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Max RX Payload Size** field.

Login

1 Set the login retry limit in the **Retry Limit** field. You can set a value from 0 to 100 retries. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Retry Limit** field.

2 Set the login retry delay in the **Retry Delay** field. You can set a value from 1 to 60 seconds. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Retry Delay** field.

3 Set the number of milliseconds that a port will delay before sending the GID_PT discovery frame in the **Settle Delay** field.

4 Set the Registered State Change Notification (RSCN) service by selecting the **RCSN Response During Login** check box and selecting Enabled or Disabled from the drop-down list. By default, this service is turned disabled.

5 Set the State Change Registration (SCR) Value. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **SCR** field.

6 Enable or disable **RSCN Response During Login**. When an RSCN is received, this option will add a message to the port log, indicating the Destination ID to which the RSCN pertains, and the RSCN received counter will be incremented. The port will then send a discovery frame to the Name Server to determine the state of the Destination ID(s) in question.

Automatic Name Server Query

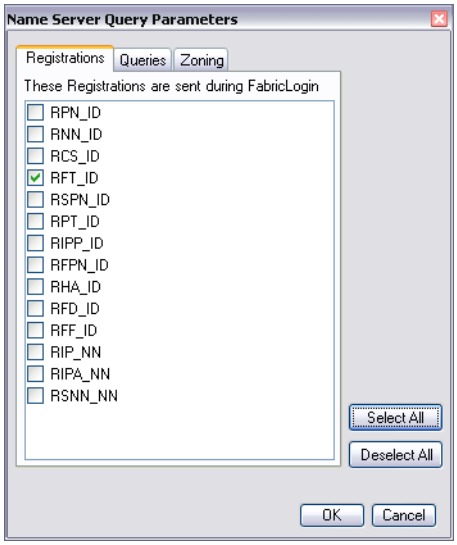
With this feature enabled, the port performs automatic name server queries and discoveries with the selected parameters during login process.

To set the parameters used during name server query and discovery:

1 Select the **Parameters** check box.

2 Click on the pencil icon to open the **Name Server Query Parameters** dialog box.

Figure 37: Name Server Query Parameters Dialog



3 Select the check boxes corresponding to the parameter you want to use.

4 Click **OK** to save your selection.

OX_ID

1 Select the Originator Exchange Identifier (OX_ID) mode from the **Mode** drop-down list. The options are:

Multi-frame Exchange Incrementing

All transmitter traffic streams for a given Physical N_Port are given a unique OX_ID prior to starting the test. In Multi-frame Exchange Incrementing OX_ID mode, the number of frames per sequence, per exchange (OX_ID) depends on the Exchange Length value set in the **Profile Parameters** sub-tab in the **Traffic Pattern Editor** tab. The next frame from this stream is the first frame of the next sequence with SEQ_CNT returning to zero. See Chapter 5, "Creating and Managing Traffic Patterns" for user control of these values.

Single-frame Exchange Incrementing

Consecutive frames generated from a single Load Tester port will have a new OX_ID. There is no relationship between the OX_ID chosen and the stream or traffic profile engine. Define a lower and upper bound. The step size is always 1.

Single-frame Exchange Random

Consecutive frames generated from a single Load Tester port will have a new OX_ID. There is no relationship between the OX_ID chosen and the stream or traffic profile engine. Define a lower and upper bound.

2 Set the minimum value for the OX_ID in the **Minimum** field. This minimum value will be used when the incrementing and random modes are selected. You can set a value from 0 to 65535. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Minimum** field. This option is only applicable for single-frame exchange modes.

3 Set the maximum value for the OX_ID in the **Maximum** field. This maximum value will be used when the incrementing and random modes are selected. You can set a value from 0 to 65535. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Maximum** field. This option is only applicable for single-frame exchange modes.

4 Set the seed value in the **Seed** field.

A seed is the initial OX_ID pattern value. The random generator is initialized once using the seed, and the subsequent patterns will be generated automatically in a random manner. Use the **up** or **down** button to increase or decrease the value, or you may enter the value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Seed** field. This option is only applicable for Single-frame Exchange Random OX_ID mode.

FEC Mode

The FEC Mode group box is enabled only when the selected ports are configured as 16G speed.

Select **Disabled** or **Enabled** in the drop-down menu to disable or enable the FEC mode.

Enabling the FEC Mode allows you to enable the FEC layer in PHY when generating traffic. The FEC Parity Errors are listed in the RX Physical Ports when Errors are selected (see Table 9 on page 75).

After you are done, Click **Apply** on the FC Ports Configuration tab to save the changes you made or click **Cancel** to discard them.

Click **Ok**. Your settings are applied to the selected ports.

BB_Credit Recovery

This configuration setting will enable the ports to perform BB Credit Recovery. BB_SCs and BB_SCr primitives are used to account for exchange of frames and R_RDY primitives. This setting is only available in Fibre Channel ports.

1. To enable the BB_Credit Recovery feature and option, choose **Enabled** from the **Enable** drop-down menu. Please note that BB_SCs and BB_SCr primitives will be sent after transmission of 2^BB_SC_N number of frames or reception of 2^BB_SC_N number of R_RDYs.
2. To set a non-zero BB_SC_N value (1 - 15) for the selected ports, select **BB_SC_N**. The value will be used when BB Credit Recovery is enabled.
3. To set an interval in number of frames to transmit (1 - 0x7fffffff) for the selected ports, select **Frame Drop Interval**. When BB Credit Recovery is enabled in each such interval, a specific number (Frame Drop Count) of consecutive frames will be dropped.
4. To set a frame count (0 - 0xffff) for the ports, select **Frame Drop Count**. When BB Credit Recovery is enabled in each Frame Drop Interval, this specific number of consecutive frames will be dropped.
5. To set an interval in number of credits to transmit (1 - 0x7fffffff) for the selected ports, select **Credit Drop Interval**. When BB Credit Recovery is enabled in each such interval, a specific number (Credit Drop Count) of consecutive credits will be dropped.
6. To set a credit count (0 - 0xffff) for the ports, select **Credit Drop Count**. When BB Credit Recovery is enabled in each Credit Drop Count Interval, this specific number of consecutive credits will be dropped.

   For Frame/Credit Drop Interval and Frame/Credit Drop Count, the Drop Count does not happen within the Interval but after the Interval.

   It will be like this:

   Frame Drop Interval = 8; Frame Drop Count = 3

   7 frames - [8th drop] - [9th drop] - [10th drop] - 7 frames - drop - drop - drop...

Fibre Channel Source WWN

1. Click on the **WWN** button to configure the WWN or port name of the selected port. **The Fibre Channel Source WWN** dialog box will open which allows you to set the source WWN options of the individual ports.
2. Click **Apply** to implement the changes you made to the WWN settings, or click **Ok** to save the WWN settings and close the dialog box.

Clock Synchronization Ordered Set (SYN)

Configure the Clock Synchronization Ordered Set (SYN) parameters for each port. The configuration settings are:

Mode – This checkbox and the drop-down list defines which mode the port plays. There are five options to select from:

- **Server** initiates a Real-Time Clock (RTC) and transmits the RTC value in Clock Sync primitives.
- **Client** detects the Clock Sync Primitives on the RX and automatically updates its RTC with the value in the primitive.
- **AllFunction** behaves as both Server and Client at the same time.
- **ServerWithoutTx** behaves as server but does not transmit Clock Sync primitives.
- **ClientWithoutRx** behaves as client but does not receive Clock Sync primitives to update its RTC.

Note: This is the first step in using Clock Synchronization Ordered Set.
For complete information, refer to "Clock Sync Ordered Set" on page 25.

Initial RTC Value – defines the initial value of RTC. This parameter is available only for the Clock Sync Server (that is, when **Mode** = **Server**, **AllFunction**, or **ServerWithoutTx**). The default value is "all 0". The range of Initial RTC Value is from 0 to 4398046511103 ($2^{42}-1$).

Interval of SYN – defines the interval of SYN sent by Server. This parameter is available only for the Clock Sync Server (that is, when **Mode** = **Server**, **AllFunction**, or **ServerWithoutTx**). The interval range is from 100µs to 10s. You can configure any value with a 100µs step size. The default value is 100µs.

Advanced

Click the **Blind Equalization** button (see page 55) to execute blind equalization for the selected port. Enabling the **Blind Equalization** button when the ports are 8G displays the Advanced area. See page 55.

Note: The Serializer/Deserializer (SERDES) performs equalization based on its current parameters. In the event that these parameters are not sufficient to establish link then blind equalization can be performed. Blind equalization will reset the equalizer in order to reacquire link. While the link is being reacquired, the incoming traffic will be disrupted.

Implicit Fabric Login

Implicit Fabric Login bypasses Fabric Login with the switch, and allows the Load Tester port to begin transmitting data once the link is in the Active State.

1. Select **Enabled** or **Disabled** from the **Enable** drop-down menu.
2. Enter the Tx buffer-to-buffer credits of the physical port in the **Tx Credits** field. This will adjust the Tx buffer-to-buffer credits of the physical port while in Implicit Fabric Login mode.
3. Set the Fibre Channel S_ID used during Implicit Fabric Login in the **FC Source Id** field.

Port Alternate D_ID

Enter an alternate DID address for the port. Manage the use of the alternate Destination ID in the **Traffic Pattern Profile Parameters** section.

Click **Apply** on the FC Ports Configuration tab to save the changes you made or click **Cancel** to discard them.

Click **Ok**.

Improved ELS Response (8G Ports Only)

Improved ELS Response enables the Rx ports of 8G FC port configurations to respond to ELS command frames more quickly with an R_RDY response. The improved ELS response is only for the incoming ELS frames with command code greater than 0x7e. Since the software still needs to process the other ELS frames, these other ELS frames will not be responded to as quickly. This is only applicable for 1, 2, 4, and 8G FC ports.

1. Select **Enabled** or **Disabled** from the **Enable** drop-down menu.

Emulator Mode

Select **Disabled** or **Enabled** in the **FCF Emulator** drop-down menu to disable or enable the FC switch or Fibre Channel Forwarder (FCF) Emulator.

Enabling the FCF Emulator allows this port to emulate an FCF. The selected port should be connected to another Load Tester port that is not running the FCF Emulator. The two ports must be in the Link Active state (perform Link Initialization) before attempting to login or start a test. The FCF Emulator port should be configured as a receive-only port.

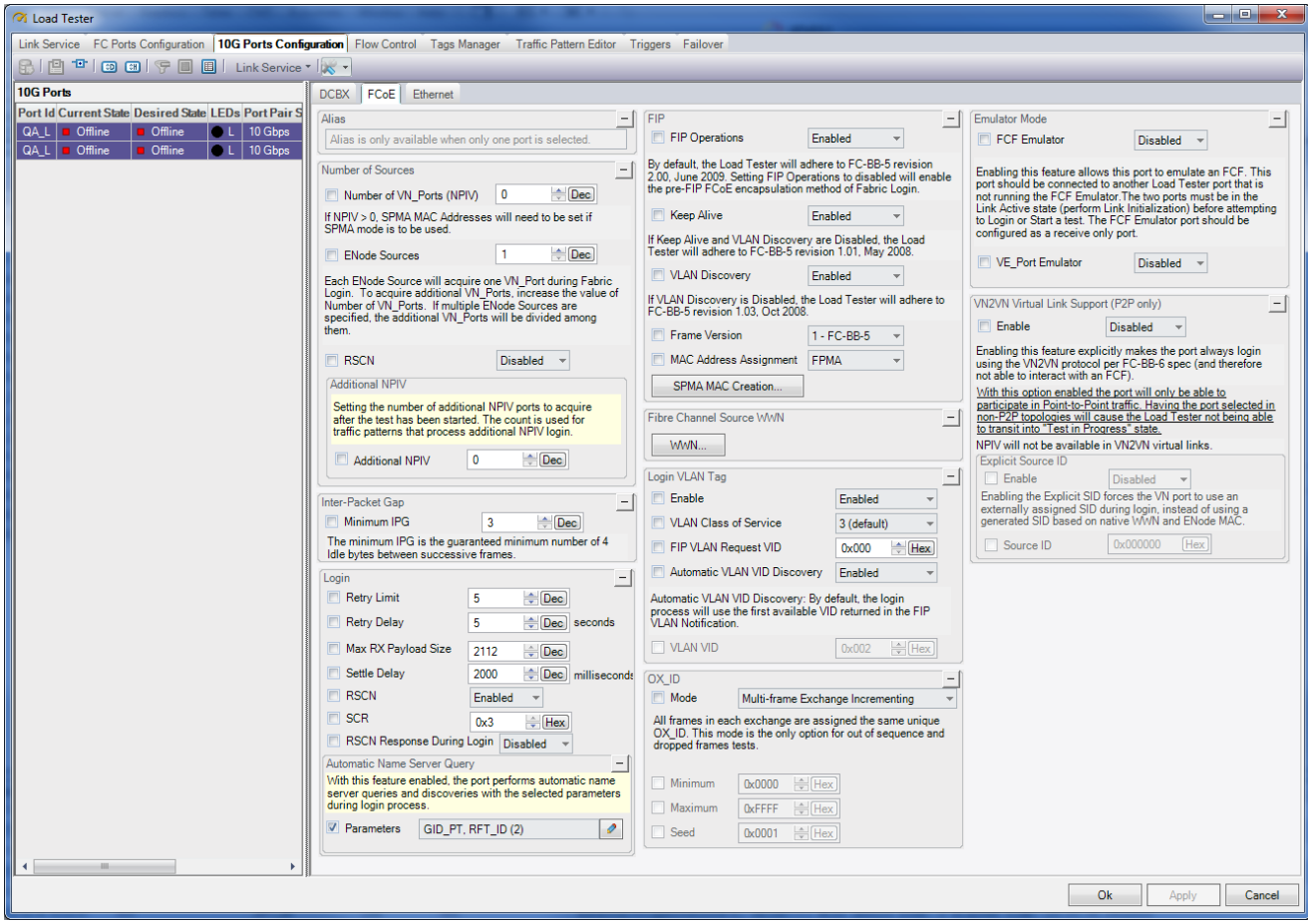
After you are done, Click **Apply** on the FC Ports Configuration tab to save the changes you made or click **Cancel** to discard them.

Click **Ok**. Your settings are applied to the selected ports.

Configuring FCoE Ports

Once you have locked the 10G ports for use with Load Tester, you can use the **10G Ports Configuration** tab to configure the settings for those ports. You can also access a port's configuration setup by right-clicking on the Parameters Status table (described on page 30) and selecting **Configure port** or **Configure multiple ports**.

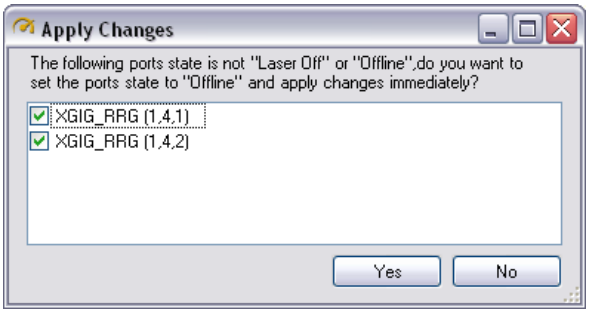
Figure 38: 10G Ports Configuration Tab



To configure 10G ports:

1. Click on the **Configuration** drop-down button on the Xgig Maestro main window.
2. Select **Configure FCoE Ports** to open the **FCoE** sub-tab in **10G Ports Configuration** tab in the Load Tester Device Window.
3. Select the port from the list on the left panel. The configuration panel on the right will update with the settings set by the user for the selected port.

Note: The Load Tester **10G Ports Configuration** tab does not allow port configurations to be applied when the selected port(s) are in states other than **Laser Off** and **Offline**. When the selected port(s) are in the other states (**Link initialization**, **Fabric Login**, or **Nport Login** as examples), you can edit the ports configuration tab parameters and select **Apply**. When this is done, the **Apply Changes** dialog box is displayed.



If you select the **Yes**, the port states are changed to **Offline** and the configuration changes are applied immediately. If you select **No**, the changes are discarded and you are returned to the ports configuration tab.

FCoE Tab

To configure FCoE ports, do the following:

Alias

Set the alias for the selected port. Enter the alias in the **Alias** text field. You can set the alias if only one port is selected.

Number of Sources

1 Set the number of virtual ports to use on the port in the **Number of VN_Ports(NPIV)** field. You can set up to 255 virtual ports in addition to the Physical S_ID. (Not available when **VN2VN Virtual Link Support** is enabled.)

Note: If both the VN_Ports (NPIV) and Additional NPIV fields are utilized for traffic generation, the total number of these two fields cannot exceed 255 ports.

2 Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the field.

If you enter an NPIV value greater than zero (0), you will need to set the Virtual Ethernet MAC addresses for LAN, or SPMA MAC addresses if you will use SPMA for SAN.

3 Set the number of ENode Sources in the **ENode Sources** field.

Each ENode Source will acquire one VN_port during Fabric Login. To acquire additional VN_Ports, increase the value of the Number of VN_Ports. If multiple ENode Sources are specified, the additional VN_Ports will be divided among them.

4 Set the Registered State Change Notification (**RSCN**) service by selecting the check box and selecting Enabled or Disabled from the drop-down list. By default, this service is disabled.

5 Configuring virtual ports causes Virtual Addresses and Exchange Replication to be updated.

Note: After configuring NPIV or Additional NPIV count, go to Profile Parameters tab and check Virtual Addresses Requested per Port and Exchange Replication value are correct. Please update if needed.
– Virtual Addresses Requested per Port value should be equal to the sum of NPIV and Additional NPIV configured for every Traffic Pattern.
– Exchange Replication value is equal to the sum of NPIV and Additional NPIV values **plus "1"**.
Refer to "Virtual Addresses Requested Per Port (SAN profile) / Virtual End Stations Created Per Port (LAN profile)" and "Exchange Replication" on page 143.

Additional NPIV

Incremental NPIV ports can be enabled to test other test patterns. Up to 255 additional NPIV ports may be added.

Note: If both the VN_Ports (NPIV) and Additional NPIV fields are utilized for traffic generation, the total number of these two fields cannot exceed 255 ports.

Set the number of additional NPIV to use on the port in the Additional NPIV field.

You can set the number of additional virtual ports using the **up** or **down** button to increase or decrease the value, or enter the new value directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the field. Changing the additional NPIV value automatically selects the Additional NPIV check box.

Configuring virtual ports causes Virtual Addresses and Exchange Replication to be updated.

Using Additional NPIV

These are the steps to perform additional NPIV login.

With the 10G ports locked and Load Tester plugin launched:

1 If desired, configure Number of VN_Ports (NPIV) count in the default traffic pattern for each port on 10G Ports Configuration tab. See "Number of Sources" on page 99. (Note: This is not required for Additional NPIV Login).

2 Configure Additional NPIV count for each port in 10G Ports Configuration tab. See Additional NPIV above.

3 Configure/Create (Copy recommended) one or more new traffic patterns. See Chapter 5, "Creating and Managing Traffic Patterns on page 127. Copy Traffic Pattern will ensure all the settings in default traffic pattern will be inherited by the new traffic pattern.

If you are using Create New Traffic Pattern, please be sure to update Virtual Addresses Requested per Port and Exchange Replication values in Profile Parameters tab. See the following note for more information.

Note: After configuring NPIV or Additional NPIV count, please go to Profile Parameters tab and check Virtual Addresses Requested per Port and Exchange Replication value are correct. Please update if needed.
– Virtual Addresses Requested per Port value should be equal to the sum of NPIV and Additional NPIV configured for every Traffic Pattern.
– Exchange Replication value is equal to the sum of NPIV and Additional NPIV values **plus "1"**.
Refer to "Virtual Addresses Requested Per Port (SAN profile) / Virtual End Stations Created Per Port (LAN profile)" and "Exchange Replication" on page 143.

4. For each of these new traffic patterns with Additional NPIV count configured, ensure that they will not run on a global start by unselecting the Run on Global Start check box. See "Run on Global Start" on page 148.

   Refer to the note in step 3 above.

5. Return to the main Load Tester window and view the Traffic Tab at the bottom of the window, ensuring that you are seeing the Tx Pattern Based View. This is shown in Figure 24 on page 67.

6. Start the test using the **Start test** button described on page 18.

   - Traffic patterns that are configured as "Run on Global Start" will start running and process Fabric Login and normal NPIV login and generate streams defined within this traffic pattern. All ports will go into the "Test in progress" state.
   - Traffic patterns that are not configured to run on global start, they will stay in "paused" state. These paused traffic patterns will not generate any data traffic.

7. Once the test is running, click the **Activate** button on the Additional NPIV Login column for the paused traffic patterns. This is shown in Figure 24 on page 67.

   Once the test has started, all ports will process Fabric Login and normal NPIV login. Traffic patterns that are configured as "Run on Global Start" will start running and streams defined within this traffic pattern be generated. Other traffic patterns will stay in the "paused" state. These paused traffic patterns will not generate any data traffic. Then, all ports will go into the "Test in progress" state.

8. You can refer to the Tx Port Based View shown in Figure 26 on page 70 to see the ports that are running. In this illustration, note that the physical port (Stream Index 0) and its four virtual ports (Stream Index 1–4) are running one traffic pattern while the two additional virtual ports (Stream Index 5 and 6) are running another traffic pattern.

Inter-Packet Gap

1. Set the guaranteed minimum number of idles between successive frames in the **Minimum IPG** field. You can set a value from 3 to 65535.

2. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the Minimum IFG field.

Login

1. Set the login retry limit in the **Retry Limit** field. You can set a value from 0 to 100 retries. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Retry Limit** field.
2. Set the login retry delay in the **Retry Delay** field. You can set a value from 1 to 60 seconds. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Retry Delay** field.
3. Set the login retry limit in the **Max RX Payload Size** field. You can set a value from 0 to 100 retries. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Max RX Payload Size** field.
4. Set the number of milliseconds that a port will delay before sending the GID_PT discovery frame in the **Settle Delay** field.
5. Set the Registered State Change Notification (RSCN) service by selecting the **RCSN Response During Login** check box and selecting Enabled or Disabled from the drop-down list. By default, this service is turned disabled.
6. Set the State Change Registration (SCR) Value. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **SCR** field.
7. Enable or disable **RSCN Response During Login**. When an RSCN is received, this option will add a message to the port log, indicating the Destination ID to which the RSCN pertains, and the RSCN received counter will be incremented. The port will then send a discovery frame to the Name Server to determine the state of the Destination ID(s) in question.

FIP

1. Enable or disable the FCoE Initialization Protocol (FIP) operations for the port by selecting **Enabled** or **Disabled** from the **FIP Operations** drop-down menu.

   By default, the Load Tester will adhere to FC-BB-5 revision 2.00, June 2009. Setting FIP Operations to Disabled will enable pre-FIP FCoE encapsulation method of Fabric Login.
2. Enable or disable the Keep Alive frames/timers (Tx and Rx) for the port(s) by selecting **Enabled** or **Disabled** from the **Keep Alive** drop-down menu.

   If **Keep Alive** and **VLAN Discovery** are set to **Disabled**, the Load Tester will adhere to FC-BB-5 revision 1.01, May 2008.
3. Enable or disable the VLAN Discovery for the port by selecting **Enabled** or **Disabled** from the **VLAN Discovery** drop-down menu.

   If VLAN Discovery is Disabled, the Load Tester will adhere to FC-BB-5 revision 1.03, Oct. 2008.
4. Set the FIP Version for the port from the **Frame Version** drop-down menu.
5. Select the MAC Address Assignment mode to be used on the port selecting **FPMA** or **SPMA** from the **MAC Address Assignment** drop-down menu. If you select SPMA, click the **SPMA**

MAC Creation... button to open the SPMA MAC Creation dialog box where you can view the Base and Step set for the ports.

Fibre Channel Source WWN

1. Click on the **WWN** button to configure the WWN or Port name of the selected port. **The Fibre Channel Source WWN** dialog box will open where you can set the source WWN options of the individual ports.
2. Click **Apply** to implement the changes you made to the WWN settings, or click **Ok** to save the WWN settings and close the dialog box.

Login VLAN Tag

1. Enable or disable the VLAN tags during the FCoE login process by selecting **Enabled** or **Disabled** from the **Enable** drop-down menu.
2. Set the numeric Class of Service (COS) value by selecting the value from the **VLAN Class of Service** drop-down list.
3. Set the FIP VLAN Request VID. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **FIP VLAN Request VID** field
4. Enable or disable **Automatic VLAN VID Discovery** by selecting **Enabled** or **Disabled** from the **FCoE Login** drop-down menu.

   By default, the login process will use the first available VID returned in the FIP VLAN Notification.
5. Set the VLAN VID for the port if you disabled **Automatic VLAN VID Discovery**. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **VLAN VID** field.

OX_ID

1. Select the Originator Exchange Identifier (OX_ID) mode from the **Mode** drop-down list. Options are **Multi-frame Exchange Incrementing**, **Single-frame Exchange Incrementing**, and **Single-frame Exchange Random**.

Multi-frame Exchange Incrementing

In this mode, all transmitter traffic streams for a given Physical N_Port are given a unique OX_ID prior to starting the test. In Multi-frame Exchange Incrementing OX_ID mode, the number of frames per sequence, per exchange (OX_ID) depends on the Exchange Length value set in the Profile Parameters window in the Traffic Pattern Editor tab. See Chapter 5, “Creating and Managing Traffic Patterns” for user control of these values.

Single-frame Exchange Incrementing

In this mode, consecutive frames generated from a single Load Tester port will have a new OX_ID. There is no relationship between the OX_ID chosen and the stream or traffic profile engine. Define a lower and upper bound. In Single-frame Exchange Incrementing mode, the step size is always 1.

Single-frame Exchange Random

In this mode, consecutive frames generated from a single Load Tester port will have a new OX_ID. There is no relationship between the OX_ID chosen and the stream or traffic profile engine. Define a lower and upper bound.

2 Set the minimum value for the OX_ID in the **Minimum** field. This minimum value will be used when the incrementing and random modes are selected. You can set a value from 0 to 65535. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Minimum** field. This option only applicable for single-frame exchange modes.

3 Set the maximum value for the OX_ID in the **Maximum** field. This maximum value will be used when the incrementing and random modes are selected. You can set a value from 0 to 65535. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Maximum** field. This option only applicable for single-frame exchange modes.

4 Set the seed value in the **Seed** field.

A seed is the initial OX_ID pattern value. The random generator is initialized once using the seed, and the subsequent patterns will be generated automatically in a random manner.

This option is only applicable for Single-frame Exchange Random OX_ID mode.

Emulator Mode

Select **Disabled** or **Enabled** in the **FCF Emulator** drop-down menu to disable or enable the FCoE switch or Fibre Channel Forwarder (FCF) Emulator.

Enabling the FCF Emulator allows this port to emulate an FCF. The selected port should be connected to another Load Tester port that is not running the FCF Emulator. The two ports must be in the Link Active state (perform Link Initialization) before attempting to login or start a test. The FCF Emulator port should be configured as a receive-only port.

Select **VE_Port Emulator** to enable the E-Port Emulation, exchange ELP Frames, and maintain the 10G link. You have to connect Load Tester ports like doing an FCF Emulator, and Enable VE_Port Emulator for both ports.

After you are done, Click **Apply** on the 10G Ports Configuration tab to save the changes you made or click **Cancel** to discard them.

Click **Ok**. Your settings are applied to the selected ports.

VN2VN Virtual Link Support (P2P only)

Enable enables or **Disable** disables the VN_Port to VN_Port (VN2VN) virtual link support.

This is implemented in compliance to the VN to VN virtual link protocol defined for FC-BB-6 to enable the Load Tester FCoE ports to establish virtual links directly between ENodes without involving real or emulated Fibre Channel Forwarder (FCF). Once VN2VN operation is enabled on a pair of ports in a loopback and assigned to a Point to Point (PT2PT) protocol traffic, the ports will be able to login to each other and start blasting frames.

The VN2VN operation is completely exclusive with the VE/VF emulators on a Load Tester port. Enabling VN2VN will automatically disable the emulators and vice versa. When VN2VN is enabled, **Number of VN Ports (NPIV)** is not available in the **Number of Sources**.

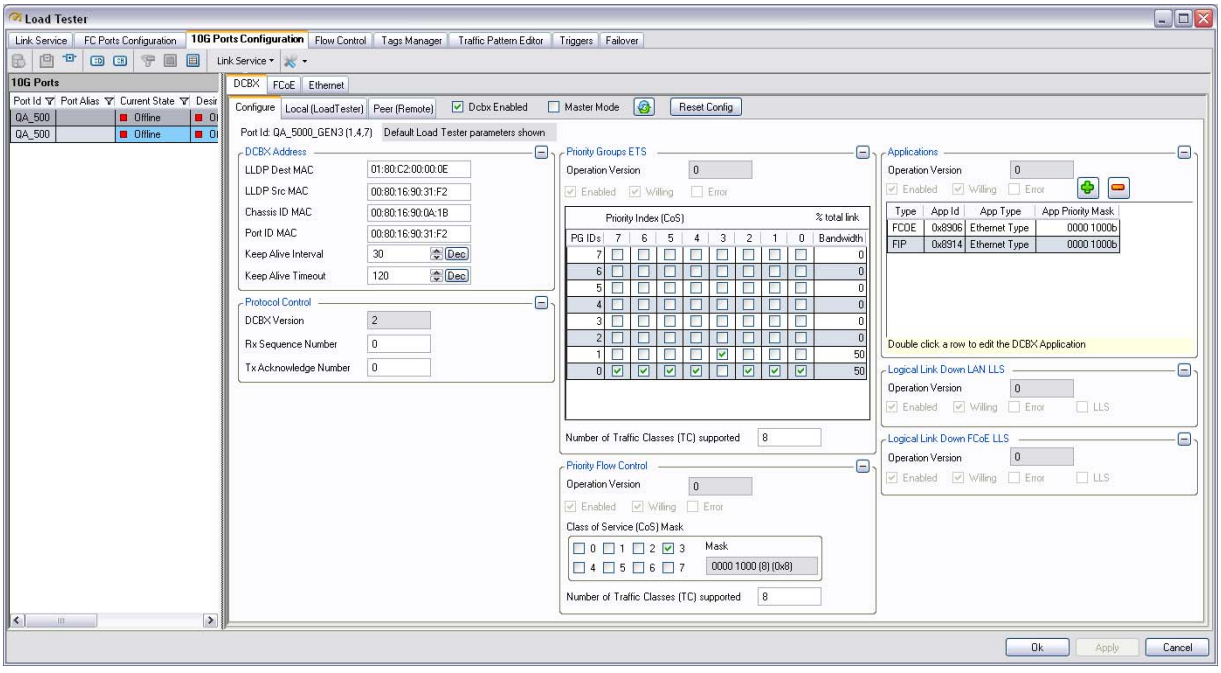
Explicit Source ID

Enabled enables (or **Disabled** disables) the usage of a explicitly assigned Source ID (S_ID) to be used in VN2VN operation instead of the negotiated S_ID acquired during pre-login.

DCBX tab

The DCBX sub-tab lets you manage the DCBX parameters and settings of the FCoE ports locked to Load Tester.

Figure 39: DCBX Sub-tab



To set the DCBX parameters of the FCoE ports locked to the Load Tester, do the following:

1. Click on the **Configuration** drop-down button on the Xgig Maestro main window.
2. Select **DCBX Parameters**. This will open the **DCBX Parameters** sub-tab in the 10G Ports Configuration tab in the Load Tester Device Window. Alternatively, you can right-click on the

FCoE port in the Parameters Status Table and select **DCBX Parameters**. This will open the **DCBX Parameters** dialog box, which is the same as the **DCBX Parameters** sub-tab.

3 Select the port from the list on the left panel. The configuration panel on the right will update with the settings for the selected port.

4 Enable or disable the DCBX by selecting or unselecting **DCBX Enabled**.

5 Enable or disable DCBX master mode operation for the port(s) by selecting or unselecting **Master Mode**. If Master mode is enabled, the selected port will set the DCBX "willing" bits to zero and will not adjust its settings to match those of its peer.

6 Click the **Refresh all DCBX Settings** button to update the settings of the DCBX sub-tab.

7 Click the **Reset Config** to return all settings to their default values.

Configure Tab

The **Configure** tab lets you set the DCBX settings to be sent to the port's peer.

DCBX Address

1 Set the destination Ethernet MAC address in the **LLDP Dest MAC** field.

2 Set the source Ethernet MAC address in the **LLDP Src MAC** field.

3 Set the Xgig chassis Ethernet MAC address used for DCBX exchanges in the **Chassis ID MAC** field.

4 Set the Port ID MAC address in the **Port ID MAC** field.

5 Set the LLDP (DCBX) interval timer that governs the repeat frequency of outgoing DCBX frames in the **Keep Alive Interval** field. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Keep Alive Interval** field.

6 Set the LLDP (DCBX) Time To Live value that is inserted into all outgoing DCBX frames in the **Keep Alive Timeout** field. Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Keep Alive Timeout** field.

Protocol Control

1 Set the DCBX sequence number for the current exchange in the **Rx Sequence Number** field.

2 Set the DCBX acknowledgment counter for the current exchange in the **Tx Acknowledge Number** field.

Priority Groups ETS

1 Set the Priority groups settings in this pane. The first column lists the Priority Group IDs (0-7).

2 Select the Priority Index or COS for the corresponding Priority Group ID.

Priority Flow Control

1. Select the DCBX Priority Flow Control Administration Mode enabled mask in the **Class of Service (CoS) Mask** pane. Each bit represents a Class of Service (COS) for which PFC is enabled.
2. Enter the **Number of Traffic Classes (TC) supported.**

Applications

The Applications pane displays the DCBX Application Protocol Feature. By default there will be two (2) applications listed in the application list.

To add a new application:

1. Click the **Add application** button to open the **DCBX Application** dialog box.
2. Enter the new application's ID in the **App ID** field.
3. Select the new application's Type from the **App Type** drop-down menu.
4. Select the application priority mask by choosing the appropriate check boxes in the **App Priority Mask** section.
5. Click **Ok**.

To delete an application:

1. Select the application to delete from the application list.
2. Click on **Remove application**.

Logical Link Down LAN LLS

This pane will display the DCBX Logical Link Down LAN Logical Link Status (LLS) flag values.

Logical Link Down FCoE LLS

This pane will display the DCBX Logical Link Down Link Logical Link Status (LLS) flag values.

Local (Load Tester) Tab

The **Local** tab displays the DCBX related settings for the selected port that it has acquired from its peer. When the Master Mode is enabled, the ports own settings will be displayed.

Peer (Remote) Tab

The **Remote** tab displays the DCBX settings or configuration of the port's peer. By default, when the Master Mode is disabled, the settings displayed in the **Local** tab will be the same as the **Remote** tab.

Ethernet tab

The Ethernet sub-tab lets you manage the Ethernet parameters and settings of the FCoE ports locked to Load Tester.

To configure Ethernet ports:

1. Click on the **Configuration** drop-down button on the Xgig Maestro main window.
2. Select **Configure Ethernet Ports** to open the **Ethernet** sub-tab in the 10G Configuration tab in the Load Tester Device Window.
3. Select the port from the list on the left panel. The configuration panel on the right will update with the settings for the selected port.
4. Set the alias for the selected port. Enter the alias in the **Alias** text field. You can set the alias if only one port is selected.
5. Enable or disable the FCoE Login by selecting **Enabled** or **Disabled** from the **FCoE Login** drop-down menu. If you prefer to use only Ethernet traffic, select **Disabled**.
6. Click the **MAC/IP Address Configuration** button to open the **MAC/IP Configurations** window where you can set the number of MAC sources to use and block of IP addresses to be associated with selected port. Note that it is up to you to ensure that the IP addresses are in the intended subnet and that there are no duplicate addresses in the session.

MAC/IP Address Configuration Window

The MAC/IP Configurations window lets you set the number of MAC sources used by a selected port. It also allows you to set the first or Base Ethernet Source MAC Address when blasting Ethernet frames. This value is then incremented by the Step value to determine additional Ethernet MAC Address values.

To set the MAC addresses:

1. Select the port from the drop-down menu.
2. Enter the number of MAC sources to be associated to a specific port.
3. Enter the first Ethernet Source MAC Address in the Base field.
4. Enter the step value in the Step field.
5. Click **Generate IP Addresses** to apply the settings and generate the MAC Addresses. The **IP Address Settings** grid will be updated with the new settings.

