IxExplorer User Guide

Version 1.0

Release 8.13 EA

October 2016

Contacting Ixia

Corporate Headquarters	Ixia Worldwide Headquarters 26601 W. Agoura Rd. Calabasas, CA 91302 USA +1 877 FOR IXIA (877 367 4942) +1 818 871 1800 (International) (FAX) +1 818 871 1805 sales@ixiacom.com	Web site: www.ixiacom.com General: info@ixiacom.com Investor Relations: ir@ixiacom.com Training: training@ixiacom.com Support: support@ixiacom.com +1 818 595 2599
EMEA	Ixia Europe Limited Part 2nd floor, Clarion House, Norreys Drive Maidenhead, UK SL6 4FL +44 (1628) 408750 FAX +44 (1628) 639916 salesemea@ixiacom.com	Support: support-emea@ixiacom.com +40 21 301 5699
Asia Pacific	Ixia Pte Ltd 210 Middle Road #08-01 IOI Plaza Singapore 188994	Support: support-asiapac@ixiacom.com +91 80 4939 6410
Japan	Ixia KK Nishi-Shinjuku Mitsui Bldg 11F 6-24-1, Nishi-Shinjuku, Shinjuku-ku Tokyo 160-0023 Japan	Support: support-japan@ixiacom.com +81 3 5326 1980
India	Ixia Technologies Pvt Ltd Tower 1, 7th Floor, UMIYA Business Bay Cessna Business Park Survey No. 10/1A, 10/2, 11 & 13/2 Outer Ring Road, Varthur Hobli Kadubeesanahalli Village Bangalore East Taluk Bangalore-560 037, Karnataka, India +91 80 42862600	Support: support-india@ixiacom.com +91 80 4939 6410
China	Ixia Technologies (Shanghai) Company Ltd Unit 3, 11th Floor, Raffles City, Beijing Beijing, 100007 P.R.C.	Support: support-china@ixiacom.com 400 898 0598 (Greater China Region) +86 10 5732 3932 (Hong Kong)

Change: 4150211, *Date:* September 24, 2013

[This page intentionally left blank]

Contents

About This Guide

The information in this section is provided to help you navigate this guide and make better use of its content. A list of related documentation is also included.

Purpose

This guide provides information about IxExplorer theory, features, functions, and options, as well as additional test setup details. (5.70122909)

Manual Content

This guide contains the following sections:

Section	Description
About This Guide	Provides information on this guide, including its purpose, content, and related documentation. Also explains how to contact technical support.
Chapter 1, IxExplorer Overview	Provides an introduction to the operation and configuration of the Ixia system.
Chapter 2, IxExplorer Operation	Describes the means of operating the Ixia hardware through the IxExplorer software.
Chapter 3, Explore Network Resources	Discusses the main display of IxExplorer and how it provides access to all hardware features.
Chapter 4, Stream and Flow Control	Discusses the construction and assembly of data streams.
Chapter 5, Frame Data-Basic Frame Structure	Discusses the assembly of dynamically changeable data frames that are packaged into streams.
Chapter 6, Frame Data-Protocol Control	Discusses the assembly of Protocol information for insertion into stream packets.
Chapter 7, Frame Data-User Defined Fields (UDF)	Discusses the assembly of user defined data for insertion into stream packets.
Chapter 8, Packet View	Discusses the means by which frame data may be previewed before it is sent to the DUT.
Chapter 9, IxRouter Window	Discusses general use of the IxRouter window.
Chapter 10, Protocol Interfaces	Discusses the use of protocol interfaces through IxRouter.
Chapter 11, ARP	Discusses the use of the Address Resolution Protocol (ARP).
Chapter 12, ICMP/ PINGv4	Discusses the use of the Internet Control Message Protocol (ICMP) and Packet Internet Groper version 4 (PINGv4).
Chapter 13, Filter Properties	Discusses the programming and operation of the controls that dictate when and how much data is captured by each port's capture buffer. Programming of user defined statistics is also covered here.
Chapter 14, Capture View	Discusses the means by which the IxExplorer is used to view captured data from each port's capture buffer.

Section	Description
Chapter 15, Statistic View	Discusses the means by which statistics from one or more ports may be viewed.
Chapter 16, Packet Group Statistic View	Discusses the means by which latency can be studied for one or more ports.
Chapter 17, Card Properties	Discusses the properties associated with load modules.
Chapter 18, Port Properties - 10/100/1000 Ethernet Family	Discusses the properties of Ethernet ports and their programming.
Chapter 19, Port Properties-POS and ATM Families	Discusses the properties of Packet over SONET and ATM ports, and their programming. Also covers option port protocols such as SRP and RPR.
Chapter 20, Port Properties-10 GE and UNIPHY Families	Discusses the properties of 10 Gigabit Ethernet and UNIPHY ports and their programming.
Chapter 21, Port Properties- 40/100 GE Family	Discusses the properties of 40 and 100 Gigabit High Speed Ethernet ports and their programming.
Chapter 22, Port Properties- NGY Family	Discusses the properties of NGY ports and their programming.
Chapter 23, Port Properties- FCM Family	Discusses the properties of FCM ports and their programming.
Chapter 24, Port Properties- Xcellon-Flex Family	Discusses the properties of Flex ports belonging to Xcellon-Flex card family and their programming.
Chapter 25, Port Properties-XDM10G32S Load Module	Discusses the properties of Xdensity card family and their programming.
Chapter 26, Port Properties-Xcellon-Lava Load Module	Discusses the properties of Lava card family and their programming.
Chapter 27, Port Properties-Xcellon-Multis Load Module	Discusses the properties of Xcellon-Multis card family and their programming.
Chapter 28, Port Properties-Novus and Novus-R Load Modules	Discusses the properties of Novus card family and their programming.
Chapter 29, Port Properties-VM	Discusses the IxVM port properties.
Chapter 30, MII Registers	Discusses the Media-Independent Interface (MII) registers.
Chapter 31, Stream Properties - Warnings/ Information Messages	Discusses the warning and informational messages which may appear on the Warnings page of IxExplorer Stream Properties during port configuration.
Chapter 32, IxVM	IxVM is Ixia's virtual test port product that enables you to use Linux virtual machines (VMs) to generate test traffic.
Appendix A, Using ScriptGen	Describes how to start and operate the ScriptGen application.

Section	Description
Index	Provides a comprehensive index listing for the manual.

Related Documentation

The following manuals may help you learn more about IxExplorer. The manuals are available on the CD shipped with the application, as well as on the Ixia Web site at

- *Ixia Platform Reference Manual.* Provides a detailed list of all currently supported Ixia chassis and Ixia load modules, as well as general information regarding various technologies covered by Ixia products.
- *IxServer User Guide*. Details the usage of the IxServer GUI for operation on an Ixia chassis.
- *IxOS Tcl Development Guide.* Describes the structure and conventions of the IxExplorer Tcl API and provides detailed information on all API commands.

In addition to these manuals, IxExplorer context-sensitive Help is available. By pressing F1 or the application's Help button, information about the displayed application window appears. Help content can also be accessed from the Help's table of contents or index.

Technical Support

You can obtain technical support for any Ixia product by contacting Ixia Technical Support by any of the methods mentioned on the inside cover of this manual. Technical support from Ixia's corporate headquarters is available Monday through Friday from 06:00 to 18:00, Pacific Standard Time (excluding American holidays). Technical support from Ixia's EMEA and India locations is available Monday through Friday, 08:00 to 17:00 local time (excluding local holidays).

[This page intentionally left blank]

Chapter 1 - IxExplorer Overview

This section contains information about the following:

- *IxExplorer Manuals*
- *Advice to Readers*
- *New in Version 8.13 EA*

IxExplorer Manuals

The use of the IxExplorer GUI is covered in two separate manuals:

- *IxExplorer User Guide* (this manual)
- *IxNetwork User Guide* (IxNetwork must be installed)

Advice to Readers

The Getting Started Guide should be used during the installation of each Ixia chassis. The *Ixia Platform Reference Guide* should also be used.

Those unfamiliar with the Ixia architecture would find it best to read the *Theory of Operation: General* and *Theory of Operation: Protocols* chapters (in the *Ixia Platform Reference Guide*), followed by the *IxExplorer Operation* and *Explore Network Resources* *chapters. These provide a thorough understanding of the Ixia architecture, both in theory and in practice.*

The remaining chapters of the manual may be read in preparation for programming or as reference material as needed. The entire text of this manual is included with the IxExplorer software as help files. It may be referenced at any time during the operation of the software.

New in Version 8.13 EA

No new features are added for 8.13 EA.

Chapter 2 - IxExplorer Operation

The IxExplorer software is the principal means used to program Ixia hardware, and to perform testing on network devices. This chapter is an overview of the facilities provided by the IxExplorer software and a guide on how to use those facilities.

This chapter is divided into several sections:

- *General Operation: Discusses the means of starting IxExplorer and the general layout of its functional windows.*
- *Multi-User Operation: Discusses the simultaneous control operations of IxExplorer.*
- *Transmit Operations: Discusses the transmit operations available.*
- *Capture Operations: Discusses the capture operations available.*
- *Latency Operations: Discusses the operations associated with latency measurements.*
- *Statistics Operations Discusses the statistics operations available.*
- Other Operations: Discusses other possible operations:
  - *Active Stream Configuration*
  - *Collect Diagnostic Logs*

General Operation

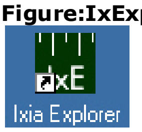
This section details starting IxExplorer and basic tasks, basic IxExplorer windows, and the concept of 'workspaces.' These topics are covered in the sections listed below:

- *Starting IxExplorer*
- *IxExplorer Windows*
- *Chassis Save*

Starting IxExplorer

The IxExplorer software comes preinstalled on the Ixia chassis computer; it can also be installed on any Windows-based system. In all cases, an icon is normally installed on the desktop and appears as shown in the following figure. The IxExplorer application can be started by double-clicking the following icon:

Figure:IxExplorer Icon



The *Chassis Address Dialog* is displayed.

Alternatively, IxExplorer can be started from the Start menu (*Start* > *Programs* > *Ixia* > *Ixia IxExplorer*), to display the *Chassis Address* dialog, as described in *Chassis Address Dialog*.

IxExplorer can also be used with a simulated 'demonstration' chassis, running on a PC workstation. When using a demonstration chassis, the IxServer software should be started before IxExplorer; through *Start* > *Programs* > *Ixia* > *Ixia Server* or by double-clicking the IxServer icon. The IxServer icon is shown in the following figure:

Figure:IxServer Icon

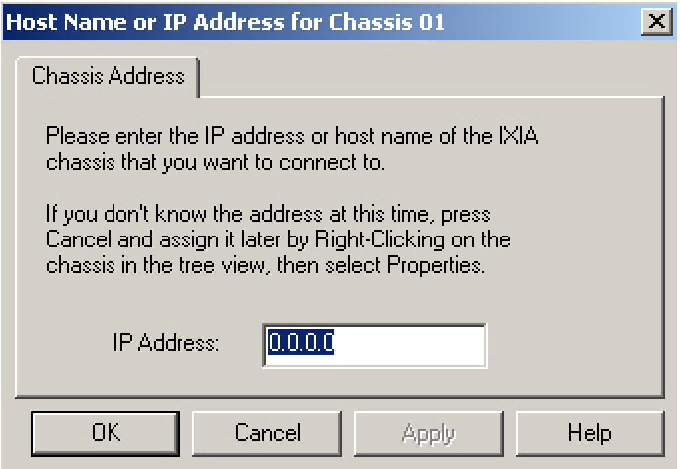
For more information on IxServer and the demonstration mode, see the *IxServer User Guide*.

> **NOTE** IxExplorer should not be run on a chassis, except for small test cases.

Chassis Address Dialog

After starting IxExplorer (by clicking the IxExplorer icon, or through the Start menu) a dialog appears asking for the address of the chassis, as shown in the following figure:

Figure:Chassis Address Dialog

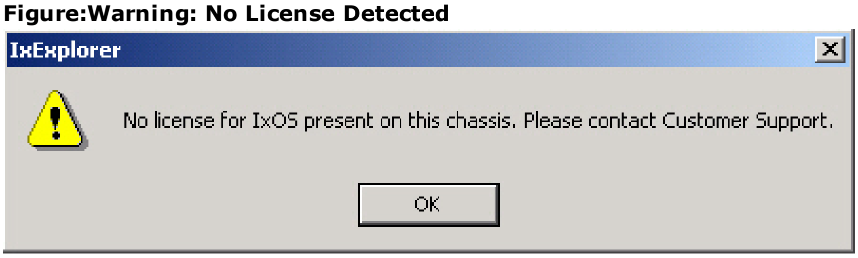


After entering the name of the chassis or its IP address, click *OK*. The IxExplorer main window is displayed, as shown in the following figure.

> **NOTE** If the demonstration server is installed and running, enter 'loopback' into this field to access simulated load modules.

If no valid license for the IxServer is detected, a warning is displayed, as shown in the following figure:

Figure:Warning: No License Detected



IxExplorer Windows

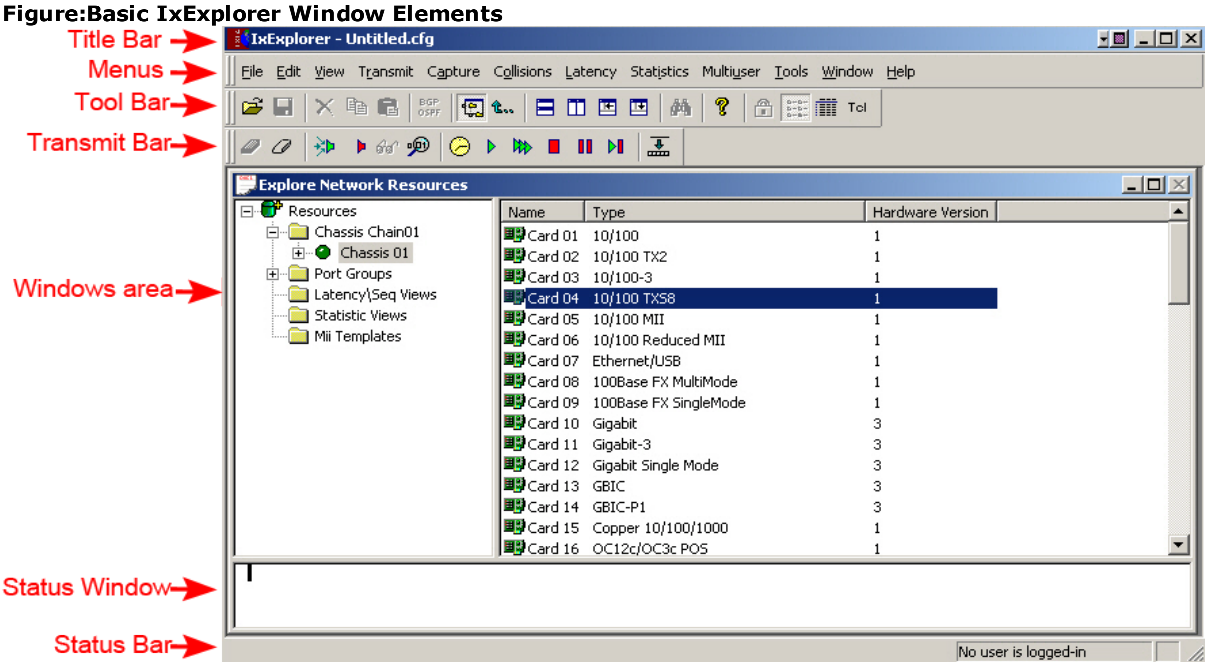
The main interface to the IxExplorer software, and therefore the Ixia hardware, is through the many windows, dialogs, and tabs that IxExplorer displays. The following sections describe some of the basic components of IxExplorer:

- *Main Window*
- *Explore Network Resources Window*
- *Capture View Window*
- *Packet Group Statistics View Window*
- *Statistic View Window*
- *IxRouter Window*

Main Window

The IxExplorer main window is the first window displayed when running IxExplorer, and the starting point for many operations. This window is opened by clicking the IxExplorer icon, or by selecting IxExplorer from the Start menu. The general layout of the IxExplorer main window is shown in the following figure:

Figure:Basic IxExplorer Window Elements



The basic elements of the IxExplorer Window are described in the following table:

Table:Basic IxExplorer Window Elements

Element	Description
Title Bar	Displays the name of the program (IxExplorer) plus the name of the work-space/configuration file in use. See *Chassis Save* for additional information.
Menu Bar	Location for the IxExplorer Menus. For information on the *File > Open* option, see *Chassis Save*.
Tool Bar	A standard Windows tool bar containing file, display, and help related icons.
Transmit Bar	An Ixia-specific toolbar that allows easy access to transmit and capture oper-ations.
Windows Area	The bulk of the window accommodates one or more specific IxExplorer win-dows. These include: • *Explore Network Resources Window*

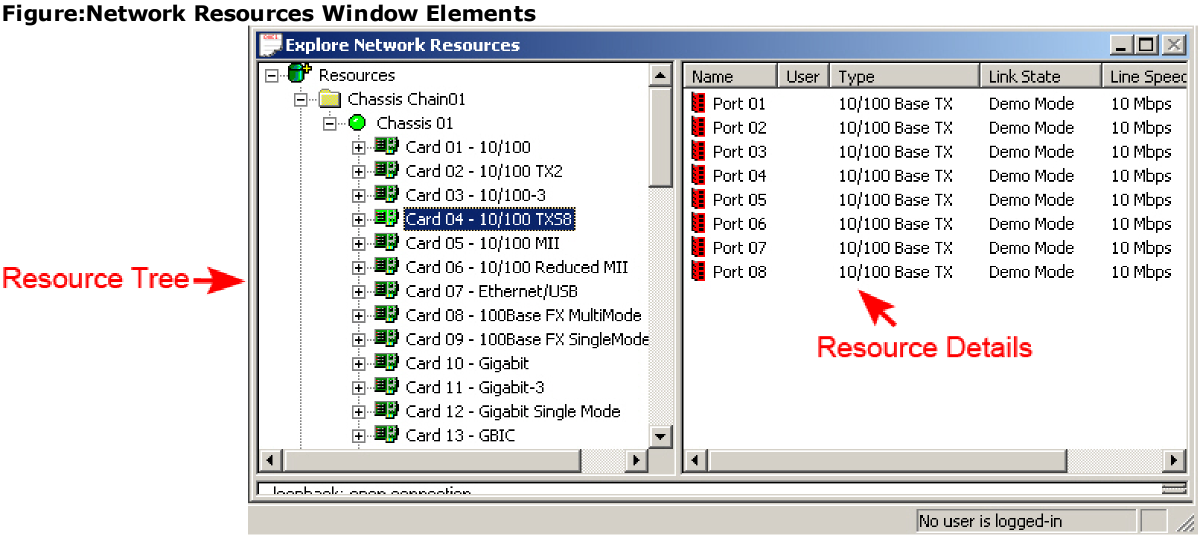
Element	Description
	• *Capture View Window* • *Packet Group Statistics View Window* • *Statistic View Window* • *IxRouter Window*
Status Window	Shows advisory messages sent from the server. Right- clicking in the window brings up a simple menu allowing the window to be cleared and the font for the window to be set.
Status Bar	Displays various status messages during IxExplorer operation.

Explore Network Resources Window

The Explore Network Resources window is located within the IxExplorer Main window, and shows the hierarchy of Ixia hardware resources on the left side of the window. The details view on the right side shows detailed information for the item selected in the left side.

An example of the Explore Network Resources window is shown in the following figure:

Figure:Network Resources Window Elements



The Explore Network Resources window is where most setup and programming of Ixia hardware is performed. It is discussed fully in its own chapter (*Explore Network Resources*).

The left side of the display holds a tree which consists of the Ixia architecture hierarchy, from Chassis Chain down to Port level. For any item selected on the left side, the right side of the screen shows details for the selected item. This is sometimes a listing of contained items, and sometimes an active display, as in the Statistic View.

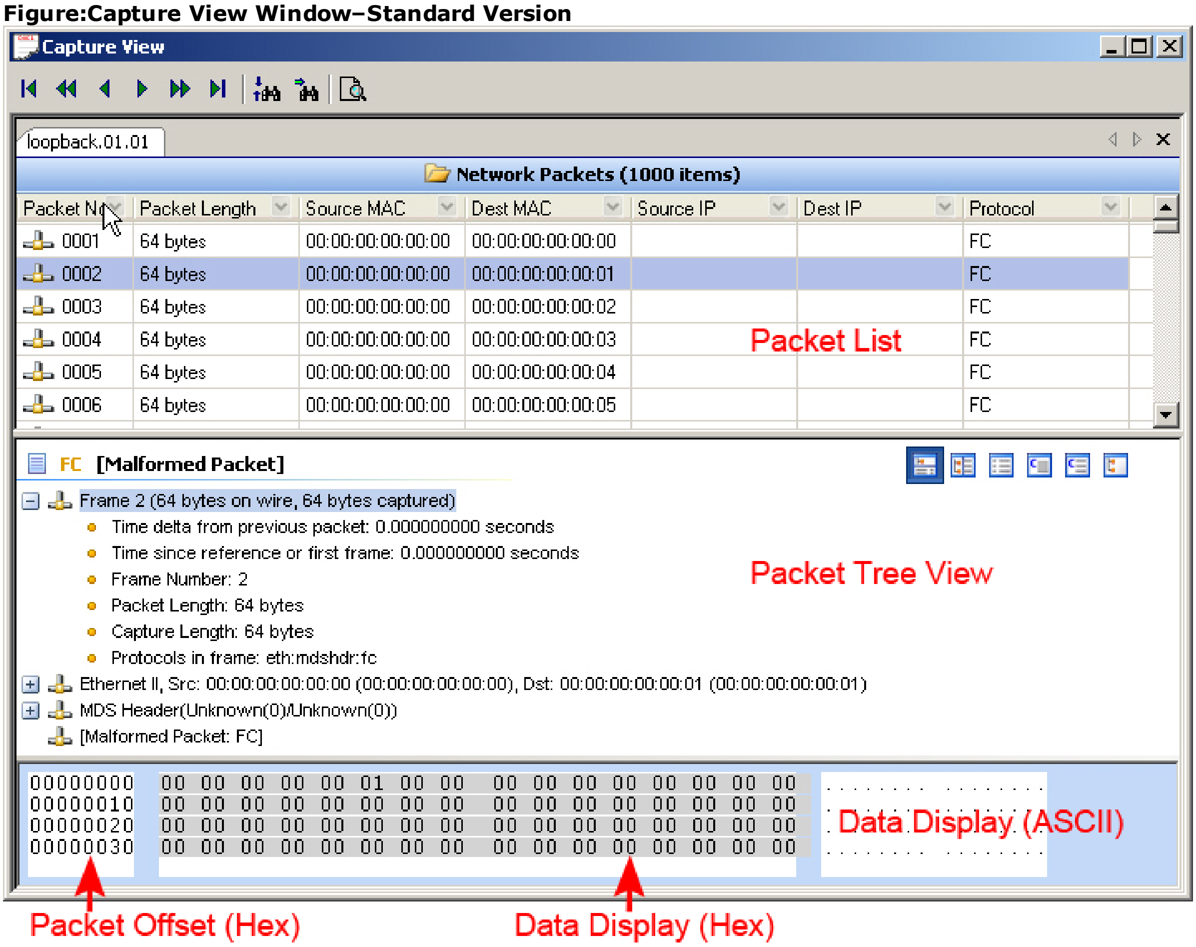
The various columns in the Resource details display may be rearranged to suit individual user preferences, by using the click-and-drag method to select the header of the column and move it to its new position.

Capture View Window

The Capture View is used to examine the data recorded from the DUT. The Capture View is accessed by selecting a port in the Resource tree, and then double-clicking *Capture View* from the list of options in the Resource details view. The Capture View is discussed more thoroughly in *Capture View*.

An example of the Capture View window is shown in the following figure:

Figure:Capture View Window–Standard Version



The standard *Capture View* window is split into panels, from top to bottom. These are described in the following table:

Table:Capture View Dialog Windows

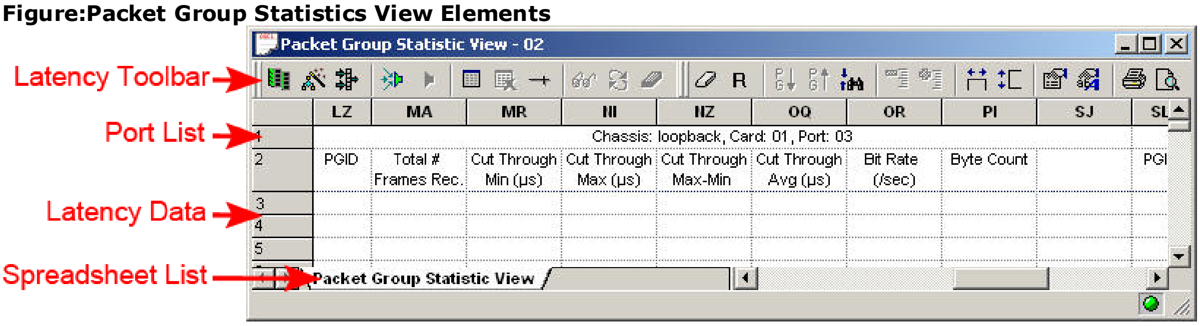
Window	Contents
Packet List (upper)	Packet List: A list that contains columns for a packet number, packet length, the destination address, the source address, timestamp data, and the error status of the frame. These fields are described in *Table:Capture View– Packet List Fields*.
Packet Tree View (lower)	Packet Tree View, expandable to show the parameters of the selected packet..
Hex and ASCII Data	Hexadecimal and ASCII byte display of the contents of the selected packet

Packet Group Statistics View Window

The Packet Group Statistics View is used to collect and analyze latency data across one or more ports, and to collect statistics on sequence checking. A new Packet Group Statistics View is opened by right-clicking *Packet Group Statistics Views* under *Global Views* in the Resource tree, and then selecting the *New* option in the menu. An existing Packet Group Statistics View is opened by selecting *Packet Group Statistics Views* under *Global Views* in the Resource tree, and then double-clicking one of the saved views in the Resource detail display. The Packet Group Statistics View is described thoroughly in *Packet Group Statistic View*.

An example of the Packet Group Statistics View window is shown in the following figure:

Figure:Packet Group Statistics View Elements



The elements of this window are described in the following table:

Table:Packet Group Statistics View Elements

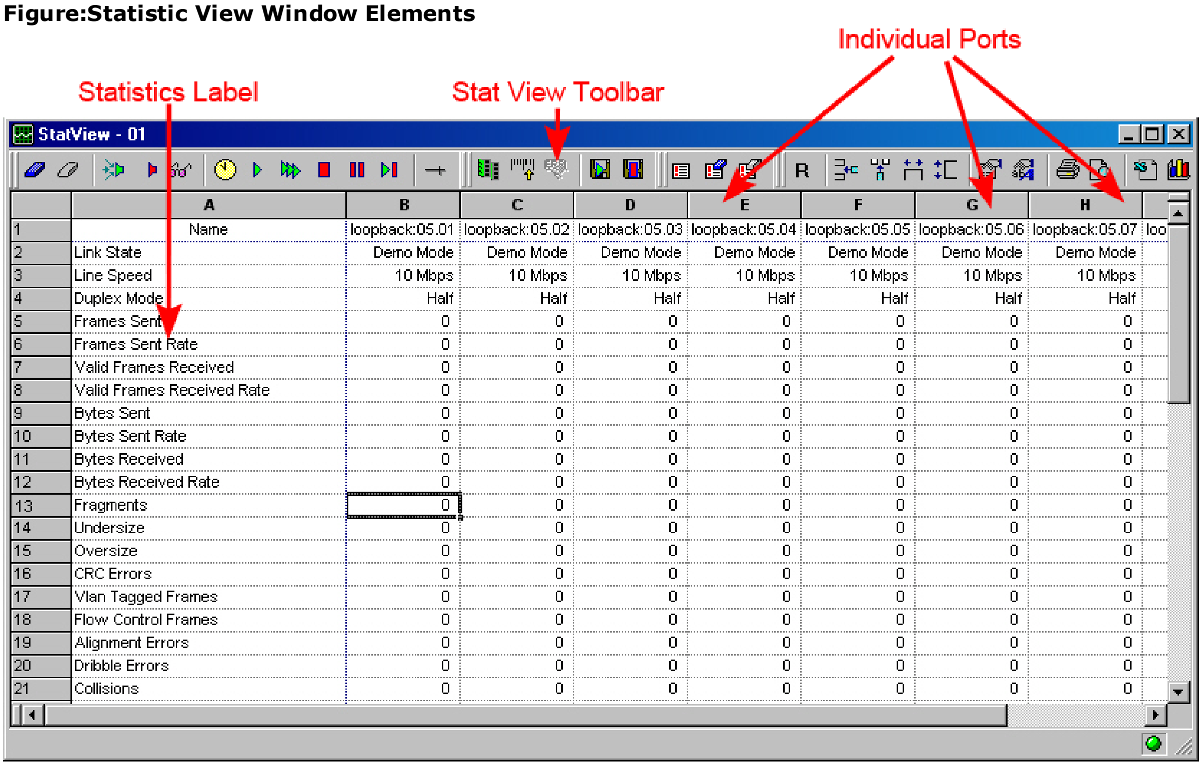
Element	Description
Latency Tool-bar	A special toolbar used to initiate/terminate latency measurements and for the manipulation of latency data.
Port List	Table headings for each of the ports in the latency group.
Latency Data	The actual latency data. Data is listed by time slice (if used) and then by Packet Group ID.
Spreadsheet List	Data snapshots may be created and are saved as separate tabbed spread-sheets, listed here.

Statistic View Window

Statistic Views are used to monitor various statistics for a single port or a group of ports. A new Statistic View is opened by right-clicking the *Statistic Views* under *Global Views* in the Resource Tree, then selecting the *New* option from the menu. An existing Statistic View is opened by selecting *Statistic Views* in the Resource Tree, then double-clicking one of the saved views from Resource detail display. Statistic Views are discussed thoroughly in *Statistic View*.

An example of the Statistic View window is shown in the following figure:

Figure:Statistic View Window Elements



The elements of the Statistic View window described in the following table:

Table:Statistic View Elements

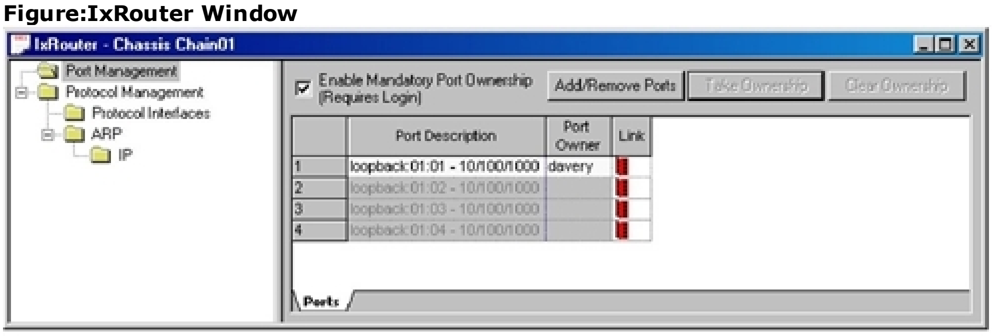
Element	Description
Stat View Toolbar	A custom toolbar used to control transmit, capture, and statistics operations.
Statistics Labels	The labels for each of the rows of the display. These are the statistics chosen for the set of ports in a Statistics Group.
Individual Ports	The column headings show the individual ports that are a part of the Statistics Group.