To set the IP Addresses

1. Click on the cell of the IP Address property you want to edit for every MAC address. For example, if you want to change the number of IP sources for the first MAC address row, click on the cell under the IP Sources column.
2. Enter the value.
3. Once done, click **Close**.

Inter-Packet Gap

1. Set the guaranteed minimum number of idles between successive frames in the **Minimum IPG** field. You can set a value from 3 to 65535.

2 Use the **up** or **down** button to increase or decrease the value, or enter it directly. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button at the right side of the **Minimum IPG** field.

Address Learning

1 Select **Enable** to enable Ethernet MAC Learning for the selected port.
2 Select the length of the Learning Frames to be sent for each MAC address in use by the port from the **Frame Size** drop-down menu.

Port Based Override VLAN

If this is **Enabled**, the value set will be used during blasting of traffic.

1 Select Class of Service.
2 Select the class from the drop-down menu.

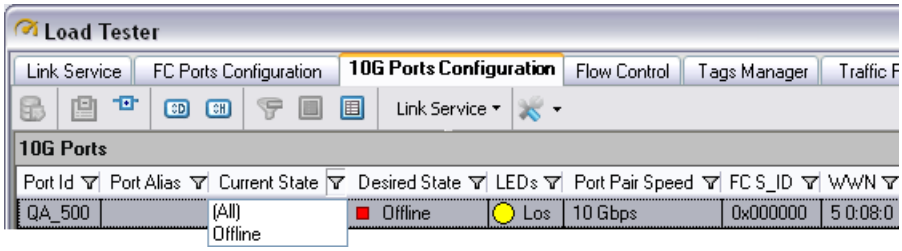
Organizing Ports

Each port property column has a **Filter** button to allow you to apply filters.

To apply a filter:

1 Click on the **Filter** button and a drop-down list will appear listing all values for that property from all ports (refer to Figure 40).

Figure 40: Filter Options



2 Select the appropriate value.

The filter icon for that property now appears blue to indicate the filter has been applied. You can apply additional filters to further refine the list of ports.

Configuring the Flow Control Tab

You can configure the traffic flows for individual or multiple FC or FCoE ports locked to Load Tester through the **Flow Control** tab in the Load Tester Device Window. The **Flow Control** tab is divided into the Ports list and the flow control settings.

Figure 41: Flow Control Tab for FC

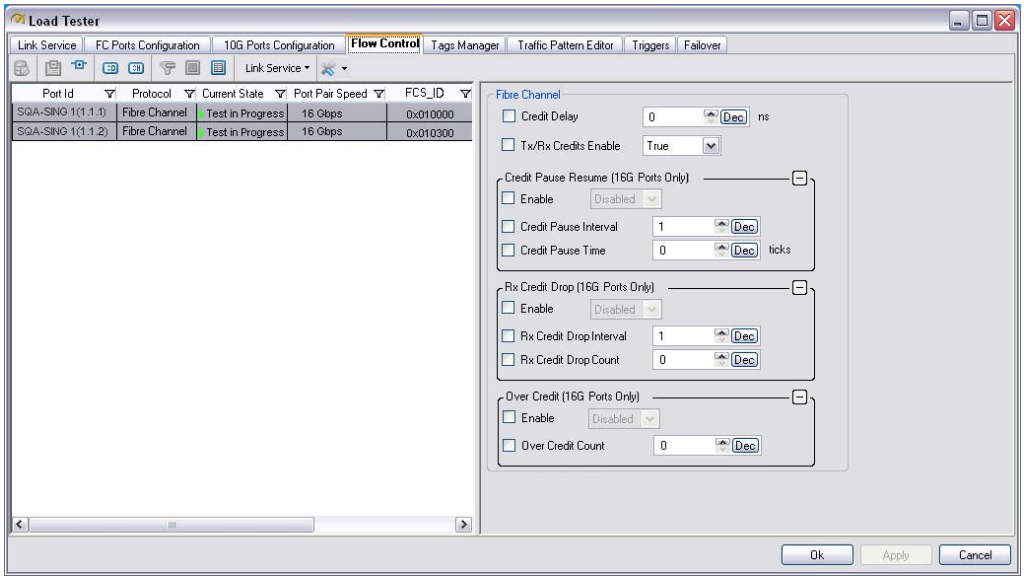
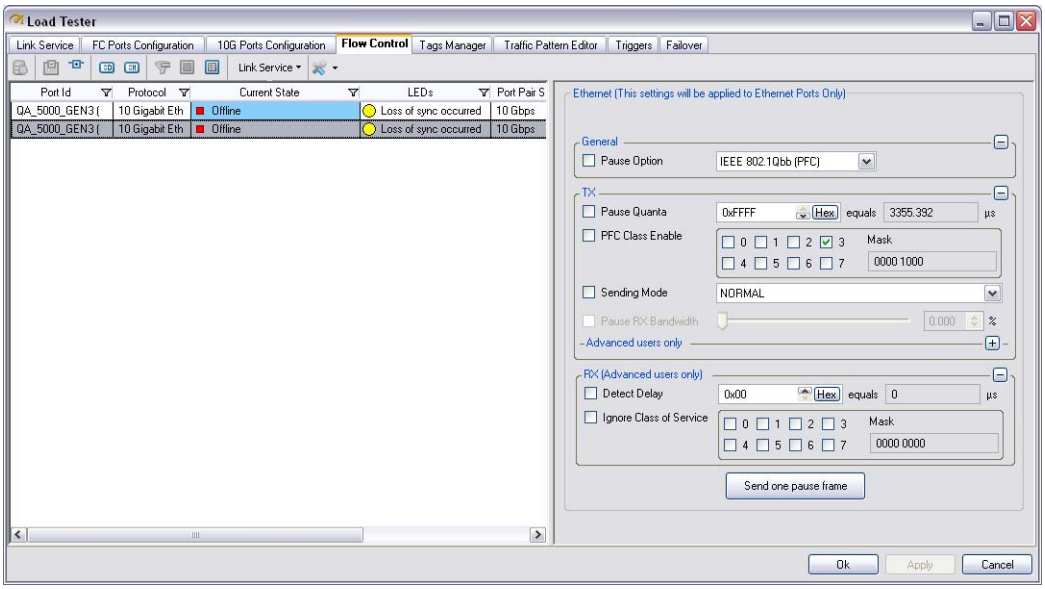


Figure 42: Flow Control Tab for FCoE



Note: If both FC and FCoE ports are selected, the Flow Control settings will not be available to be changed.

Flow Control Parameters (FC)

These flow control settings for Fibre Channel Ports are displayed in Figure 41:

Credit Delay

This option assists the user in creating slow device emulation in a Fibre Channel environment. The port will require that N nanoseconds have elapsed before issuing another credit.

The table below provides the duration (in nanoseconds) of one tick.

- For 4G and 8G blades, this is the period required to transmit one Dword.
- For 16G blades, this is the period required to transmit two Dwords.

Table 12: Duration per Transmitted Tick

Speed	Blade	Tick Duration
16 Gig	16G Blade	4.71 ns
8 Gig	16G Blade	9.41 ns
8 Gig	8G Blade	4.71 ns
4 Gig	16G Blade	18.8 ns
4 Gig	8G/4G Blades	9.41 ns
2 Gig	8G/4G Blades	18.88 ns
1 Gig	8G/4G Blades	37.64 ns

For any given speed, a nanosecond delay less than values above will have no effect.

To create a slow device the delay value must exceed the frame transmit time for the given speed.

```
16G Blade:      (((frame size SoF-EoF) + minimum IFG) /8) * ns per 2 Dwords
4G/8G Blades:   (((frame size SoF-EoF) + minimum IFG) /4) * ns per Dword
```

For example, in the case of a 4G Blade, a full size payload with a minimum IFG of 6 is 2172 bytes.

```
2172 / 4 = 543 Dwords
543 * 9.41 = 5109.63 -> 5109 ns per frame
```

To create a slow device the value provided must exceed 5109.

A value of 10219 will reduce throughput by approximately 50% at 4 Gig.

Tx/Rx Credits Enable

This turns the credit engine on/off which enables/disables the credit functions.

Credit Pause Resume (16G Ports Only)

Enable

This enables Load Tester to send credits and receive frames for the specified number of credit transmissions/frame receipts (or **Credit Pause Interval**) and then pause for a specified time (or **Credit Pause Time**) before the process begins again.

Credit Pause Interval

This sets the number (1 to 0x7fffffff) of frames received before pausing this cycle.

Credit Pause Time

This sets the time in ticks (1 to 0x7fffffff) that the pause is allowed before resuming the credit transmissions/frame receipts cycle.

Note: The time in nanoseconds of 1 tick is different based on the speed of the 16G blade. The following shows the speed and the equivalent time in nanoseconds for 1 tick: 16G - 4.71ns; 8G - 9.41ns; 4G - 18.88ns

Rx Credit Drop (16G Ports Only)

Enable

After receiving the specified number of credits (**Rx Credit Drop Interval**), this enables Load Tester to drop the specified number of consecutive credits (Rx Credit Drop Count), starting from the last credit received in each interval. Dropped credits are credits replaced with IDLEs. After the specified number of credits are dropped, this process begins again.

Rx Credit Drop Interval

This sets the number (1 to 0x7fffffff) of credits to receive before starting to drop the consecutive credits. Dropping of credits begin with the last credit received in each interval.

Rx Credit Drop Count

This sets the number (0 to 0xffff) of consecutive credits that are dropped and replaced with IDLEs.

Over Credit (16G Ports Only)

Note: The **Over Credit** feature may only be configured when the selected ports are in the Offline or Laser Off (pre-login) states. The **Credit Pause Resume** and the **Rx Credit Drop** features may be configured when the selected ports are in any state, including while a test is running.

Enable

This enables a Load Tester port to operate with a greater Tx Credit Count than the negotiated value at login by the configured **Over Credit Count** setting.

Over Credit Count

This sets the number (0 to 0x7fff) of extra frames that are to be transmitted over the negotiated Tx Credit Count (refer to Max **TX Credits** and **TX Credits Available** on the Physical Ports tab and **TX Credits** on the Traffic tab's TX Pattern Based View).

Flow Control Parameters (FCoE)

These flow control settings for Ethernet Ports are displayed in Figure 42:

General

Pause Option

This option lets you set whether the PFC Pause frames are enabled. If selected, PFC Pause frames are detected and transmitted; otherwise non-PFC Pause frames are detected and transmitted.

TX

Pause Quanta

This is the time defined in PAUSE quanta sent in the PAUSE frame.

PFC Class Enable

This option allows you to set the class enable vector that will be sent in a PFC pause frame.

The bits set in the bitmask correspond to the classes of service that will be paused in the receive datapath. This API only applies when PFC is enabled.

Sending Mode

This option allows you to configure the Load Tester to transmit pause frames at a constant interval/rate.

Possible modes are:

NORMAL - Load Tester does not generate test pause frames.

TXOFF_ONLY - Using TXOFF_ONLY mode means sending PAUSE frames with non-zero pause time (TXOFF) only. The time from one PAUSE frame to the next PAUSE frame (pause duration) is set in "TX off TX off" duration.

If pause quanta is equal to pause duration then the traffic will always be paused. Normally, pause quanta should be smaller than pause duration.

TXOFF_TXON - In this mode, Load Tester sends PAUSE frames with non-zero pause time (TXOFF) followed by a zero pause time frame (TXON). The duration from one TXOFF to next TXON is the "TX off TX on" duration. The duration from one TXOFF to the next TXOFF frame is set in the "TX off TX off" duration.

TXOFF_REPEATED_TXON_REPEATED: In this mode, LT sends repeated pause frames with non-zero pause time (TXOFF) followed by repeated pause frames with zero pause time. The interval between 2 consecutive TXOFF frames or 2 consecutive TXON frames is set in "Repeat Interval".

Pause RX Bandwidth

This option allows you to set the percentage of time the RX datapath will be paused in step-sizes of 1/1000 of a percent.

Note only those enabled classes of service will be paused in PFC Mode.

This option lets you specify the desired RX datapath bandwidth. Sometimes we may not be able to achieve the bandwidth input without adjusting some other parameters, such as settings for the Pause Quanta Value, TX off TX off duration, and others. If this is the case it will set the bandwidth to the closest possible and you can get the real bandwidth by calling the corresponding get function.

For advanced users, the following options are available:

TX off TX off duration

This option specifies the duration between sending the first TXOFF pause frame and the next TXOFF pause frame.

TX off TX on duration

This option only applies when sending mode selected is **TXOFF_TXON** or **TXOFF_REPEATED_TXON_REPEATED**. In these modes, this option specifies the duration between sending the (first) TXOFF pause frame and the (first) TXON pause frame.

Note the value set in this option should be less than the value set with **Pause Quanta** option, and the value set here needs to be less than the value set in **TX off TX off duration** (if it is non-zero). Invalid value will get warning message, and the pause frames may not be generated correctly and the **Pause RX Bandwidth** may not get the correct result.

Repeat Interval

This option only applies when **TXOFF_REPEATED_TXON_REPEATED** is set as the sending mode.

It configures the duration between two consecutive TXOFF pause frames OR the duration between two consecutive TXON pause frames.

Note the value set in this API needs to be less than the value set with the **TXOFF_TXON** option. Invalid value will get warning message, and the pause frames may not be generated correctly and **Pause RX Bandwidth** may not get the correct result.

RX

These options are for advanced users only.

Detect Delay

This option allows you to delay the RX detection of pause frames. The step-size for this value is 51.2 ns (1 pause quanta).

Ignore Class of Service

This API allows the user to specify which classes of service will be lossy based on a bitmask.

Lossy channels ignore received pause frames.

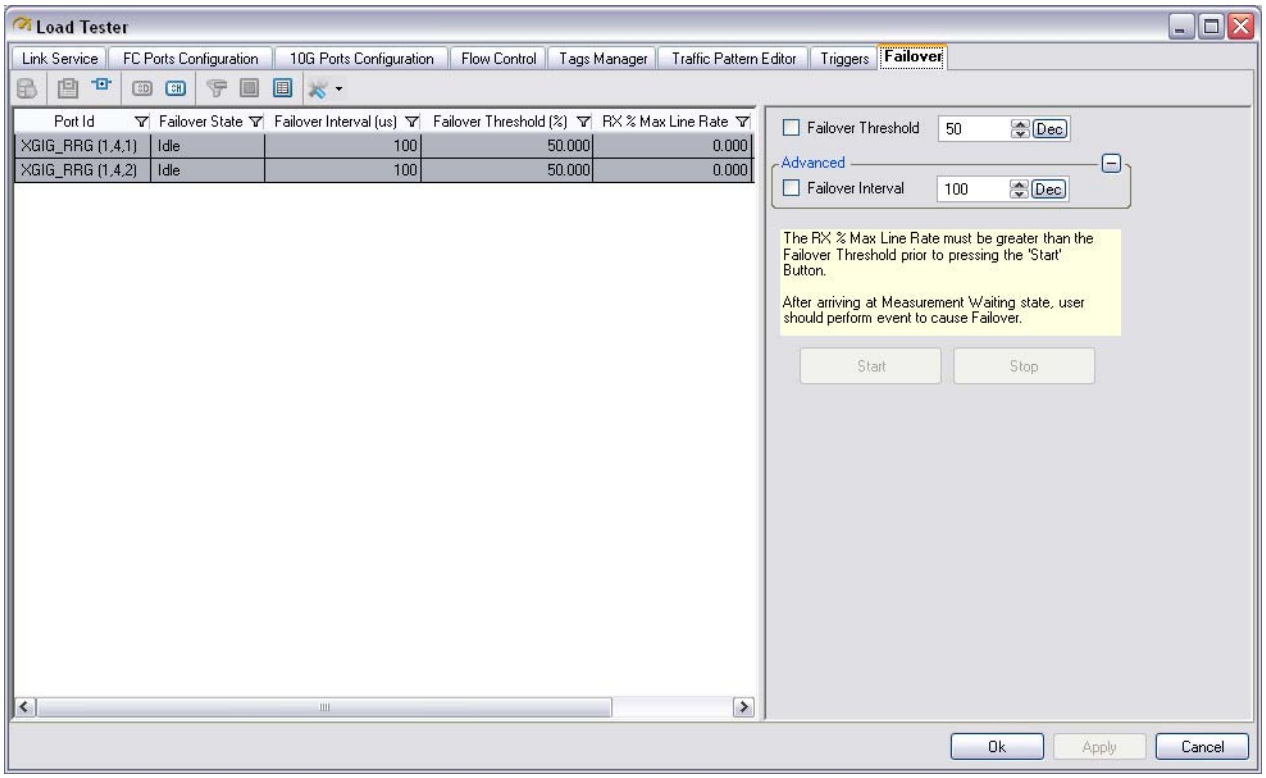
Send one pause frame button

This button invokes all ports to send a single pause frame when selected.

Configuring the Failover Tab

The Failover tab lets you set the failover settings for Fibre Channel Load Tester ports. Failover occurs when the Rx % Max Line Rate falls below the failover threshold.

Figure 43: Failover Tab



Note: Only 4G and 8G FC ports are displayed in the ports list. Failover is not supported in 10G FCoE.

Operation buttons on the Ports List in the Failover tab are listed below:

Apply - sends the changes in the configuration to the locked ports.

Expand Groupboxes - expands all the configuration groupboxes

Collapse Groupboxes - collapses all the configuration groupboxes

Numeric Editors in Decimal - change all the numeric editors into decimal format

Numeric Editors in Hexadecimal - change all the numeric editors into hexadecimal format

Clear Filters - removes all filters set for the Ports List

Select all Ports - select all ports listed in the Ports List

Deselect all Ports - deselect all ports selected

The options in the Failover settings are:

Failover Threshold

This option lets you set the threshold, in terms of percentage of the maximum line rate (1 - 99), for the selected port. This option is only supported on Fibre Channel ports.

Failover Interval

This option lets you set a time interval in number of microseconds (1 - 0x133A8) for the selected port(s). The system determines whether the traffic count reaches a defined threshold in each interval. This option is only supported on Fibre Channel ports.

Start Button

Pressing this button will start timing failover occurrences in the selected port(s).

Stop Button

Pressing this button will stop timing failover occurrences in the selected port(s).

Note: The RX % Max Line Rate of the selected port(s) must be greater than the Failover Threshold prior to pressing the **Start** button.

Once the selected port(s) arrives at **Measurement Waiting** state, you should perform event to cause Failover.

Configuring Multicast/Broadcast Ports

Once you have locked ports on a legacy 8G blade for use with Load Tester and selected the Multicast/Broadcast option from the **Configuration** button (see page 17), you can access the Multicast/Broadcast Configuration tab is opened so you can configure the settings for these ports. The Multicast configuration is described below and the Broadcast configuration is described on page 121.

Multicast Configuration

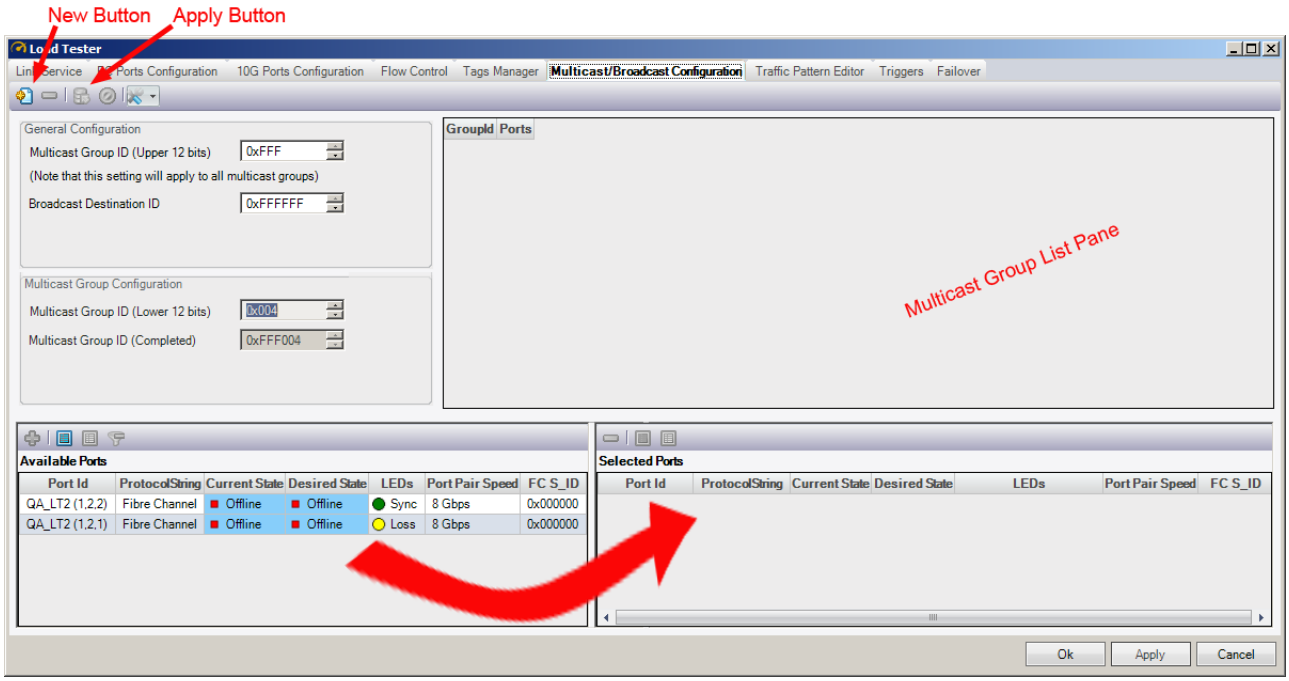
To configure a multicast:

Note: If you have the need, Multicast allows you to set up Implicit Fabric Login for all ports. If you would like Implicit Fabric Login, do this as the first step. Refer to "Implicit Fabric Login" on page 96 for instructions.

Multicast/Broadcast Configuration Tab

1 From the main Load Tester tab, select the **Configuration** button and choose **Multicast/ Broadcast** from the list of options. Refer to Figure 3 on page 17. This opens the **Multicast/ Broadcast Configuration** tab shown in Figure 44.

Figure 44: Multicast Configuration



2 In the General Configuration pane, set the Multicast Group ID (Upper 12 bits) to the desired value.

When the Multicast Group ID (Upper 12 bits) is modified, the update will apply to all of the groups that have been created.

3 Select the **New** button. This makes the Multicast Group Configuration pane active.

4 In the Multicast Group Configuration pane, set the Multicast Group ID (Lower 12 bits) to the desired value. Note that the complete group ID is displayed in the Multicast Group ID (Completed) text box.

5 Drag and drop the desired port(s) from the Available Ports list to the Selected Ports list. See the large arrow near the bottom of Figure 44.

6 Click the **Apply** button to create the Multicast Group which is now displayed in the Multicast Group List pane in the upper right pane. The multicast group's Group ID and Port(s) are displayed.

7 Repeat steps 3 through 6 to create additional multicast groups. A maximum of 256 groups are allowed.

If needed, multiple ports can be selected for each Multicast Group ID created. Up to a maximum of 64 ports can be selected for each Group ID.

8 When all of the groups are created, select the Traffic Pattern Configuration tab.

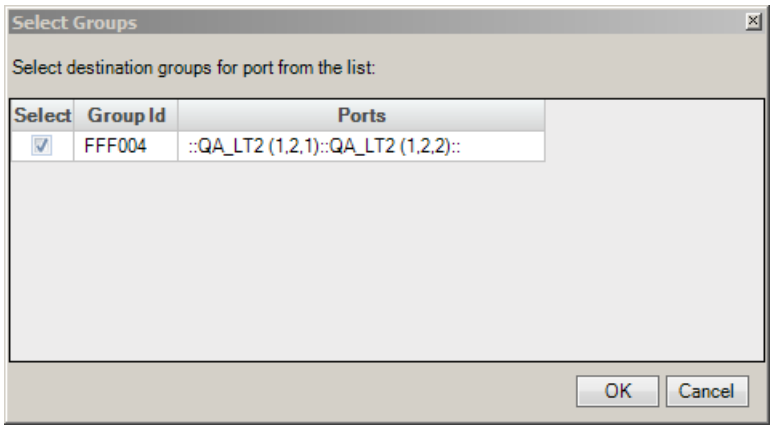
Traffic Pattern Configuration Tab

9 On the Topology tab of the Traffic Pattern Configuration tab, select **Multicast** from the Topology drop-down list. See "Topology" on page 130.

10 On the Ports Selection tab of the Traffic Pattern Configuration tab, drag and drop the desired port(s) from the Available Ports pane to the Selected Ports pane. See "Available Ports Pane" on page 131 and "Selected Ports Pane" on page 132.

11 For the first port in the Selected Ports pane, select the **Change...** button in the Groups column to display the Select Groups dialog box (shown in Figure 45).

Figure 45: Select Groups Dialog Box



12 Select the destination groups for port and then click the **OK** button. The destination group IDs for the port are now displayed in the Destination Groups column on the Ports Selection tab.

13 Repeat steps 11 and 12 for additional ports.

14 Click the **Apply** button to apply the changes and then click the **OK** button to close the Traffic Pattern Editor window.

The Multicast configuration is now complete.

Broadcast Configuration

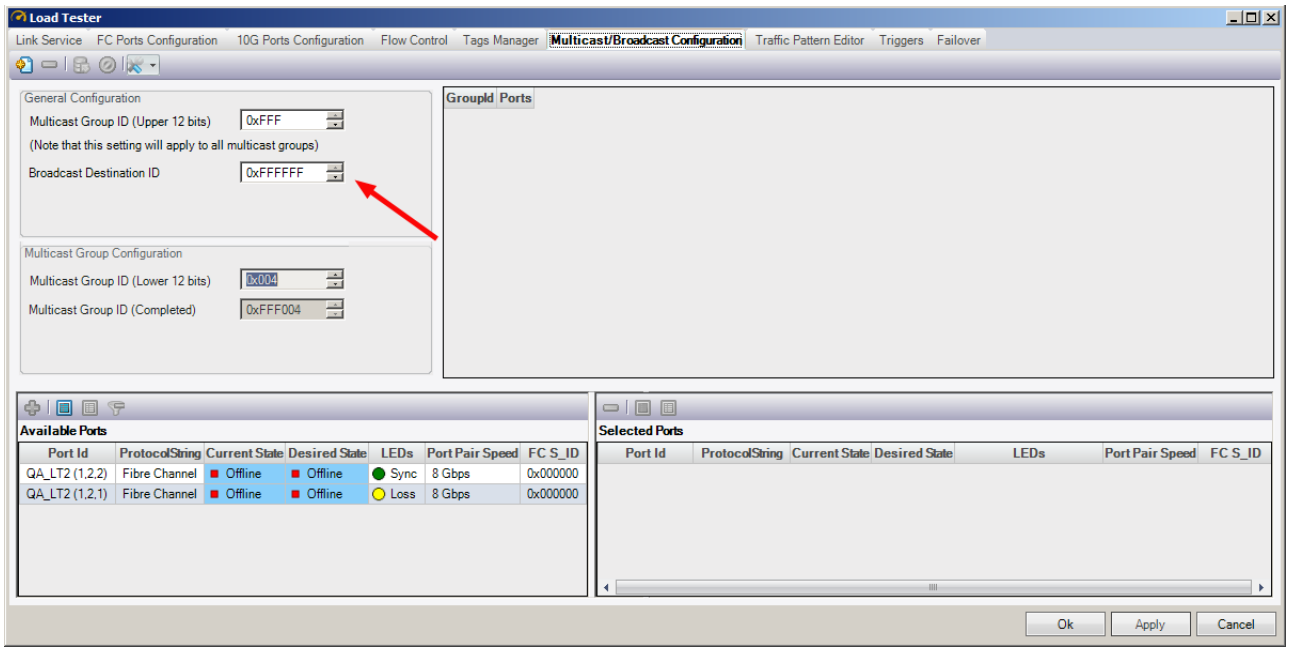
To configure a broadcast:

Note: If you have the need, Broadcast allows you to set up Implicit Fabric Login for all ports. If you would like Implicit Fabric Login, do this as the first step. Refer to "Implicit Fabric Login" on page 96 for instructions.

Multicast/Broadcast Configuration Tab

1 From the main Load Tester tab, select the **Configuration** button and choose **Multicast/ Broadcast** from the list of options. Refer to Figure 3 on page 17. This opens the **Multicast/ Broadcast Configuration** tab shown in Figure 46.

Figure 46: Broadcast Configuration



2 In the General Configuration pane, set the Broadcast Destination ID to the desired value.

3 Click the **Apply** button to apply the Broadcast Destination ID.

4 Select the Traffic Pattern Configuration tab.

Traffic Pattern Configuration Tab

5 On the Topology tab of the Traffic Pattern Configuration tab, select **Broadcast** from the Topology drop-down list. See "Topology" on page 130.

6 On the Ports Selection tab of the Traffic Pattern Configuration tab, make sure the desired port(s) are in the Selected Ports pane.

For the Broadcast topology, ports are placed in the Selected Ports pane. However, for other topologies, ports are placed in the Available Ports pane. See "Available Ports Pane" on page 131 and "Selected Ports Pane" on page 132.

7 Click the **Apply** button to apply the changes and then click the **OK** button to close the Traffic Pattern Editor window.

The Broadcast configuration is now complete.

Chapter 4

Creating Tags

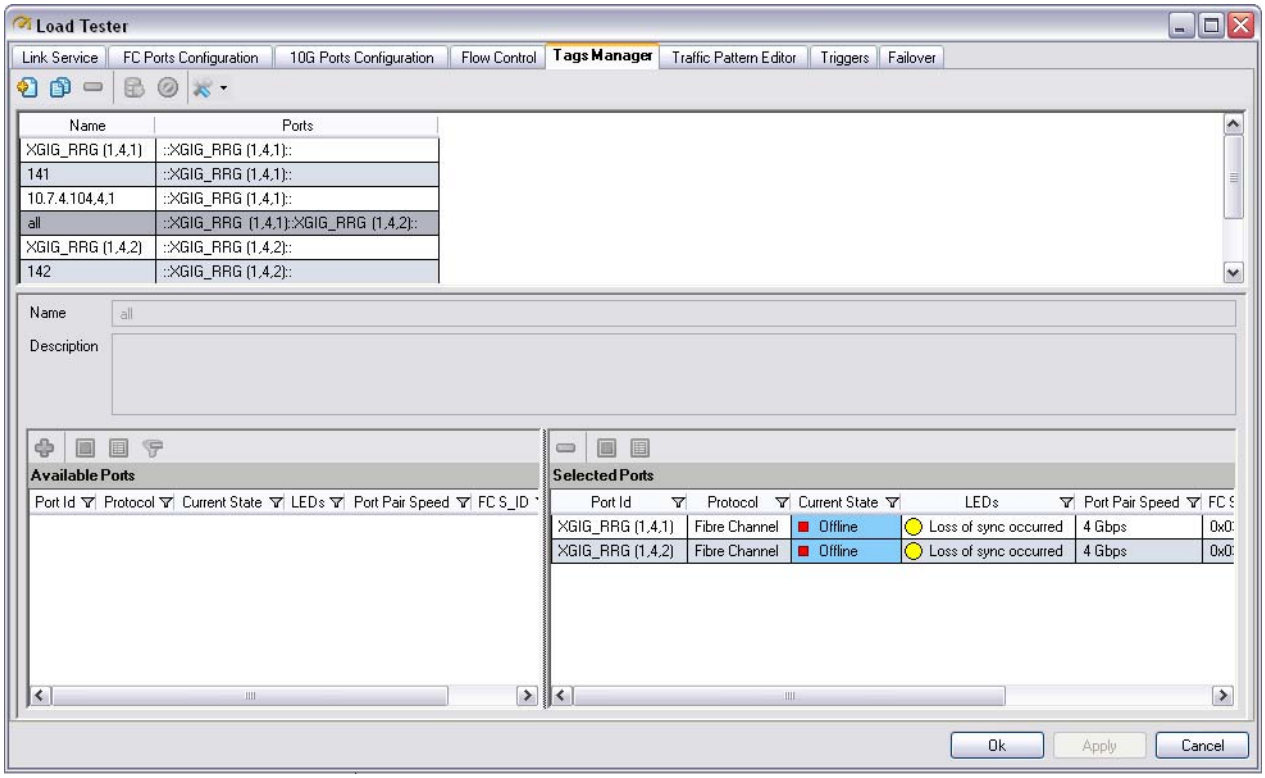
In this chapter:

Tags are an organizational tool for ports in Load Tester. A tag contains a name, a description, and a list of ports to which the tag is applied. You can apply a tag to any number of ports. When configuring ports, configuring traffic patterns, or setting up multi-port link service, you can use tags to quickly find a pre-defined set of ports that you want to performs an action on. When a tag uses an API command as a parameter, the API command will apply to all the ports associated with the tag.

The Tags Manager

The Tags Manager tab allows you to create, edit, or delete the tags used by Load Tester (refer to Figure 47).

Figure 47: Tags Manager Tab.



Available tags are listed on the tags list with their description. Selecting a tag from the list will update the **Name** and **Description** fields at the lower part of the dialog box. The **Selected Ports** list will also be updated with the ports associated with the selected tag.

Note: System tags cannot be deleted. Systems tags are the tags created by the load tester when a user opens the port.

Creating Tags

To create tags:

1. Click the **New**  button. The tags list will be disabled and focus will be on the lower half of the dialog box.
2. Enter a name for the tag in the **Name** text box.
3. Enter a description for the new tag in the **Description text** box. A detailed description makes the tag easier to use.
4. Click on the port to include into the tag in the **Available Ports** list. To sort or organize the list of ports available refer to Chapter 3 “Organizing Ports”.
5. Click the **Add** button to add the selected port to the **Selected Ports** list.
6. Click the **Apply**  button.

The new tag is added to the tags list.

Copying Tags

To copy tags:

1. Select the tag to copy from the tags list.
2. Click the **Copy**  button. The name of the tag will be appended with “**(Copy)**”.
3. Enter a new name for the copied tag or retain it.

The new tag is added to the tags list.

Editing Tags

To edit tags:

1. Select the tag you want to edit from the Tags list.
2. Add a new port to the tag by selecting the port to add and clicking the **Add** button from the **Available Ports** list**.**
3. Remove a port from the tag by selecting the port from the **Selected Ports** list and clicking the **Delete** button.

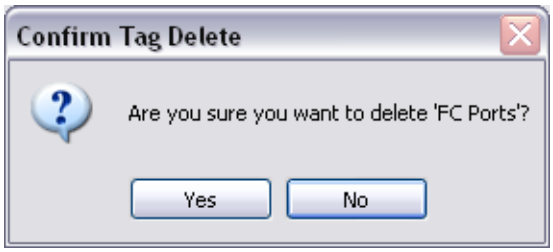
The tag is updated in the tags list.

Deleting Tags

To delete tags:

1. Select the tag to delete from the tags list.
2. Click the **Delete** button.
3. Click **Yes** on the **Deleting tag** dialog box.

Figure 48: Tag Deletion Confirmation Dialog Box



The tag is deleted in the tags list.

Chapter 5

Creating and Managing Traffic Patterns

In this chapter:

The term traffic pattern applies to a traffic profile engine. Each Physical N_Port can have up to eight traffic profile engines. Each traffic profile engine contains a traffic pattern configuration, which is a combination of Physical N_Port traffic topologies and traffic configuration settings such as traffic type and payload type, payload size, and seed information.

The Traffic Pattern concept allows a group of ports that have been assigned with a port topology to also share all the configurations related to the traffic profile engines. When you create a traffic pattern, each port that transmits in the traffic pattern will allocate a single Traffic Profile Engine. In the case where the Port Topology is bi-directional, all ports will allocate a single Traffic Profile Engine.