IxRouter Window

The IxRouter window allows configuration of routing protocols including BGP, OSPF, ISIS, RSVP-TE, LDP, RIP, RIPng, IGMP, and PIM-SM, as shown in the following figure. See the *IxNetwork User Guide* for additional information on protocol configuration.

To open, click **IxRouter** in the toolbar.

Figure:IxRouter Window



The fields and controls in the main IxRouter window (showing Protocol Selections) are described in the following table:

Table:Main IxRouter Window Elements

Field/Control	Description
Enable Mandatory Ownership	If this option is slected, port ownership is required before protocols can be configured for the port. First, log on as a user, and then take ownership of the port(s). This must be cleared in order for the list of protocols to display.
List of Protocols	A tree structure which presents the protocols and access to various levels of configuration windows, depending on the protocol selected. Enable Mandatory Ownership must be cleared in order for the list of protocols to display.
Port Selection window	The window where protocols are selected for use with available ports.The protocols in the grid are dimmed for ports that do not support those protocols.

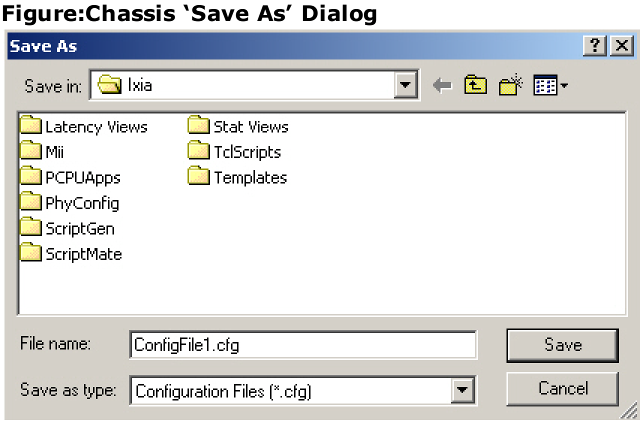
NOTE IxNetwork must be installed for full window functionality. Without IxNetwork, only limited ARP and Ping functions are allowed.

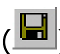
Chassis Save

All GUI configuration programming work can be saved in a configuration file.

When installed, each copy of IxExplorer is configured to use a default file named *Untitled.cfg* (file extension *.cfg* indicates it is a configuration file). The name of the file may be changed in the *File* > *Save As...* dialog which is shown in the following figure:

Figure:Chassis 'Save As' Dialog



The default location for saving chassis is the same directory used to hold the Ixia software: `C:\Program Files\Ixia`, and all have the *.cfg* extension. In the figure above, the current configuration is being saved into a new file named `ConfigFile1.cfg`. IxExplorer continues to use this file for future saves. The chassis is saved each time the *Save* operation is performed (either *File* > *Save*, or by using the *Save* icon () in the main toolbar). In addition, the chassis is automatically saved on exit if the *Auto Save on Close* option is set (either *File* > *Auto Save On Close* or through the *Tools* > *Options* dialog).

See also *Chassis, Card, and Port Files* for information on saving files for individual parts of the configuration.

Workspace operations are explained in the following sections:

- *Chassis Merge Dialog*
- *Creating a Chassis Icon*
- *Chassis, Card, and Port Files*

Chassis Merge Dialog

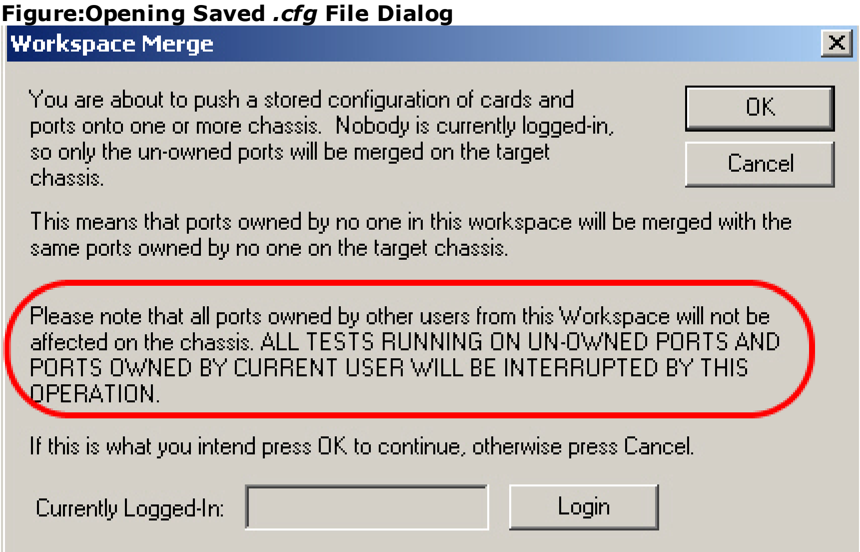
IxExplorer normally starts by opening the default `Untitled.cfg` workspace. A different, previously saved file may be opened with the open command (either *File* > *Open*, or by using the *Open* icon () in the main toolbar). When a saved *.cfg* file is opened, a dialog appears, as shown in the following figure.

It is extremely important to pay attention to the caution message in this dialog:

CAUTION All ports owned by other users from this chassis are not affected on the chassis. ALL TESTS RUNNING ON UN-OWNED PORTS AND PORTS OWNED BY THE CURRENT USER ARE INTERRUPTED BY THIS OPERATION.

The saved port configuration settings in the chassis file are pushed onto any unowned ports (and if you are logged on, onto ports owned by you). This initialization process stops any test that is currently in operation on those ports. Ports owned by other users are not affected.

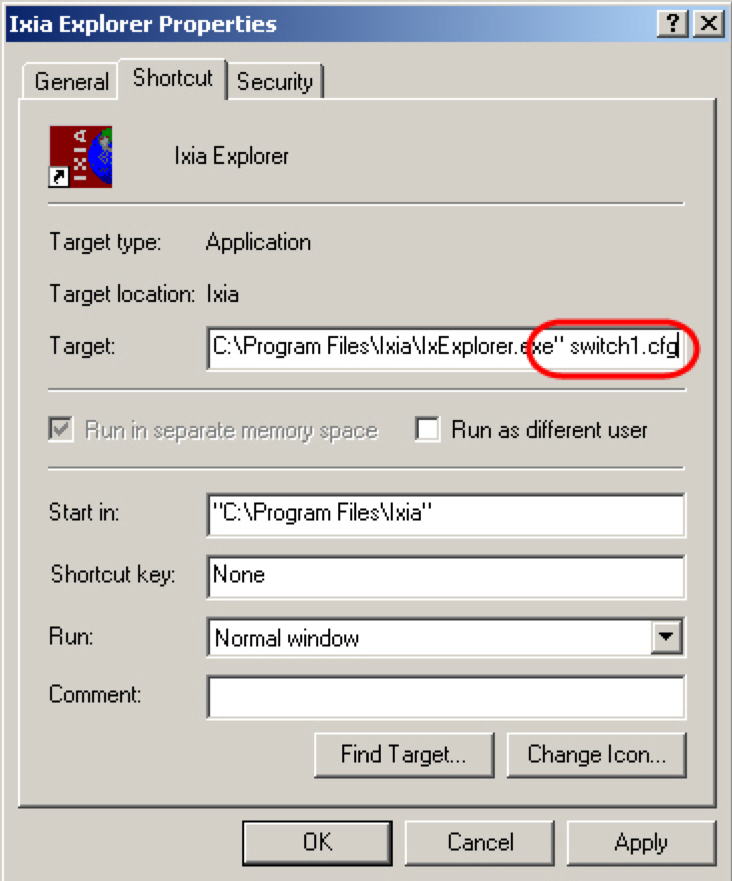
Figure:Opening Saved *.cfg* File Dialog



Creating a Chassis Icon

It is also possible to invoke the IxExplorer application with the name of the chassis file as an argument. This is accomplished by modifying the properties of the IxExplorer icon (or a copy of the icon) to include the file as an argument. To modify the properties, right-click the Ixia IxExplorer desktop icon. Select *Properties* and add the file to the end of the entry in the *Target:* field as shown in the following figure:

Figure:Creating IxExplorer Icon for a Specific Chassis



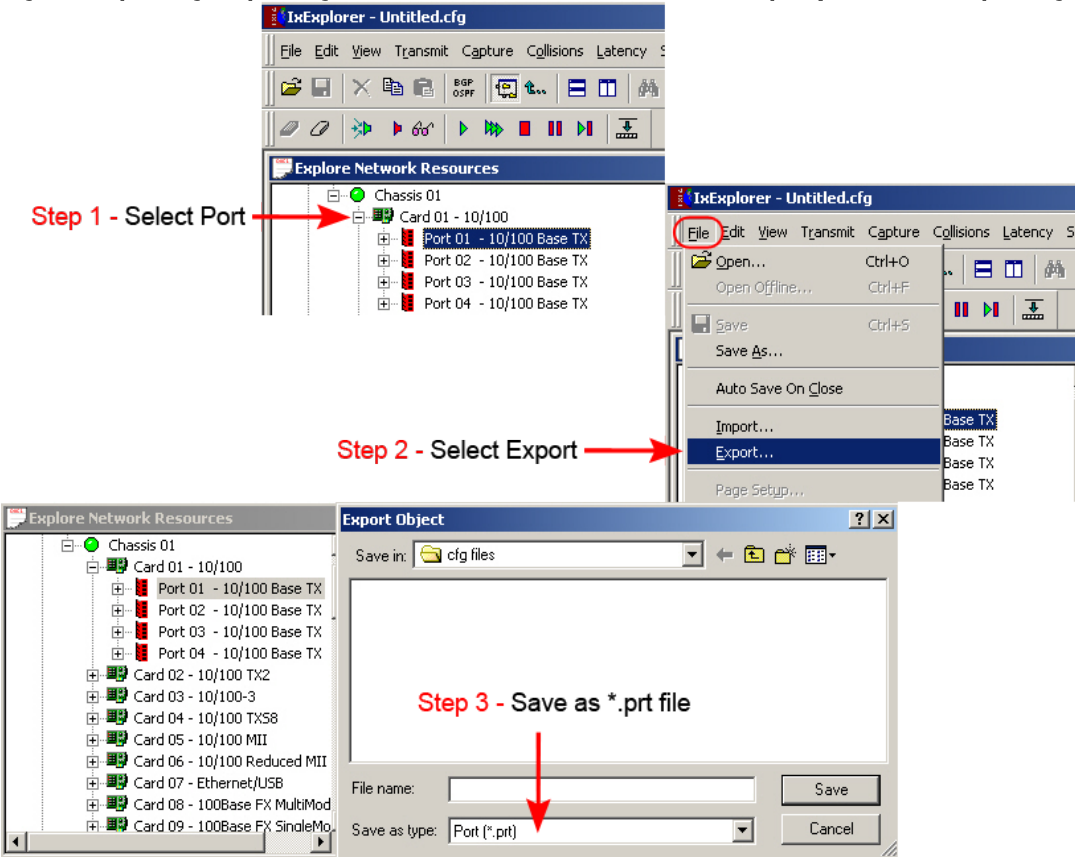
Chassis, Card, and Port Files

Configurations for individual elements, such as chassis or a port, may be exported to a named file, and then imported for use at a later time. The following file extensions are used:

- **.chs**—for a Chassis
- **.crd**—for a Card (Load Module)
- **.prt**—for a Port

The method for exporting or importing configuration files for these elements is shown in the following figure. An example is shown for exporting a port (*.prt) file. The same method is used for import, using the *Import Object* dialog, and for the other types of files (**.chs* and **.crd*). The files are saved to the Ixia program folder by default.

Figure:Importing/Exporting Chassis, Card, and Port Files—Example (shown for exporting Port file)



Multi-User Operation

IxExplorer provides an optional means of coordinating the sharing of chassis ports among multiple users. If a single person is using a chassis, multi-user commands are not required. You may perform any operation on any port.

NOTE For information on the IxRouter login, *Login Window*.

With IxExplorer's multi-user facilities, each user logs in with an arbitrary name. You may 'take ownership' of any and all ports that are not used by other users. The owner of a port has the ability to read data and program the port, while all other users have read-only access to the port. An owner may 'clear ownership' of their ports, making them available for other users. You may take ownership of a port owned by someone else, with an optional warning message. Any user may 'clear all ownership.'

NOTE We NEVER support multiple clients simultaneously changing data on one port. The rule is: one port-one owner for each system test.
The ownership model should not be used to have one script take ownership of a port and another script take ownership of that same port with the same user-name because one client may be working with a copy of the port configuration that has been made invalid by another owner.

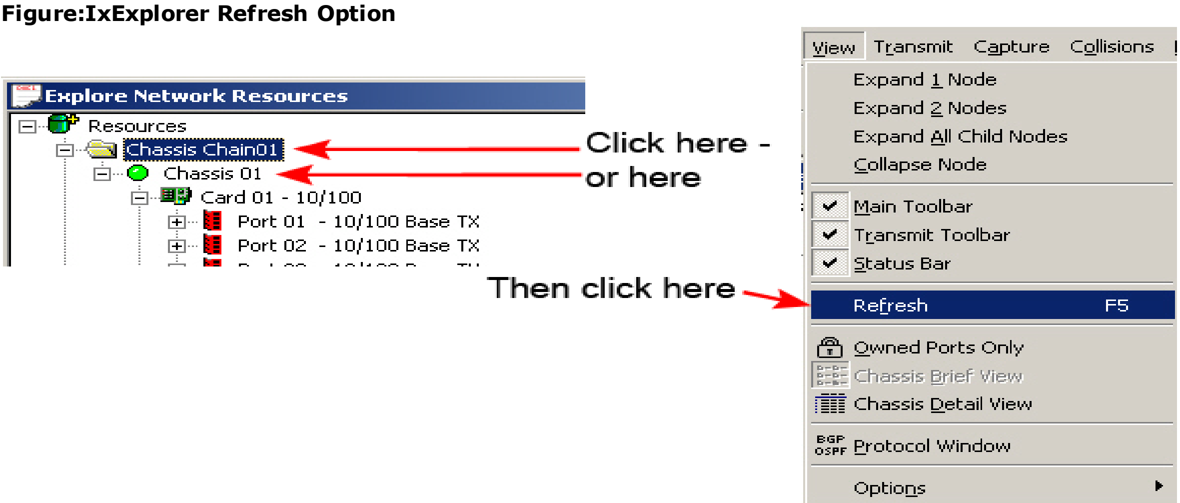
The two basic modes of multi-user operation are referred to as:

- **Secured Mode**: Users are either Administrators or Operators. All users are required to be registered and to login. Administrators can login and take or clear ownership of ports. Operators can only view data. See *Chassis Secure Mode* and *Secure Mode—User Properties Dialog* for additional information on Secured Mode.

- **Unsecured Mode**: All users are considered 'Administrators' and login and take or clear ownership of ports on unsecured chassis, subject to multi-user port ownership rules. All chassis are initially configured in this mode. See *Setting a Chassis Back to Unsecured Mode* for information on returning a chassis to Unsecured mode.

Use the manual **Refresh** option (in the **View** menu) at any time to refresh the IxExplorer window. It shows a status update for a shared chassis or chassis chain, useful when tracking ownership of ports by other users.

Figure:IxExplorer Refresh Option



IxExplorer provides a further distinction of roles between users. Administrators are privileged users who may take ownership of ports, configure their characteristics, and initiate tests using those ports. Operators are non-privileged users who may only view characteristics and measured data at the chassis, card, and port levels.

The following sections explain the use of Multi-User operations:

- *IxExplorer Login*
- *User Management*
- *Show Owned Ports*

IxExplorer Login

IxExplorer Multi-user mode starts with a Login, accessed from the top menu bar item, *Multiuser*, as shown in the following figure:

Figure:Multi-User Mode Login Dialog

The *User Login/Logout* dialog sets a name for use when logging into the chassis. The name chosen should be distinct from other chassis users. Different login names can be used to distinguish different projects implemented within a single chassis.

The following sections detail Login operations, such as setting and unsetting Secure Mode.

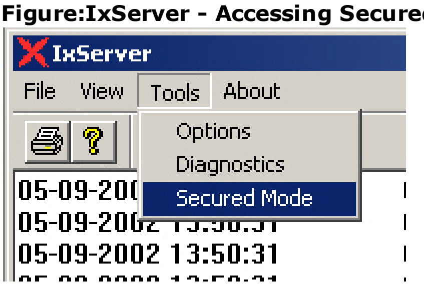
- *Chassis Secure Mode*
- *Setting a Chassis Back to Unsecured Mode*
- *Logging into a Secured Chassis with IxExplorer*

NOTE The Auto Login at Startup check box allows IxExplorer to login previous connections. When selected, users who disconnected from the chassis but did not log out are automatically logged in when reestablishing a connection to the chassis (from the same client workstation).
Login and the auto login does not establish ownership of ports.

Chassis Secure Mode

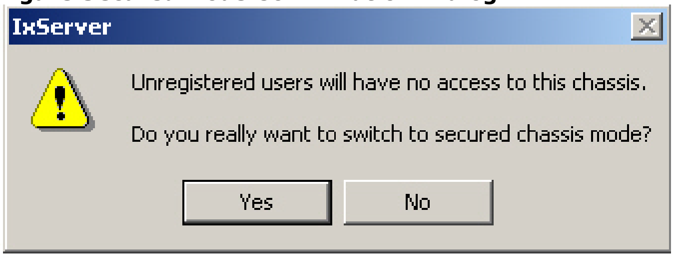
For the first-time login on a chassis, you have Administrative privileges by default, and can elect to enable Secure mode on the chassis. To enable Secured Mode on the chassis access the IxServer screen. In the main toolbar, select Tools, then Secured Mode, as shown in the following figure:

Figure:IxServer - Accessing Secured Mode



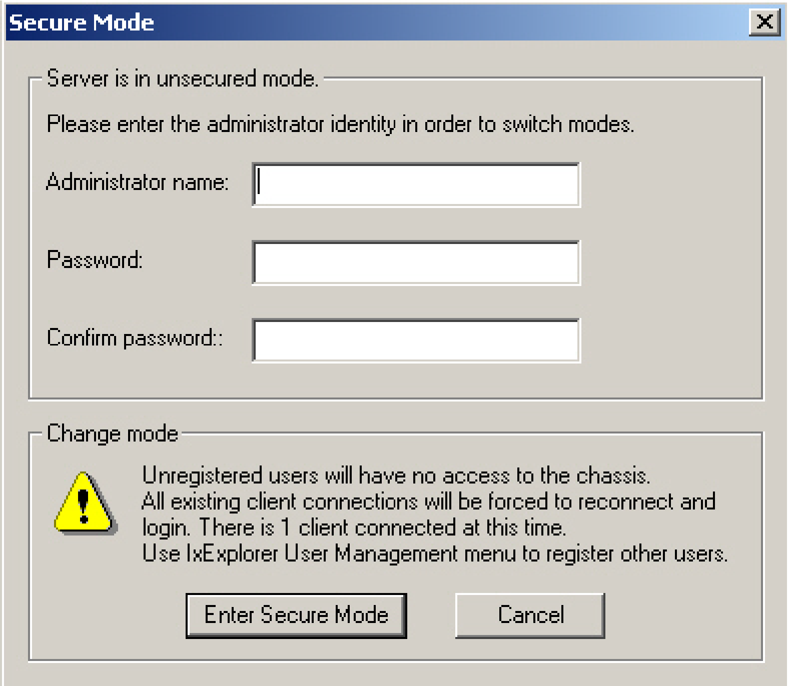
In the list, click *Secured Mode* to open the *Secured Mode* dialog, shown in the following figure:

Figure:Secured Mode Confirmation Dialog



Click the *Yes* button to display the *Secure Mode* dialog, which is shown in the following figure:

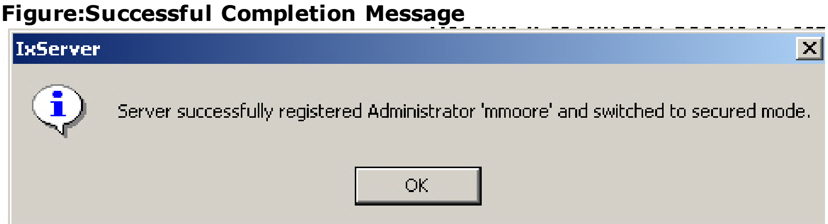
Figure:Secure Mode Dialog



NOTE The warning in this dialog states: *All Unregistered Users will have no access to the chassis. All existing client connections will be forced to reconnect and login. There is (x) client connected at this time. Use* ***IxExplorer User Management*** *to register other users*.

To complete the process, click *Enter Secure Mode*. A completion message appears, as shown in the following figure:

Figure:Successful Completion Message

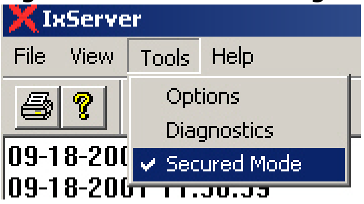


All users wanting to use a secured chassis must be registered. This is accomplished by using IxExplorer. See *Figure:User Management Dialog—Secure Mode User List* for additional information.

Setting a Chassis Back to Unsecured Mode

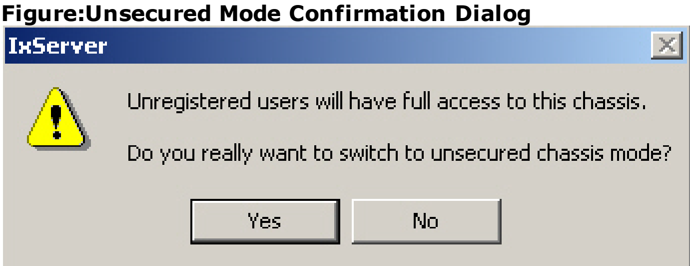
To change the chassis back to unsecured mode, access the IxServer and select Secure Mode, as shown in the following figure:

Figure:IxServer—Accessing Enabled Secure Mode



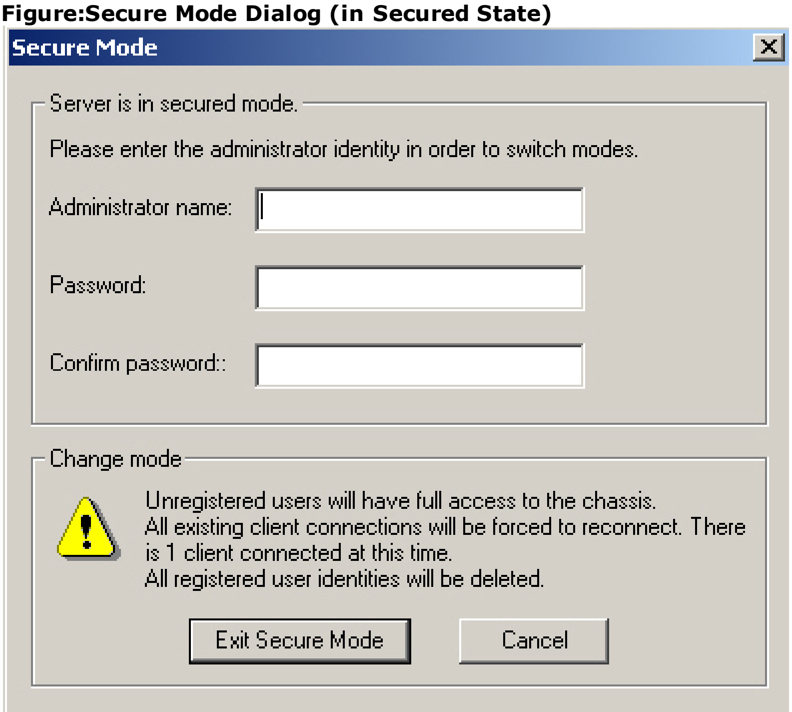
In the list, click **Secured Mode** to display a confirmation dialog, shown in the following figure:

Figure:Unsecured Mode Confirmation Dialog



Click **Yes** to open the **Secure Mode** dialog, which is shown in the enabled state in the following figure:

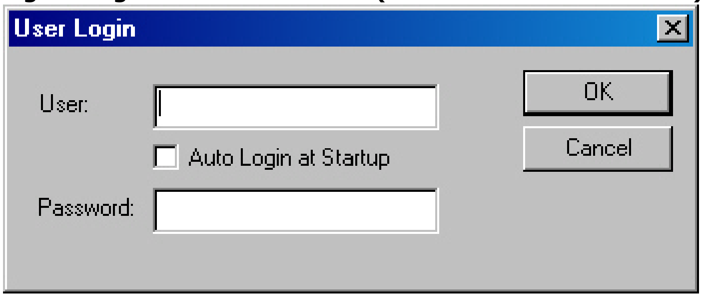
Figure:Secure Mode Dialog (in Secured State)



Logging into a Secured Chassis with IxExplorer

The IxExplorer **User Login Password** field is enabled by the Secure mode, so from that point on, all users must enter a password to access the chassis. The Secure Mode login is shown in the following figure:

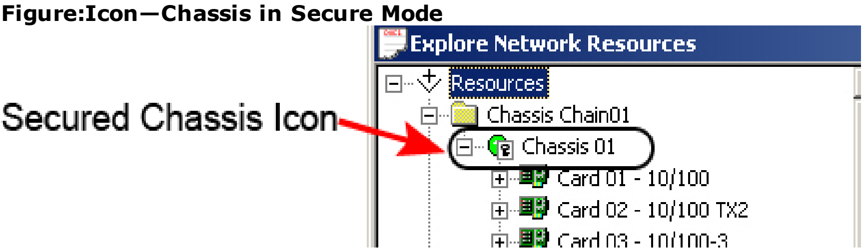
Figure:Login for Secured Mode (with Password Protection)



Once a login name has been established, it appears in the lower right-hand corner of the IxExplorer main window status bar. Any of the multi-user commands may then be used. Multi-user operations work with respect to a set of one or more ports, which may cover any level of the resource chain, starting at the chassis level. When the set of ports is defined at a high level, such as the chassis, all lower level entities (cards and ports) are also enabled for multi-user operation.

The icon indicating a secured chassis is shown in the following figure:

Figure:Icon—Chassis in Secure Mode



Port ownership is displayed in the resource chain display, in (parentheses), for each port. The multi-user operations at Chassis Chain, Chassis, Card, and Port levels are described in the following table:

Table:Multi-User Operations

Operation	Description
Clear My Ownership	Relinquishes ownership of all ports owned by the currently logged-in user in the current set of selected ports.
Clear All Ownership	Relinquishes ownership of all ports in the current set of selected ports. If any of the ports are owned by another user, then a warning may appear. The presence of the warning is determined by a setting in *Options*.
Take Own-ership	Takes ownership of all the ports in the current set of ports. If any of the ports are owned by another user, then a warning may appear. The presence of the warning is determined by a setting in *Options* . *To display only the owned ports, see Show Owned Ports.*
User Man-agement	Invokes a dialog that allows easy global tracking of user ownership of resources. See *User Management* for more details.
Who's Logged In	Available only from the main menu bar, *Multiuser* menu. Displays a list of currently logged-in users in the Status window.

User Management

The User Management operation invokes a dialog which allows all ownership to be viewed and/or modified within a single display. Three modes are available for this dialog:

- *User Management Port List.*
- *User Management User List.*
- *User Management—Secure Mode User List.*

CAUTION

If an IxExplorer user is not utilizing a named configuration file, the Untitled.cfg file is used by default. In this case, the default configuration values are pulled from the chassis (IxServer). Additional users can share resources (owned ports) on the chassis without affecting tests in progress. But, if you have created or re-opened a named configuration file, IxExplorer pushes that chassis configuration to the chassis. In that case, multiple users/owners of ports on that chassis can stop tests in progress.

Ongoing tests in a multi-user environment may be **stopped** under the following conditions:

1) One user opens a named configuration file (xxxxxx.cfg), and starts a test sequence on owned ports.

2) A second user logs on, or the same user logs on with a different login name.

3) The second user is also an owner on some or all of the active ports.

Result: The **ports** owned by the second user,**including ports shared with the first user**,**are updated by IxExplorer as part of the initialization process**. This means that, even if the shared ports were in the middle of a test,**all testing (including transmission of packets) is stopped on those ports**.

See Chassis Merge Dialog for additional information.

User Management Port List

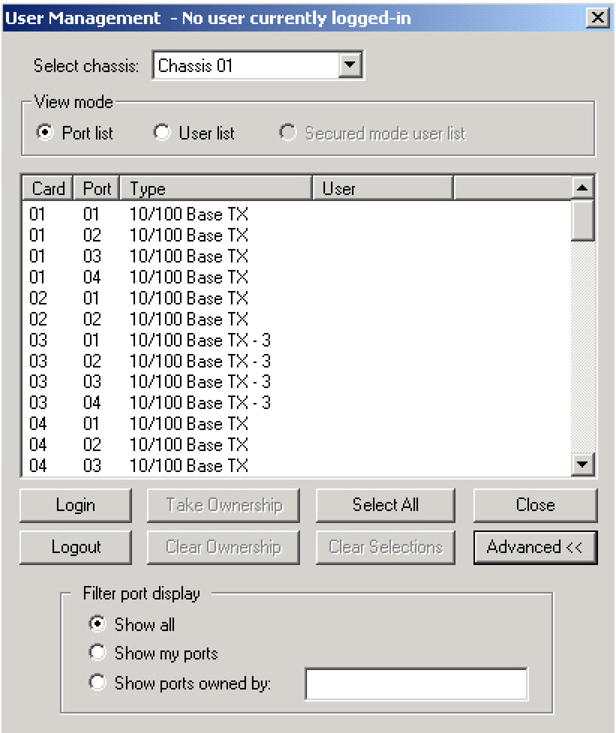
The User Management Port list displays all ports with their port type and current owner. The list is accessed by opening the *User Management* dialog (through *Multiuser* > *User Management*) and selecting the *Port List* option button.

NOTE

We NEVER support multiple clients simultaneously changing data on one port. The rule is: one port-one owner for each system test.
The ownership model should not be used to have one script take ownership of a port and another script take ownership of that same port with the same username because one client may be working with a copy of the port configuration that has been made invalid by another owner.