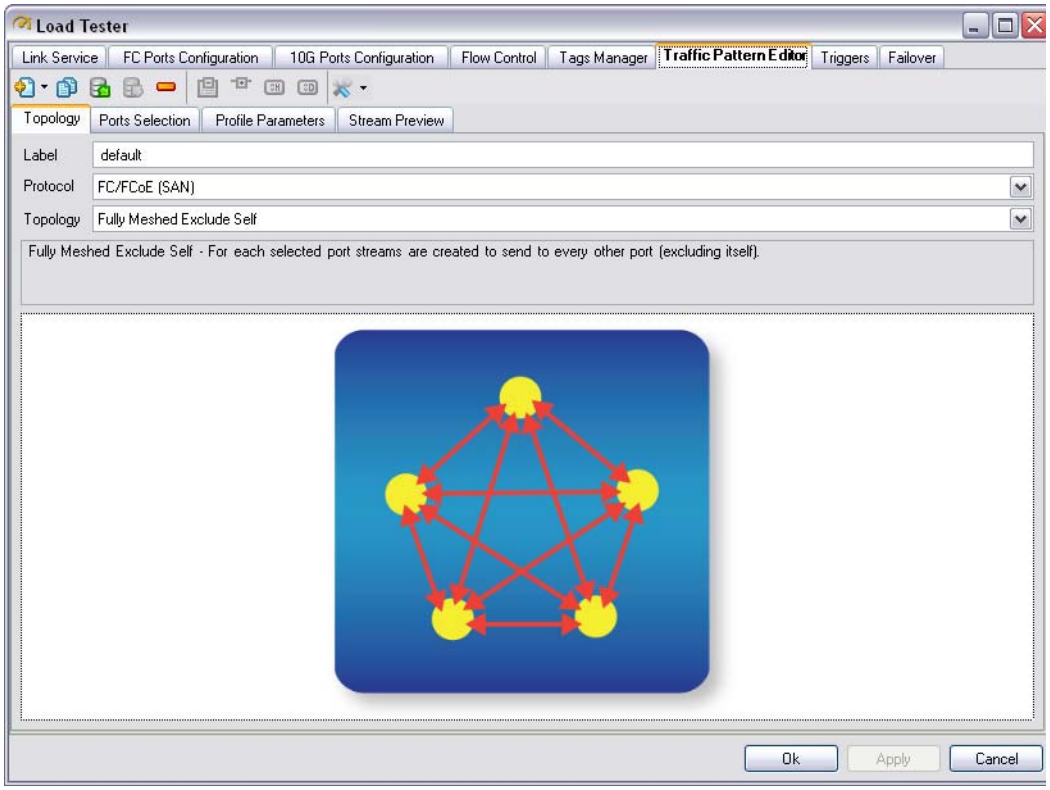
Creating and saving traffic patterns is a good way to preserve test configurations so that you can reuse them.

Traffic Pattern Editor Tab

The Traffic Pattern Editor tab is where you create or edit a traffic pattern to be used by the Xgig Load Tester.

Note: The traffic pattern is not editable while a test is in progress.

Figure 49: Traffic Pattern Editor Tab



Operation buttons on the Ports Configurations tabs are listed below:

Create New - lets you create a new traffic pattern manually or by using the Traffic Pattern Wizard

Copy - creates a copy of the traffic pattern and appends “(Copy)” to the Label. You can then save the new traffic pattern with any change you made.

Load - opens a dialog box where you can select the traffic pattern to edit.

Apply - sends the changes in the traffic pattern to the Load Tester.

Delete - deletes the currently loaded traffic pattern.

Expand Groupboxes - expands all the configuration group boxes

Collapse Groupboxes - collapses all the configuration group boxes

Numeric Editors in Decimal - change all the numeric editors into decimal format

Numeric Editors in Hexadecimal - change all the numeric editors into hexadecimal format

There are three sub-tabs: **Topology**, **Ports Selection**, and **Profile Parameters**. These three tabs are further discussed in the following sections.

Topology

This tab lets you configure the topology to be used by a traffic pattern.

Label

This field contains the name of the traffic pattern.

Protocol

This field lets you select the protocol to use with the traffic pattern.

Topology

This lets you select the topology used by the traffic pattern.

When you change from a topology with high number of ports such as fully-meshed topology, to a topology with less ports, such as partially meshed or point-to-point topology, the unneeded or unused ports will still be displayed with "Test in Progress" state in the TX Ports and RX Physical Ports tables.

Description box

This pane contains the description of the topology selected in the Topology drop-down menu.

Topology diagram

This pane displays the graphical representation of the topology currently selected in the Topology drop-down menu.

Ports Selection

This tab lets you configure the ports used in the selected traffic pattern.

Label

Displays the traffic pattern name

Protocol

Displays the protocol used by the traffic pattern

Stream Generation Mode

This function adjusts the topology table generation for the selected traffic pattern. The default of round robin conforms to RFC 2889 section 5.1.3, the weighted option (prior to Maestro 6.1) generates topologies where all the source ports begin with the same destination port.

Topology

Displays a graphical representation of the selected topology. To see the list of available topologies, click on the button to open the drop-down list.

Selection

This option lets you choose whether to select the ports to be used with the traffic pattern by individual ports or by tags.

Note: Selection is disabled for Point-to-Point Bidirectional and Point-to-Point Unidirectional topologies. The **Select by Ports** selection is chosen by default for these topologies.

Also note that when virtual ports are available in these topologies, the source/destination port pair must be physical port. Dragging and dropping NPIV ports will add NPIV ports to its physical port in a form as “PhysicalPort::Index1::Index2::IndexN”.

Weighted Ports

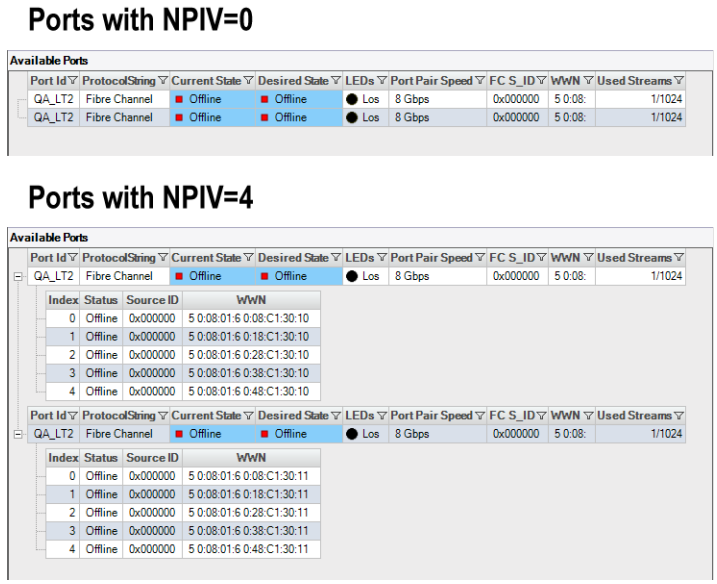
This option allows you to select the weighted port for traffic generation. When a port is set as a “Weighted Port”, all source ports sends first to that port.

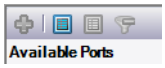
Available Ports Pane

Lists the ports locked as Load Tester that are available for use with the traffic patterns.

Figure 50 shows the physical ports available without virtual ports and both the physical and virtual ports available. Both physical and virtual ports may be selected *individually* and moved to the Selected Ports pane(s). Note that with NPIV ports and Index 0 representing the physical port itself, the total number of ports displayed is the NPIV setting (NPIV = 4) plus the physical port (or a total of 5 ports in this case).

Figure 50: Available Physical and Virtual Ports



The operation buttons on this pane are: 

Add to Selected Ports - moves the selected port to the Selected Ports list.

Select all Ports - selects all ports in the list

Deselect all Ports - unselects all ports in the list

Clear Filters - removes all the filters that were set for the list of ports.

To add ports from the Available Ports pane to the Selected Ports pane(s):

1. Select the port from the list. You may select physical or virtual ports individually.
2. Click on the **Add to Selected Ports** button. You can also click and drag the port from the Available Ports to the Selected Ports.
3. Repeat the step above for the rest of the ports you want to add.

Selected Ports Pane

Note: The name of this pane changes based on the topology selected.
– This pane is named the **Selected Ports** when the selected topology is Self, Pair Port, Pair Port Tx Odd, Pair Port Tx Even, Fully Meshed Exclude Self, and Fully Meshed Include Self. (**Mono mode**)
– Two panes are displayed (named **Selected Source Ports** and **Selected Destination Ports**) when the selected topology is either Meshed Bidirectional or Meshed Unidirectional. (**Source/Destination mode**)
– This pane is named the **Selected Ports Pairs** when the selected topology is either Point-To-Point Bidirectional or Point-To-Point Unidirectional. (**Pair mode**)

Lists the ports that are used in the traffic pattern.

The operation buttons on this pane are: 

Removes Selected Ports - moves the selected port to the Available Ports list.

Select all Ports - selects all ports in the list

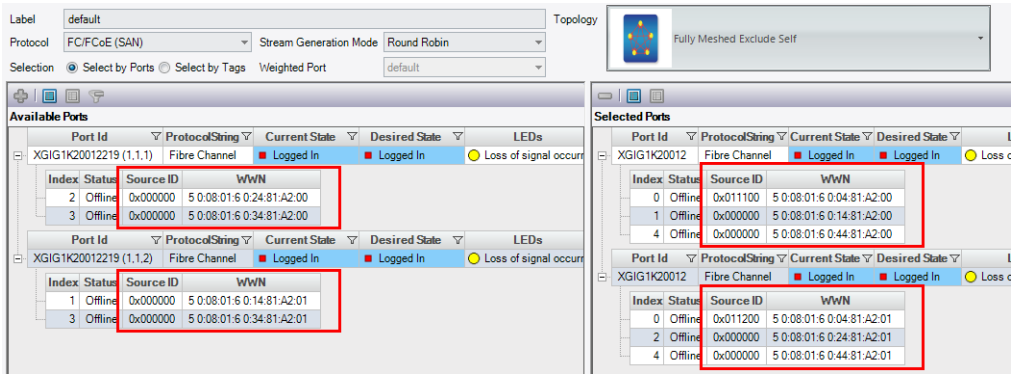
Deselect all Ports - unselects all ports in the list

To remove a port from the Selected ports:

1. Select the port from the list. You may select physical or virtual ports individually.
2. Click on the **Remove from Selected Ports** button. You can also click and drag the port from the Selected Ports to the Available Ports.
3. Repeat the step above for the rest of the ports you want remove.

Running the test will add the Source ID and the World Wide Name (WWN) values to the ports as shown in Figure 51.

Figure 51: Source ID and WWM Values Added



Profile Parameters

This tab lets you configure the parameters of the profile to use with the traffic pattern.

Label

This displays the traffic pattern name.

Protocol

This field displays the protocol used for the traffic pattern.

Topology

This field displays the topology used for the traffic pattern.

Load Characteristics Pane

This pane contains options to configure the load characteristics of the traffic pattern.

Desired throughput

Sets the throughput of the traffic pattern. The term ‘average’ means the average throughput expects to achieve over the duration of several bursts. The software will automatically adjust the user input value to the closest possible value.

When sending non-Dword-aligned frames, the full line rate will not be maintained according to the protocol specification.

Note: Due to 16G hardware limitation, certain settings or combination of settings in Load Tester may result in the configured line rate and/or IFG not being achieved. This can happen when the gap between data frames becomes too small, and/or data frames is not Dword-aligned.
Examples of such settings include the following (or combinations of the following):
-- small/zero payload size
-- low IFG (e.g. 3,4)
-- payload size that is not 8N+4
When such conditions happen, Load Tester may insert additional gap in the form of IDLE/ARB(FF), which can result in larger IFG which will affect throughput.

Continuous

Select **Continuous** to use a traffic profile with a continuous load. You can adjust the intended load before or during the test.

Burst

Select **Burst** to create a traffic profile with an average load and a burst load for a specified number of frames.

If you select Burst, **Burst Throughput** and **Burst Length** options would be available for editing.

Burst Throughput - load during the burst

Burst Length - the number of frames sent during a single burst.

Burst Time

This field displays the burst time (in microseconds) for specific traffic. If **Continuous** mode is selected, this field will display the length of time in microseconds from SOF to EOF for each frame transmitted. If **Burst** mode is selected, this field will display the length of time in microseconds from start to end of burst including Idles between burst frames.

This is only valid if all ports are configured for at the same speed.

Idle Time

This fields displays the idle time (in microseconds) for the specified traffic. If **Continuous** mode is selected, this field will display the length of time in microseconds between each frame sent. The amount of time Idles are sent. If **Burst** mode is selected, this field will display the length of time in microseconds between burst frame sets. The amount of time Idles are sent between bursts.

This is only valid if all ports are configured for at the same speed.

Intra-Burst Frame Time

This field displays the frame time within a burst. If **Continuous** mode is selected, this field will display the length of time in microseconds between each frame sent. The amount of time Idles are sent. If **Burst** mode is selected, this field will display the length of time in microseconds between each frame sent. The amount of time Idles are sent between frames in the burst.

This is only valid if all ports are configured for at the same speed.

Intra-Burst Idle Time

This field displays the idle time within a burst. If **Continuous** mode is selected, this field will display the length of time in microseconds from SOF to EOF for each frame transmitted. If **Burst** mode is selected, this field will display the length of time in microseconds from start to end of burst including Idles between burst frames.

This is only valid if all ports are configured for at the same speed.

Frame Characteristics

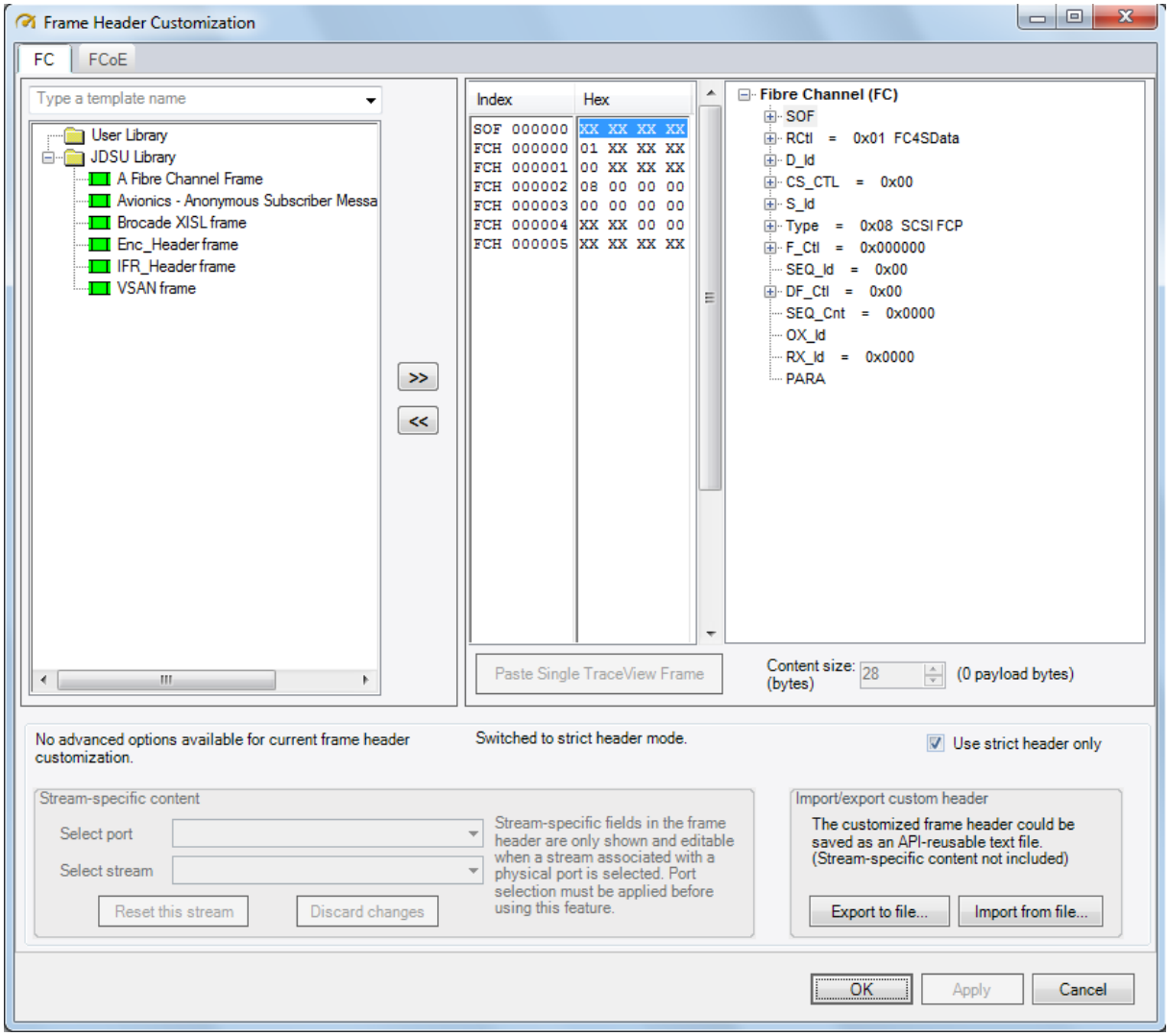
This pane lets you configure the frame characteristics of the payload to be used with the traffic pattern.

Header

This section allows you to configure the header customization (except 1G, 2G, and 4G ports). Select **Enable frame header customization** to enable the feature. Once enabled, you can specify the frame content by:

- clicking on the pencil icon to open the Frame Header Customization window where you can customize the frame, or;
- clicking on the folder icon to open a browser window where you can locate a frame header template to use for the frame header.

Figure 52: Frame Header Customization Window



Note: When customizing a frame header template, the **RCTL** field must be set to 01 (FC4SData) and the **Type** field must be set to 08 (SCSI FCP). Otherwise, the frames are not data frames and will not be counted as data frames by Load Tester's receiving ports.

Advanced FC-AE-ASM Messaging Options

The Frame Header Customization window allows you to configure advanced FC-AE-ASM messaging options. Messages are sequences of fix-sized frames which share a unique message ID and use the PARA field within the FC header to indicate its relative byte offset within the message. You can configure all fields of FC-AE-ASM header. Table 13 shows the FC-AE-ASM header format.

Table 13: FC-AE-ASM Header Format

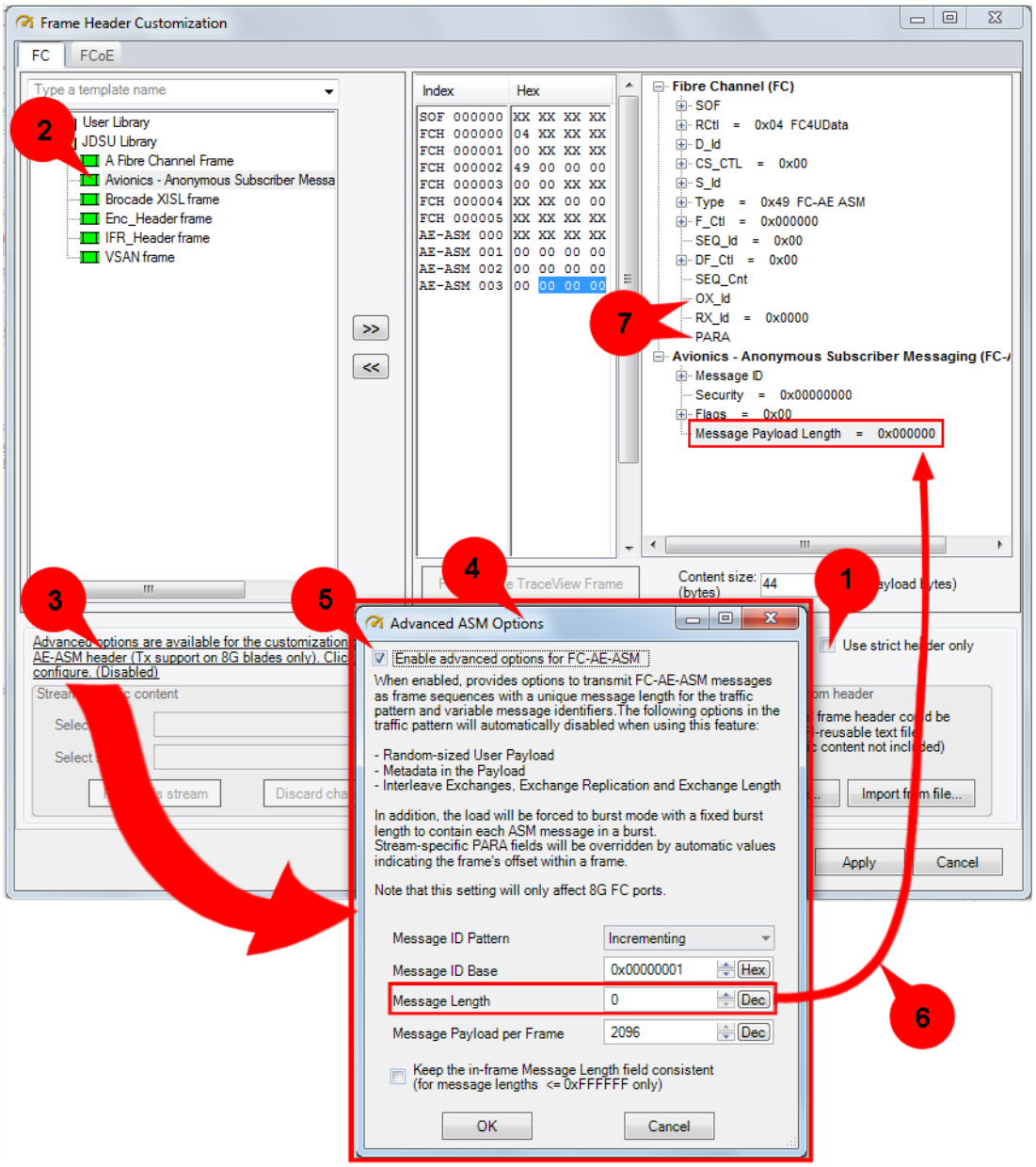
Bytes	0		1	2	3
0–3	Message ID				
4–7	Reserved - Security				
8–11	Reserved				
12–15	L	Priority	Message Payload Length (Bytes)		

Load Tester state calculates and fills the PARA field in the FC frame header based on the defined frame size and message payload length.

Referring to Figure 53, you can access and edit the advanced FC-AE-ASM messaging options by:

1. From the **Frame Header Customization** window, deselect the **Use strict header only** check box (1).
2. Double-click the **Avionics - Anonymous Subscriber Messaging (FC-AE-ASM)** selection (2) to display the following link.
3. Select **Advanced options are available for the customization of FC-AE-ASM header (Tx support on 8G blades only). Click here to configure. (Disabled)** (3) to open the **Advanced ASM Options** dialog box (4).

Figure 53: Enabling Advanced FC-AE-ASM Messaging Options



4 In the **Advanced ASM Options** dialog box, select the **Enable advanced options for FC-AE-ASM** check box (5).

5 Modify the **Advanced ASM Options** dialog box fields to meet your requirements.

Message ID Pattern **Message ID Base**	Generate a unique message ID for the FC-AE-ASM frames. You need to select an ID pattern (either **Incrementing**, **Random**, or **Fixed**) and specify the base value for the ID (**0** to **0xFFFFFFFF**)
Message Length	Set the total length of the ASM payload message.

Message Payload per Frame	Sets the length of the ASM message to be carried by each frame. This overrides the fixed payload size set on the Profile Parameters tab.
Keep the in-frame Message Length field consistent check box	When selected, adjusts the **Message Payload Length** (displayed in the **Frame Header Customization** window) to match the **Message Length** field for message lengths equal to or less than 0xFFFFFF. See the arrow extending from the **Message Length** field (6).

Note that the **PARA** and the **Message ID** fields (7) are left empty.

6 Select the **OK** button.

Frame Customization Window Extended Headers for ENC/VFT/IFR Limitation

When configuring the **Frame Header Customization** window's Extended Headers for ENC, VFT, or IFR headers and using the Configurable Frame Header feature, all the header settings entered are applied to all data frames created for all streams associated with all Tx ports in the traffic pattern. This includes S_ID/D_ID/OX_ID for ENC headers, F_ID for VFT headers, and SF_ID/DF_ID for IFR headers. These IDs cannot be configured with different values between streams. All Tx ports in the traffic pattern share the same Extended Header settings.

If you need frames created with different ID settings in the ENC, VFT, or IFR headers, you can use multiple traffic patterns with a single stream created in each traffic pattern as a work-around. Using multiple occurrences of "Pair Port Tx Odd" and "Pair Port Tx Even" to select one port pair in each traffic pattern will result in one port with a single stream per traffic pattern. The frame headers in each stream can then be configured with unique ID values to define the traffic patterns.

As an example, to set up extended headers for ENC on four ports:

1 Lock all of the ports. In this example, we are using ports: (1,1,1) (1,1,2) (1,1,3) (1,1,4)

2 Create four traffic patterns as described below. This results in only one port pair within a single stream created in each traffic pattern.

Default - change topology to "Pair Port Tx Odd", select port pair (1,1,1) (1,1,2)
TrafficPattern1- change topology to "Pair Port Tx Even", select port pair (1,1,1) (1,1,2)
TrafficPattern2 - change topology to "Pair Port Tx Odd", select port pair (1,1,3) (1,1,4)
TrafficPattern3 - change topology to "Pair Port Tx Even", select port pair (1,1,3) (1,1,4)

3 Launch the Frame Header Customization window and configure the ENC extended headers as desired for each traffic pattern.

4 Start the test. Each of the four ports will transmit frames with a uniquely-defined ENC extended header for the port.

Payload Characteristics

This pane lets you configure the payload to use with the traffic pattern.

Auto-generated

Select this option if you want the Load Tester to generate the payload for the traffic automatically. Otherwise select **User-defined**.

Payload Content

This menu allows you to select payload pattern from the **Pattern** drop-down list.

Options are:

- Fixed
- Incrementing
- Decrementing
- RotateLeft
- RotateRight
- Random
- CJPAT
- CRPAT
- CSPAT
- 32 Bit Noise
- Long Mixed

For SAN traffic, payload is the FC payload data, and for LAN traffic, payload is the part after Ethertype and before CRC.

Starting Value

This function lets you set the starting payload value. The Traffic Frame Pattern Seed must be between 0x0 to 0xFFFFFFFF.

User-defined

This field lets you use your own payload template.

Payload template (user-defined data) should only contain Hex characters,
e.g. "01 02 A1 EF ...", and formatting characters, e.g. Space, Tab, and Enter.
A buffer will be created for template data. The buffer size is determined by the port type:

- FC 4G and 8G ports: 512 bytes
- FC 16G ports (all speeds): 1024 bytes
- FCoE ports: 1024 bytes

If the size of the template data is less than the buffer size, zeros will be appended to fully occupy the buffer. If you select the **Repeat Content** check box, the buffer will then be repeatedly used in frame payload.

You can use the **Traffic Payload Pattern Editor** (by clicking the **Editor**  icon) to create a new payload template. The template content and way the content is used are as described above. The application will automatically prompt you to save the new template. The new template must be saved before it can be used. To select an existing template to use, click the **Open File**  icon.

Payload Size (Bytes)

This pane contains options to configure the payload size.

- For SAN traffic, the payload size is the size of FC payload, and the default payload size for SAN profile is 2112 bytes.
- For LAN traffic, the payload size is counted starting from the Ethertype and ending right before CRC. The default payload size for LAN profile is 1024 bytes. The payload size includes the 2 zero pad bytes before user data defined in the Payload section. Per protocol specification, the full line rate will not be maintained with non-Dword-aligned frames. The payload size must be 4N+2 to keep the frame Dword-aligned when the custom frame header is not used.

Fixed

This option lets you set the payload size to a fixed value.

Random

This option lets you set the payload size to a random value. The payload will be randomized between the minimum and maximum values you will set.

Minimum

This option lets you set the minimum size for the payload if you selected to use a random payload size.

Maximum

This option lets you set the maximum size for the payload if you selected to use a random payload size.

Oversized

This option lets you use oversized frames in the payload.

Undersized

This option lets you use undersized frames in the payload. With the Frame Header, the minimum payload size is 32 bytes. However with the Frame Characteristic's Header and VLAN Tags disabled and with the Ethertype's Traffic Type set to UDP, and the Additional group's Truncate Meta-data selected, the Payload Size is fixed at 18 bytes.

Metadata

The **Include Meta-data (Signature)** check box allows Load Tester to generate a signature at the end of each frame's payload. The signature for SAN profiles is 24 bytes long while LAN profiles are 32 bytes long. The **Truncate Meta-data** check box allows smaller signatures.

EOF

This function will configure the EOF of FCoE frame protocol. This is not active until the **Enable frame header customization** check box is selected.

Stream/Exchange Characteristics

This pane contains options to configure the Stream or exchange characteristics.

Note: If you wish to control the bandwidth of an individual stream, you must dedicate a single profile (traffic configuration) which contains both the source and destination end points. The 2 port 10Gig blade provides up to 6 traffic configuration per port and the 8 port 10Gig blade provides 8.

Exchange Length

This option lets you instruct the HW to limit the number of frames in an exchange to the value you specify. This option is for FCoE(SAN) only. It is not applicable for FCoE(LAN).

Interleave Exchanges (SAN profile) / Interleave Streams (LAN profile)

When this check box is selected, the HW sends 1 frame from each entry in the table until all entries have sent before allowing the next entry to send again. When the check box is not selected, the HW sends N number of frame from each table entry where N is given by the field "Exchange Length" (for SAN) or "Number of Frames before advancing to next stream" (for LAN). The check box is selected by default.

Number of Frames before advancing to next stream

This function instructs the HW to continue sending N frames from each table entry before moving to the next entry in the table. This option is available for FCoE(LAN) only.

Virtual Addresses Requested Per Port (SAN profile) / Virtual End Stations Created Per Port (LAN profile)

This function allows you to limit how many virtual ports (NPIVs) to use per port for this traffic pattern during traffic topology configuration. A port may have acquired 5 NPIV addresses but a source V port count of 0 will not use any of them for topology generation. Please note that this count does not include the S_ID acquired by the physical Load Tester port.

Note: When "Additional NPIV" ports are added for an FC port, the Virtual Addresses Requested Per Port field is updated automatically to reflect the change in the number of ports. The total number of ports identified should be equal to the number of NPIV Ports plus the number of Additional NPIV Ports. See page 89 for FC ports and page 99 for FCoE ports.

Exchange Replication

This option lets you set the number of times to repeat the existing traffic configuration. If a source port is configured to transmit to 3 other ports, it will have three table entries (one for each destination).

A repeat count of 2 will create 6 table entries where each set of port targets is duplicated.

A 4 Gig blade has a limit of 512 table entries. An 8 Gig blade, a 10 Gig blade, and a 16 Gig blade have a limit of 1024 table entries.

When the **Max** button is selected, the maximum exchange replication number is calculated based on the topology, the source and destination ports. This value is displayed in the text box at the left.

Load Tester has a limit on the total number of streams allowed for each port. 512 streams are allowed for 1/2/4G ports and 1024 streams are allowed for all other ports. When looking at the total number of streams for a given port, all active profiles using the port must be considered. The **Max** button provides the number to make sure the maximum exchange replication is within the allowable limit for each port selected. In some cases, the calculated maximum exchange replication number may be slightly below the allowable limit.

For example,

Topology = Meshed Bidirectional
Number of ports = 4 (Assume the maximum streams allowed for this port type = 1024)
Source: Port 1
Destination: Port 2, 3, 4

The **Max** button will calculate the maximum Exchange Replication = 341 (1024/3) based on allowable limit.

Note: When "Additional NPIV" ports are added for an FC port, the Exchange Replication field is updated automatically to reflect the change in the number of ports. The total number of ports identified should be equal to the number of NPIV Ports plus the number of Additional NPIV Ports **plus "1"**. See page 89 for FC ports and page 99 for FCoE ports.

As an alternative to using the value calculated by the **Max** button, you may manually entering a value is also acceptable. However, if the value that you enter exceeds the calculated maximum value, an error indicating that the total number of streams exceeds the allowable limit will occur and be displayed in the log window.

Note: Only the number of streams within the allowable limit will be generated. If this error is observed in the log window and there are multiple active profiles, revisit the active profiles and use the **Max** button to recalculate the maximum exchange replication number.

OX_ID Base

This option lets you set the starting OX_ID when **Multi-frame Exchange Incrementing OX_ID** mode is selected. This option is not available for LAN profile.

OX_ID Step

This options lets you set the spacing between consecutive **OX_IDs when Multi-frame Exchange Incrementing OX_ID** mode is selected. This option is not available for LAN profile.

Exclude first S_ID

This option lets you control whether the source phy address is excluded or included during traffic topology generation. Port phy addresses are excluded only if there are NPIV addresses available. This option is not available for LAN profile.

Exclude first D_ID

This option lets you control whether the destination phy address is excluded or included during traffic topology generation. The actual destination phy address is port specific and configurable in the FC Ports Configuration tab. This option is not available for LAN profile.

Use Alternate D_ID

This option lets you use an alternate destination phy address during traffic topology generation. Port phy addresses are excluded only if there are NPIV addresses available. This option is not available for LAN profile.

Total Exchanges Created

This field displays the total number of exchanges created. Click on the **Calculate** button to submit all the settings you set so that the total number exchanges created will be displayed on the **Total Exchanges Created** field.

VLAN Tags

This pane contains options for the VLAN tag. The drop-down list allows you to select either:

- **First VLAN Tag (IEEE 802.1Q)** to support Virtual LANs on an Ethernet network. allows a single VLAN header to be inserted into an Ethernet frame.

- **Second VLAN Tag (IEEE 802.1ad)** to support stacked Virtual LANs (also known as QinQ) which allows multiple VLAN headers to be inserted into a single frame.

When selected, the **Enabled** check box enables the VLAN type selected in the drop-down list above to be used with the Traffic Pattern. The VLAN Tag is used on all traffic streams associated with the traffic pattern.

Class of Service

This option lets you select the Class of Service (COS) with the VLAN Tag. The default COS for SAN profile is 3 and the default COS for LAN profile is 7.

VLAN ID

This option lets you set the VLAN ID to use. You can either select **AUTO** to automatically generate the VLAN ID or enter a value. Please note that when sending Ethernet traffic with the switch, you must change the VLAN ID of the traffic pattern configuration to the configured Ethernet VLAN ID of the switch.

VLAN Tag

This field shows the VLAN ID to be used.

Use VLAN ID Range

This option lets you enable or disable the VLAN ID Range feature. If the VLAN ID Range feature is enabled, the COS Mask feature will be disabled and the Enable COS Mask options will not be available.

VLAN ID Base

This function sets the starting Vlan ID value or base if the VLAN ID Range feature is enabled. A base of 1 and step of 1 will create VLAN IDs of 1 2 3 4 5 ...

A popular topology of point to point will require the user to increase the number of streams by increasing **Exchange Replication** field on the Profile Parameters dialog of the Traffic Pattern Editor.

There is an individual port limit of 1024 VLAN IDs. Four ports will be required to cover the complete VLAN ID number space.

VLAN ID Step

This option lets you set the VLAN ID step value if the Traffic VLAN ID Range feature is enabled.

A base of 1 and step of 1 will create VLAN IDs of 1 2 3 4 5 ...

A popular topology of point to point will require the user to increase the number of streams by increasing **Exchange Replication** field on the Profile Parameters dialog of the Traffic Pattern Editor.

There is an individual port limit of 1024 VLAN IDs. Four ports will be required to cover the complete VLAN ID number space.

VLAN ID End

This option lets you set the VLAN ID end value if the Traffic VLAN ID Range feature is enabled.

Enable COS Mask

This option will override the Class of Service setting of the VLAN Tag with the classes of service that are specified in the mask. To enable a class of service, click the check box next to the corresponding class of service. This option is not available for LAN.

This allows the current traffic profile to run over multiple classes of service.

Ethertype

This pane contains the details for the Ethertype.

Ethertype

This field lets you specify the Ethertype value for LAN Profile. For SAN profile this is hard-coded to 0x8906 (FCoE Ethertype), and for LAN profile this defaults to 0x0800 (IP Ethertype) but the user can enter other Ethertype.

Traffic Type

This drop-down menu lets you specify the ethernet traffic type. You can select CUSTOM, TCP, or UDP.

IP TTL

This option lets you set the Time To Live value of the TTL tag that is in the IP Header.

Port for source

This option lets you set source port value in the TCP or UDP header of the transmitted TCP or UDP frames.

Port for destination

This option lets you set destination port value in the TCP or UDP header of the transmitted TCP or UDP frames.

Enable 12-byte IFG

This option enables 12-byte IFG, which is required for reaching Ethernet full line rate for a traffic pattern. It can only be enabled in TCP or UDP mode. When Enabling 12-byte IFG, the Average Load must be set to 100% and that the Payload Size should be 1024 for TCP, and 1028 for UDP.

Alternate SoF Position

The Alternate SoF Position feature alternates the position of the SOF so it is flip-flopping by 4 bytes during frame generation. This feature will work for frames that are evenly divisible by 8. If not, the idles will flip flop.

Error Injection

This pane contains the options for Error Injection. For LAN, only "Ethernet CRC" is available.

FC/FCoE CRC

Selecting this option will force Fibre Channel CRC errors to be generated for all frames generated by the specified traffic pattern. A simple way to use this feature is to create a CRC error traffic configuration with minimum load that is not enabled at the start of a test. During the test errors may selectively generated with the resume and pause buttons. For Ethernet ports, this will generate embedded FC CRC errors within the FCoE packet.

Ethernet CRC

This option will force Ethernet CRC errors to be generated for all frames generated by the specified traffic pattern. A simple way to use this feature is to create a CRC error traffic configuration with minimum load that is not enabled at the start of a test. During the test errors may selectively generated with the resume and pause buttons.

FC/FCoE SOF

This option will force Fiber Channel SOF errors to be generated for all frames generated by the traffic pattern. Possible errors are:

NONE, which sends frames without SOF. For FC it will send FC IDLE instead, and for FCoE it will send 0x00 instead.

INVALID, which sends frames with invalid SOF: it will flip bit 0 of the SOF.

FC/FCoE EOF

This option will force Fiber Channel EOF errors to be generated for all frames generated by the specified traffic pattern. Possible errors are:

NONE, which sends frames without EOF. For FC it will send FC IDLE instead, and for FCoE it will send 0x00 instead.

INVALID, which sends frames with invalid EOF: it will flip bit 0 of the EOF.

FC SOF and EOF Replacement (16G ONLY)

This pane lets you set how FC SOF and EOF replacements will be done. This option is only available when 16G FC blades are used.

Select the replacement for the normal data frame SOF primitive from the **Replace SOF** with drop-down menu.

Select the replacement for the normal data frame EOF primitive from the **Replace EOF** with drop-down menu.

Additional

Include Meta-data (Signature)

This option will set whether to include or exclude Meta-data from the frame in specified traffic pattern. This option must be selected to enable latency measurements.

Note: When Meta-data is removed from the payload, Rx Latency values, Rx Stream Data Frame count, and Misdirected frame detection are no longer available.

Truncate Meta-data

This option will set whether to truncate Meta data within the frame in the specified traffic pattern. This setting is only valid for UDP frame generation. This feature is meant for users that desire minimum size UDP traffic. To create a minimum size frame, VLAN tags must be disabled and payload maximum and minimum must be set to zero. Minimum allowable payload size if Meta-data is truncated is 16 bytes.

Note: When meta data is truncated, those frames will NOT increment any of the RX stream counters. This is because the only information transmitted when the meta data is truncated is the port ID. The ONLY LT Core RX counter that can increment when meta data is truncated is the global misdirected frame counter.

Run on Global Start

This option controls whether the traffic pattern is enabled when the test is started. If this option is not selected/enabled, the traffic pattern will be set to be paused once started.

When using NPIV ports with Additional NPIV ports, this value is selected for the NPIV ports and unselected for the Additional NPIV ports.

Note: When the user has configured a Load Tester Traffic Configuration to inject CRC Errors and inject Invalid SOF Errors, when the frames are received by an Xgig Analyzer the frames will not be decoded since it requires a valid SOF, so the CRC field will not be recognized and no CRC error will be displayed. It is expected that a switch will discard any frames with invalid SOF and/or CRC errors so it should be noted that the destination Load Tester port will not receive and thus will not display counts of these invalid frames.

Traffic Alternate D_ID Mode

This option lets you enable or disable use the alternate DID for ports transmitting traffic.

Stream Preview

This tab displays the Tx Stream Table Preview and gives you the ability to overwrite it. This feature is available for LAN protocol TCP or UDP only.

Stream Preview Pane

The streams of the selected ports are displayed in this pane. From this pane you can click the "plus" besides each listed port to display and edit the streams.

Address Learning

This pane contains the **ARP** button that you can use to retrieve the correct addresses for the streams.

User Overwriting

This pane allows you to overwrite the address learning frame settings of the selected ports. It has the following buttons:

Reload streams

Use this button to ensure that the data of the streams reflect your settings.

Save user Edited streams

Use this button to save the changes you made to the streams.

Remove changes from selected

Use this button to remove the changes you made to a selected stream.

Remove changes from all

Use this button to remove all the changes you made to all the streams.

Creating Traffic Patterns

To create a new traffic pattern, configure the options on each tab of the Traffic Pattern Editor.

Adjust the settings in the Topology tab

1. Go to the **Traffic Pattern Editor** tab from the Load Tester Device window. By default the Traffic Pattern Editor tab will open with a new traffic pattern with default settings.
2. Enter a name or label for the new traffic pattern in the **Label** text box.
3. Select **FC/FCoE (SAN)** or **Ethernet (LAN)** from the **Protocol** drop-down list.
4. Select the traffic pattern topology from the **Topology** drop-down list. The description section and the topology diagram will be updated according to the topology selected.

Adjust the settings in the Ports Selection tab

1. Select the ports to use in the traffic pattern from the **Available Ports** pane.
2. Click on the **Add to Selected Ports** button to move the selected ports from the **Available Ports** pane to the **Selected Ports** pane.

Adjust the settings in the Profile Parameter tab

Load Characteristics pane

1. Set the throughput of the traffic pattern in the **Average Load** field. The term ‘average’ means the average throughput out expects to achieve over the duration of several bursts. Use the **up** or **down** button to increase or decrease the value, or enter it directly.
2. Specify if the value you set in the **Average Load** field is in **MBps** or a percentage (**%**) of theoretical maximum line rate. The term ‘average’ means that a link can be oversubscribed, in which case the desired or intended loads of each traffic profile may not be achieved.
3. Select the traffic profile type to use:

   Select **Continuous** to use a traffic profile with a continuous load. You can adjust the intended load before or during the test.

   Select **Burst** to create a traffic profile with an average load and a burst load for a specified number of frames.

   If you select **Burst**, you must also set the **Burst Load** (the load during the burst) and **Burst Length** (the number of frames sent during a single burst).The Burst length must be greater than 1.

   Click the **Calculate** button to update the following fields:

   - Burst Time
   - Idle Time
   - Intra-Burst Frame Time
   - Intra-Burst Idle Time

Note: The **Calculate** button and the **Apply** button perform the same action. When you click on **Calculate**, the profile parameters are submitted to the server to build the traffic configuration model. The traffic configuration model is used to create the calculation values. The traffic configuration calculations use all the profile parameters.

Payload Characteristics pane

1 Select the **Auto-generated** option if you prefer to have the payload generated by the Load Tester or if you prefer to use your own payload content, select **User-defined**.

If you chose to use auto-generated payloads, select the payload pattern from the **Payload Content** drop-down menu. The options are:

- Fixed
- Incrementing
- Decrementing
- RotateLeft
- RotateRight
- Random
- CJPAT
- CRPAT
- CSPAT
- 32 Bit Noise
- Long Mixed

2 Specify the start value for the payload in the **Starting value** field. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.

A seed is the initial payload pattern value. The random generator is initialized once using the seed, and the subsequent patterns will be generated automatically in a random manner.

3 Select the type of payload size to use.

Select **Fixed** to specify the size of the payload. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.

Select **Random** to set the payload size between a minimum and maximum size.

4 Set the minimum size of the payload in the **Min Size** field. To get a fixed size payload both the minimum and maximum payload size field must be the same. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.

To get random payload size generation between an upper and lower bounds (inclusive), use the **Min Size** and **Max Size** fields.

5 Set the maximum size of the payload in the **Max Size** field. To get a fixed size payload both the minimum and maximum payload size field must be the same. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.

To get random payload size generation between an upper and lower bounds (inclusive), use the **Min Size** and **Max Size** fields.

Select **Oversized** option to use oversize frames in the payload.

Stream/Exchange Characteristics

1. Set the **Exchange Length** to your desired value. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.
2. Select **Interleave Exchanges (SAN profile) / Interleave Streams (LAN profile)** to instruct the hardware to continue sending N frames from each table entry before moving to the next entry in the table.
3. Select **Interleave Exchange** if you want the HW to send 1 frame from each entry in the table until all entries have sent before allowing the first entry to send again. When leave unselected, the HW sends N number of frame from each table entry where N is given by the field **Exchange Length** (for SAN) or **Number of Frames before advancing to next stream** (for LAN).
4. Limit how many virtual ports (NPIVs) to use per port for this traffic pattern during traffic topology configuration by setting the value the **Virtual Addresses Requested Per Port** field. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.
5. Set the number of times to repeat the existing traffic configuration by entering the limit in the **Exchange Replication**. If a source port is configured to transmit to 3 other ports, it will have 3 table entries one for each destination. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.
6. Set the **OX_ID Base** value. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.
7. Set the **OX_ID Step** value. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button.
8. Select **Exclude first S_ID** to exclude the source phy address during traffic topology generation. Port phy addresses are excluded only if there are NPIV addresses available.
9. Select **Exclude first D_ID** to exclude the destination phy address during traffic topology generation. Port phy addresses are excluded only if there are NPIV addresses available.
10. Click **Calculate** to update the value in the **Total Exchanges Created** field.

VLAN Tag

1. Select **Use VLAN Tag** to enable assigning a VLAN Tag to the Traffic Pattern. The VLAN Tag will be used on all traffic streams associated with the traffic pattern.
2. Select the **Class of Service**. A user may select from 0 to 7 classes of service (CoS) for a single traffic configuration.
3. Enter the **VLAN ID**. To show the value in hexadecimal or decimal format, click on the **Hex** or **Dec** button. Select **AUTO** to set the VLAN ID automatically based on the value returned from the FCF during login.
4. Select **Enable COS Mask**.
5. Select the appropriate check box. Each number represents a Class of Service (COS) for which PFC is enabled.

Ethertype

This field displays the Ethertype value which indicates the protocol used in the data field of the frame.

Error Injection

1. Select **FC/FCoE CRC** to force Fibre Channel CRC errors to be generated for all frames generated by the specified traffic pattern. A simple way to use this feature is to create a CRC error traffic configuration with minimum load that is not enabled at the start of a test. During the test errors may selectively be generated with the resume and pause buttons. For Ethernet ports, this will generate embedded FC CRC errors within the FCoE packet.
2. Select **FC/FCoE SOF** to force Fiber Channel SOF errors to be generated for all frames generated by the traffic pattern. Possible errors are:

   NONE, which sends frames without SOF. For FC it will send FC IDLE instead, and for FCoE it will send 0x00 instead.

   INVALID, which sends frames with invalid SOF: it will flip bit 0 of the SOF.
3. Select **FC/FCoE EOF** to force Fiber Channel EOF errors to be generated for all frames generated by the specified traffic pattern. Possible errors are:

   NONE, which sends frames without EOF. For FC it will send FC IDLE instead, and for FCoE it will send 0x00 instead.

   INVALID, which sends frames with invalid EOF: it will flip bit 0 of the EOF.
4. Select **Ethernet CRC** to inject Ethernet CRC errors when the Ethernet Protocol is selected for the traffic pattern.

Additional

1. Select Include Meta-data (Signature) to set whether to include or exclude Meta-data from the frame in specified traffic pattern.
2. Select the **Run on global start** check box.

Note: When you select **Run on global start**, the traffic pattern you are creating or editing will start when the **Start** button from the Load Tester main window is clicked. Do not select this option if you do not want to start that traffic pattern when the **Start** button on the Load Tester main window is clicked.
If this is not selected, the traffic pattern will be configured but in a paused state when the test is started. You may activate this traffic configuration with the **Resume** button.

Click **Ok** to save the new traffic pattern or click **Apply** to implement any change you made to the settings.

Using the Traffic Pattern Wizard

Another option to create a new traffic pattern, is the Traffic Pattern Wizard. The wizard lets you setup a new traffic pattern in five steps.

You can launch the Traffic Pattern Wizard by:

1. Clicking the **Configuration** drop-down arrow from the Load Tester main tab and selecting **Traffic Pattern Wizard**; or,
2. Clicking the **Create New** drop-down arrow in the Traffic Pattern Editor tab in the Load Tester Device Window and selecting **New using Wizard.**

Once the wizard is opened, options will be the same as the Traffic Pattern Editor but will be displayed in sequential pages. Refer to "Traffic Pattern Editor Tab" on page 129 for descriptions of the options.

Editing Traffic Patterns

To edit a traffic pattern:

1. Go to the Traffic tab from the Load Tester main window.
2. Select the traffic pattern from the **Pattern Based View**.
3. Click on the **Edit**  button. The **Traffic Pattern Editor tab** appears.
4. Do the necessary revisions to the selected traffic pattern.
5. Click **Ok** when you are done.

Deleting Traffic Patterns

To delete a traffic pattern:

1. Go to the Traffic tab on from the Load Tester window.
2. Select the Traffic Pattern from the **Pattern Based View**.
3. Click the **Delete**  button. A confirmation box will appear.
4. Click **Yes**.

Chapter 6

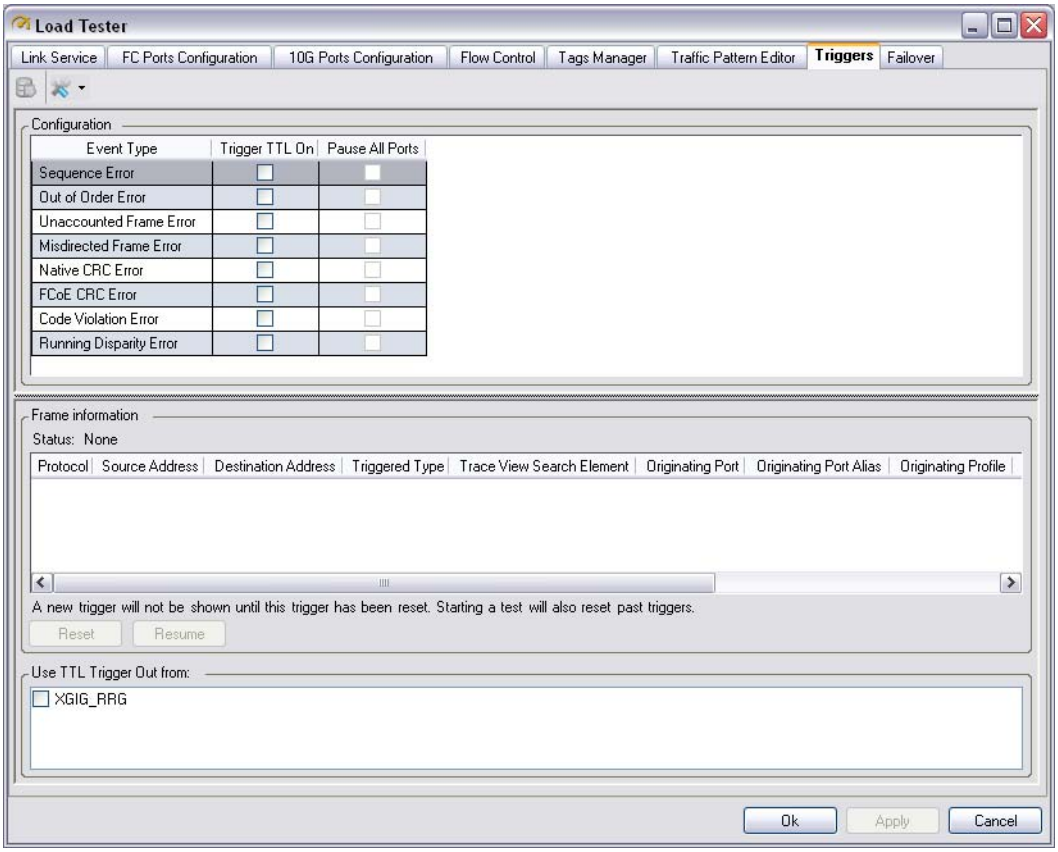
Editing Triggers

In this chapter:

The Triggers Tab

The Triggers tab displays all the available triggers you can set when you run a test in Load Tester. This tab allows you to enable triggering based on error events and configure all Load Tester ports to pause test when trigger conditions.

Figure 54: Triggers Tab



Configuration

The **Configuration** pane lists all the event types that Load Tester use as triggers to log errors.

The event types are:

- **Sequence Error** - If a frame arrives that is not the expected successor (increase by one) then a sequence error trigger is invoked.
- **Out Of Order Error** - If a frame arrives that is not the expected successor and has a sequence count less than the previous arrived frame, and then an out-of-order error trigger is invoked.
- **Unaccounted Frame Error** - If the final frame of the sequence arrives and there is at least one frame that has not arrived then an unaccounted frame trigger is invoked.
- **Misdirected Frame Error** - If a frame that was not destined for the Load Tester port arrives, a misdirected error is invoked.
- **Native CRC Error** - If a data transmission does not pass the cyclic redundancy check, a Native CRC error is invoked. This can be an FC CRC error for Fibre Channel or an Ethernet CRC error for Ethernet frames.
- **FCoE CRC Error** - If a data transmission does not pass the cyclic redundancy check in, a CRC error is invoked. An FCoE CRC Error is the embedded FC CRC error for FCoE frames only.
- **Code Violations Error** - If a 10-bit transmission character is not decoded to a valid data or control character using the validity checking rules specified for the 8b/10b transmission code, and then a code violation error is invoked.
- **Running Disparity Error** - If there have been a predominance of 1's or 0's in the binary stream of encoded transmission characters, then a running disparity error is invoked.

Frame information

The **Frame information** pane provides you with information about the traffic (data) frame that was received on a port that registered that error.

Use TTL Trigger Out From

The **Use TTL Trigger Out from** pane allows you to select the chassis to use to trigger TTL out from.

Editing Triggers

To edit a trigger:

1. Click on the **Triggers** tab from the Load Tester Device Window.
2. Select or unselect the **Trigger TTL On** check box for the Event Type you want to use.
3. Select or unselect the **Pause All Ports** check box for the Event Type you want to pause all ports at the trigger.
4. Click on **Resume** to resume running the triggers. Note that once you resume running a trigger, all information will be lost.
5. Click **Apply**.

Chapter 7

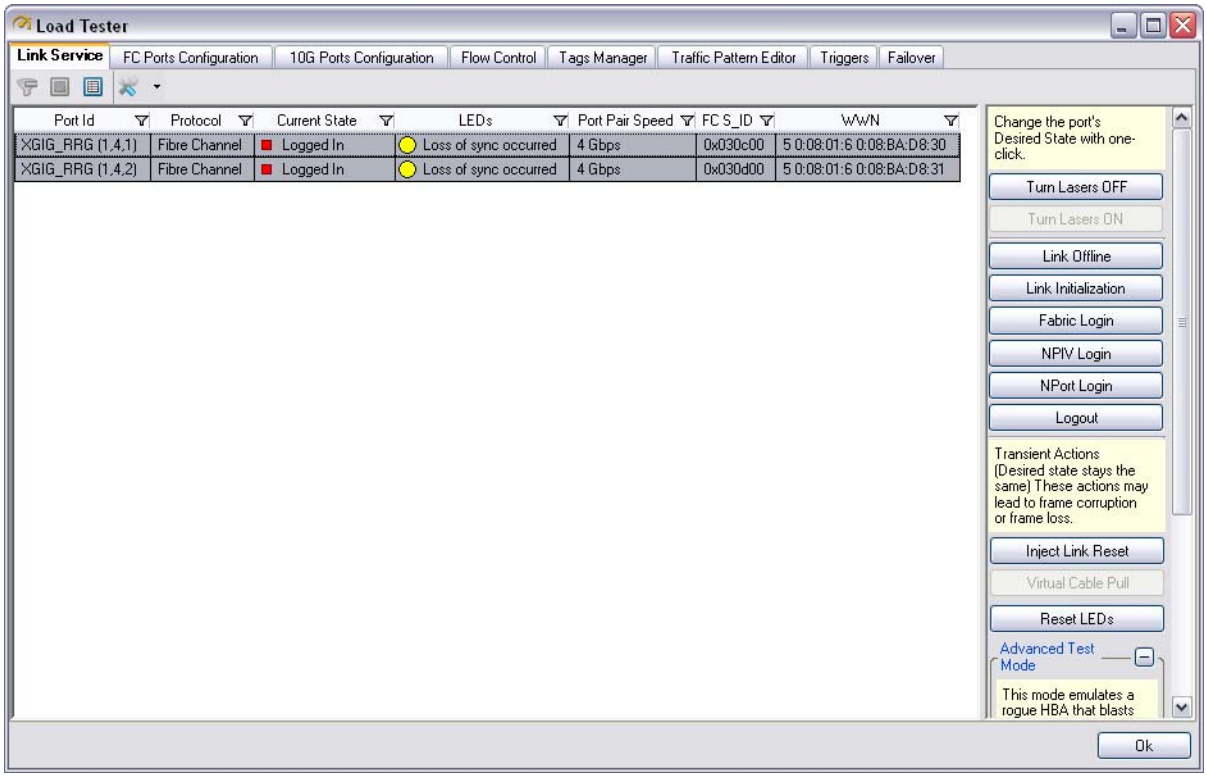
Managing Multiple Link Services

In this chapter:

Link Service Tab

The Multiple Link Service tab displays all the ports on the chassis that are locked as Load Testers and also the different Link Service options you can set for the ports. To learn more about the options, refer to "Using the Parameters Context Menu for Fibre Channel Ports" on page 52 or "Using the Parameters Context Menu for FCoE Ports" on page 57.

Figure 55: Link Service Tab



Managing the Link Service Operations

To activate or deactivate the Link Service operations for ports:

Select ports

1. Select the port or ports to manage from the list.
   For more information on how to filter the ports listed, refer to "Organizing Ports" on page 110.
2. To select multiple ports, hold down the *Ctrl* key while clicking on the ports to manage.

Select Link Service action

1. Click **Turn Lasers OFF** to turn the lasers off for the selected port(s).
2. Click **Turn Lasers ON** to turn the lasers on for the selected port(s).
3. Click **Link Offline** to put the port(s) on an offline state.
4. Click **Link Initialization** to initialize the links.
5. Click **Fabric Login** to login the port(s) to the Fabric.
6. Click **NPIV Login** to log the port(s) to the switch to request NPIV addresses for the port.
7. Click **NPort Login** to log the port(s) to the other ports.
8. Click **Logout** to log the port(s) out.

Capture trace

1. Select the **Port Capture** option from the **Launch a Tool...** button to open the Port Capture dialog box. Refer to "Launch a Tool" on page 19.
2. Select the desired ports and then click the Start Capture button  to begin trace capture for the selected port(s).
3. Click the Stop Capture button  to stop the trace capture for the selected port(s).

   When you click on the Stop Capture button, the captured file is automatically launched. You must have Xgig Analyzer to view the captured trace file.

Select Transient Actions

1. Click **Inject Link Reset** to reset the credit count for the port(s) by entering the LR1 State, and following the Link Reset protocol.
2. Click **Virtual Cable Pull** to turn the port(s) laser off, and then turn it back on to simulate a cable pull while a test is running. The port(s) will automatically attempt to Login, and if successful, will resume running the test.
3. Click **Reset LEDs** to reset the status LEDs for the port(s) on the Xgig blade and the Parameters Status table.

Select Advanced Test Mode actions

1. Click **Start Blasting FLOGi Continuously** to initiate a continuous Blast FLOGI test.

   Blast FLOGI is a special error mode for testing Switch recovery. The Load Tester ports blasts a canned FLOGI frame at the switch continuously.

2. Click **Stop Blasting FLOGi Continuously** to stop the continuous FLOGi blast.

3. Click **Enable Rx Credits** to instantly adjust the Rx buffer-to-buffer credits of the physical port, which will be used in the Fabric Login and Port Login frames.

   This option can also be enabled in the **RX Physical Ports** panel under the **RX Physical Ports** sub-tab of the **Traffic** tab.

4. Click **Disable Rx Credits** to stop using Rx Credits.

Chapter 8

Configuring Test Summary Reports

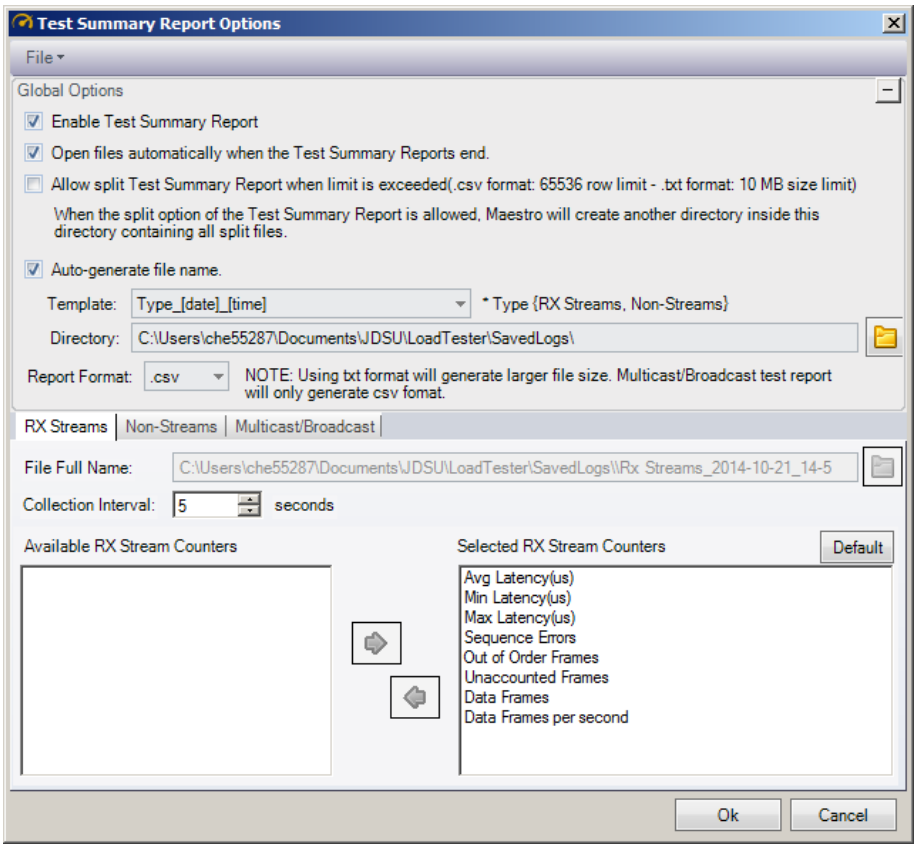
In this chapter:

The Test Summary Report summarizes the information collected during the test. The Test Summary Report is generated after a test is completed. Load Tester generates two reports; one report is for stream data collected, and the other is non-stream data collected. The reports can be saved as either .txt or .csv files.

Test Summary Report Options Dialog Box

The **Test Summary Report Options** dialog box displays all the options for the test summary reports. To open the Test Summary Report Options dialog box, click on the **Configuration** button on the Load Tester Device window and select **Test Summary**.

Figure 56: Test Summary Report Options Dialog



The Test Summary Report dialog box has the following options:

File Button

This button lets you open recently saved stream and non-stream Test Summary Reports (TSR).

Global Options

This pane contains general options for the Test Summary Report.

Enable Test Summary Report

This option runs the Test Summary Report at the start of the test to collect during the test.

Open files automatically when the Test Summary Reports end

This option opens the generated Test Summary Report file after the test completes depending on the **Report Format** selection, either .txt or .csv.

Allow split Test Summary Report when limit is exceeded

This option applies differently based on the selected file format.

- .csv files – this option is applicable when number of report rows exceeds 65536. Use this to save the test report when it exceeds the Microsoft Excel row limitation of 65536.
- .txt files – this option is applicable when the file size exceeds 10 MB.

This option creates a subdirectory (in the specified directory) with a folder name the same as the test summary report file and appended with "**_split**". Then it saves the report as smaller files (whose file sizes are close to the format limit) into the newly-created subdirectory.

Example

Given that the test summary report is in .csv format and would be named:

Rx Streams_user12345_2010-07-22_14-46-43

The application will create a subdirectory (for the split files) named:

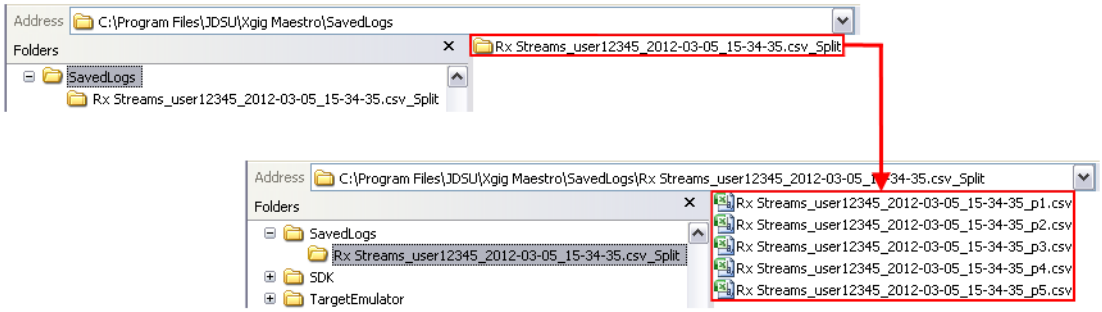
Rx Streams_user12345_2010-07-22_14-46-43.csv_Split

The split files saved in this subdirectory are:

- named: **Rx Streams_user12345_2010-07-22_14-46-43**
- appended with: "**_pN**" suffix where N is an integer number starting from 1
- given the **.csv** extension

For example, a file named **Rx Streams_user12345_2010-07-22_14-46-43_p1.csv** would be the first file created. Refer to Figure 57.

Figure 57: Split Test Summary Report Subdirectory



Auto-generate file name

This option automatically sets the filename for the Test Summary Report. If unchecked, you can specify a filename to use in the "File Full Name" text box.

Template

This drop-down menu lets you select the format of the auto-generated file name of the Test Summary Report.

Directory

This text field lets you specify where the auto-generated Test Summary Report will be saved. You can click on the **Browse** button to locate the directory in your computer.

Report Format

This drop-down list box lets you select which format to generate the test summary report. You may select from either comma-separated values format (.csv) or plain text format (.txt).

Selecting .txt format will generate larger log files. Please take this into consideration when running long duration tests and/or larger number of ports.

RX Streams Tab

This tab contains options for the reporting of RX stream information.

File Full Name:

This text field is enabled when you did not select Auto-generate file name option on the Global Options pane. This text field lets you specify where generated Test Summary Report will be saved. You can click on the **Browse** button to locate the directory in your computer.

Collection Interval

This field lets you specify the interval time (in seconds) for the collection of data that will be included in the Test Summary Report.

Available RX Stream Counters

This pane lists all available RX Stream counters that can be included Test Summary Report.

Note: Static information from the test, i.e. port configuration data, is not included in the Available RX Stream Counters pane. The static information is automatically included in the Test Summary Report. Only dynamic information, such as counter values, is listed.

Selected RX Stream Counter

This pane displays the selected RX Stream counters that will be included in the Test Summary Report.

Default button

The **Default** button arranges selected RX Physical Ports counters according to their default sequence in the **RX Streams** tab**,** under the **RX** tab in the **Traffic** tab of the Load Tester module main screen.

Non-Streams Tab

This tab contains RX and TX non-stream information, i.e., RX Physical Port counters and TX Ports counters.

File Full Name:

This text field is enabled when you did not select Auto-generate file name option on the Global Options pane. This text field lets you specify where the generated Test Summary Report will be saved. You can click on the **Browse** button to locate the directory on your computer.

Collection Interval

This field lets you specify the interval time (in seconds) for the collection of data that will be included in the Test Summary Report.

RX Physical Port counters Tab

This tab lets you select which Available RX Physical Ports counters will be included in the Traffic Summary Report.

Available RX Physical Ports counters

This pane lists all available RX Physical Ports counters that can be included in the Traffic Summary Report.

Note: Static information from the test, for example port configuration data, is not included in the Available RX Physical Ports counters pane. The static information is automatically included in the Test Summary Report. Only dynamic information, such as counter values, is listed.

Selected RX Physical Ports counters

This pane displays the selected RX Physical Ports counters that will be included in the Test Summary Report.

Default button

The **Default** button arranges selected RX Physical Ports counters according to their default sequence in the **RX Physical Ports tab** under the **Traffic Tab** of the Load Tester module main screen.

TX Ports counters Tab

This tab lets you select which Available TX Ports counters will be included in the Traffic Summary Report.

Available TX Ports counters

This pane lists all available TX Ports counters that can be included in the Traffic Summary Report.

Note: Static information from the test, for example port configuration data, is not included in the Available TX counters pane. The static information is automatically included in the Test Summary Report. Only dynamic information, such as counter values, is listed.

Selected TX Ports counters

This pane displays the selected Tx Ports counters that will be included in the Test Summary Report.

Default button

The **Default** button arranges selected TX Ports counters according to their default sequence in the **TX Port Based View** tab under the **TX** tab in **Traffic Tab** of the Load Tester module main screen.

Multicast/Broadcast Tab

This Multicast/Broadcast tab contains options for the reporting of Multicast and Broadcast information.

File Full Name:

This text field is enabled when you did not select Auto-generate file name option on the Global Options pane. This text field lets you specify where generated Test Summary Report will be saved. You can click on the **Browse** button to locate the directory in your computer.

Multicast/Broadcast Counters

This pane displays the multicast/broadcast Rx counters (Rx Multicast Data Frames, Rx Broadcast Data Frames, Rx Unicast Data Frames, and Total Rx Frames) included in the Test Summary Report.

Configuring Test Summary Reports

Configuring Global Options

To configure the Global Options of the Test Summary Reports, do the following:

1. Open the **Test Summary Report Options** dialog box.
2. Select the **Enable Test Summary Report** check box to enable the test summary report feature and generate test summary reports after a test is completed.
3. Select the **Open files automatically when the Test Summary Reports end** check box to open the generated .csv or .txt files after the test is completed.
4. If desired, select **Allow split Test Summary Report when limit is exceeded**.

   The limit is based on the selected file format:

   - .csv files – this option is applicable when number of report rows exceeds 65536. Use this to save the test report when it exceeds the Microsoft Excel row limitation of 65536.
   - .txt files – this option is applicable when the file size exceeds 10 MB.
5. Select the **Auto-generate file name** check box to automatically generate the file name of the files that are created. Depending on the **Report Format** selection, the files will be in either .csv or .txt format. Enter the directory path where the generated files will be saved. You can use the **Browse** buttons to locate the folder on your computer.

Configuring Rx Streams Options

1. Click the **RX Streams** tab.

2 If you did not select the **Auto-generate file name** option from the **Global Options** pane, enter the file's full path and name in the **File Full Name:** text box.

3 Enter the interval time for collecting the data in the **Collection Interval** box. You can use the up or down arrow to change the value.

4 Select the RX Stream counter to include in the report from the **Available RX Stream Counters** pane.

5 Click the **Add** button (represented by green arrow pointing right). Repeat until all the counters to include are listed in the **Selected RX Stream Counters** pane.

6 Click the **Default** button if you want to rearrange the selected counters according to their original sequence.

7 To remove a counter from the Selected RX Streams Counters pane, select the counter then click on the **Remove** button (represented by a green arrow pointing left).

Configuring Non-Streams Options

1 Click the **Non-Streams** tab.

2 If you did not select the **Auto-generate file name.** option from the **Global Options** pane, enter the file's full path and name in the **File Full Name:** text box.

3 Enter the interval time for collecting the data in the **Collection Interval** box. You can use the up or down arrow to change the value.

4 Click the **RX Physical Port counters** tab.

5 Select the RX Physical Ports counter to include in the report from the **Available RX Physical Ports counters** pane.

6 Click the **Add** button (represented by green arrow pointing right). Repeat until all the counters to include are listed in the **Selected RX Physical Ports counters** pane.

7 Click the **Default** button if you want to rearrange the selected counters according to their original sequence.

8 To remove a counter from the **Selected RX Physical Port counters** pane, select the counter then click on the **Remove** button (represented by a green arrow pointing left).