The User Management Port list is shown in the following figure:

Figure:User Management Port List Dialog



In this dialog, ownership for all ports may be viewed and modified. The scrolling list displays information about port type and ownership. The controls available for this dialog are described in the following table:

Table:User Management Port List Controls

Control	Description
Select chassis	Allows selection of a chassis defined in the Resource window.
Port List/User List/Secure Mode User List	Alternates between the port list, user list, and the secure mode user list. If only a subset of all ports are shown in the display due to other dialog operations, then the phrase '** Port display is filtered **' appears. This filtering may be modified by the use of the *Advanced* dialog (see below).
Login	Invokes the *Login* dialog, allowing the current user to logout or login as a different user.
Take Ownership	Takes ownership of all of the ports selected in the scrolling region. Warnings may appear for ports owned by other users.
Clear Ownership	Clears ownership of all ports selected in the scrolling region. Warnings may appear for ports owned by other users.
Select All	Selects all ports in the scrolling regions.
Clear Selections	Clears all the selections in the scrolling region.
Close	Closes the dialog.
Advanced	Opens the *Advanced* dialog, which contains the Filter Port display box at the bottom of the page.
Filter Port Display	Allows the list of ports in the scrolling window of the dialog to be filtered for one of:

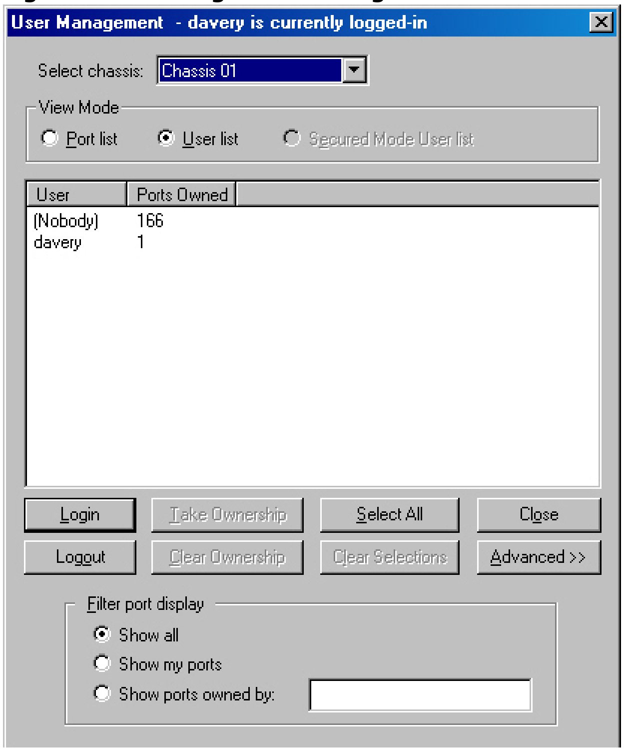
Control	Description
	• all users, • the currently logged in user, or • a particular user.

User Management User List

The User Management User list displays all users currently logged on to the chassis, and what ports they own. The list is displayed by opening the *User Management* dialog (through *Multiuser > User Management*) and selecting the *User List* option button.

The User List view of the *User Management* dialog is shown in the following figure:

Figure:User Management Dialog—User List



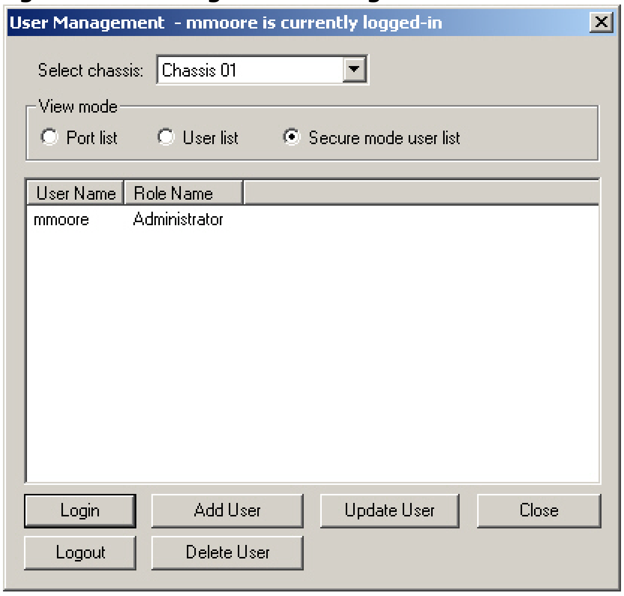
The display summarizes the number of ports owned by users as well as unowned ports. The controls available for this dialog are described in the following table. In addition, double-clicking a single user's entry causes an automatic transition back to the Port List mode. In this mode, the display is filtered for the selected user.

User Management—Secure Mode User List

When a chassis chain has been enabled in Secure Mode, the Secure Mode User List choice is enabled. This view allows to be registered as users for secured chassis. The list is displayed by opening the *User Management* dialog (through *Multiuser > User Management*) and selecting the *Secure mode user list* option button.

The Secure Mode User List view of the *User Management* dialog is shown in the following figure:

Figure:User Management Dialog—Secure Mode User List



Rows of the scrolling region are filled with the User Names of secure mode users, and the Role for each user. The controls available for this dialog are described in the following table:

Table:User Management Secure Mode User List Controls

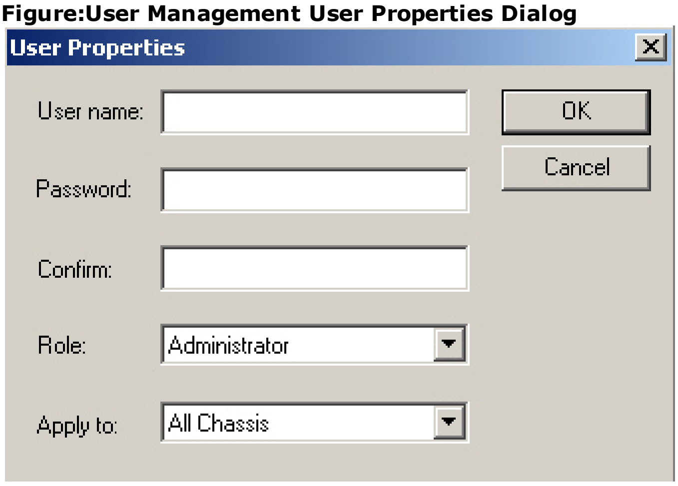
Control	Description
Select Chassis	Allows selection of any of the chassis defined in the Resource window.
Port List/User List/Secure Mode User List	Alternates between the Port list, User list, and Secure Mode User list. If only a subset of all ports are shown in the display due to other dialog operations, then the phrase '** Port display is filtered **' appears. This filtering may be modified by the use of the *Advanced* dialog (see below).
Login	Invokes the *Login* dialog, allowing the current user to logout or login as a different user.
Logout	Allows the user to logout.
Add User	Invokes the *User Properties* dialog, for entering additional secure mode users, their passwords, roles, and chassis to which they are allowed access. See *Secure Mode—User Properties Dialog*.
Delete User	Deletes a user from secure mode.
Update User	Invokes the *User Properties* dialog, where the secure mode status can be modified for users. See *Secure Mode—User Properties Dialog*.
Close	Closes the dialog.

Secure Mode—User Properties Dialog

The *User Properties* dialog allows an administrator to add users to a chassis in Secure mode, and determine their user role. The dialog is accessed by opening the *User Management* dialog (through *Multiuser > User Management*), selecting the *Secure mode user list* option button, and then selecting the *Add User* button.

The *User Properties* dialog is shown in the following figure:

Figure:User Management User Properties Dialog



The controls available for the *User Properties* dialog are described in the following table:

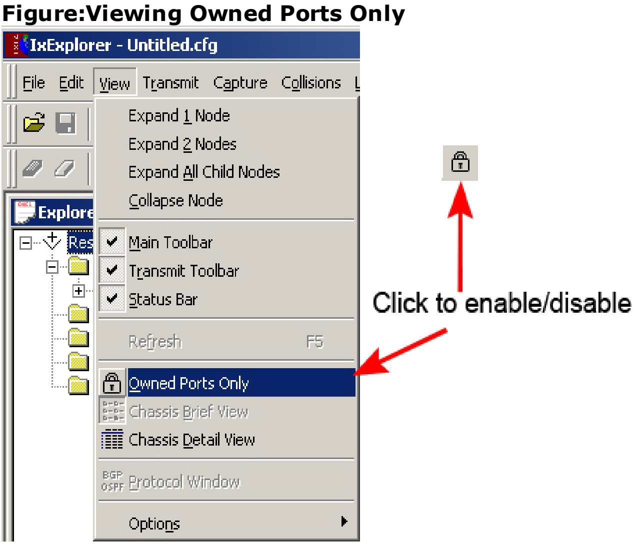
Table:User Management User Properties Dialog

Control	Description
User name	The name of the user. If this dialog is used to update a user, this field should not be modified.
Password	The password for this user.
Confirm	Enter the password for this user again, for confirmation.
Role	One of: Administrator or Operator (Operator has view-only privileges.) The default is Administrator.
Apply to	A list of the chassis that you have access to. The default selection is *All Chassis*.

Show Owned Ports

Once you have taken ownership of selected ports, the Resources tree can be modified to display **only** the owned ports. With a Chassis Chain, Chassis, Card, or Port selected and highlighted, go to *View* in the main menu bar, and select *Owned Ports Only*, as shown in the following figure. The icon appears to be clicked, and only ports owned by the logged-in user is displayed in the Resources tree.

Figure:Viewing Owned Ports Only



To disable this feature, return to the *View* menu, and reselect *Owned Ports Only*. All ports are then displayed. This feature may also be enabled/disabled by clicking the icon in the main IxExplorer toolbar.

Transmit Operations

Transmit operations work with respect to a set of ports. A set of ports may be at any level of the resource chain: chassis chain, chassis, card, or port. Each level of the chain includes all ports in lower levels. In addition, Port Groups and Statistics groups may be used to define a set of ports.

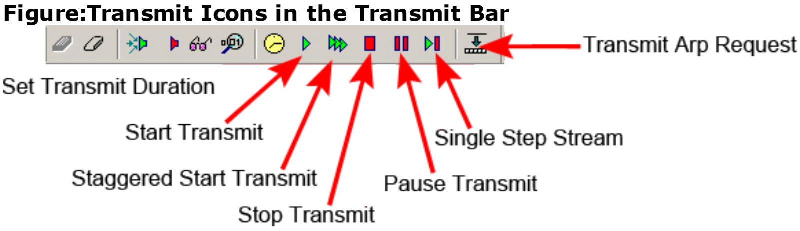
The transmit operations are described in the following table:.

Table:Transmit Operations

Operation	Description
Start Transmit	Starts the transmission operation on all ports in the present set of ports. If no transmit operation has been performed, or if a Stop Transmit operation was last performed, then transmission begins from the first stream of each port. If a Pause Transmit operation was last performed, then transmission begins at the next packet on all ports.
Staggered Start Transmit	The same operation is performed as in Start Transmit, except that the start operation across ports is artificially staggered. The time between ports is in the range of 25-30 ms.
Stop Transmit	Stops the transmission operation on all ports in the present set of ports. A subsequent Start Transmission or Step Stream commences from the first stream of each port.
Pause Transmit	Stops the transmission operation on all ports in the present set of ports at the end of their current packet. A subsequent Start Transmission or Step Stream commences at the next packet.
Single Step Stream (or Step Transmit)	Causes one packet to be applied on all ports in the present set of ports. NOTE Single step transmit causes a pause that interferes with the sending of async frames. Select single step and until a stop or start transmit is issued on a sync stream, async traffic is not sent.
Set Transmit Duration	Enables setting the days, hours, minutes, and seconds duration of the transmission operation.
Clear Timestamps	Timestamps are optionally embedded into transmitted data; Instrumentation Box *for details. This operation clears all timestamps on all ports back to 0.*
Transmit ARP Request (or Send ARP Request)	Causes an ARP request to be transmitted on the port for the first IP address found in the packet's streams. ARP requests are only available after ARP is enabled in the IxRouter window. Refer to *ARP*.

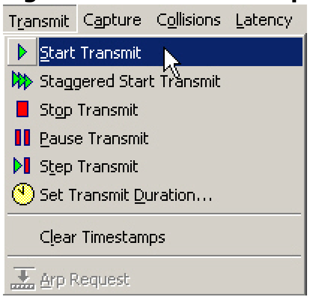
Once a set of ports is defined, transmission operations can be implemented from a number of locations. One place is in the Transmit toolbar as shown in the following figure:

Figure:Transmit Icons in the Transmit Bar



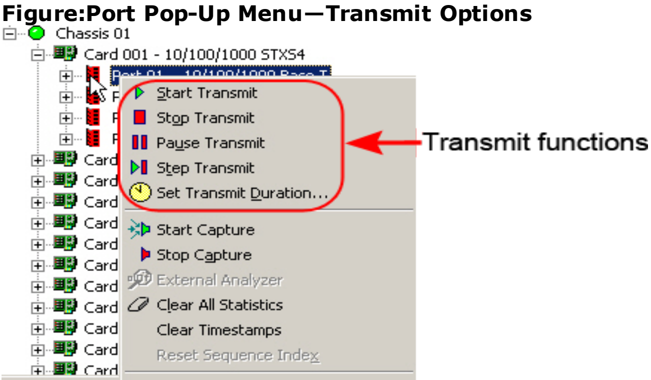
Another location where transmit functions can be accessed is through the menu bar at the top of the IxExplorer window as shown in the following figure:

Figure:Transmit Menu Options



Transmit functions can also be accessed through pop-up menus at any level of the Resource tree, as shown in the following figure:

Figure:Port Pop-Up Menu—Transmit Options



Capture Operations

Data Capture operations work with respect to a set of ports, similar to transmit operations.

Most ports may be configured for 'raw' data capture or Packet Group/Latency operation. Refer to the *Ixia Platform Reference Manual* for a complete list of load module features. This setting is the *Receive Mode* for the port. In addition, some ports may be configured to force collisions within packets. The Capture operations are described in the following table:

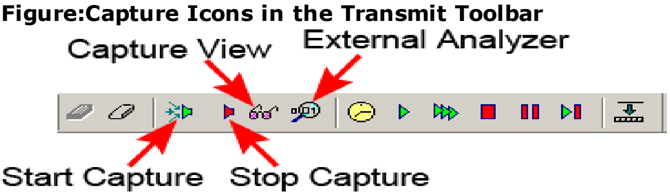
Table:Capture Operations

Operation	Description
Start Capture	Enables capture on all ports in the present set of ports whose receive mode is set to data capture. Frames are not actually captured until the Capture Trigger condition is satisfied.
Stop Capture	Stops capture on all ports in the present set of ports.

Operation	Description
Clear TimeStamps	Timestamps are optionally embedded into transmitted data; Instrumentation Box *for details. This operation clears all timestamps on all ports back to 0.*
View	Opens the Capture View window for a port which has been selected in the tree. *Capture View Window* for additional information.
Filters	Opens the Filter Properties dialog for a port which has been selected in the tree.*Filter Properties Tab* for additional information.