9 Click the **TX Ports counters** tab.

10 Select the TX Ports counter to include in the report from the **Available TX Port counters** pane.

11 Click the **Add** button (represented by green arrow pointing right). Repeat until all the counters to include are listed in the **Selected TX Port counters** pane.

12 Click the **Default** button if you want to rearrange the selected counters according to their original sequence.

13 To remove a counter from the **Selected TX Port counters** pane, select the counter then click on the **Remove** button (represented by a green arrow pointing left).

Appendix A

Getting Started with Xgig Load Tester

In this chapter:

Overview

Getting started with the Xgig Load Tester is a simple and quick process that does not require a fibre channel switch. If you want to learn how to use Load Tester, the examples shown below will show you how to generate traffic using two ports looped back to each other through an Xgig Analyzer.

An Xgig Analyzer is not required but this will assist with traffic verification. The loop back configuration without a switch will require additional steps that will be explained. If you have a Fibre Channel switch you can go directly to Performing a Test with a Fibre Channel Switch.

Performing Self Test without a Switch

You can perform a Self Test in Load Tester without using Fibre Channel switch through the use of a loop back configuration. The process of performing the self test has been broken down into the following discussion.

Please note that it is assumed that the name and or IP address of the chassis is known.

Starting the Xgig Load Tester

To start the Xgig Load Tester application:

1 Go to **Start> All Programs> Viavi> Xgig Maestro**.

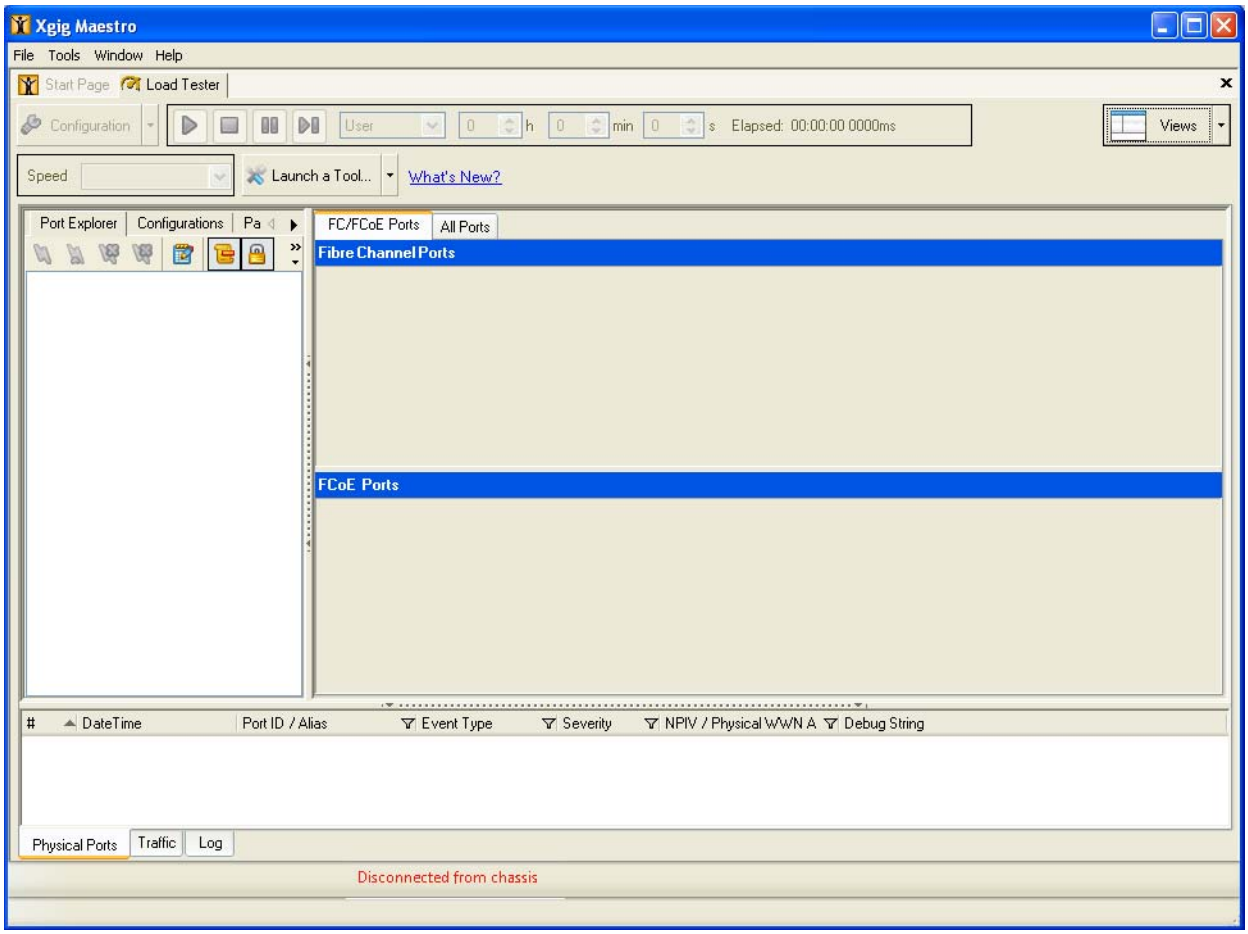
The Xgig Maestro application opens with the **Maestro Global** tab (Figure 58).

Figure 58: Xgig Maestro Start Window

2 Click on **Xgig Load Tester** under **Maestro Plugins**.

Your Xgig Maestro application will now look similar to Figure 59.

Figure 59: Xgig Load Tester Window



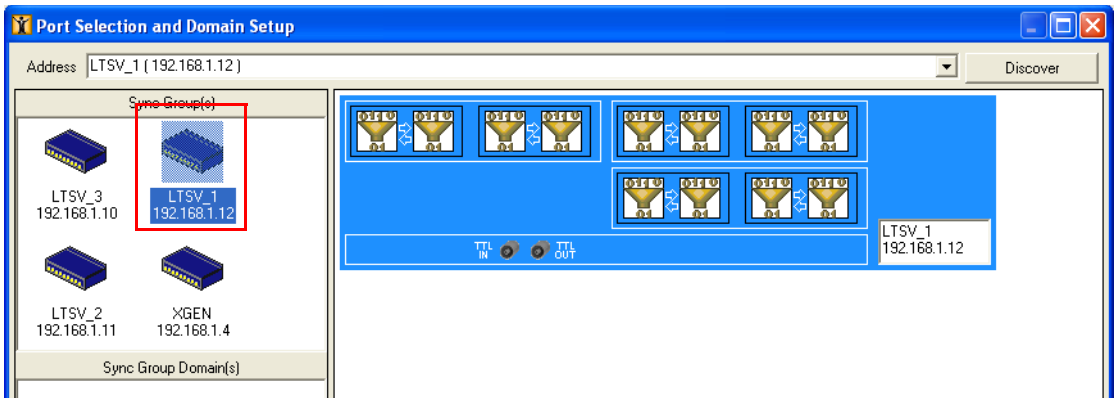
Locking the ports to use in the Load Tester

1 Click the **Port selection and domain setup...** 

.

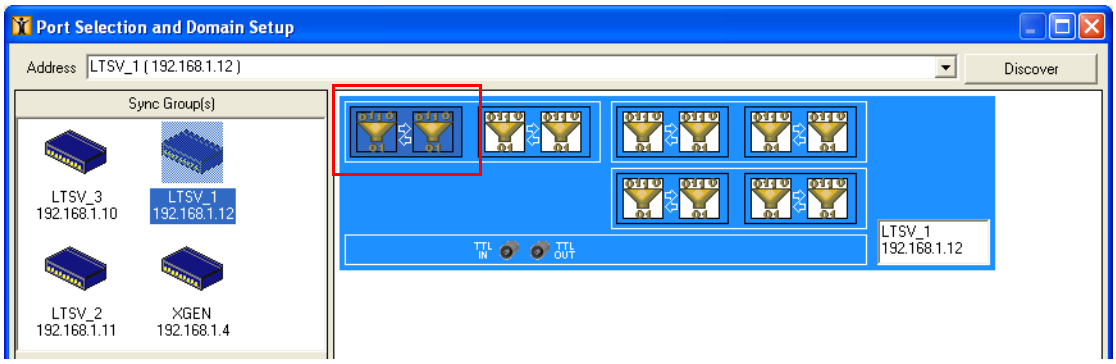
2 Select your chassis from the **Port Selection and Domain Setup** dialog box (Figure 60).

Figure 60: Selected Chassis



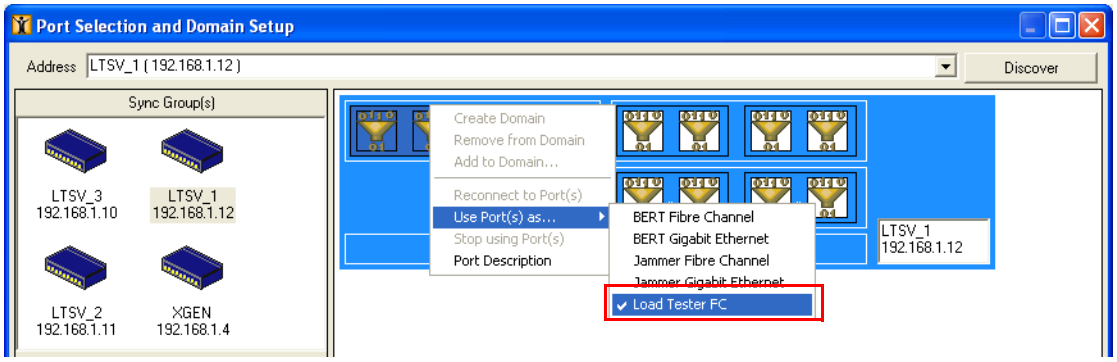
3 Click on the ports you wish to use to highlight them.

Figure 61: Selected Ports



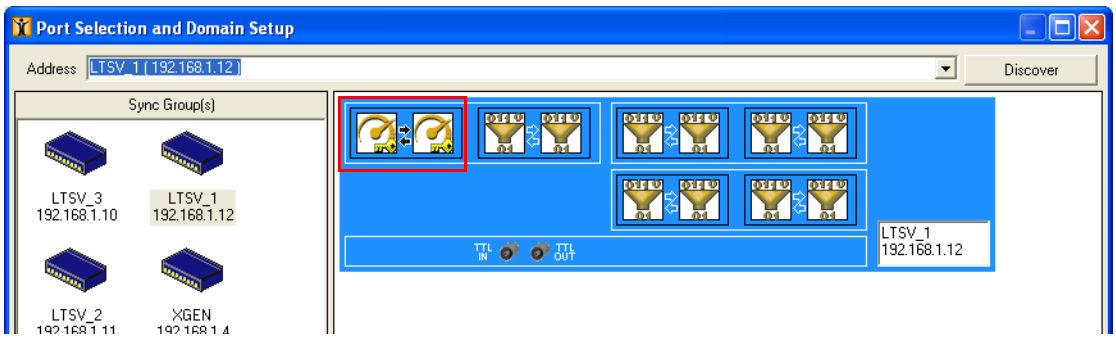
4 Right-click on one of the ports and select **Use Port(s) as...** and then select **Load Tester FC/ FCoE**.

Figure 62: Locking the ports as Load Testers



You will now see your two selected ports locked and ready for use. (Refer to Figure 63).

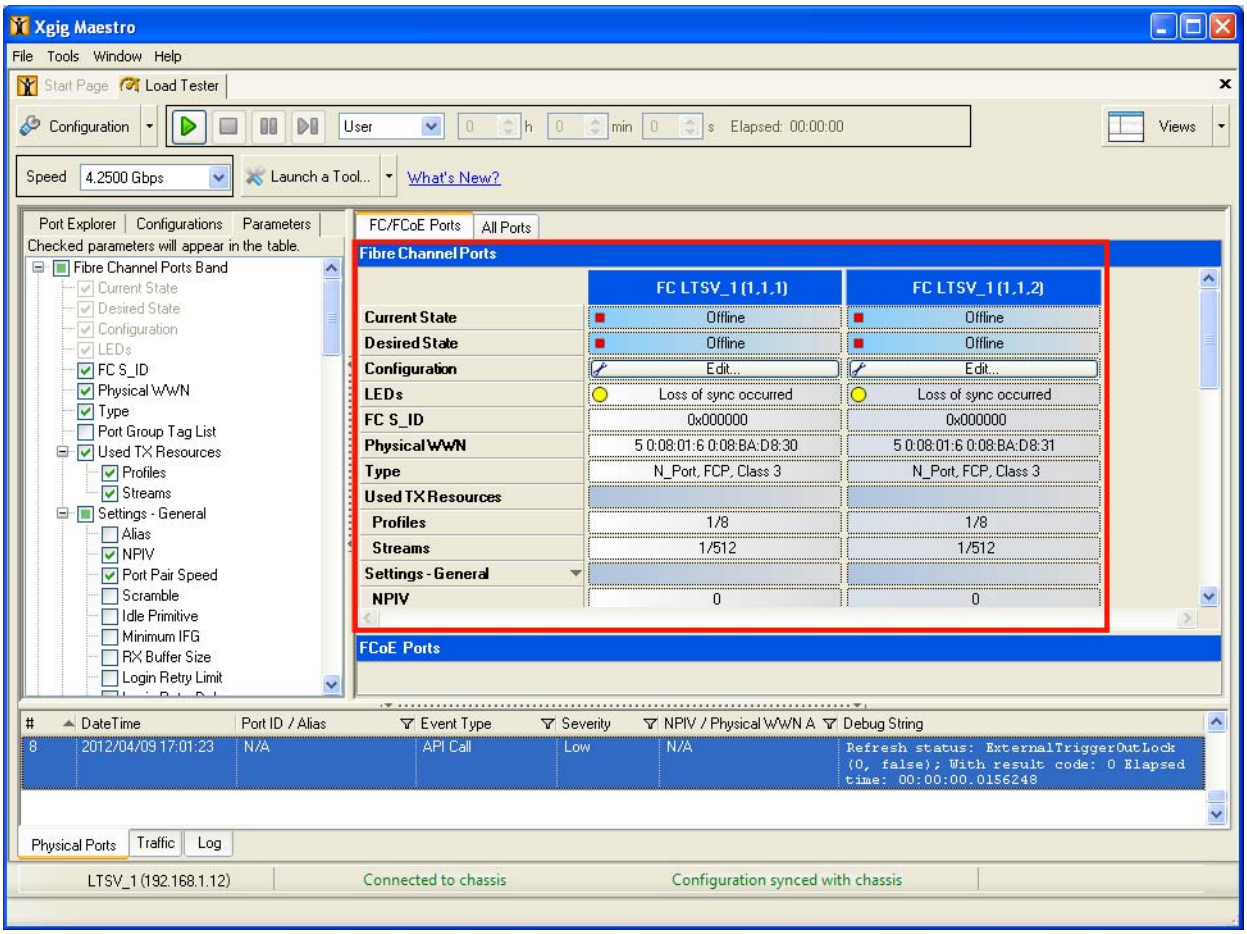
Figure 63: Locked ports



5 Click the **Close** button to close the dialog box.

Your Maestro Load Tester session will now appear similar to Figure 64.

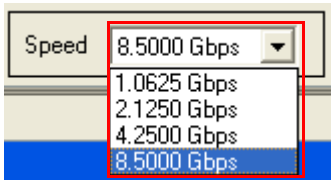
Figure 64: Load Tester window with locked ports



Setting the Speed for the Test

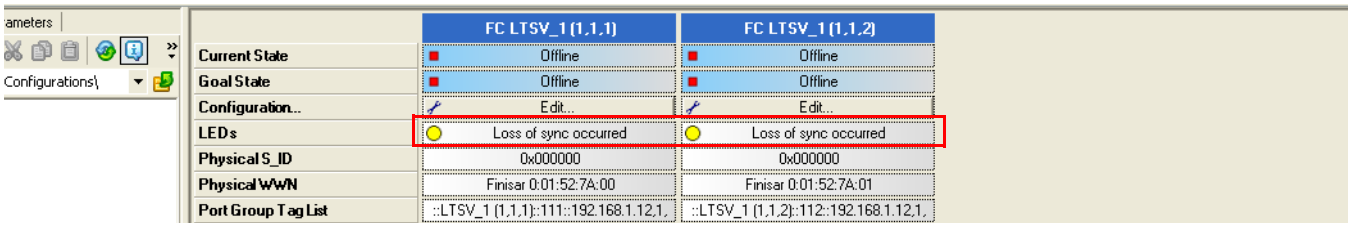
After locking the ports as Load Testers, you should verify if the speed of the link is correct. To quickly set the link speed for your hardware setup, select the speed to use (in Gbps) from the **Speed** drop-down menu found in the upper left corner (refer to Figure 65).

Figure 65: Speed Drop-down Menu



You will notice that the LEDs with the **Loss of sync occurred** status may have turned yellow if they were previously red (refer to Figure 66).

Figure 66: Loss of Sync occurred LED status



Editing the Topology

Near the bottom of the window you will see three tabs labeled **Physical Ports**, **Traffic** and **Log**.

To edit the topology:

1 Click on the **Traffic** tab to display the **TX** tab.

Figure 67: Traffic tab

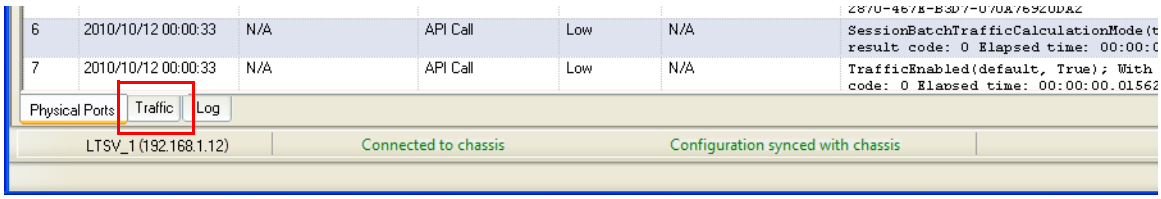
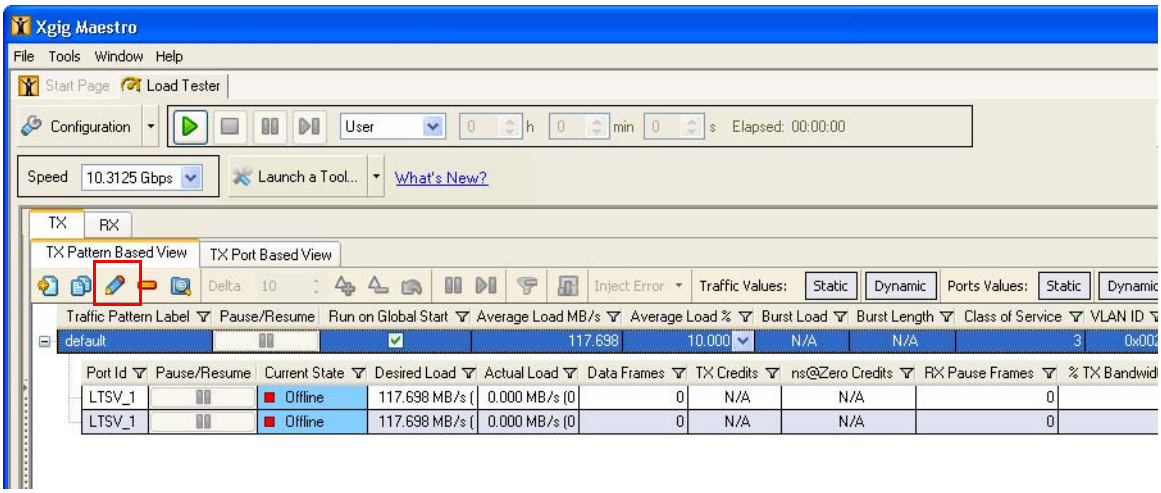
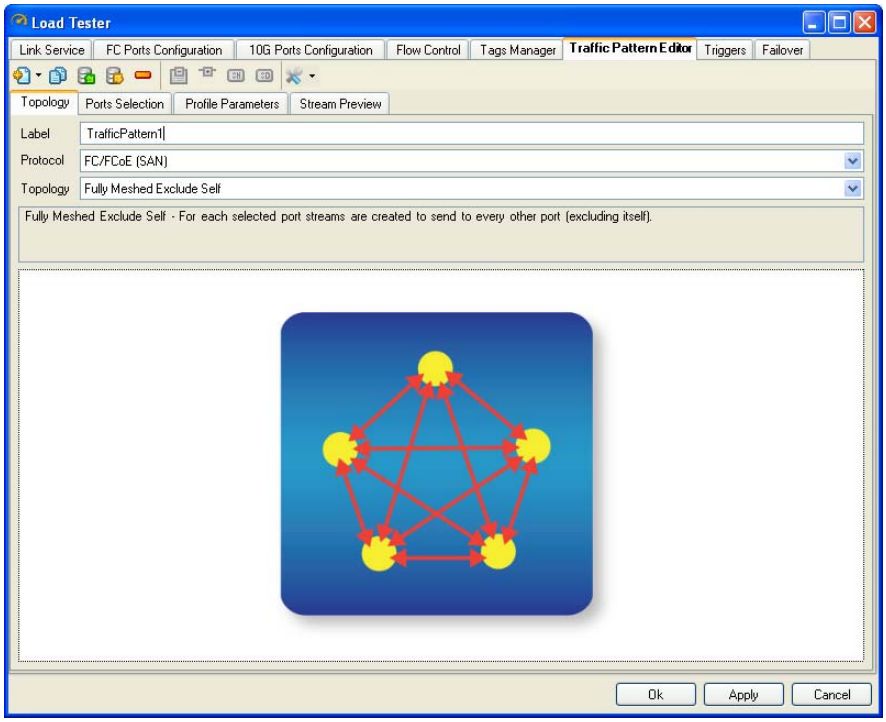


Figure 68: TX tab in the Traffic tab



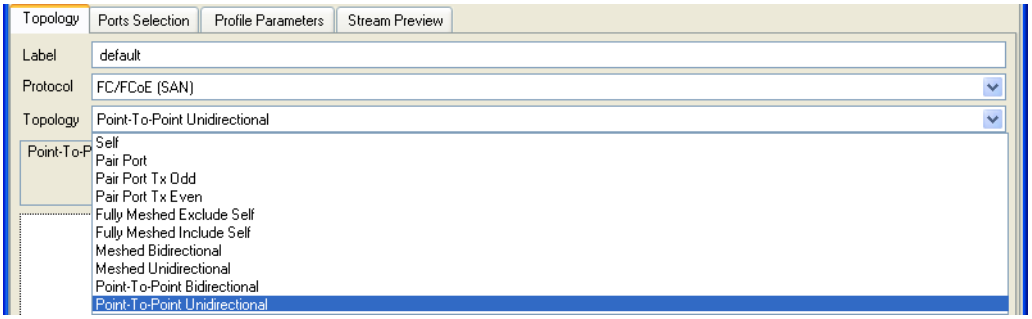
2 Click the pencil icon to open the **Traffic Pattern Editor** tab in the Load Tester Device Window so you edit the default traffic configuration provided for you.

Figure 69: Traffic Pattern Editor Tab



3 Change the topology to **Point to Point Unidirectional** from the **Topology** drop-down menu.

Figure 70: Topology drop-down menu

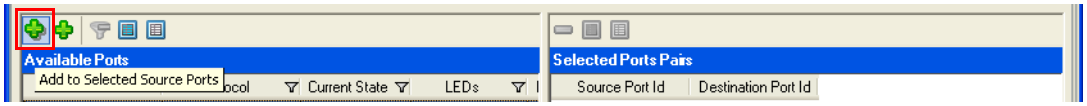


The topology column is now set to **Point to Point Unidirectional**.

4 Click on the **Ports Selection Tab** to select ports for the traffic pattern.

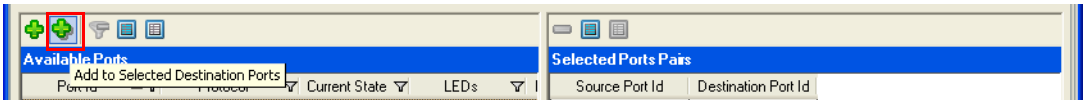
5 Select the first port from the **Available Ports** pane and add it to the source port list by clicking **Add Selected Ports to Source** button (Figure 71).

Figure 71: Add Selected Ports to Source



6 Select the second port and add it to the destination port list by clicking **Add Selected Ports to Destination**.

Figure 72: Add Selected Ports to Destination

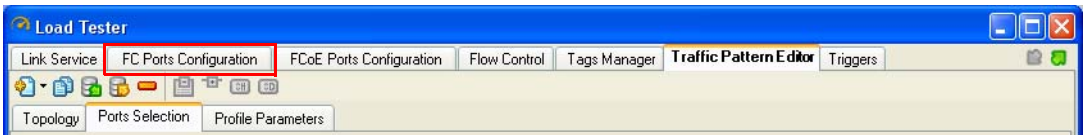


7 Click **Apply** on the Traffic Pattern Editor tab to save the changes you made.

Enabling Emulator Mode

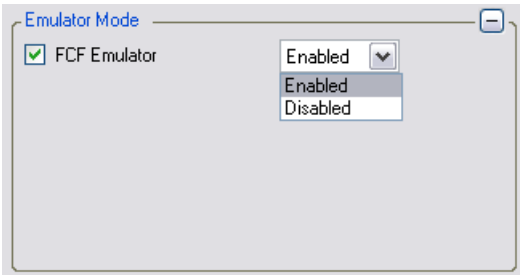
1 Click the FC Ports Configuration tab as shown in Figure 73.

Figure 73: Open the FC Ports Configuration Tab



2 In FC Ports Configuration tab, click the **FCF Emulator** drop-down menu and select the Enabled selection from the list. Refer to Figure 74.

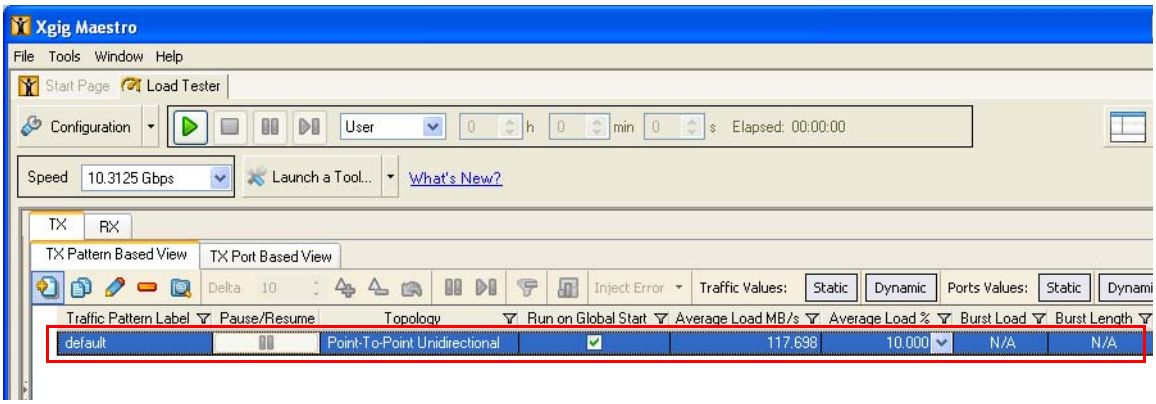
Figure 74: Emulator Mode Area



3 After you are done, click **Apply** on the FC Ports Configuration tab to save the changes you made.

4 Click **Ok** to close the dialog box. The **default** traffic bar has been changed.

Figure 75: Changed traffic bar



5 Click on the **Physical Ports** tab at the bottom of the window to display the ports.

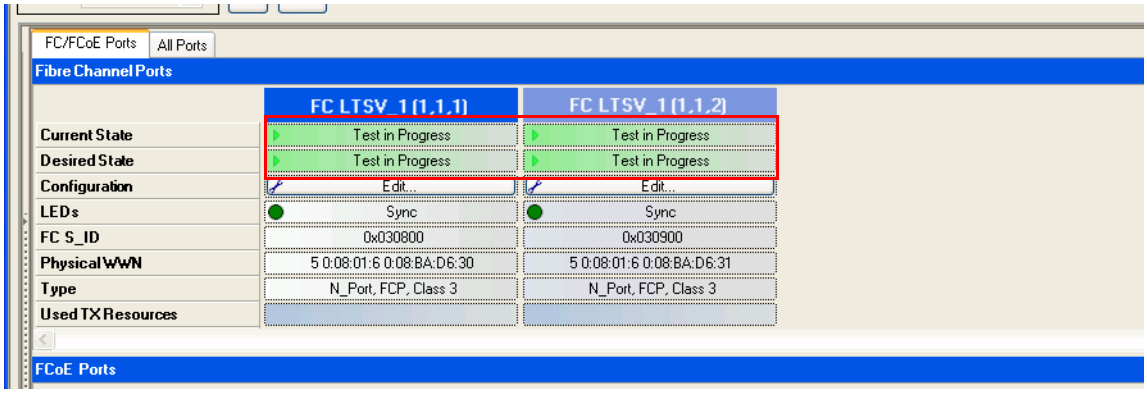
Starting the Test

To start the traffic, click on the **Start** 

button at the top of the window.

You will notice that current and goal states of the ports change from **Offline** to **Test in Progress**.

Figure 76: Test in Progress State



You have now started a test and traffic is now being sent from one port to another.

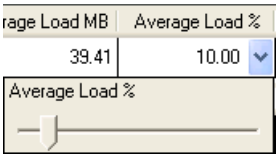
Adjusting the Load on the fly

If you have an analyzer connected you will notice that the test is running but the load is only 10%. It is simple to adjust the load while the test is running.

To adjust the load:

1. Click on the **Traffic** tab to show the **TX** tab.
2. Click on the plus sign (**+**) next to the **default** traffic pattern to display the ports in the traffic configuration.
3. Mouse over to the **10.00** in the **Average Load %** column to activate the arrow down  button.
4. Click the arrow down button to activate the **Average Load %** slider.

Figure 77: Average Load % Slider



5. Click and drag the slider up to **50%**.
6. If you drag the slider down to **0** and the traffic load will drop to zero. Moving it back to **50** or **100%** will increase the load which you can verify with both the analyzer, if you are using one, and the counters displayed in the **Traffic** tab. For now just leave it at **50%**.

Stopping the test

To stop the test, click the **Stop** 

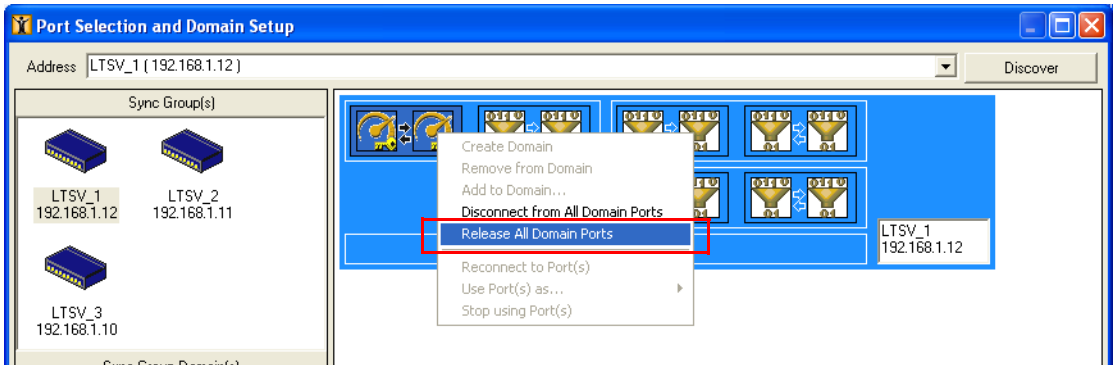
button on the upper part of the window.

Unlock the ports

To unlock the ports you locked for the test:

1. Click on the **Port selection and domain setup** button to open the **Port Selection and Domain Setup** dialog box.
2. Click on the locked ports to highlight them.
3. Right-click on one of the locked port icons and select **Release All Domain Ports** (refer to Figure 78).

Figure 78: Release All Domain Ports



4. Click the **Close** button to close this dialog box.

You are now done; you may exit the Maestro application.

Performing a Test with a Fibre Channel Switch

If you have a Fibre Channel switch, you can run a test in Load Tester by using the following discussion. It is assumed that the name and or IP address of the chassis is known.

Starting the Xgig Load Tester

To start the Xgig Load Tester application:

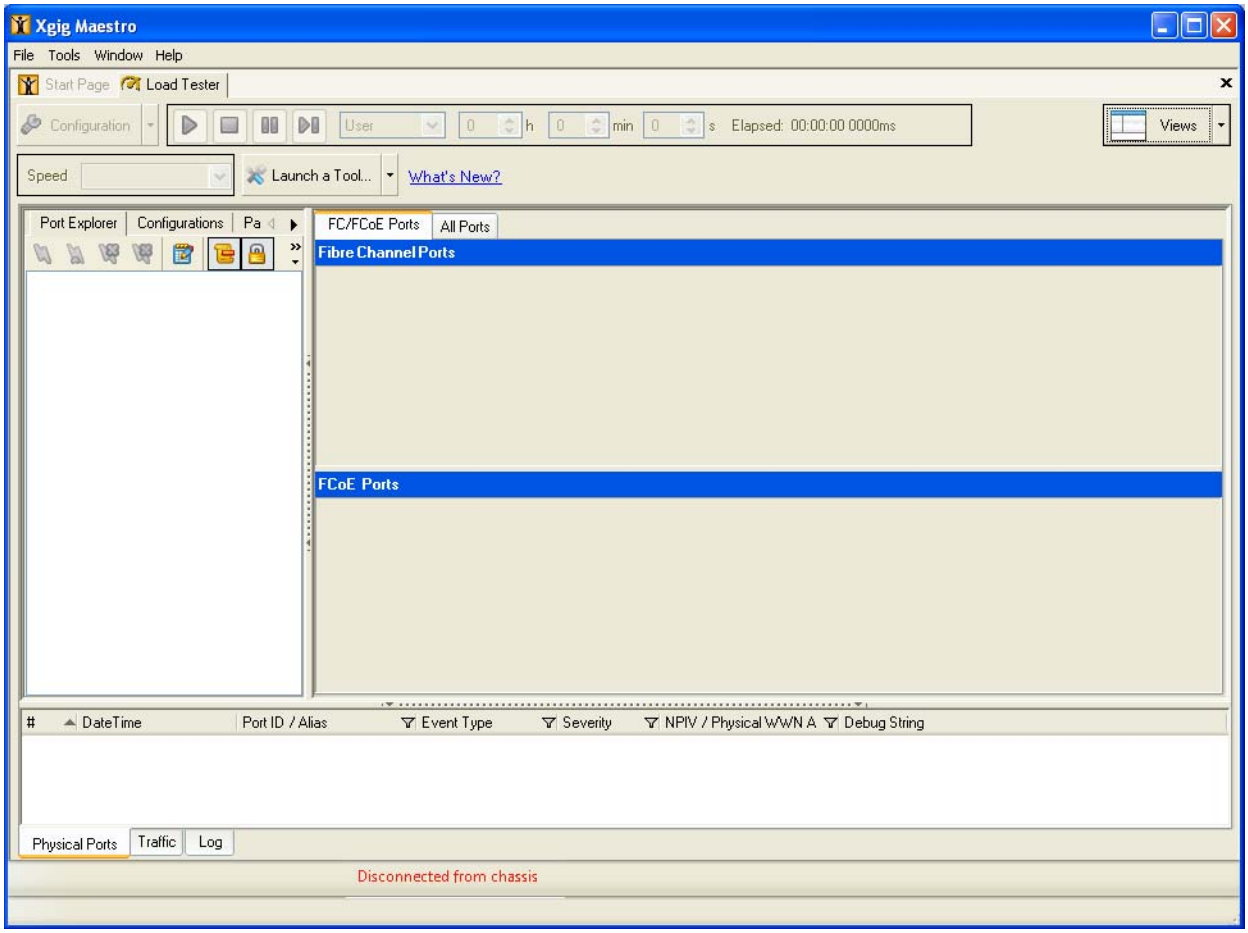
1 Go to **Start> All Programs> Viavi> Xgig Maestro**

The Xgig Maestro application will be opened.

2 Click on the **Load Tester** tab.

Your Xgig Maestro application will now look similar to Figure 79.

Figure 79: Xgig Load Tester Window



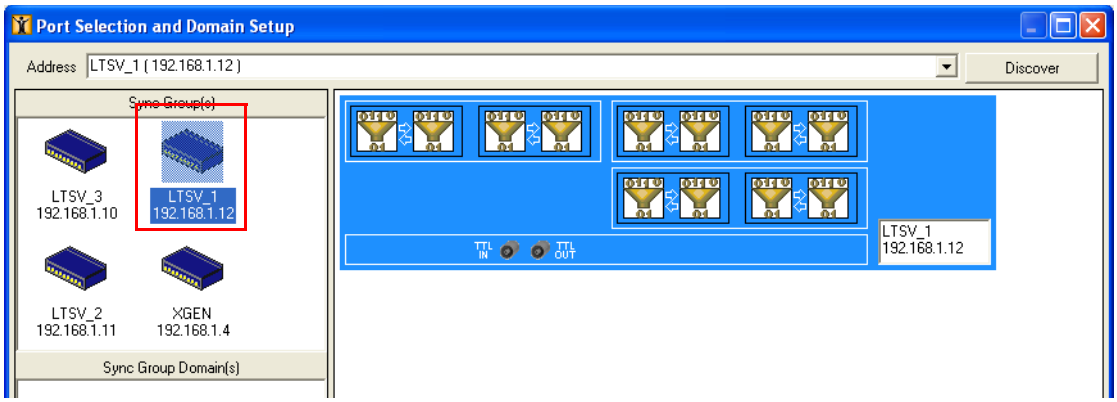
Locking the ports to use in the Load Tester

1 Click the **Port selection and domain setup...** 

.

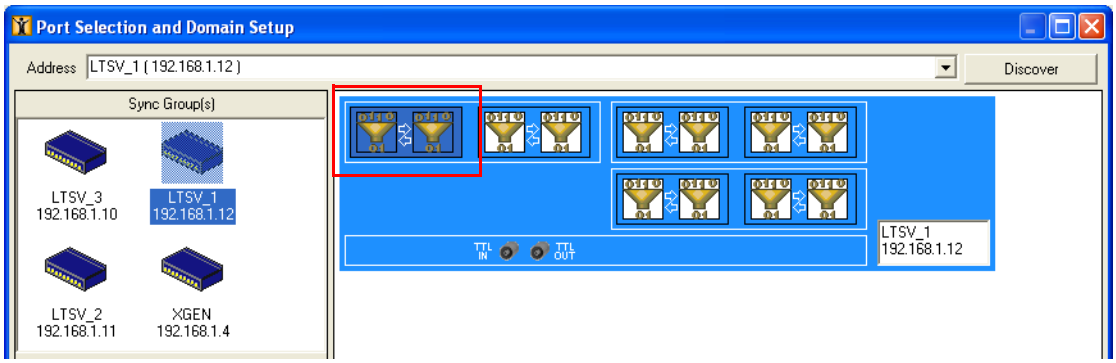
2 Select your chassis from the **Port Selection and Domain Setup** dialog box (Figure 80).

Figure 80: Selected Chassis



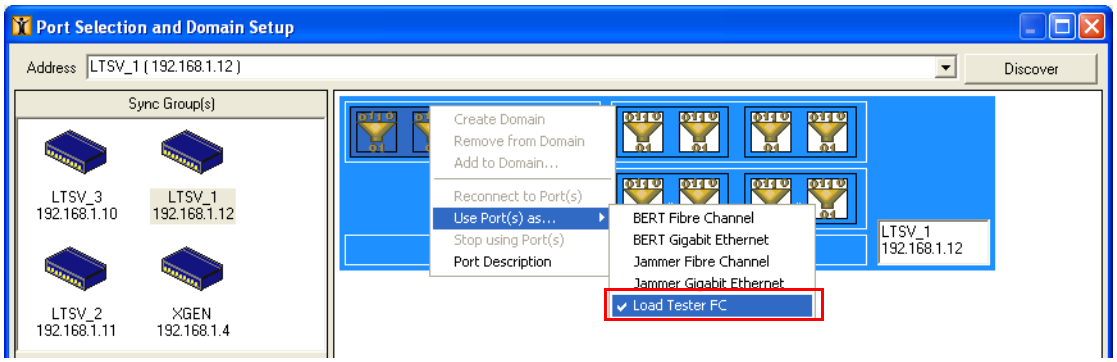
3 Click on the ports you wish to use to highlight them.

Figure 81: Selected ports



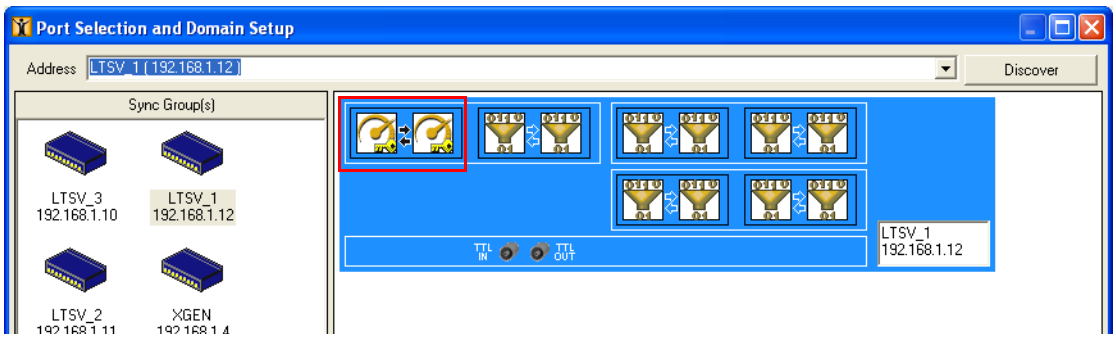
4 Right-click on one of the ports and select **Use Port(s) as...** and then select **Load Tester FC/ FCoE**.

Figure 82: Locking the ports to Load Tester



You will now see your two selected ports locked and ready for use. (Refer to Figure 83).

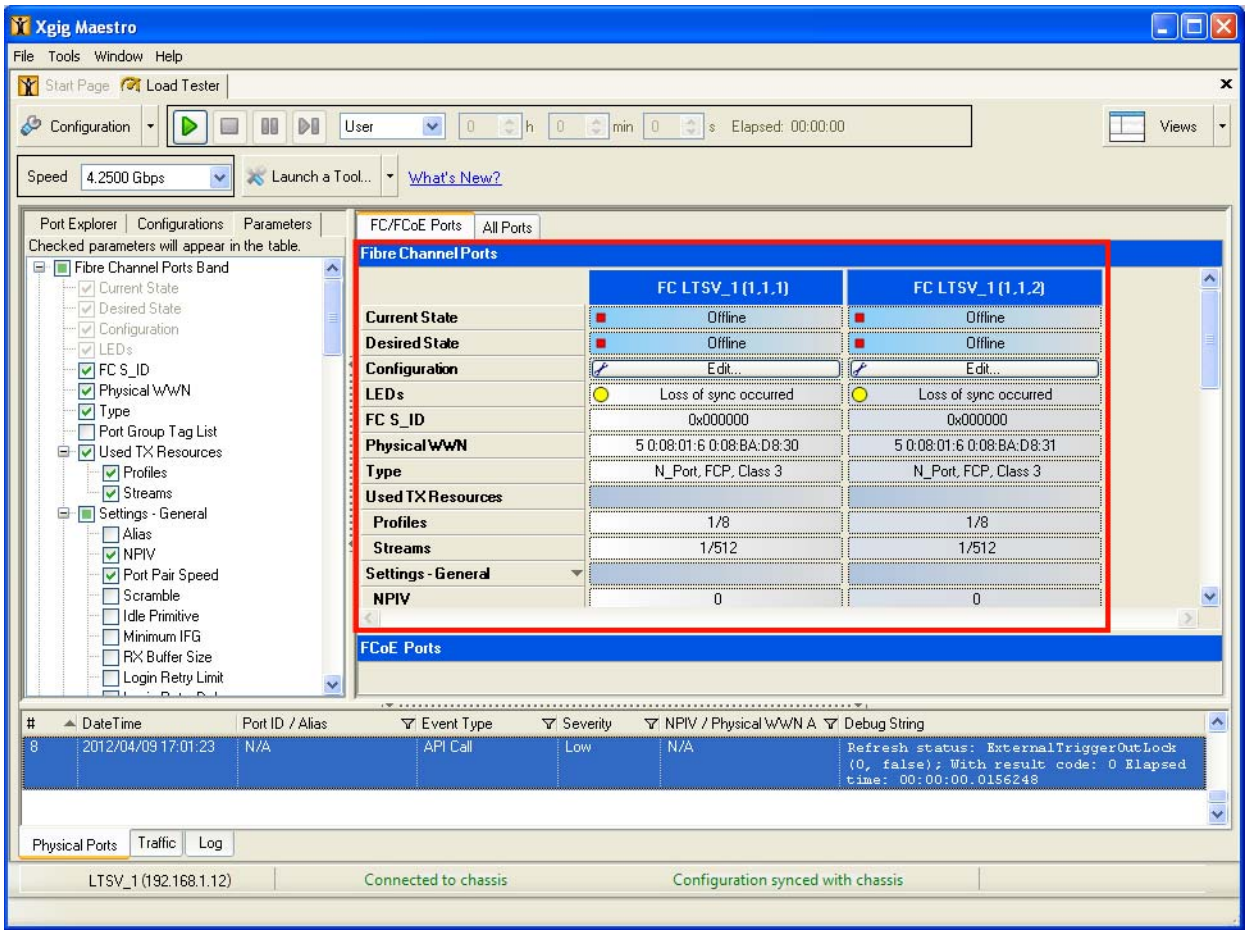
Figure 83: Locked ports



5 Close the dialog box.

Your Maestro Load Tester session will now appear similar to Figure 84.

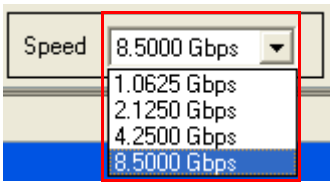
Figure 84: Load Tester window with locked ports



Setting the Speed for the Test

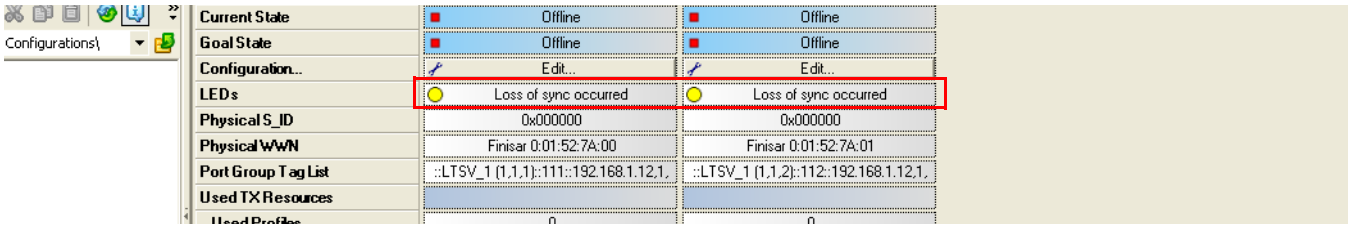
After locking the ports as Load Testers, you should verify if the speed of the link is correct. To quickly set the link speed for your hardware setup, select the speed to use (in Gbps) from the **Speed** drop-down menu found in the upper left corner (refer to Figure 85).

Figure 85: Speed Drop-down Menu



You will notice that the LEDs with the **Loss of sync occurred** status may have turned yellow if they were previously red (refer to Figure 66).

Figure 86: Loss of Sync occurred LED status

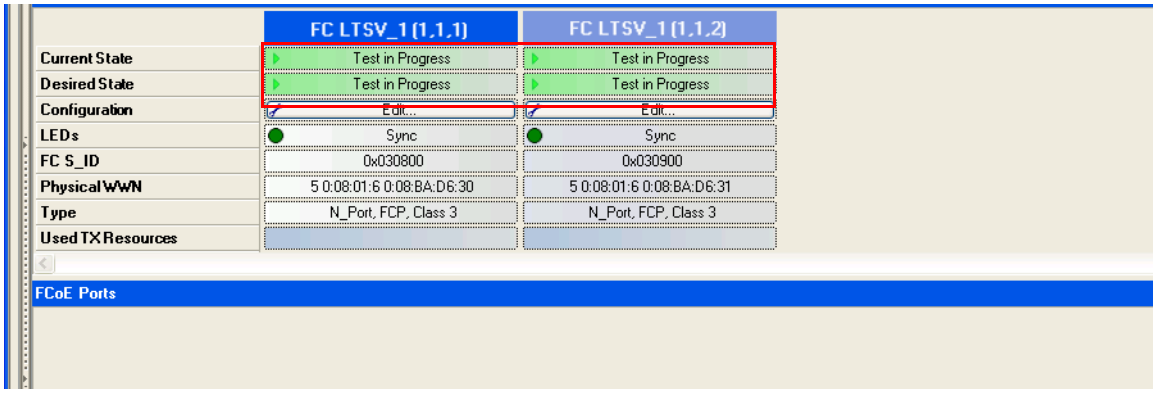


Starting the Test

To start the traffic, click on the **Start** button at the top of the window.

You will notice that current and goal states of the ports change from **Offline** to **Test in Progress**.

Figure 87: Test in Progress State



You have now started a test and traffic is being sent from one port to another.

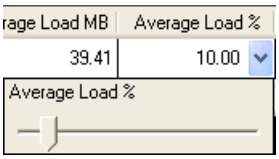
Adjusting the Load on the fly

If you have an analyzer connected you will notice that the test is running but the load is only 10%. It is simple to adjust the load while the test is running.

To adjust the load:

1. Click on the **Traffic** tab to show the **TX** tab.
2. Click on the plus sign (**+**) next to the **default** traffic pattern to display the ports in the traffic configuration.
3. Mouse over to the **10.00** in the **Average Load %** column to activate the arrow down button.
4. Click the arrow down button to activate the **Average Load %** slider.

Figure 88: Average Load % Slider



5. Click and drag the slider up to **50%**.
6. Now drag the slider down to **0** and the traffic load will drop to zero. Moving it back to **50** or **100%** will increase the load which you can verify with both the analyzer, if you are using one, and the counters displayed in the Traffic tab. For now just leave it at **50%**.

Stopping the test

To stop the test, click the **Stop** button on the upper part of the window.

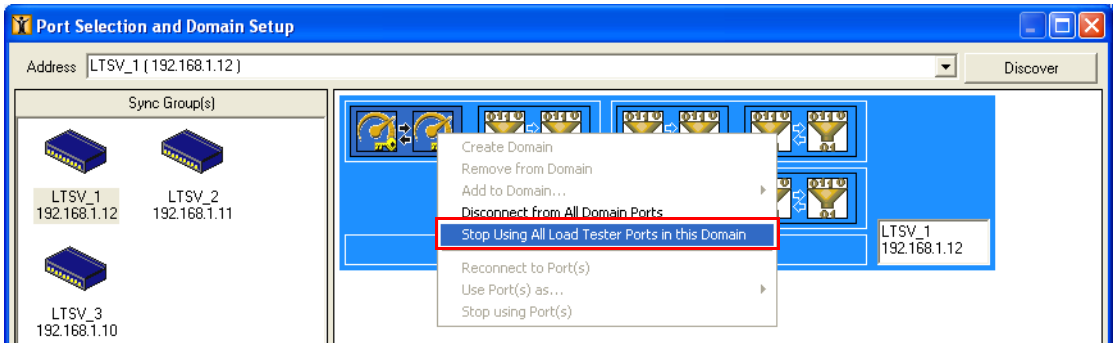
Unlock the ports

To unlock the ports you locked for the test:

1. Click on **Port selection and domain setup** button to open the **Port Selection and Domain Setup** dialog box.
2. Click on the locked ports to highlight them.

3 Right click on one of the locked port icons and select **Stop Using All Load Tester Ports in this Domain** (refer to Figure 78).

Figure 89: Stop Using All Load Tester Ports in this Domain



4 Click the **Close** button to close this dialog box.

You are now done; you may exit the Maestro application.

Saving a Configuration

Load Tester allows you to save a configuration that you have setup or used. The following discussion describes the process of saving your Load Tester configuration. Please note that it is assumed that the name and or IP address of the chassis is known.

Starting the Xgig Load Tester

To start the Xgig Load Tester application:

1 Go to **Start> All Programs> Viavi> Xgig Maestro**

The Xgig Maestro application will be opened.

2 Click on the **Load Tester** tab.

Your Xgig Maestro application will now look similar to Figure 59.

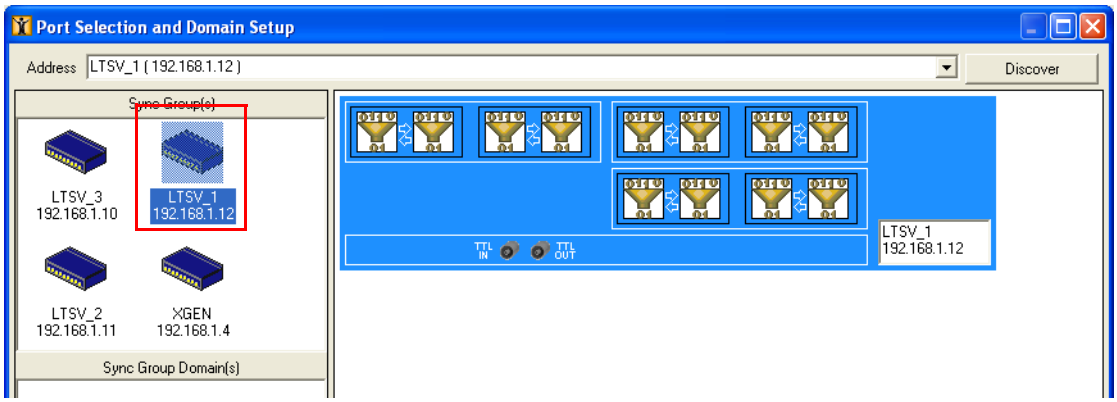
Locking the ports to use in the Load Tester

1 Click the **Port selection and domain setup...** 

.

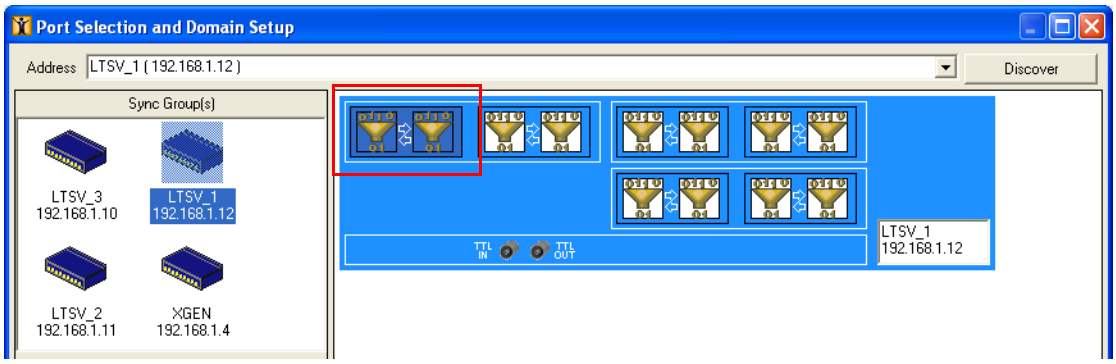
2 Select your chassis from the **Port Selection and Domain Setup** dialog box (refer to Figure 90).

Figure 90: Selected Chassis



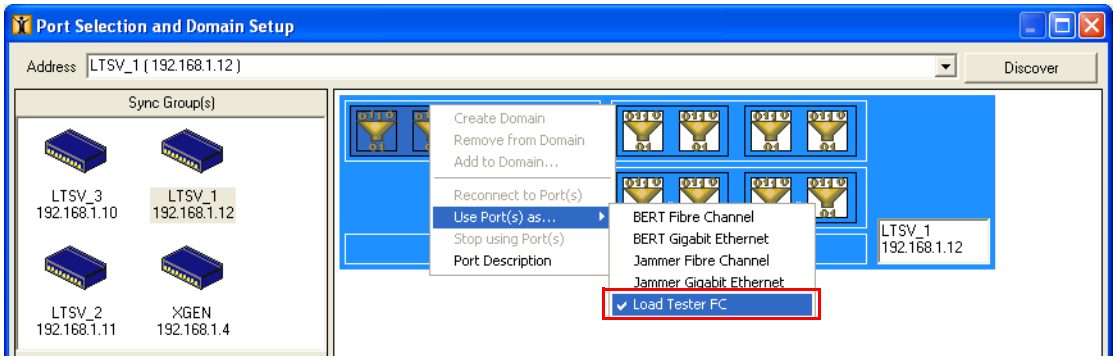
3 Click on the ports you wish to use to highlight them.

Figure 91: Selected Ports



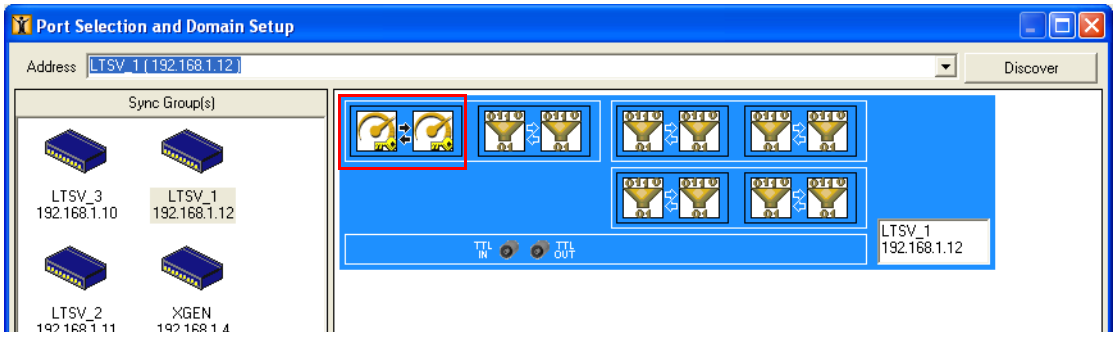
4 Right-click on one of the ports and select **Use Port(s) as...** and then select **Load Tester FC/ FCoE**.

Figure 92: Locking the ports to Load Tester



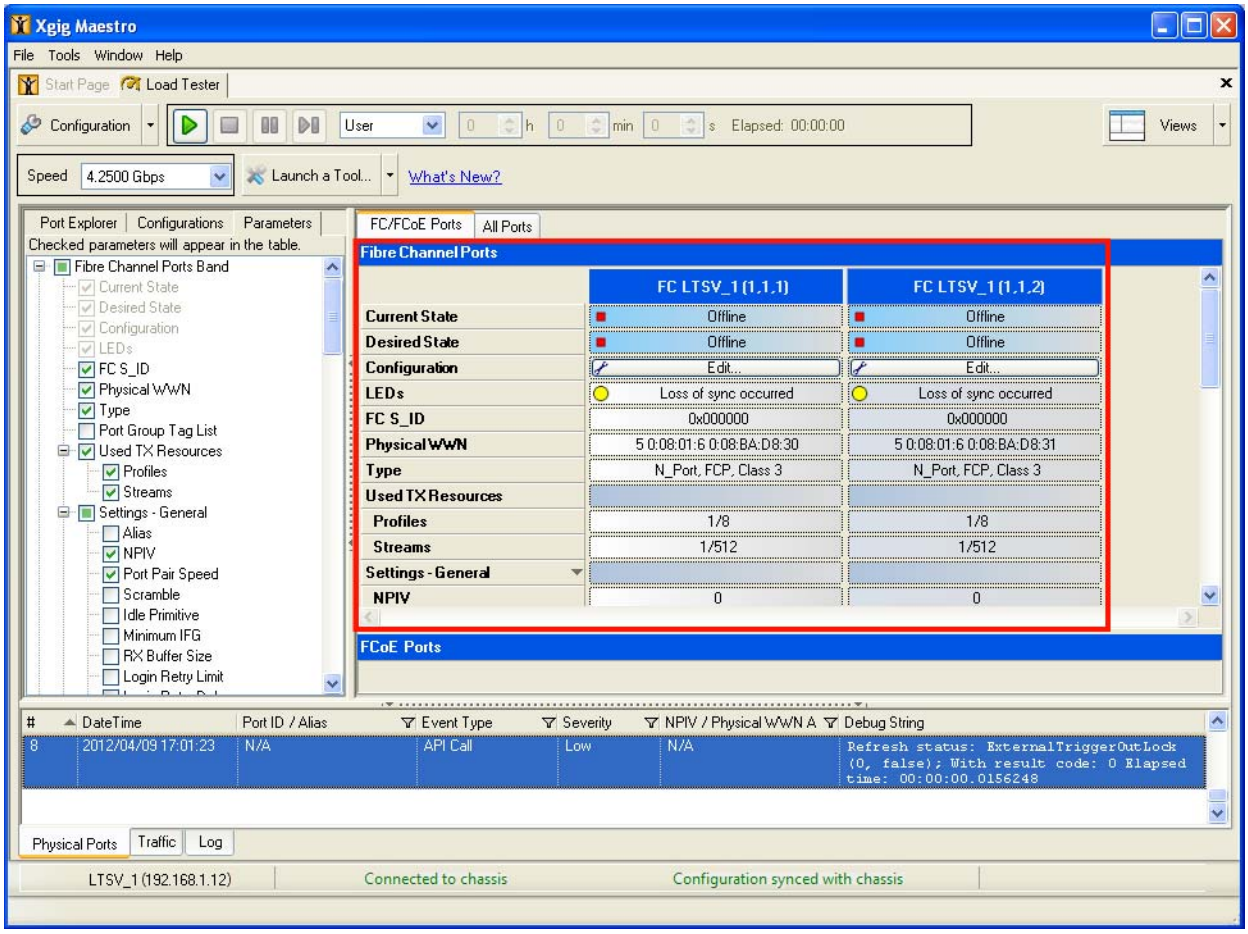
You will now see your two selected ports locked and ready for use (refer to Figure 63).

Figure 93: Locked ports



5 Close the dialog box. Your Maestro Load Tester session will now appear similar to Figure 94.

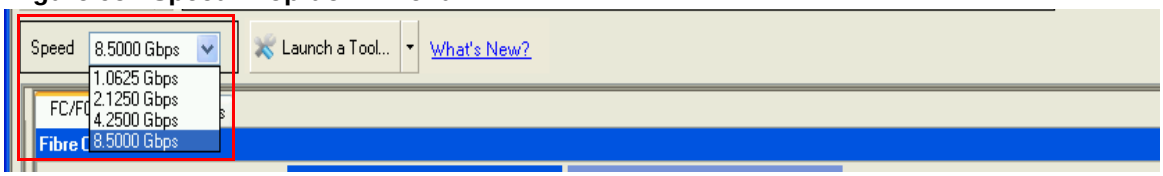
Figure 94: Load Tester window with locked ports



Setting the Speed for the Test

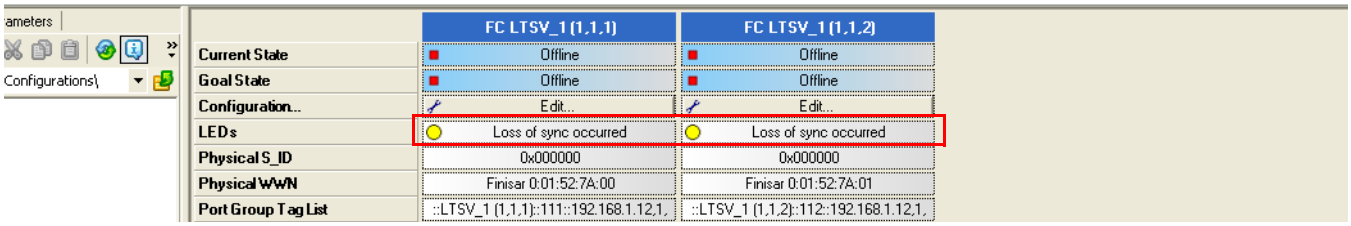
After locking the ports as Load Testers, you should verify if the speed of the link is correct. To quickly set the link speed for your hardware setup, select the speed to use (in Gbps) from the **Speed** drop-down menu found in the upper left corner (refer to Figure 65).

Figure 95: Speed Drop-down Menu



Now you will notice that the LEDs with the **Loss of sync occurred** status may have turned yellow if they were previously red (refer to Figure 66).

Figure 96: Loss of Sync occurred LED status

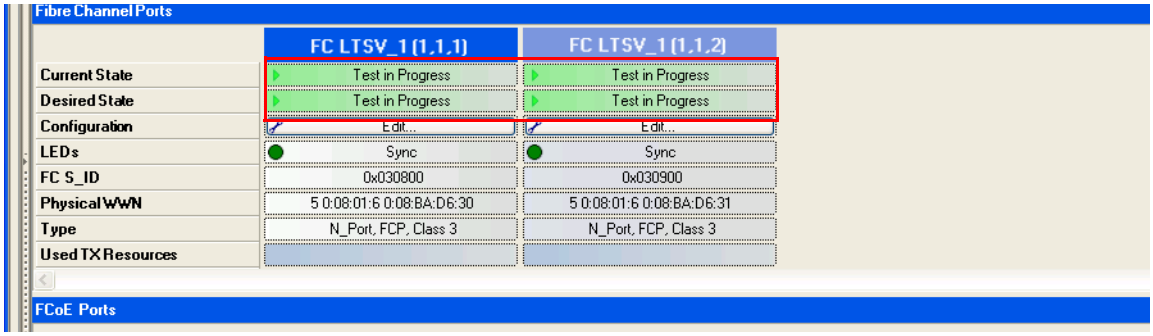


Starting the Test

To start the traffic, click on the **Start** button at the top of the window.

You will notice that current and goal states of the ports change from **Offline** to **Test in Progress**.

Figure 97: Test in Progress State



You have now started a test and traffic is being sent between the ports. You also now have a working configuration that you can save.

Stopping the test

Before the current working configuration, you should stop the test.

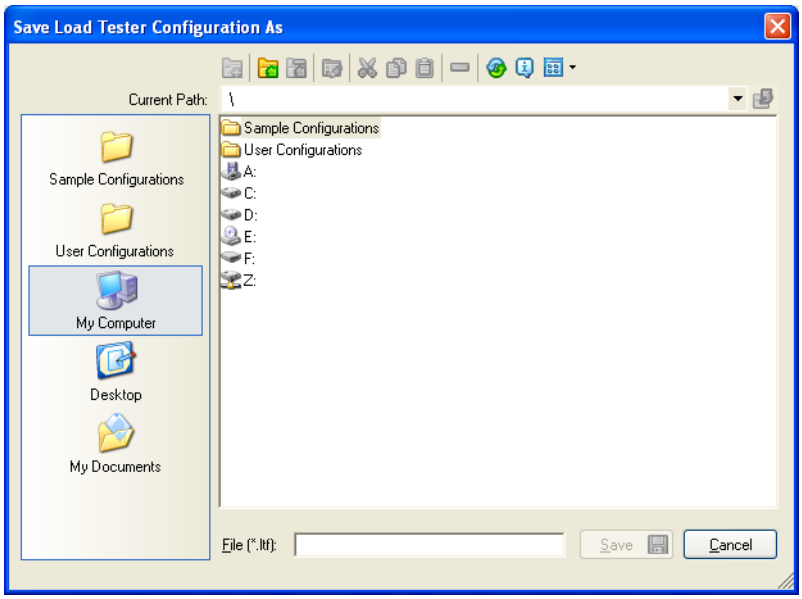
To stop the test, click the **Stop** button on the upper part of the window.

Saving the Configuration

To save the configuration:

1 Click the **Configuration** button in the top of the window and select **Save Configuration** from the drop-down menu to open the **Save Load Tester Configuration As** dialog box.

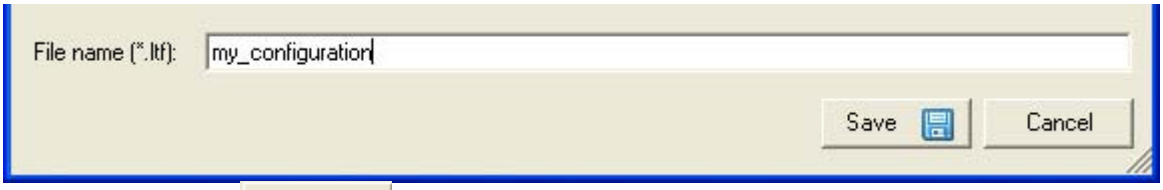
Figure 98: Save Load Tester Configuration As dialog box

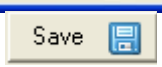


2 Create a name for the configuration that you wish to save.

For this example we will use **my_configuration**.

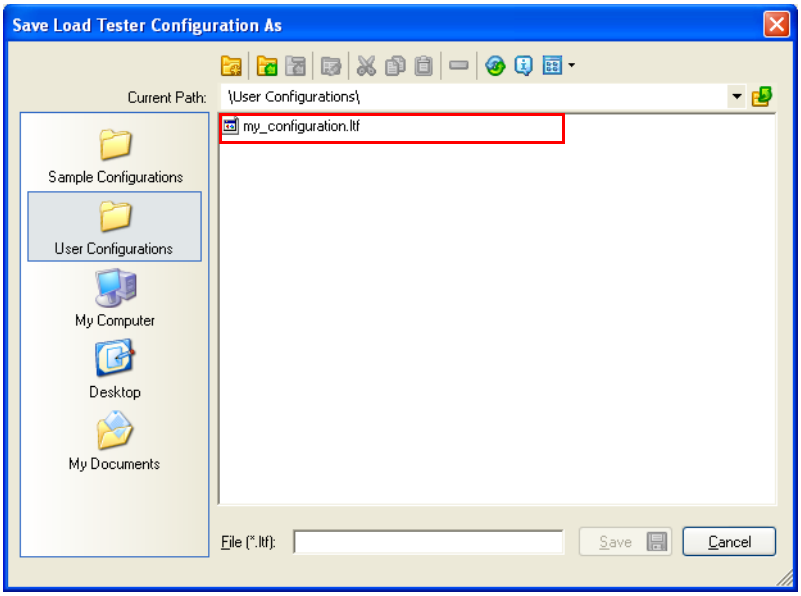
Figure 99: File name field



3 Click the **Save**  button to save your configuration.

4 As a quick check, you can click the **Save configuration** button again and see that your configuration has been saved.

Figure 100: Save Load Tester Configuration As dialog box



5 Click the **Cancel** button to close the dialog box.

Unlock the ports

Once you are done saving the Load Tester configuration you may unlock the ports already.

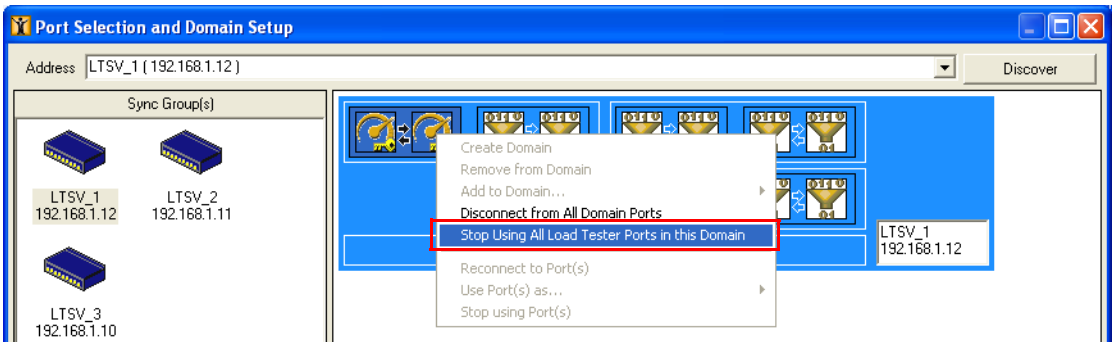
To unlock the ports you locked for the test:

1 Click on **Port selection and domain setup** button to open the **Port Selection and Domain Setup** dialog box.

2 Click on the locked ports to highlight them.

3 Right click on one of the locked port icons and select **Release All Domain Ports** (refer to Figure 101).

Figure 101: Stop Using All Load Testers Ports in this Domain



4 Click the **Close** button to close this dialog box.

You are now done; you may exit the Maestro application.