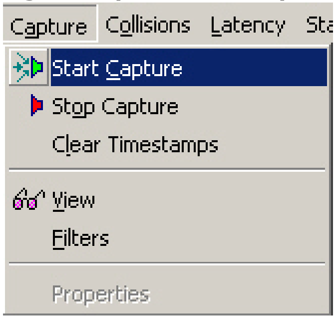
Once a set of ports has been defined, Capture operations can be implemented from a number of locations. One place is in the Transmit toolbar as shown in the following figure:

Figure:Capture Icons in the Transmit Toolbar



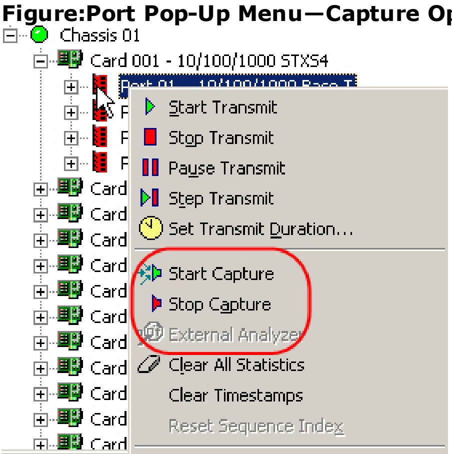
Another location is through the menu at the top of the IxExplorer window, as shown in the following figure:

Figure:Capture Menu Options



Capture operations can also be accessed through pop-up menus at any level in the Resources tree. An example of usage at the port level is shown in the following figure:

Figure:Port Pop-Up Menu—Capture Options

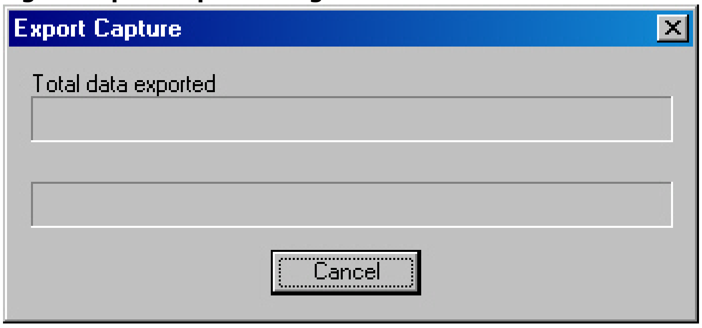


External Analyzer

The External Analyzer feature can be used directly from the chassis chain, chassis, card, or port right-click menu by selecting the *External Analyzer* option, or by clicking the

External Analyzer icon () in the Transmit toolbar. This feature exports captured data to a previously specified third party packet analyzer. When the icon (or command) is selected, the selected third party analyzer exports the capture data to a file. The progress of the capture export can be viewed in the *Export Capture* dialog. The *Export Capture* dialog is shown in the following figure:

Figure:Export Capture Progress



See External Analyzer Option for additional information.

Forced Collisions

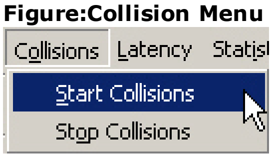
In addition to normal Capture operation, forced collisions can be generated on the receive side of 10/100 module ports, when the port is in half-duplex mode. Forced collisions operate by generating data as information is being received. See the section on Forced Collision Operation in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for a complete explanation of forced collisions. The collision operations are described in the following table:

Table:Collision Operations

Operation	Description
Start Collision	Enables collisions on all ports in the present set of ports on received data if programmed for the port and enabled (in the *Forced Collisions* tab of the *Port Properties* dialog) and the 10/100 module is operating in half-duplex mode.
Stop Collision	Stops collision operation for all ports in the present set of ports.

Once a set of ports is established, collisions for 10/100 ports with the Forced Collisions option enabled can be generated through the menu at the top of the IxExplorer window as shown in the following figure:

Figure:Collision Menu Options

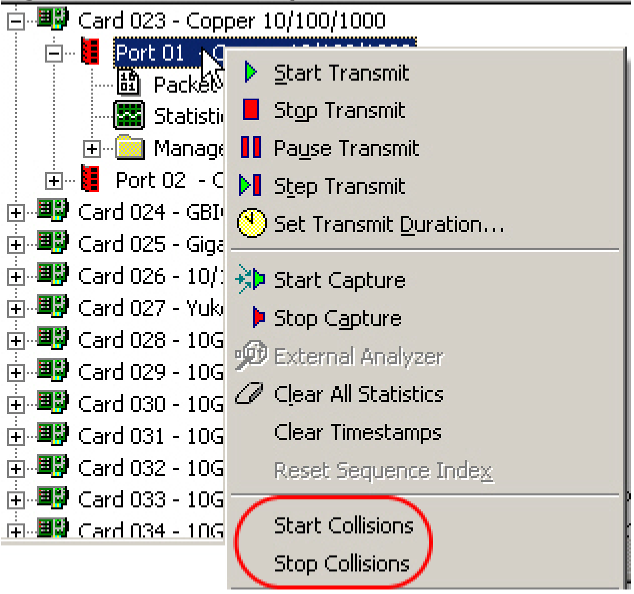


Collision operations are also available through pop-up menus at any level in the Resources tree for ports which support this feature.

NOTE To use the Forced Collisions feature, first enable Forced Collisions in Port Properties (for 10/100 modules).

An example of usage at the port level is shown in the following figure:

Figure:Collision Menu Options

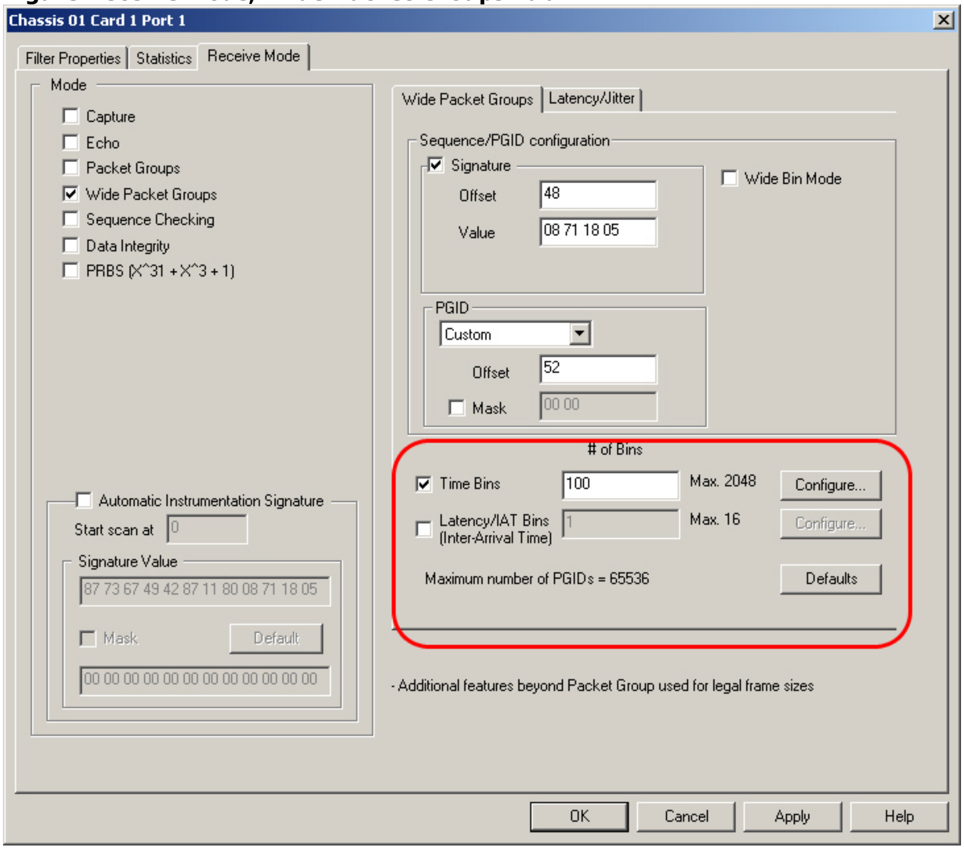


Latency Operations

For newer load modules, latency time bins are configured in each port's *Receive Mode*, *Wide Packet Groups* tab. Select **Time Bins** and the configuration fields are enabled. The latency measurements are viewed in the *Packet Group Statistic View*; refer to *Packet Group Statistic View for a complete description of Latency Views. Newer cards include these:*

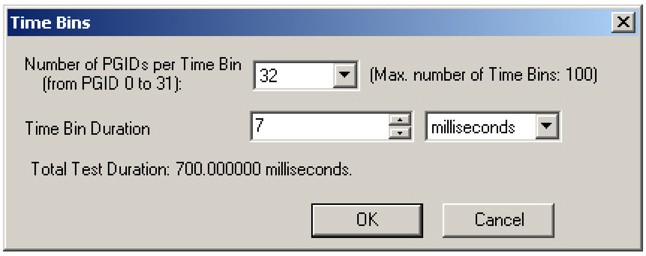
- 10/100/1000 ASM XMV12X
- 10/100/1000 STX(S)2, 4, and 24
- 10/100/1000 TX(S)4
- 10/100/1000 XMS(R)12
- 10/100/1000 LSM XMV(R)4 and 16
- 1000 SFP(S)4
- All 10GE LSM modules
- 2.5G MSM and 10G MSM
- ATM/POS 622 Multi-Rate

Figure:Receive Mode, Wide Packet Groups Tab



Click the **Configure** button to open the Time Bins dialog, where latency measurement can be configured.Table:Latency Options—Latency Type Tab for details.

Figure:Time Bins Dialog



For older 'legacy' load modules, all latency operations are initiated from a *Latency View* dialog, where one or more ports' latency stats are displayed. Legacy cards include these:

- 10GE modules (LM10GEXX and LM10GUXXX)
- OC192c POS modules (LMOC192cPOS)
- GBIC module (LM1000GBIC)
- Gigabit module (LM1000SX)
- 10/100 TXS8 module (LM100TXS8)
- OC12c/OC3c POS modules (LMOC12c and LMOC3c)

Refer to *Packet Group Statistic View* *for a complete description of Latency Views. The options in the Latency menu in the main menu bar are active only when a Latency View is displayed, as shown in the following figure.*

NOTE

Clear Timestamps simultaneously on Transmit and Receive ports together **BEFORE** starting Latency measurements.

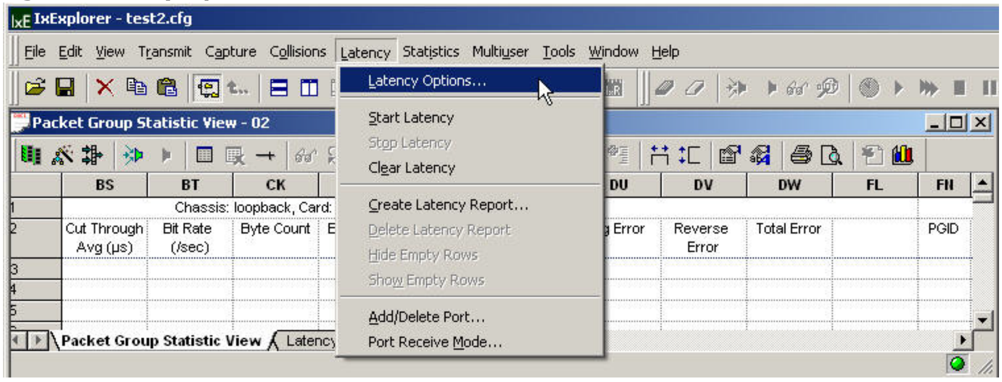
Some methods for clearing timestamps on multiple ports simultaneously are listed below:

Create a Port Group for all of the transmit and receive ports to be used in the Latency measurement. Right-click the Port Group name in the details list, and select *Clear Timestamps*.

If all of the Transmit and Receive ports are on a single card, and no other ports on that card are being used for other purposes, highlight the card in the Network Resources list, and go to the main menu bar. Click *Transmit or Capture* and select *Clear Timestamps* from the list.

Create a Statistic View for all of the transmit and receive ports to be used in the Latency Measurement. In the Statistic View, highlight ALL of the port names in the column headers. Right-click the highlighted port names and select *Clear Timestamps* from the pop-up menu.

Figure:Latency Options Menu



The latency operations available in the Latency menu are described in the following table:

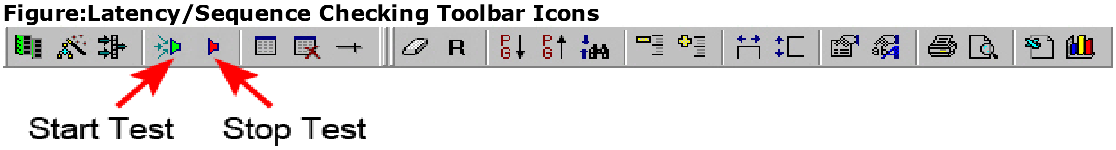
Table:Latency Operations

Operation	Description
Latency Options	Opens the *Latency Options* dialog, where the type of latency measurements can be selected.
Start Latency	Initiates latency measurements on all ports in the present set of ports whose receive mode is set for packet group operation.
Stop Latency	Stops latency measurements on all ports in the present set of ports.
Clear Latency	Clears all accumulated latency data from the spreadsheet.
Create Latency Report	Opens the *Latency Report* dialog, where a latency report can be named and added to the spreadsheet.
Delete Latency	Deletes the currently selected latency report tab.

Operation	Description
Report	
Hide Empty Rows	Only applies to a selected latency report. Deletes the rows that do not contain data in the latency report, to make the report more concise.
Show Empty Rows	Only applies to a selected Latency Report. Displays the empty rows that were hidden by the Hide Empty Rows option.
Add/Delete Port	Opens the *Select Port* dialog so ports and be added to or deleted from the spreadsheet.
Port Receive Mode	Opens the *Receive Mode* dialog for the port selected in the spreadsheet.

The toolbar at the top of the *Packet Group Statistic View* dialog allows access to the two principal operations, starting and stopping the Latency test, as shown in the following figure:

Figure:Latency/Sequence Checking Toolbar Icons



These operations are described in the following table. Information on the rest of the icons in the toolbar is found in *Packet Group Statistic View*

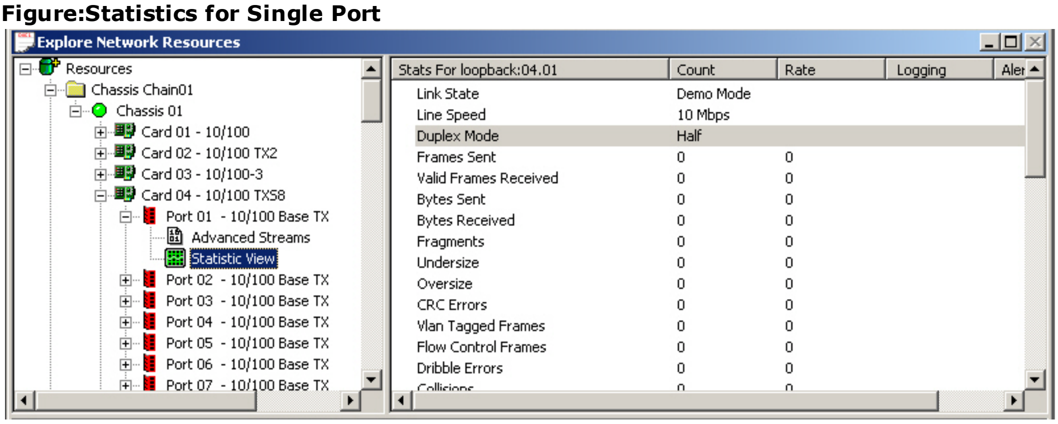
Table:Latency Toolbar Operations

Operation	Description
Start Test	Initiates latency measurements on all ports in the present set of ports whose receive mode is set for packet group operation.
Stop Test	Stops latency measurements on all ports in the present set of ports.