Loading a Configuration

Load Tester also allows you to load a configuration that you have saved. The following discussion describes the process of loading your Load Tester configuration. Please note that it is assumed that the name and or IP address of the chassis is known.

Starting the Xgig Load Tester

To start the Xgig Load Tester application:

1 Go to **Start > All Programs > Viavi > Xgig Maestro**

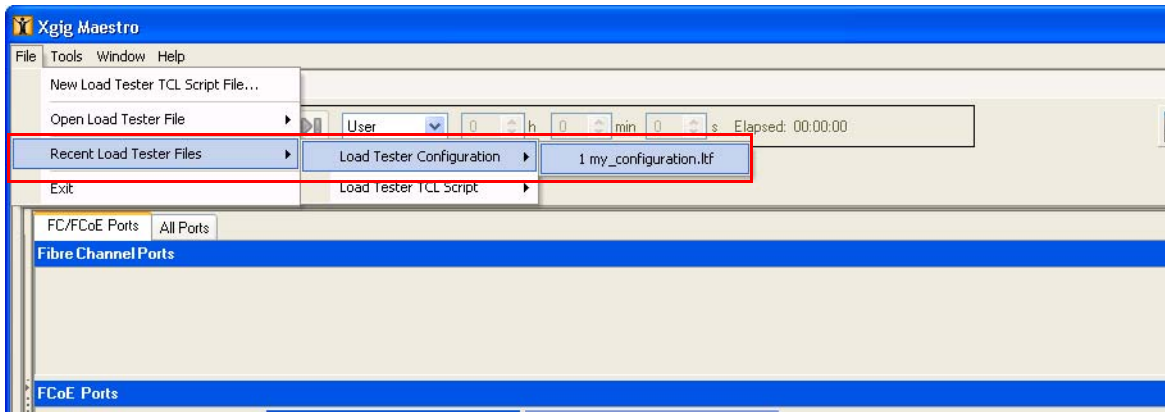
The Xgig Maestro application will be opened.

2 Click on the **Load Tester** tab.

Your Xgig Maestro application will now look similar to Figure 59.

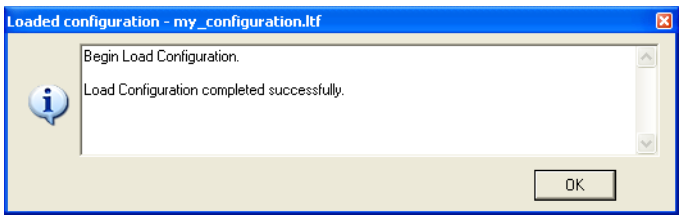
3 Open the configuration file that you saved by selecting **File > Recent Load Tester Files > Load Tester Configuration > my_configuration.ltf** from the Menu toolbar.

Figure 102: Load Recent Load Tester File



The load configuration process will begin. When the process completes, the message box (Figure 103) describing the status of the configuration load will appear.

Figure 103: Loaded Configuration message box



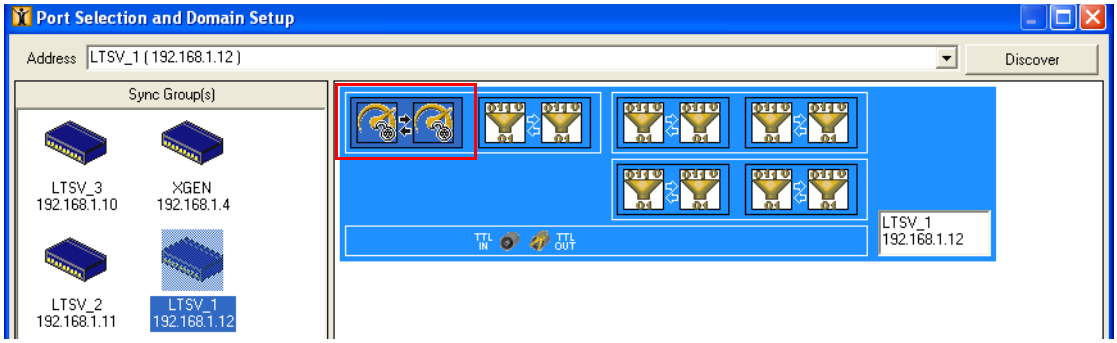
4 Click **Ok** to close the message box. The **Physical Ports** tab will still be empty.

5 Click on **Port selection and domain setup** button to open the **Port Selection and Domain Setup** dialog box.

6 Select your chassis.

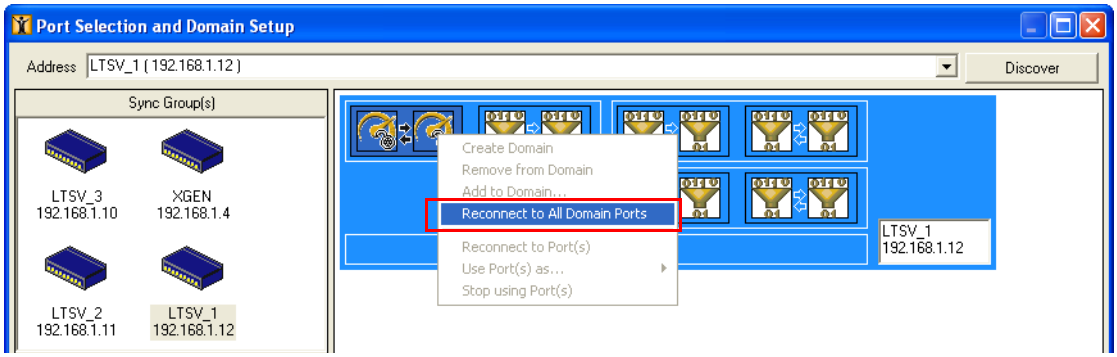
7 Click on the ports that have icons resembling opened silver locks on them (refer to Figure 104).

Figure 104: Unlocked Ports



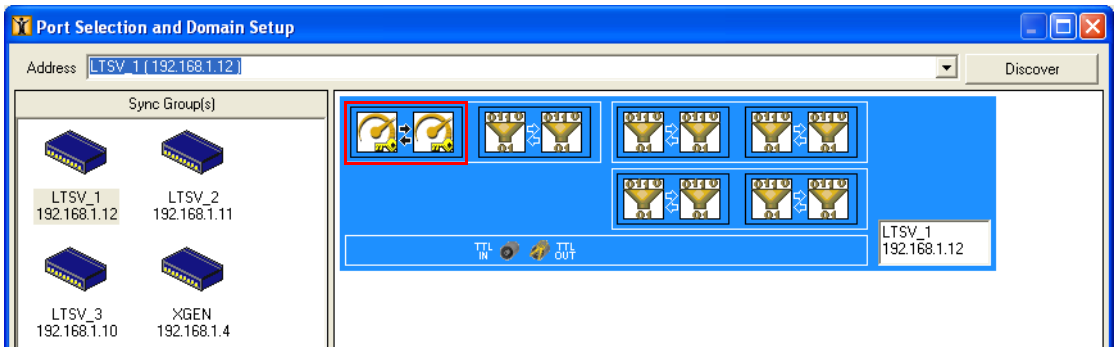
8 Right-click on one of the selected ports and select **Reconnect to All Domain Ports** (Figure 105).

Figure 105: Reconnect to All Domain Ports



The ports will now have yellow key icons (Figure 106) on them.

Figure 106: Locked Ports



9 Click the **Close** button to close this dialog.

You will now see the ports that are listed in the configuration file and have been loaded. All their settings and traffic configuration topologies have been restored. The ports will be in an offline state. You may now continue testing.

Burst Mode Explained

The following discussion is a working example of the Load Tester configuration and trace output.

The first part of the example is the typical Load Tester setup.

Starting the Xgig Load Tester

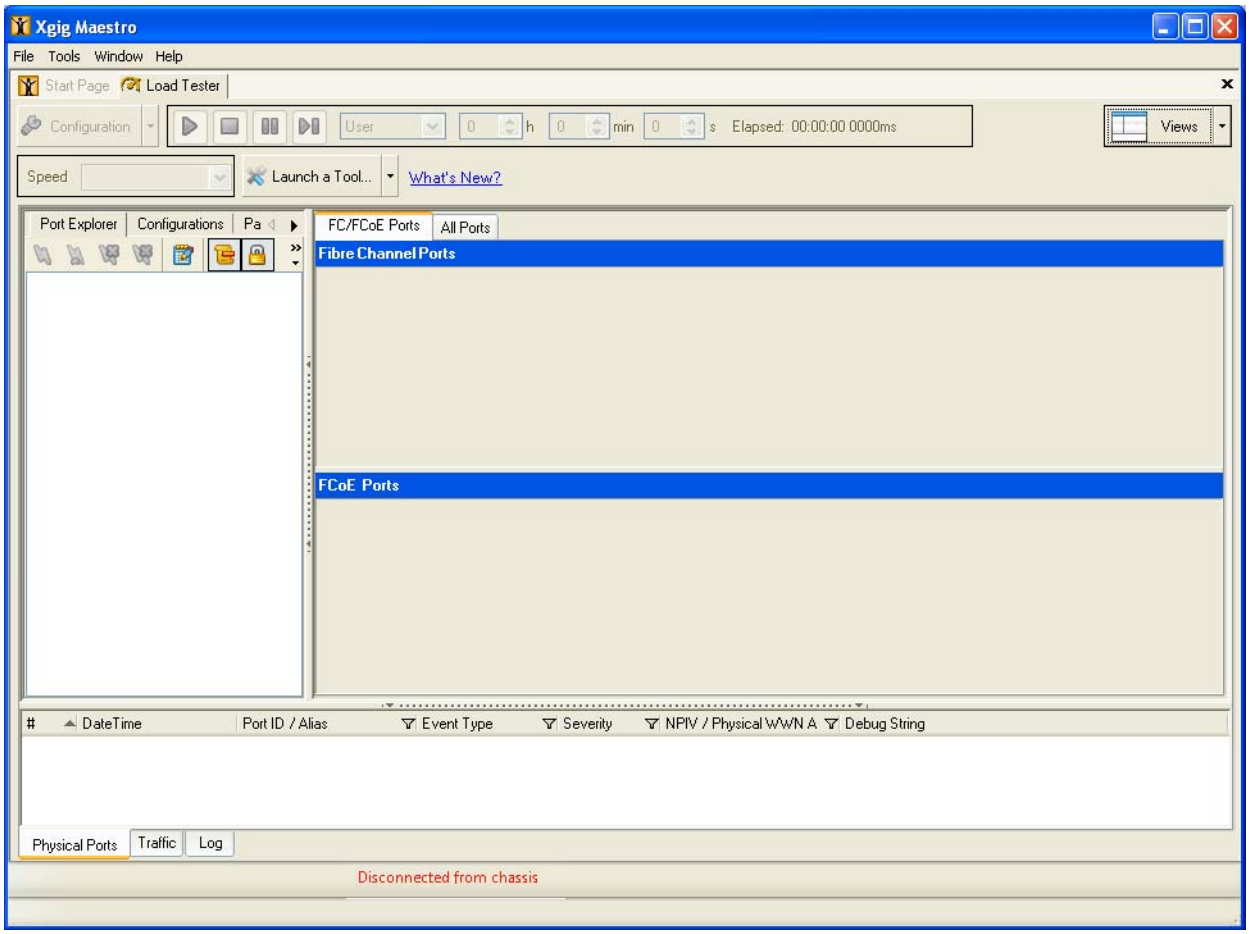
To start the Xgig Load Tester application:

1 Go to **Start> All Programs> Viavi> Xgig Maestro**

The Xgig Maestro application opens with the **Maestro Global** tab (Figure 107).

2 Click on **Load Tester** under **Load a Maestro Plugin**.

Figure 107: Xgig Load Tester Window



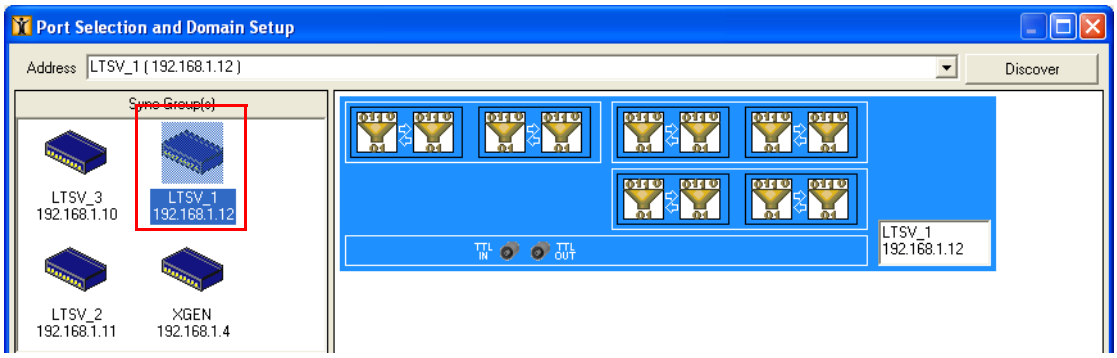
Locking the ports to use in the Load Tester

1 Click the **Port selection and domain setup...** 

.

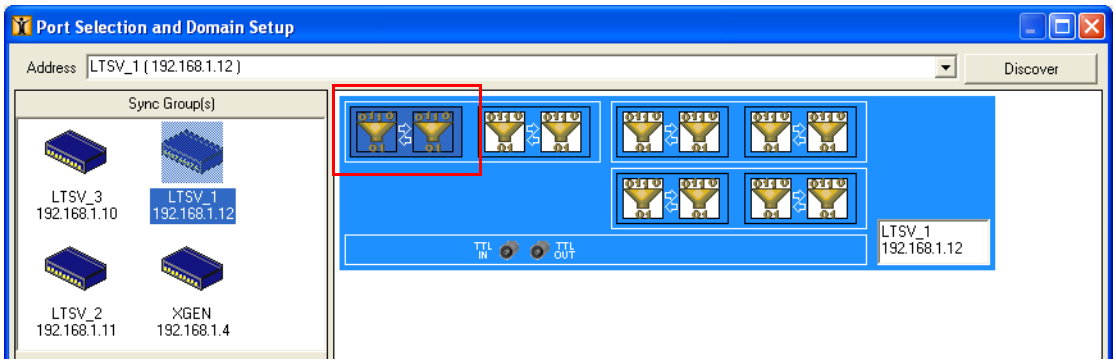
2 Select your chassis from the **Port Selection and Domain Setup** dialog box (refer to Figure 108).

Figure 108: Selected Chassis



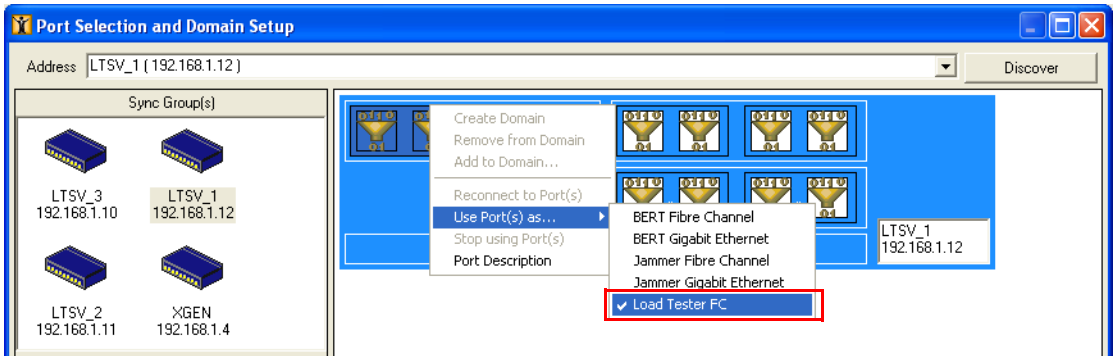
3 Click on the ports you wish to use to highlight them.

Figure 109: Selected Ports



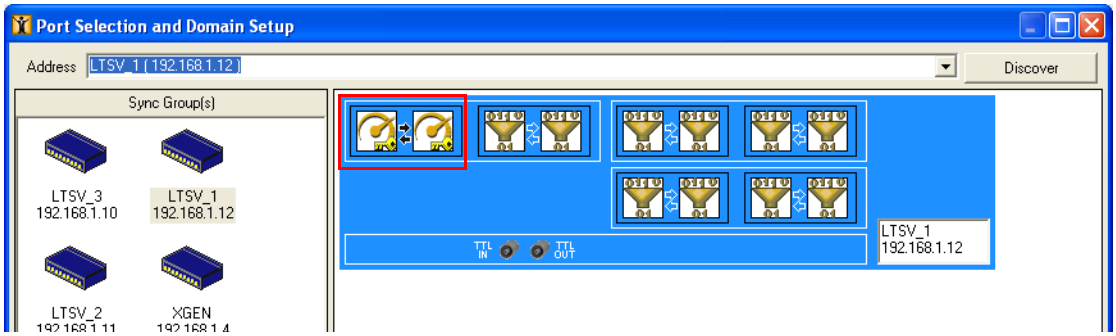
4 Right-click on one of the ports and select **Use Port(s) as...** and then select **Load Tester FC/ FCoE**.

Figure 110: Locking the ports to Load Tester



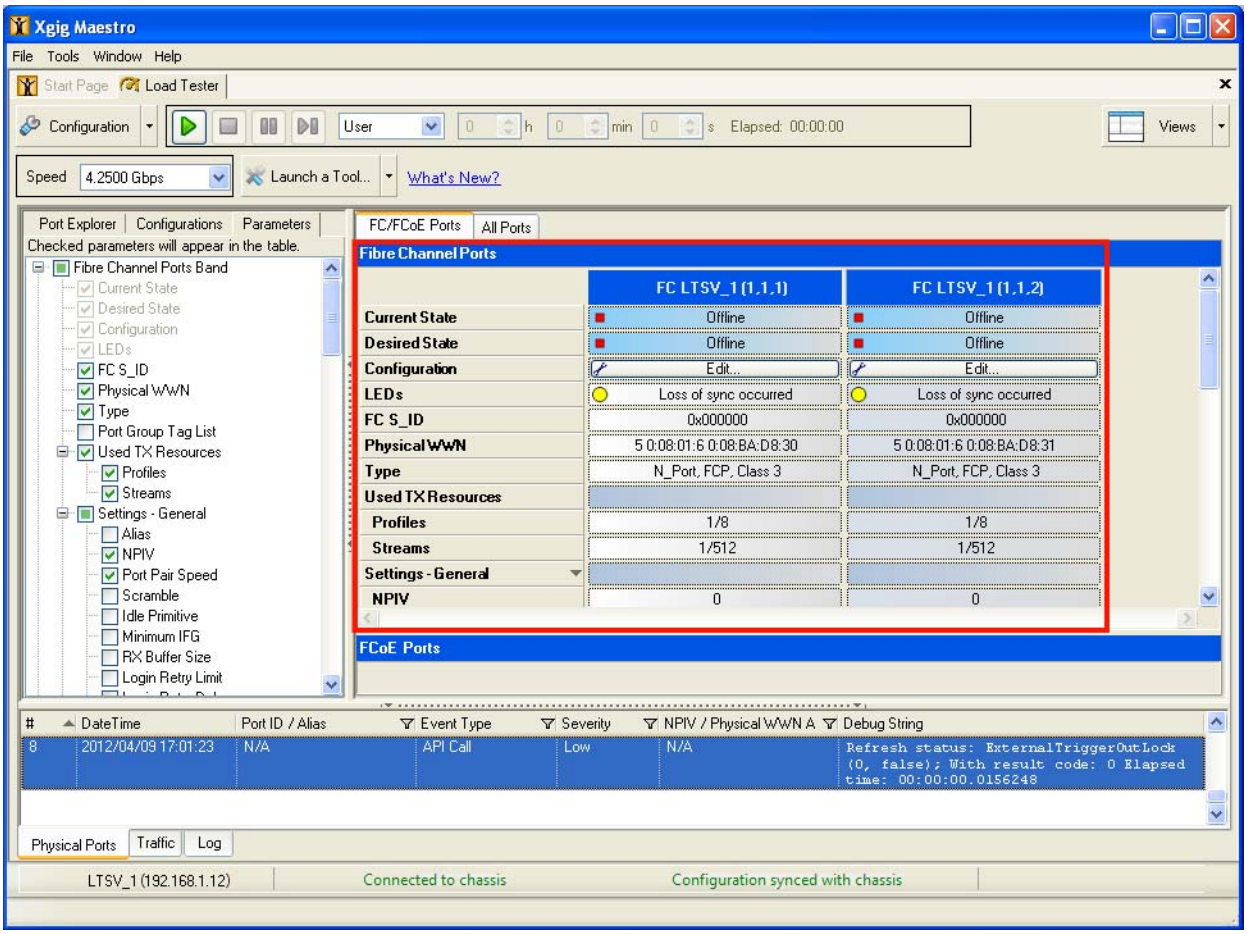
You will now see your two selected ports locked and ready for use. (Refer to Figure 111).

Figure 111: Locked ports



5 Click on the **Close** button to close the dialog box. Your Maestro Load Tester session will now appear similar to Figure 112.

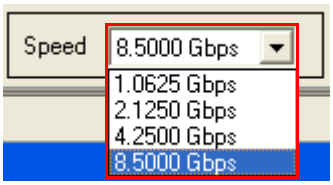
Figure 112: Load Tester window with locked ports



Setting the Speed for the Test

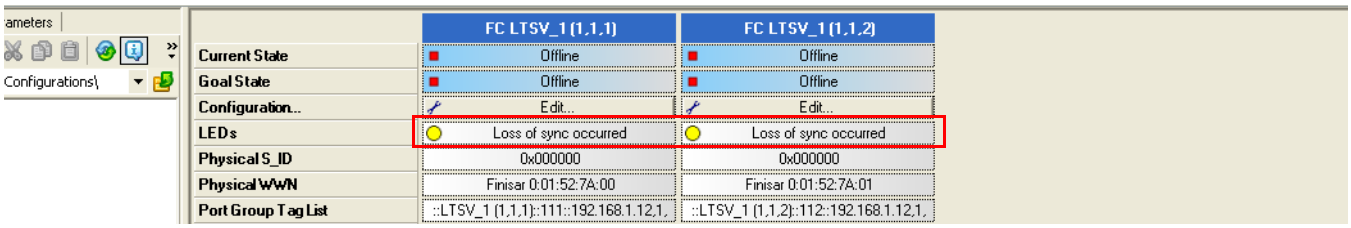
After locking the ports as Load Testers, you should verify if the speed of the link is correct. To quickly set the link speed for your hardware setup, select the speed to use (in Gbps) from the **Speed** drop-down menu found in the upper left corner (refer to Figure 65).

Figure 113: Speed Drop-down Menu



Now you will notice that the LEDs with the **Loss of sync occurred** status may have turned yellow if they were previously red (refer to Figure 66).

Figure 114: Loss of Sync occurred LED status



Editing the Topology

Once you finished setting the speed, you need to change the traffic topology. Near the bottom of the window you will see three tabs labeled **Physical Ports**, **Traffic** and **Log**.

To edit the topology:

1 Click on the **Traffic** tab to display the **TX** tab.

Figure 115: Traffic tab

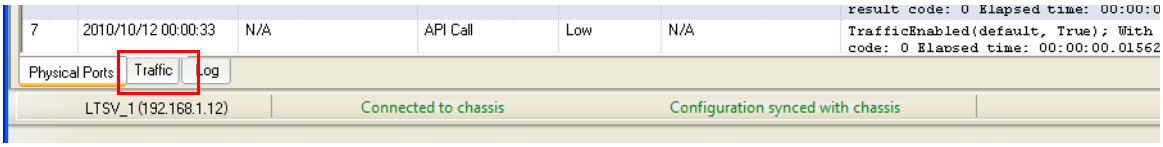
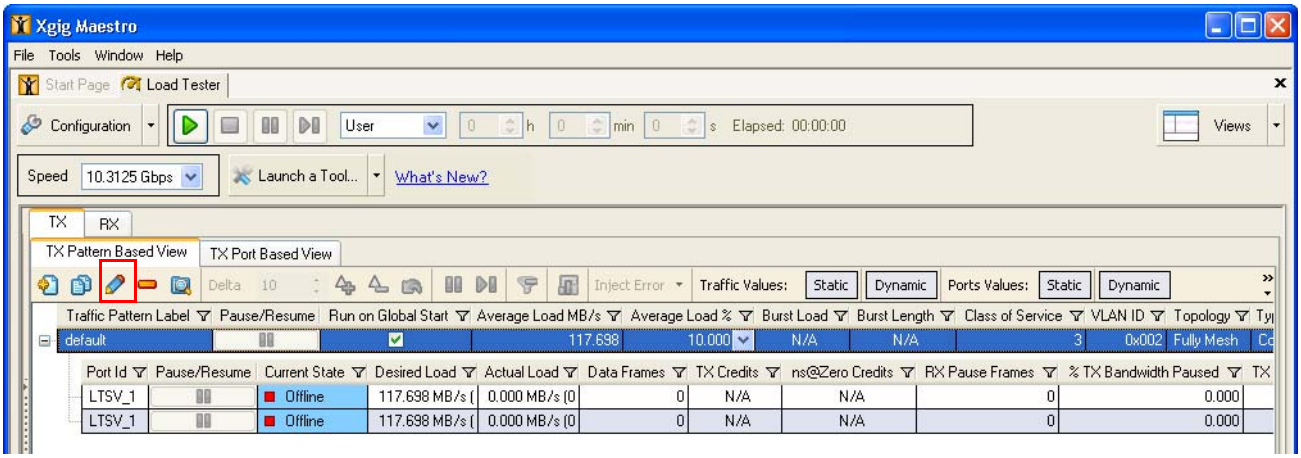
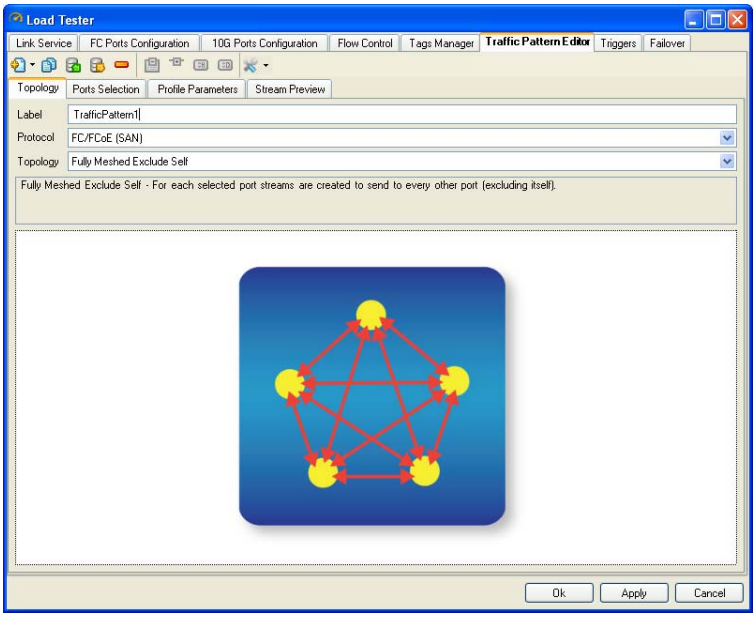


Figure 116: TX tab in the Traffic tab



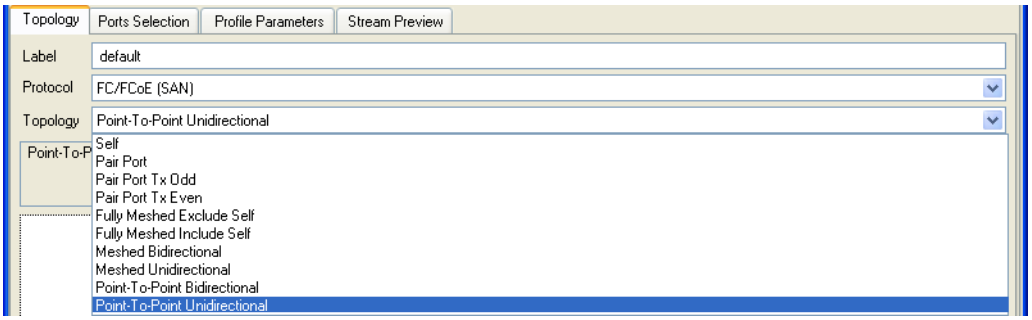
2 Click the pencil icon to open the **Traffic Pattern Editor** tab in the Load tester Device Window so you can edit the **default** traffic configuration provided for you.

Figure 117: Traffic Pattern Editor Tab



3 Change the topology to **Point to Point Unidirectional**.

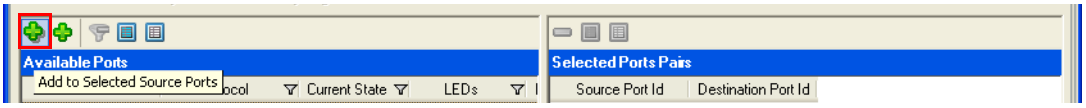
Figure 118: Topology drop-down menu



4 Click on the **Ports Selection** tab to select ports for the traffic pattern.

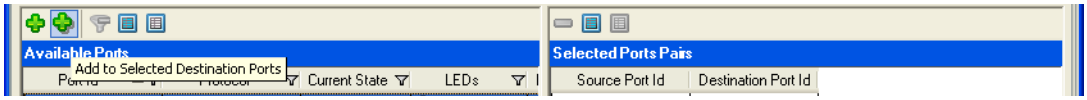
5 Select the first port from the **Available Ports** pane and add it to the source port list by clicking **Add Selected Ports to Source** button (Figure 119).

Figure 119: Add to Selected Source Ports



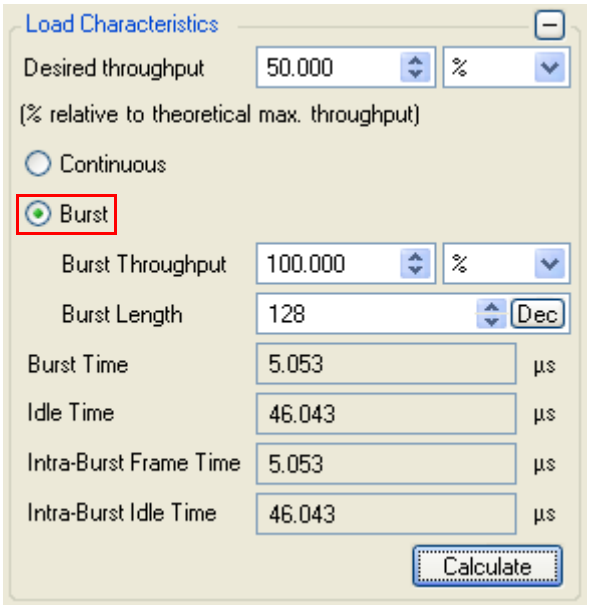
6 Select the second port and add it to the destination port list by clicking **Add Selected Ports to Destination**.

Figure 120: Add to Selected Destination Ports



7 On the **Profile Parameters** tab, select the **Burst** radio button in the **Load Characteristics** pane (Figure 121).

Figure 121: Load Characteristics Pane

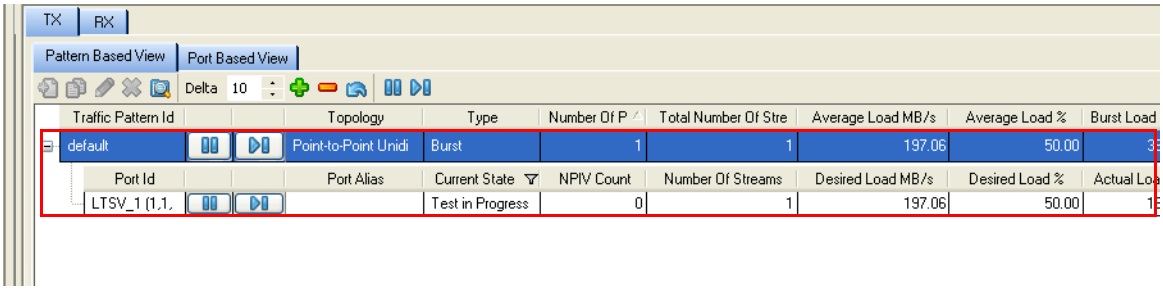


8 Set **Desired throughput** to **50.00 %**, **Burst Length** to **128**, and **Burst Throughput** to **100.00 %**.

9 Click **Ok** to close the dialog box.

10 Expand the **default** traffic pattern.

Figure 122: Changed traffic bar



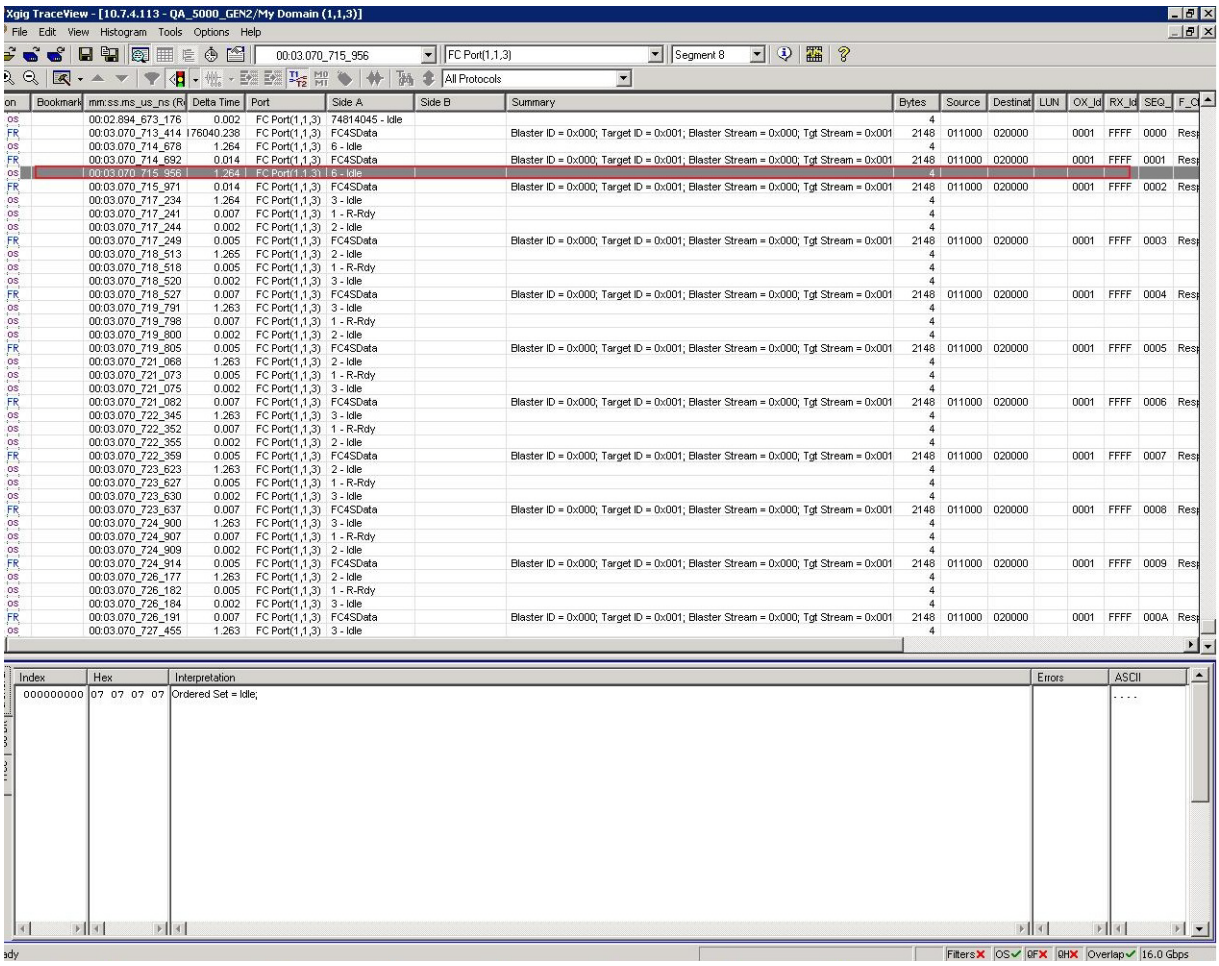
11 Click on the **Start** button at the top of the window.

Burst Mode Explanation

Below is a sample Xgig TraceView snapshot (Figure 123) of the traffic on the wire.

As you can see there are 6 idles between the frames and every 128 frames there is a gap with 69502 idles. The load on the wire is roughly equal between 100% load and Idles giving us an average load of 50%.

Figure 123: Xgig TraceView Snapshot



Note: R-Rdy is counted as an Idle as well.

In the example of the trace we have 128 full size frames (2148 bytes) with 6 idles (24 bytes) between frames which equates to 2172 bytes.

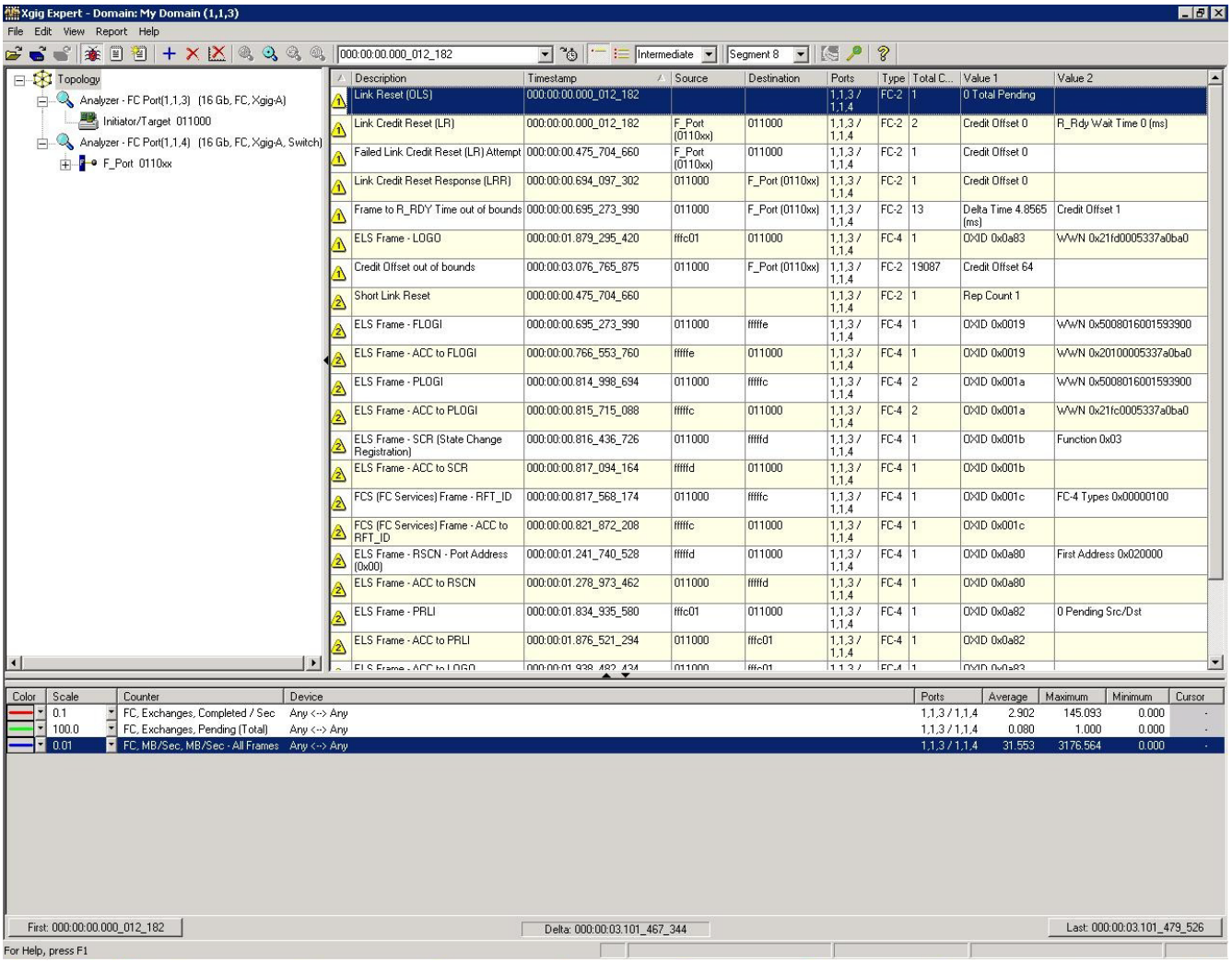
278016 bytes = **128** full size frames* (**2148** bytes + (**6** idles* 4))

278008 bytes = the gap of **69502** idles which is almost identical to the load.

The graphical representation of the load on the wire is shown in Figure 124.

You can see the digital saw tooth display of full load and no load. When summed together they represent the average load of **50%**.

Figure 124: Xgig Expert Snapshot



You can now stop the test.

Stopping the test

To stop the test, click the **Stop** button on the upper part of the window.

Unlock the ports

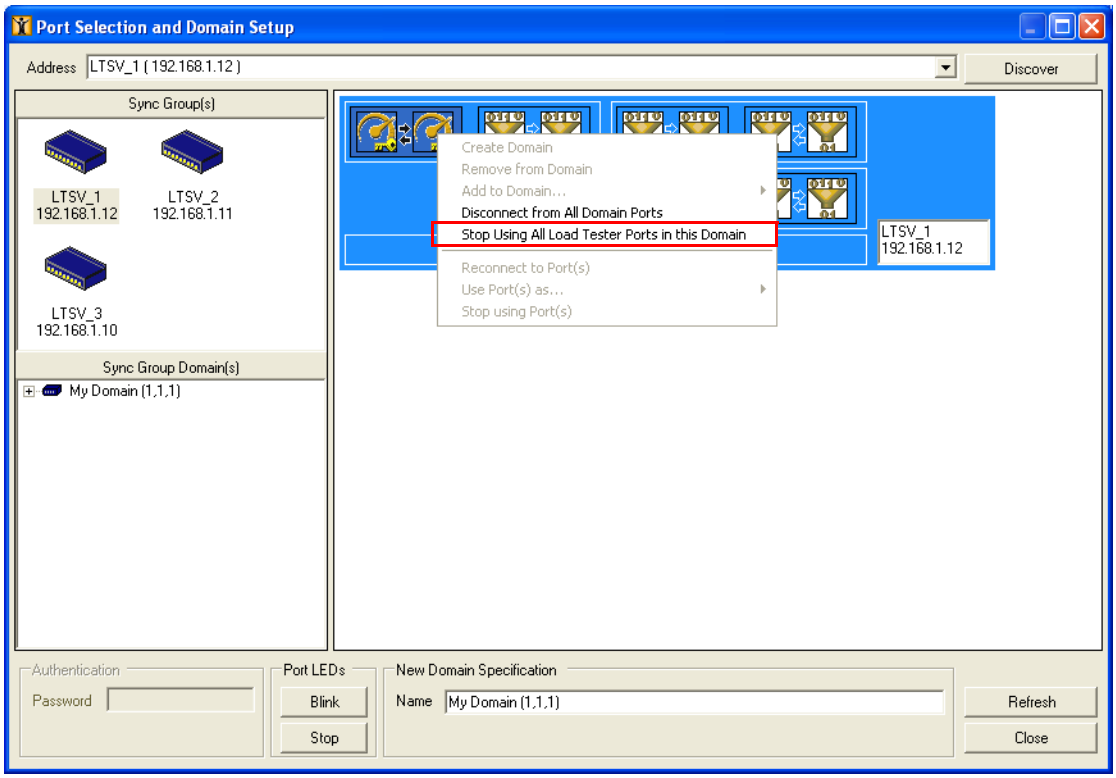
To unlock the ports you locked for the test:

1 Click on **Port selection and domain setup** button to open the **Port Selection and Domain Setup** dialog box.

2 Click on the locked ports to highlight them.

3 Right click on one of the locked port icons and select **Stop Using All Load Tester Ports in this Domain** (refer to Figure 125).

Figure 125: Stop Using All Load Tester Ports in this Domain



4 Click the **Close** button to close this dialog box.

You are now done; you may exit the Maestro application.

Appendix B

Simplifying Detection and Resolution of Missing Frames

In this chapter:

Abstract

A critical performance metric for switches is whether they drop, misdirect, or deliver frames out of order. Traditional network analysis tools fall short of being able to easily detect, monitor, and analyze these types of errors, making this a challenging and time-consuming metric for developers to measure accurately.

Xgig Load Tester offers unique capabilities for comprehensively measuring this key performance metric in even the most complex network configurations. This case study will show developers how the Load Tester can be used in conjunction with the Xgig Analyzer to accelerate development and troubleshooting of network switches, enabling error resolution in minutes. After reading this case study, developers will be able to confidently configure and connect test hardware, set triggers, detect errors, capture traces, search and locate error frames, and debug and resolve these types of errors quickly and easily.

Frame Delivery Errors

One of the key characteristics of Fibre Channel switches is that they do not lose frames or change frame order. When an expected frame is not received at its destination, there are three possible scenarios:

1. The frame actually arrives out of order.
   For example, frames are received with SEQ_CNT of 1, 2, 3, 5, 4.
2. The frame was dropped at the switch.
3. The frame was directed to the wrong destination.
   For example, even though the frame was addressed to D_ID1, it was sent to D_ID2.

Triggering the above frame delivery errors is impossible to accomplish with analysis tools only. This is the case because the capture triggers of real-time traffic can be defined based upon a single frame while capturing the mal-delivery events relies on the information of a sequence of frames.

For dropped frames or frames sent to the wrong destination, the frame never arrives at the port of interest so there's no frame off of which to trigger. For frames arriving out-of-order, intra-frame analysis does not track sequence number so these slip past as well. While it is possible to use analyzers by themselves to detect missing and out-of-order frames, the process is complex and unreliable as it is difficult to set up real-time triggers that guarantee error detection and capture.

The Xgig Load Tester

Xgig Load Tester has overcome the difficulties of detecting missing, and out-of-order frames. Load Tester is one of the multi-functional capabilities that can be licensed and enabled on Xgig Fibre Channel Blades. Emulating the end ports of Fibre Channel data links, the Load Tester is able to track frame sequences by comparing received frames against expected frames.

The Load Tester generates traffic streams to pass through switches and monitors both sides of the link to ensure that frames both arrive and arrive in the correct sequence. Because the Load Tester generates deterministic/known traffic, it detects the missing frames at its receiving paths and is able to differentiate the error events of dropped frames, out of order frames, and misdirected frames.

When detecting error events, Xgig Load Tester is also capable of triggering the Analyzer to capture the erroneous trace real time for debugging.

The Load Tester combined with the Xgig Analyzer provides the capabilities you need to detect, capture, locate, and debug missing frame errors. With the proper test setup, you will be able to capture accurate information in the trace buffer to easily find the frame in error and locate the source of the problem. Such a setup eliminates tedious guesswork and time-consuming manual searches through large trace buffers. Because the Load Tester highlights the exact frame that caused the error, developers can identify and source the errors quickly and easily.

How the Load Tester Works

The Load Tester is based on proprietary technology that enables it to verify data integrity.

There are several steps to detect the three missing and out-of-order frame scenarios:

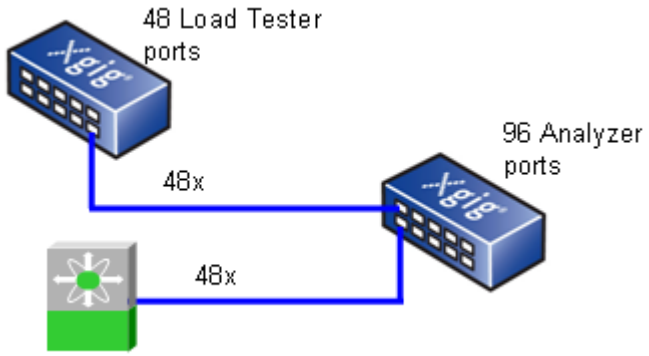
1. Configure and Connect Hardware
2. Set Triggers
3. Detect Error and Capture Trace
4. Search Trace Buffer to Locate and Identify Error
5. Debug Error

As an example, this case study will show how to configure a test setup for a 48-port switch.

Configure and Connect Hardware

The Load Tester ports are connected to 48 switch ports and the analyzer ports are put in line for capturing the traffic. Figure 126 shows the diagram of the test setup. The Analyzer does not participate in data transfers but rather observes them non-intrusively.

Figure 126: Load Tester Test Setup



The Xgig Load Tester sends out the triggering signal through the chassis trigger port. Therefore, the trigger in-port on the chassis that holds the Analyzer blades needs to be connected to the trigger out-port on the Load Tester chassis. In the case that the Load Tester and Analyzer ports are in the same chassis, a cable is required to loop back between the "trigger out" and "trigger in" ports. In this example, there are 48 Load Tester ports in 3 chassis and 96 Analyzer ports in 6 chassis. Each Load Tester chassis is associated with 2 Analyzer chassis for testing the same group of links, as shown in above figure. A few options for setting up the triggering connections are available.

Option 1: Setting up one Load Tester chassis and two Analyzer chassis as one testing group. For each group of links, connect the 2 Analyzer chassis through the cascading ports and group all 32 ports under the same time domain. Ports in the same time domain can share one trigger condition. Connect the "Trigger out" port on the Load Tester chassis to the "Trigger in" port on one of the two Analyzer chassis. This setup will allow you to cross trigger and test 16 switch ports within the group.

Option 2: The Xgig system allows for a maximum of 4 chassis to be in the same time domain (i.e., 64 ports). A special setup is required if cross triggering is required among all 48 switch ports. Use two time domains for the Analyzer ports: one domain of 64 ports (Domain 1) and the other domain of 32 ports (Domain 2). The chassis in the same domain are cascaded together. These two domains can be connected through the trigger ports on the chassis to share the same trigger from the Load Tester chassis. Select the "Trigger out" port on one chassis in Domain 1 to connect to the "Trigger in" port on one chassis in Domain 2. All three Load Tester chassis need to be cascaded together and defined in one time domain. Finally the "Trigger Out" port on one of the Load Tester chassis needs to be connected to one of the available "Trigger In" ports on the Analyzer chassis.

Management of all Load Tester ports, even across multiple Xgig chassis, is consolidated through a single PC running Maestro and Xgig Analyzer. Maestro uniquely allows users to utilize the same GUI to manage other Xgig generation functions such as BERT, Jammer, and Generator, thus eliminating the need to switch between different GUIs when using multiple tools.

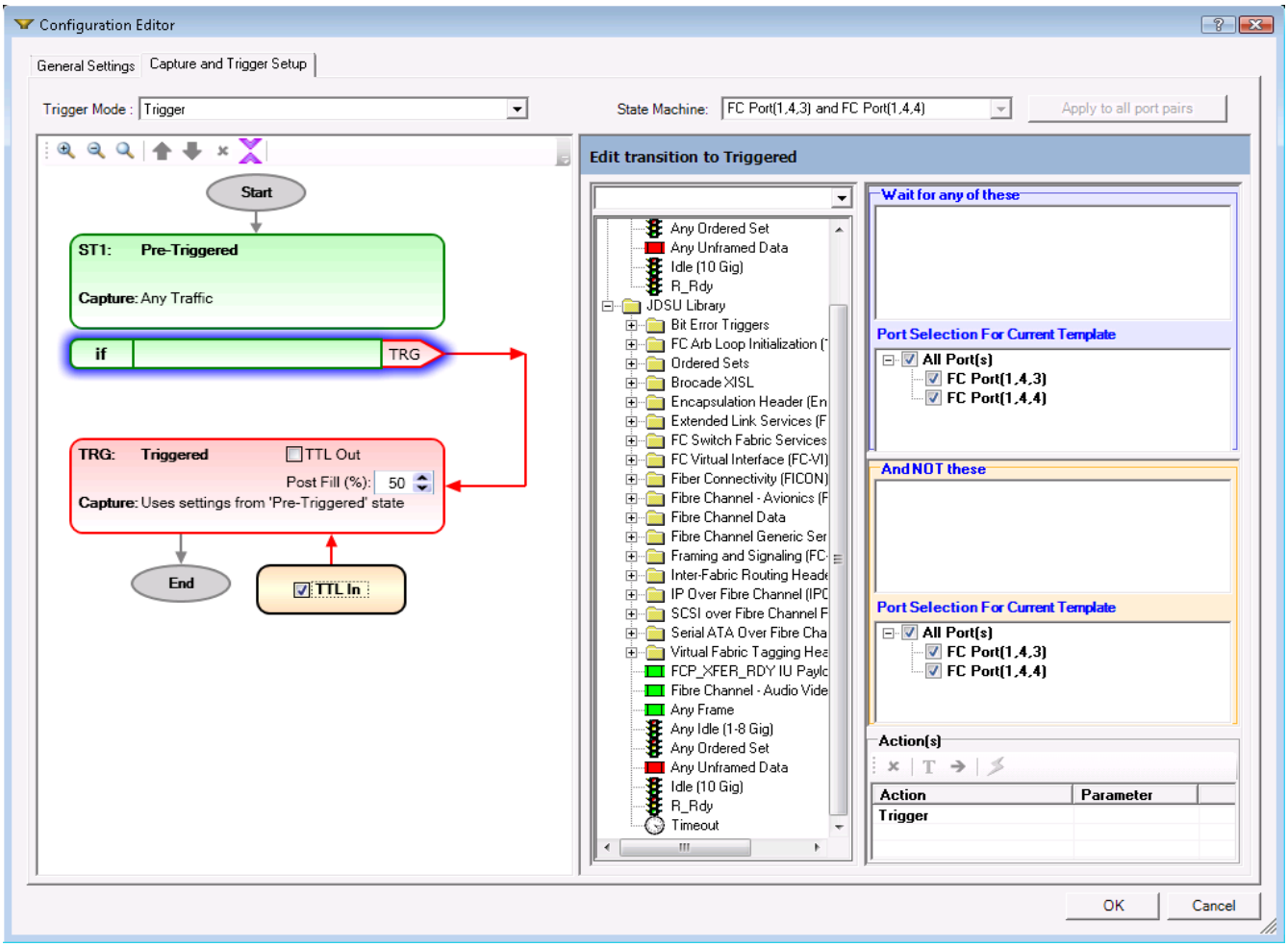
Set Triggers

With the hardware in place, it is time to configure links and set triggers. These need to be configured in both TraceControl and Maestro.

From TraceControl:

1. Select the “Capture Stop after Trigger” trigger scheme
2. Select the TTL input for the Analyzer port by dragging the TTL input template from the Viavi library to the appropriate ports in the domain template to enable the external trigger
3. Choose a “Post Trigger” field with a suggested value between 20-50% (refer to Figure 127).

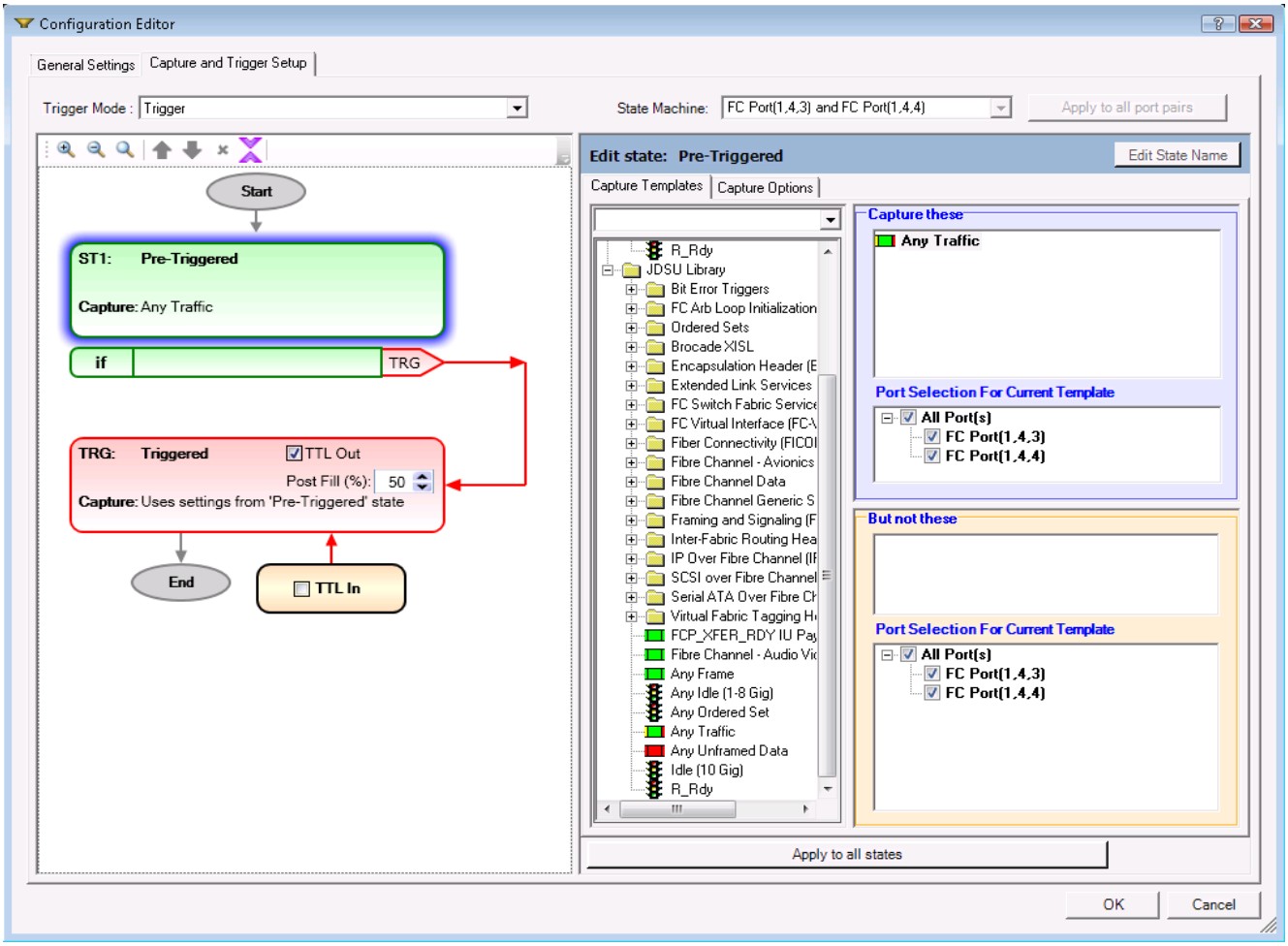
Figure 127: Choosing a “Post Trigger” field



For option 2 setup, there are following additional steps:

1. On the Analyzer chassis (Domain 1) that is connected to the Load Tester chassis, follow the steps described above to select the "TTL input" as capture stop trigger condition
2. Select "External Output Actions" on "Option" pane (Domain 1).

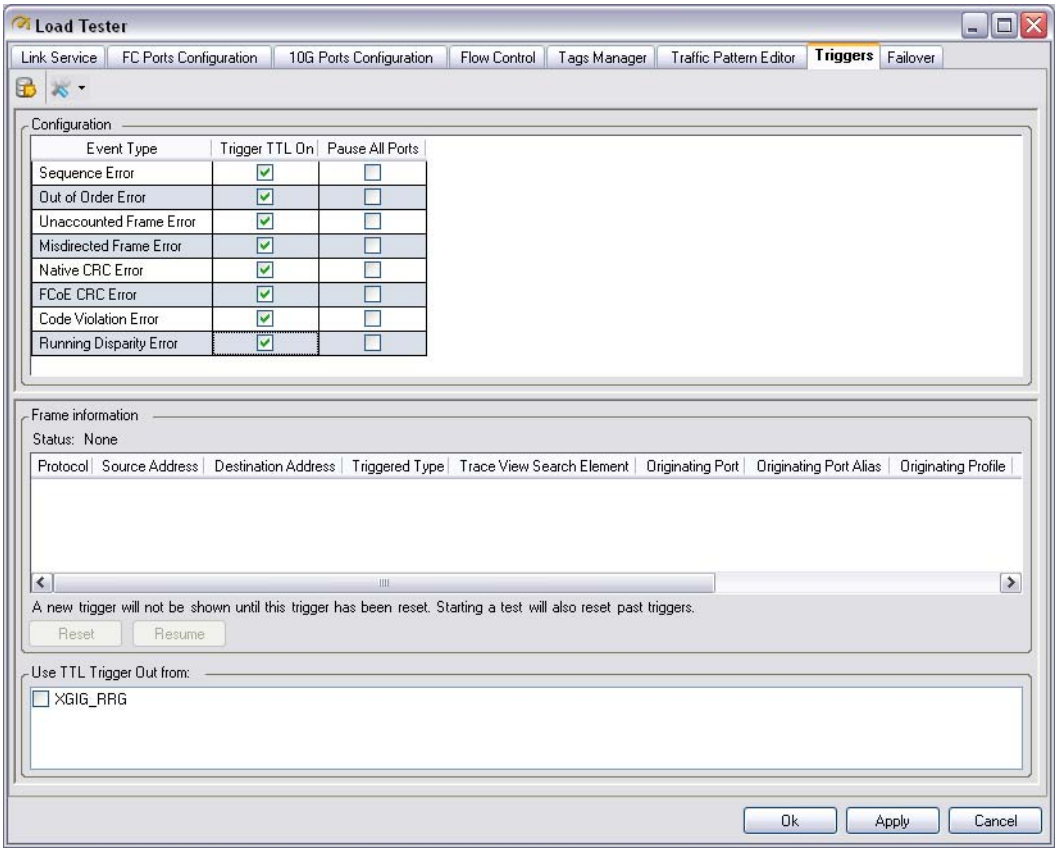
Figure 128: Selecting "External Output Actions" on "Option" pane



From Maestro Load Tester GUI,

- Select all 48 ports under the same time domain.
- Select the "Set Trigger" pane and choose "Out of Order Frame Error", "Misdirected Frame Error", and "Dropped Frame Error" to be "Trigger TTL On". If triggered, the trigger frame information will be shown in the bottom window.

Figure 129: Triggers Tab



If you plan on capturing traces for multiple errors, configure the Analyzer with multiple memory segments. The Xgig trace buffer, more than large enough for capturing multiple missing frame errors, can be divided into up to 128 segments. Each event capture will fill one segment. In this way, you can catch multiple instances of missing errors without needing to reset the trace memory. However, the Load Tester port does need to be reset from the "Trigger" pane after the trigger event for the next error event.

Detect Error and Capture Trace

Run the system until an error is detected. (If no error is detected, your system is robust and free of missing or out-of-order frame problems.)

Once the Load Tester determines that any of the three error scenarios has occurred, it will trigger the Analyzer. As the Analyzer has been collecting traffic the entire time the system has been running, this trigger actually stops traffic collection. The Xgig Analyzer offers the option to control how much post-trigger traffic to collect when you set the “Post Fill” field in the TraceControl Configuration pane.

You can now begin searching the trace buffer to identify which error scenario has occurred.

Search Trace Buffer to Locate and Identify Errors

Once an error is detected by the Load Tester and the Analyzer is triggered, you need to locate the frame that caused the error within the trace buffer. Using traditional tools, developers have to search through the trace buffer manually since they don’t know which frame caused the error.

The Load Tester simplifies this process by displaying the triggering frame, the trigger type, and key characteristics including S_ID, D_ID, OX_ID, stream frame count, and sequence count. There is also a “TraceView Search Element” value that can be used to search the trace. Armed with this information, you can use Xgig’s unique and powerful Quick Search capabilities in TraceView to quickly filter through the trace buffer and locate the trigger frame. Using other filters supported by the Analyzer, you can easily determine which of the three scenarios applies and identify related frames to help in debugging the problem.

Problem Solved

Once the problem is resolved, you can repeat these steps to continue testing the switch with other traffic patterns. Alternatively, you can create more complex topologies by moving to a full any port-to-any port configuration or introducing additional switches to the fabric.

The Xgig Testing and Analysis platform is the industry's leading Fibre Channel troubleshooting and debugging tool. Xgig's unique cross-triggering capabilities between the Load Tester and the Analyzer enable the test and capture of sophisticated network problems that would be otherwise too difficult to pursue with an analyzer alone and guarantees the accurate measurement of events such as missing frames to accelerate the troubleshooting process. With the powerful combination of Xgig Load Tester and Xgig Analyzer, backed by an intuitive GUI control application, you can guarantee switch robustness with the greatest speed and highest confidence.

Appendix C

Load Tester Login State Machine Troubleshooting

Overview

Each Load Tester port has a Login State Machine, which allows the port to transition from the current state, to a Goal State set by one of the Login functions. When a port is first opened, it is in the "Offline" state. It will remain in this state until one of the Login functions is called to set a new Goal State. A complete state transition sequence is as follows:

"Laser Off" > "**Offline**" > "Link Initializing" > "**Link Active**" > "Fabric Login in Progress" > "**Logged in to Fabric**" > "NPIV Login in Progress" > **NPIVs Logged In** > "N-Port Login in Progress" > "**Logged In**" > "**Test in Progress**"

The states displayed in **bold** are Goal States that can be set by one of the Login functions (see below). A sequence of Login functions can be called to manually transition from Goal State to Goal State, or as few as one function can be called to complete the entire transition to "Test in Progress".

For example, if the state is "Laser Off", and the client sets the Goal State to "Link Active" with the InitializeLink() function, the port will transition to the "Link Active" state, and remain in that state until another Login function is called.

On the contrary, the client can set the Goal State to "Test in Progress" with the StartDomain() function, and the port will automatically make all of the intermediate state transitions.

Timeouts and Retries

If at any point during the login process, the Load Tester port does not receive the expected reply to a login frame within the Timeout value specified by the LoginRetryDelay() function, it will retry the frame, subject to the LoginRetryCountLimit(). If the expected reply is not received after all retry attempts, the port will transition to "Port Failure".

The desired state does not change when a port enters the “Port Failure” state. If the conditions on the wire change such that the port can recover, it will attempt to do so. For example, if the peer disables its transmitter while a test is running, the Load Tester port will traverse to the “Port Failure” state (after the retries have been attempted). Once the laser is enabled again, the Load Tester port will automatically recover, and attempt to traverse back to the “Test in Progress” state.

Asynchronous Behavior

The API functions that set the port to a new Goal State are asynchronous. The function immediately returns control back to the client, while the port State Machine attempts to transition to the new Goal State. If the function returns an error, get_LastError() can be called to determine the cause of the failure.

If the function succeeds, the client can call the get_State() function to verify that the correct Goal State was achieved.

The function calls are as follows:

LaserOff() - Set the Goal State of the port to "Laser Off". The port will turn off the laser.

LaserOn() - Set the Goal State of the port to "Laser On". The port will turn on the laser.

GoOffline() - Set the Goal State of the port to "Offline".

InitializeLink() - Set the Goal State of the port to "Link Active".

Logout() - Set the Goal State of the port to "Link Active".

FabricLogin() - Set the Goal State of the port to "Logged in to Fabric". The port(s) will send Fabric Login (FLOGI) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI), Register FC Types (RFT_ID), and State Change Registration (SCR) to the Directory Server (Well Known Address 0xFFFFFC). In addition, any optional Name Server Registration Services selected will be processed after the PLOGI sequence.

NPIVLogin() - Set the Goal State of the port to "NPIVs Logged In". The port(s) will send Fabric Discover (FDISC) to the Name Server (Well Known Address 0xFFFFFE), followed by a Port Login (PLOGI) and Register FC Types (RFT_ID) to the Directory Server (Well Known Address 0xFFFFFC) if a Virtual ID (NPIV) was successfully acquired.

NPortLogin() - Set the Goal State of the port to "Logged In". The port(s) will send a Get Port Identifiers (GID_PT) to the Directory Server, to discover the available Load Tester ports in the Fabric zone. It will then send PLOGI frames to all available devices to determine which are Load Tester ports. In addition, any Name Server Discovery Queries will be processed.

StartDomain() - Set the Goal State of the port to **"**Test in Progress**"**.

Stop Domain() - Set the Goal State of the port to **"**Logged In**"**.

Fabric Login Blaster() - Set the Goal State of the port to **"**Blast Fabric Login**"**.

Stop Fabric Login Blaster() - Set the Goal State of the port to **"**Offline**"**.

State Definitions

“Laser Off” - The port laser is turned off.

“Offline” - The port transmits OLS, and does not respond to LISM input events or incoming frames.

“Port Failure” - The port has failed to complete an operation successfully after attempting the number of retries specified in the Login Retry Count Limit() function.

“Link Initializing” - The port has enabled the hardware LISM engine, and is attempting to reach the Active State. When it succeeds, the port state will transition to “Link Active”.

“Link Active” - The port's hardware LISM engine has reached the Active State.

“Logout in Progress” - The port is sending a Port Logout to the switch and waiting for an Accept. When it succeeds, the port state will transition to “Link Active”.

“Fabric Login in Progress” - The port is in the process of logging into the Fabric. This involves a series of transmitted frames, and corresponding Accept frames from the switch. When it succeeds, the port state will transition to "Logged in to Fabric".

"Logged in to Fabric" - The port has successfully logged into the fabric.

"NPIV Login in Progress" - The port is in the process of acquiring Virtual IDs from the Fabric. This involves a series of transmitted frames, and corresponding Accept frames from the switch. When it succeeds, the port state will transition to "NPIVs Logged In".

"NPIVs Logged In" - The port has successfully acquired the number of Virtual IDs specified by the NPIV ports() function.

"N-Port Login in Progress" - The port is in the process of sending Port Logins to all available Load Tester ports that are listed in the GID_PT Accept frame from the switch. When it succeeds, the port state will transition to "Logged In".

"Logged In" - The port has successfully logged in to all Load Tester ports in the switch zone.

"Test Preparation" - The Traffic Profile settings for the Global Session are collectively compiled and committed to hardware for all ports in the session. In addition, all 10G ports using an Ethernet Traffic Profile will perform Layer 2 ARP and Layer 3 ARP if necessary (TCP/UDP traffic). All Fibre Channel ports will verify maximum credits are available, and if not, issue a Link Reset (LR).

"Test in Progress" - The port is blasting data frames.

"Transmit Complete" - The port has finished transmitting the required number of data frames for a user-defined test mode (either time or frame count based). However, other ports in the session are still transmitting, so the test is not yet complete.

"Test Complete" - All ports have finished transmitting frames for a user-defined test mode (either time or frame count based).

"Blast Fabric Login" - The port is blasting a Fabric Login frame to the switch. The port will not respond to incoming frames. If a LISM input event is received, the hardware LISM engine will attempt to transition to the Active State, and then resume blasting Fabric Logins.

"Unknown State" - The port is in an unknown state.

"Ignored in Test" - A state where the port directed is ignored during testing and the port state is identified as Ignored in Test.

Log Messages

If failures occur during the login process, messages are added to the Load Tester port log. Below are some example messages.

When a timeout occurs, the log message will indicate the frame sent by the Load Tester port, the anticipated response, and the OX_ID value.

"Timeout occurred: Accept Frame was not received in response to FLOGI with OX_ID 0x0008"

When the retries have exceeded, the port will traverse to Port Failure. The log will indicate the current state and the desired state at the time the Port Failure occurred.

"Port Failure occurred during 'Fabric Login in Progress' State, while attempting to achieve State 'Logged in to Fabric'"

If an unexpected frame is received, the frame type and OX_ID are displayed.

"Unexpected ELS Accept Frame received with OX_ID X"

"Unexpected GS Accept Frame received with OX_ID X"

If a Reject is received, the log message will indicate the frame sent by the Load Tester port and the OX_ID value.

"ELS Port Reject received in response to FDISC Request with OX_ID X"

After the GID_PT is processed, a message is displayed to indicate the number of available Load Tester ports.

"There are X available Load Tester destination ports"

If there were no available Load Tester ports, or an error occurred during the Discovery process, the following log message will be displayed:

"There are no available Load Tester destination ports - verify switch zoning settings"

"GS Port Reject received in response to FC-GS RFT_ID Request - Verify switch zoning settings"

Index

November 2015
Version 8.1
English

Viavi Solutions

North America:	**1.844.GO VIAVI / 1.844.468.4284**
Latin America	**+52 55 5543 6644**
EMEA	**+49 7121 862273**
APAC	**+1 512 201 6534**
All Other Regions:	**viavisolutions.com/contacts**
email	**customer.care@viavisolutions.com**