Statistics Operations

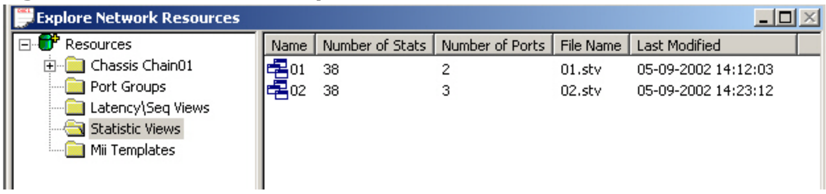
Statistics for any port may be obtained by selecting the Statistic View label listed below that port in the IxExplorer Resources tree, as shown in the following figure:

Figure:Statistics for Single Port



The selection of Statistics displayed for a port in the Resources window is not user-configurable. When multiple ports are to be displayed together, a Statistic View group should be defined and selected as shown in the following figure. This option also allows to define selected lists of statistics.

Figure:Statistic View Group Select



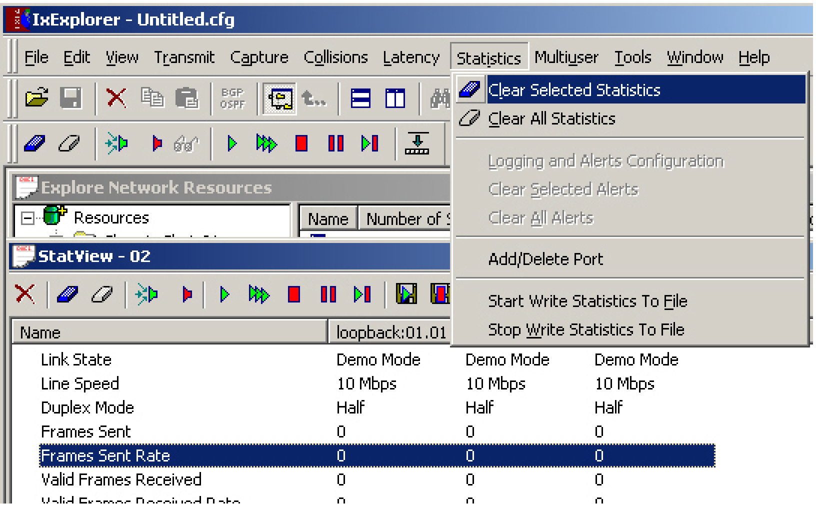
Double-clicking the Statistic View selection displays all of the applicable ports simultaneously, as shown in the following figure. The default format for Statistic Views is spreadsheet mode, as shown in this graphic*.* The alternate view is the Standard View. The display mode may be selected in the *Tools* > *Options* > *Statistic View* dialog.

Statistics, in any type of Statistic View, may be cleared (reset) at any time from a number of locations. One of those locations is the Statistic View toolbar, as shown in the following figure:

Figure:Clear Statistics Operation from the Statistic View Toolbar

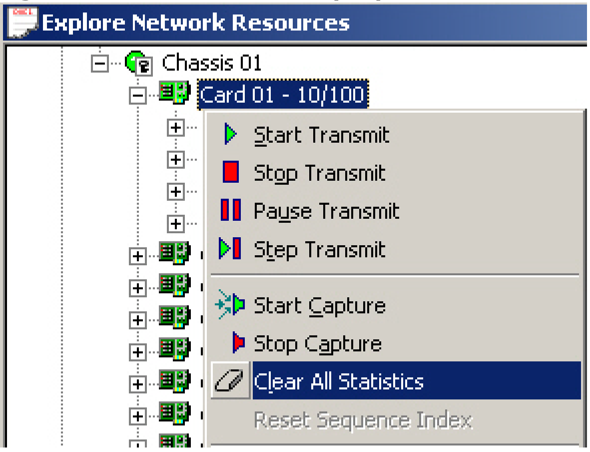
Another location is in the Statistics Menu, as shown in the following figure. The options in this menu are not active unless a Statistic View window is currently open.

Figure:Statistics Menu



The *Clear All Statistics* menu option clears **all** of the statistics for the current set of ports. Statistics can also be cleared from most pop-up menus in the Explore Network Resources display. An example for an individual load module is shown in the following figure:

Figure:Clear Statistics in Pop-Up Menu



Other Operations

Active Stream Configuration

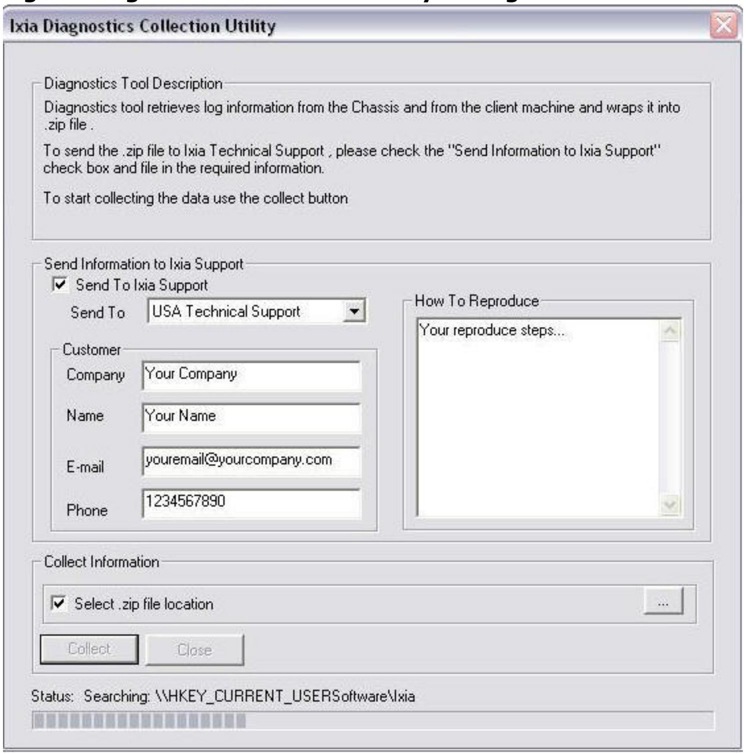
An additional operation available in conjunction with the Statistic View is called Active Stream Configuration. It allows for continuous variation of the Frame Size and the Inter-Packet Gap across a range of ports, to determine the effect on the DUT. *Active Stream Configuration for a full description. This mode of operation is not available for ports whose transmit mode is set to flows.*

Collect Diagnostic Logs

The Diagnostics Collection Utility collects log information from the chassis and from the client computer and wraps it into a comclicked (.zip) file named ixos-logs-YYYYMMDDHHMM.zip. The file can be sent to Ixia Technical Support by completing the fields in the on-screen dialog.

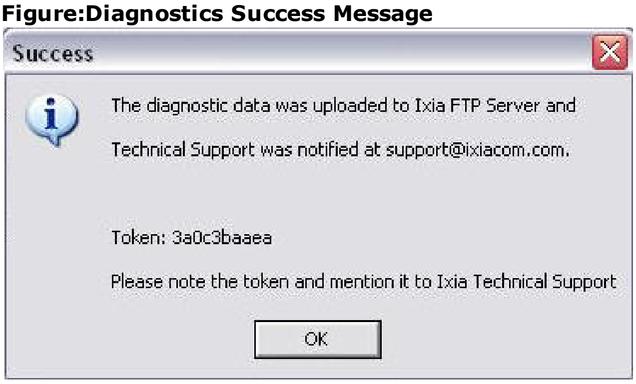
The Diagnostics tool is activated from the right-click menus for Chassis Chain, for Chassis, for Card, for Port, and from the Help menu in the top IxExplorer menu bar.

Figure:Diagnostics Collection Utility Dialog



When the log file has been uploaded to the Ixia FTP server, a message similar to that shown below is displayed. Note the token number for later reference when communicating with Ixia Technical Support.

Figure:Diagnostics Success Message



Fields and controls are described in the following table:

Table:Diagnostics Dialog

Section	Field/Control	Description
Send Information to Ixia support	Send to Ixia Support	(check box to enable) NOTE No e-mail is sent unless this is selected. See note under Collect Information, below. Select the appropriate tech support destination:

Section	Field/Control	Description
		• Asia/Pacific India USA EMEA (Europe, Middle East, Africa)
Customer	Company	Enter your company name
	Name	Enter your name
	E-mail	Enter your e-mail address (Ixia Technical Support will contact you at this address)
	Phone	Enter your telephone number, including country code (if outside USA) and area code (Ixia Technical Support will contact you at this phone).
How to Reproduce		Briefly describe the problem that the logs are related to. Tell Ixia Technical Support what you were doing (sequence of steps) when the problem occurred.
Collect Information	Select .zip file location	(check box to enable) Click the ellipsis (...) to open a standard Windows **Open** dialog, to locate and choose the .zip file to be sent. NOTE When the check box 'Send To Ixia Support' is selected and the check box 'Select .zip file location' is cleared then a default zip file is created to send the log information. When the 'Send To Ixia Support' is cleared and the check box 'Select .zip file location' is selected then a zip file is created but not sent.
	Collect	Click **Collect** button when ready to send the diagnostics log file to Ixia. When clicked, a Diagnostics Progress bar is displayed. NOTE Collect button remains disabled if **both** 'Send to Ixia Support' and 'Select zip file location' check boxes are cleared.
	Cancel	Cancel this operation and close the dialog.
Status (and progress bar)		Text shows status of the log collection process, which includes searching for files, compressing files, and sending them to Ixia. The progress bar shows progress of the log collection process.

[This page intentionally left blank]

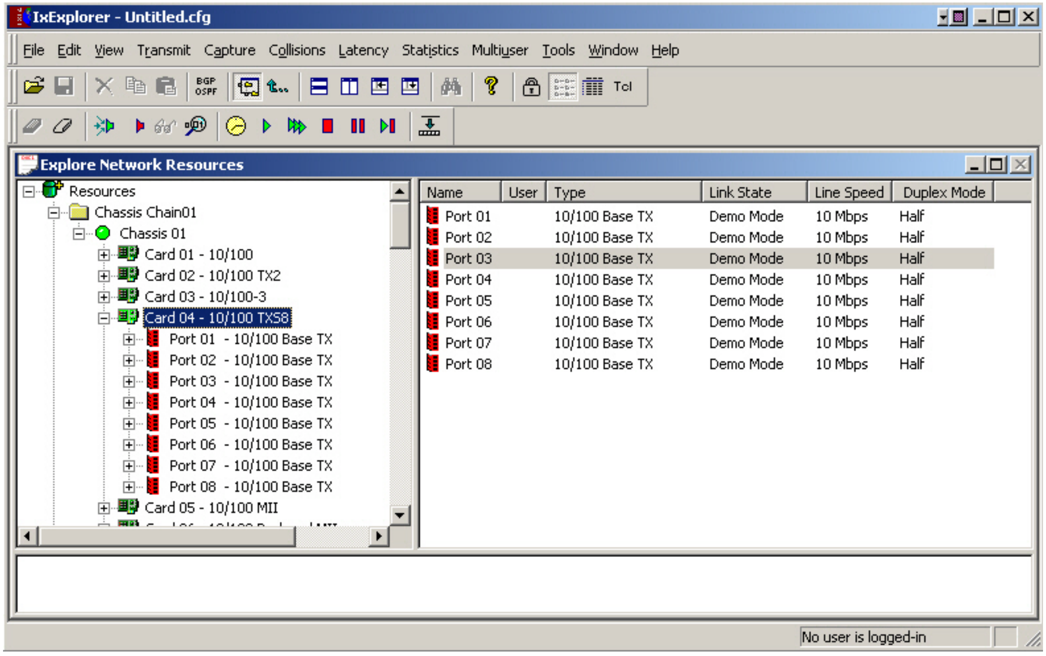
Chapter 3 - Explore Network Resources

The initial and most important display of IxExplorer is the Explore Network Resources window. It consists of a a Tree view, a Details view, a menu bar, and a toolbar.

The Explore Network Resources window is opened by double-clicking the IxExplorer icon on the desktop, or from the Start Menu by selecting *Start* > *Programs* > *Ixia* > *IxExplorer*.

The Explore Network Resources window is shown in the following figure:

Figure:Explore Network Resource Window



The Tree view on the left side of the window shows the hierarchy of Ixia hardware resources, while the Details view on the right side shows detailed information for the item selected in the left half.

This chapter covers the following major topics:

- *Chassis Chains*—Chains of chassis, including:
  - *Chassis*
  - *Cards*
  - *Ports*
- *Port Groups*—Sets of ports assigned to a group.
- *Stream Groups*—Sets of streams assigned to a group.
- *Packet Group Statistic Views*—Sets of ports grouped for Packet Group Statistic analysis.
- *Statistic Views*—Side-by-side views of statistics for multiple ports.
- *Stream Statistic Views*—Statistics for selected port streams.
- *MII Templates*—MII register template files.
- *Layouts*—Allows to save GUI layouts for future use.
- *Tools Menu Functions*—Options for IxExplorer configuration and other feature uses.

Resources

The Resources hierarchy in the Tree view consists of the following levels of devices:

Table:Resource Level Operations

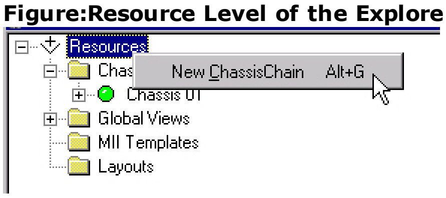
Resources	Contains all hardware definitions.
Chassis Chain	A series of connected Ixia chassis.
Chassis	A single Ixia chassis.
Cards	Plug-in Ixia load modules.
Ports	Ports on the cards.
• Capture View	Displays captured packets at the bit level.
• IxRouter Window	Allows manipulation of Routing Protocols for the port.
• Statistics	Statistics gathered by port.
• Filter, Statistics Receive Mode	Controls the filter and trigger, statistics, and receive mode options.
• Packet Streams	Streams and flows of data applied by the port.
• Port Properties	Controls the port properties options.
Circuits	Configure circuits on a port (*VCAT Circuit Properties*).
Global Views	Contains group, statistics, and other views.
Port Groups	Sets of ports grouped under a group name.
Stream Groups	Sets of configured streams grouped under a group name.
Packet Group Statistic Views	Sets of ports grouped for latency/sequence checking analysis.
Statistic Views	Different side-by-side views of statistics.
Stream Statistic Views	Statistics on a per stream basis.
MII Templates	Sets of MII template files.
MII template file	Individual MII template files.
Layouts	Saves open windows layouts.

Each level of the tree may be expanded or contracted by clicking the ⊟ or ⊞ symbol to the left of the level's label or by double-clicking the label itself. Note that the name of the configuration file being used (with *.cfg* extension) is displayed in the title bar.

Tree Operations

The Resources level is shown highlighted in the following figure, along with the pop-up menu, which is available by right-clicking *Resources*:

Figure:Resource Level of the Explore Network Resource Window



The operations available when the Resources level is selected are described in the following table:

Table:Resource Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand/contract tree elements below the current level.
New Chassis Chain	Alt+G	Add a new chassis chain. The chain is named Chassis Chain NN, where NN is the next available chain number. A chassis chain may be renamed. *Chassis Chains.*

Chassis Chains

The term *chassis chain* refers to a set of Ixia chassis that have been cabled together through their Sync In/Sync Out ports. They may also be coordinated by accurate time sources, such as GPSs, so that **all** of the ports on **all** of the chassis may be considered as a unit. It is the second level of the tree hierarchy, as shown highlighted in the following figure along with the pop-up menu available by right-clicking *Chassis Chain*.

NOTE Plugging-in or removing the sync cable while IxServer is running can cause errors that prevent the IxOS software from running. If this occurs, restart all Ixia applications.

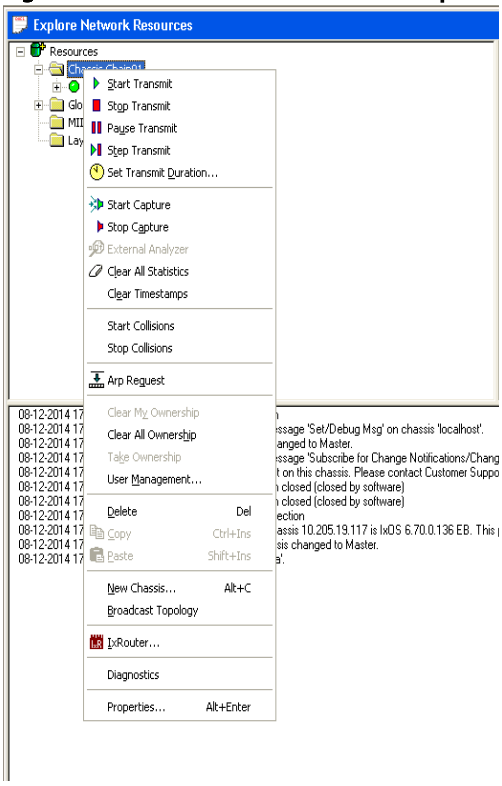
Within the chassis chain, there are three sub levels:

- *Chassis*
- *Cards*
- *Ports*

Tree Operations

Chassis chain tree operations are accessed by right-clicking the Chassis Chain folder. A menu is displayed, as shown in the following figure:

Figure:Chassis Chain Level of the Explore Network Resource Window



The operations available at the Chassis Chain level are shown in the following table. Port operations are applied to all ports on all cards in the chassis chain.

Table:Chassis Chain Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand or contract tree elements beneath the current level.
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A *Start Transmit* or *Step Transmit* operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted.
Set Transmit Duration		Sets a specific time period for transmission. Selecting this icon opens the *Set Transmit Duration* dialog, as described in *Set Transmit Duration*.
Start Capture		Enables the start of data capture operations.
Stop Capture		Disables data capture operations.
External Analyzer		Launches a third party packet analyzer. The type of analyzer launched

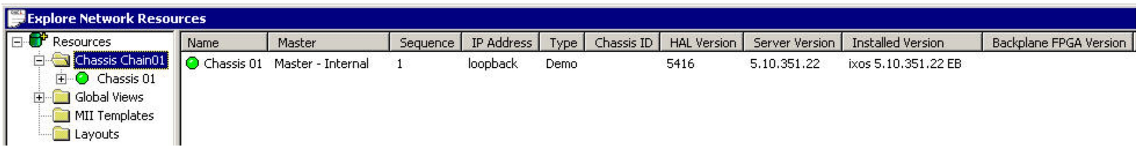
Operation	Keys/Shortcut	Description
		is determined by the settings in the *External Analyzer tab*, as described in *External Analyzer Option*. This button is only active when the analyzer type is specified in *External Analyzer* tab.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations for details.*
Clear Timestamps		Clears the global time value used in timestamps which may be included in each frame. Refer to *Instrumentation Box* for details.
Start Collisions		Enables collision generation for received data, if programmed for the port and enabled.
Stop Collisions		Stops collision generation.
ARP Request		Send an ARP packet requesting port addresses. The first IP address found in the streams for each port is used for the ARP request. ARP requests are only available after ARP is enabled in the IxRouter window.
Clear My Ownership		The current user's ownership for all ports owned by the user in the chassis chain is cleared.
Clear All Ownership		The ownership for all ports in the chassis chain is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with all ports of the chassis chain. A warning message may be displayed if a port is owned by another user.
User Management		A dialog is displayed, allowing cent-ralized, per chassis control of port ownership.
Delete	 Del	Deletes the selected chassis chain, after answering 'Yes' to a con-firmation dialog.
Copy	 Ctrl + Ins	Used with *Paste*. The item(s) selected (highlighted) are copied to the clipboard.
Paste	 Shift + Ins	Used with *Copy*. The item(s) copied to the clipboard in the 'Copy' operation are pasted into

Operation	Keys/Shortcut	Description
		the selected (highlighted) location.
New Chassis...	Alt+C	Displays the *Chassis Properties* dialog, so a new chassis can be added. The chassis is automatically named 'Chassis NN,' where NN is the next available chassis number. The chassis may be renamed. *Chassis*
Broadcast Topology		Broadcast the current chassis chain topology, configuring the current attributes on the physical chain.
IxRouter		Opens the IxRouter window. For more information on IxRouter window function for IxExplorer, see *IxRouter Window*. For more information on other protocols available in this window, see the *IxNetwork User Guide*.
Diagnostics		The Diagnostics Collection Utility collects log information from the chassis and from the client computer and wraps it into a comclicked (.zip) file named ixos-logs-YYYYMMDDHHMM.zip. The file can be sent to Ixia Technical Support. See *Collect Diagnostic Logs*.
Properties...	Alt + Enter	Invokes the *Chassis Chain Properties* dialog. *Chassis Chain Properties*.

Chassis Chain Detail Data

The Details view for a selected chassis chain shows information for each chassis in the chassis chain. See *Chassis Chain Properties for procedures used to modify chassis chain properties.*

Figure:Chassis Chain Detail



The detail data available is described in the following table:

Table:Detail Data for Chassis Chain

Column	Description
Name	The name of the chassis. Initially this is Chassis *NN*, where the number *NN* increments with each new chassis. These names, however, may be changed by you. *Chassis*.

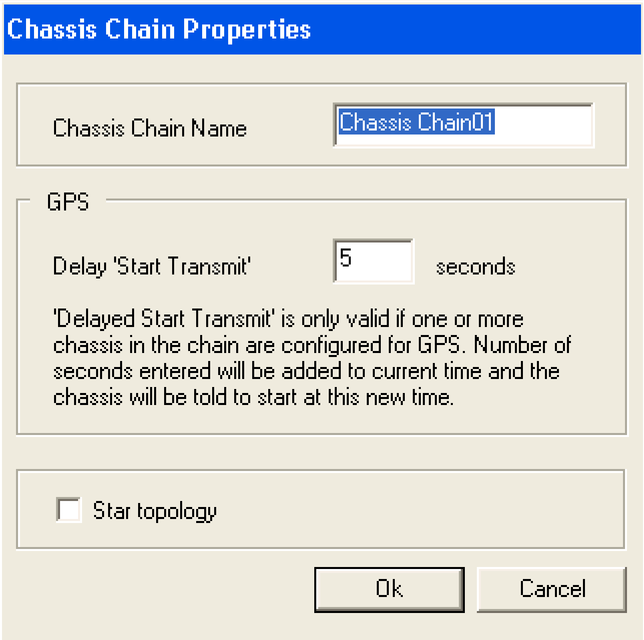
Column	Description
Master	(Read-only) Indicates the function of this chassis in the chain. • Master-CDMA • Master-GPS • Master-Internal • Slave See expanded definition in *Table:General Chassis Properties Dialog*
Sequence	This indicates where this chassis is placed in the physical chassis chain. See expanded definition in *Table:General Chassis Properties Dialog*.
IP Address	The IP Address or host name of the chassis, assigned to the chassis during installation.
Type	The chassis type. See *Ixia Platform Reference Manual* for a list of chassis types and capabilities.
Chassis ID	This is the assigned ID of the chassis. It is an arbitrarily assigned number which may be changed by you (from 0 to 255). The chassis ID should be unique among all of the chassis in a chassis chain.
HAL Version	The software version of the HAL—Hardware Abstraction Layer. The IxExplorer software refuses to talk to an IxServer or HAL instance that uses an incompatible version.
Server Version	Reserved for future use.
Installed Version	Installed version of IxOS software.
Backplane FPGA Version	Reserved for future use.
Topology	Indicates that the topology for the current chain is daisy.
Card	The card number.
Force Hotswap	This will emulate physical removal and insertion of the card identified by the number entered in the Card field. This is done for diagnostic purposes.
Reset Hardware	This button allows you to reset the hardware to factory defaults.

Chassis Chain Properties

A Chassis Chain has properties that can be modified after being created, using the Chassis Chain Properties dialog. This dialog is access by right-clicking Chassis Chain in the Tree view and selecting the *Properties* command.

The *Chassis Chain Properties* dialog is shown in the following figure:

Figure:Chassis Chain Properties Dialog



The fields and controls in the dialog are described in the following table:

Table:Chassis Chain Properties Dialog Elements

Field/Control	Description
Chassis Chain Name	The name of the entire chassis chain may be changed in this field.
Delay 'Start Transmit'	When synchronizing multiple chassis that are not physically connected through sync-in/sync-out cables, GPS servers may be used to provide the synchronization. A delay must be incorporated to allow the signal to travel from the local IxExplorer workstation to the farthest chassis and back. Distance is measured here in terms of the time that it takes to receive a return message from the remote system. A series of pings may be used to assess this time in advance.
Star topology	Select the check box to enable star topology on the current chassis chain.

Chassis

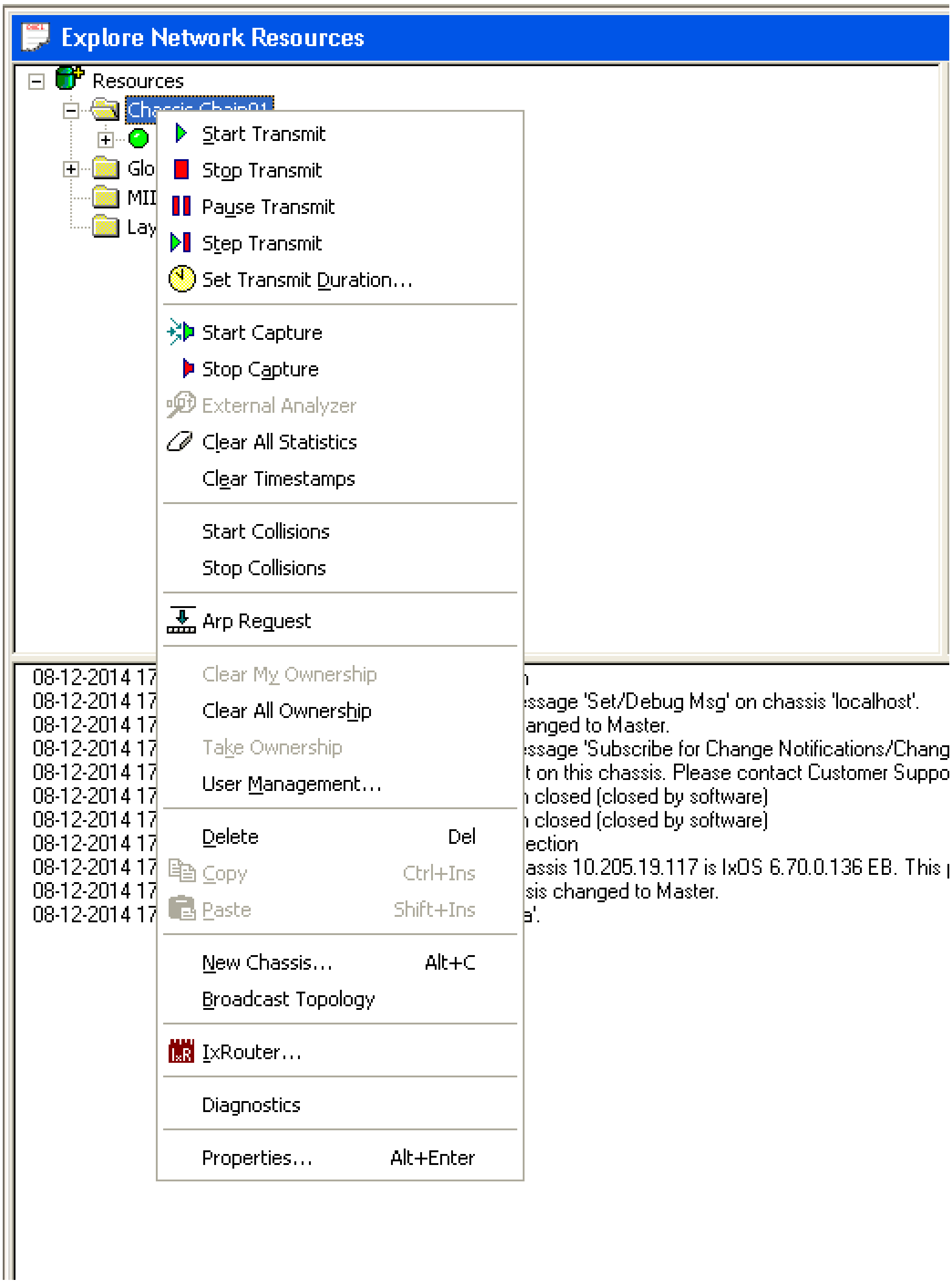
The term *Chassis* corresponds to a single Ixia chassis which holds multiple load modules. See the *Ixia Platform Reference Manual* for a list of chassis and their capabilities. One or more cards (load modules) are listed below the chassis name in the Resources tree. The IxExplorer software obtains the card type from the card itself and displays it within the tree and elsewhere.

The level of the chassis in the tree is shown in the following figure:, along with the pop-up menu available by right-clicking *Chassis*.

Tree Operations

Chassis chain tree operations for a chassis are accessed by right-clicking the Chassis Chain folder. A menu is displayed, as shown in the following figure:

Figure:Chassis Level of the Explore Network Resource Window



The operations available at the chassis level of the tree are described in the following table. Port operations to all ports on all cards in the chassis.

Table:Chassis Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand or contract tree elements beneath the current level.
Start Transmit		Starts the transmission of data.

Operation	Keys/Shortcut	Description
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A *Start Transmit* or *Step Transmit* operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted.
Set Transmit Duration		Sets a specific time period for transmission. Selecting this icon opens the *Set Transmit Duration* dialog, as described in *Set Transmit Duration*.
Start Capture		Enables the start of data capture operations.
Stop Capture		Disables data capture operations for all ports on all cards on the selected chassis.
External Analyzer		Launches a third party packet analyzer. The type of analyzer launched is determined by the settings in the *External Analyzer tab*, as described in *External Analyzer Option*. This button is only active when the analyzer type is specified in *External Analyzer* tab.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations* for details.
Clear Timestamps		Clears the global time value used in timestamps which may be included in each frame. Refer to Instrumentation Box for details.
Reset Sequence Index		When Sequence checking is in use, this resets the sequence number for the selected ports back to 0. Refer to the section on Sequence Checking Operation in the 'Theory of Operation' chapter of the Ixia Platform Reference Manual for more information.
Start Collisions		Enables collision generation for received data, if programmed for the port and enabled.
Stop Collisions		Stops collision generation.
Send ARP Request		Send an ARP packet requesting

Operation	Keys/Shortcut	Description
		addresses. The first IP address found in the streams for each port is used for the ARP request.
Enable		Enables or disables the chassis. A chassis may be automatically disabled if it runs a version of the HAL or IxServer software which is incompatible with the IxExplorer operation.
Clear My Ownership		The current user's ownership for all ports owned by the user in the selected chassis is cleared.
Clear All Ownership		The ownership for all ports in the selected chassis is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with all ports in the selected chassis. A warning message may be displayed if a port is owned by another user.
User Management		A dialog is displayed, allowing centralized, per chassis control of port ownership.
Delete	 Del	Deletes the selected chassis, after answering 'Yes' to a confirmation dialog.
Copy	 Crtl + Ins	Used with *Paste*. The item(s) selected (highlighted) are copied to the clipboard.
Paste	 Shift + Ins	Used with *Copy*. The item(s) copied to the clipboard in the 'Copy' operation are pasted into the selected (highlighted) location.
New Chassis	Alt+C	Displays the Chassis Properties dialog, so a new chassis can be added. The chassis is automatically named 'Chassis NN,' where NN is the next available chassis number. The chassis may be renamed. See Chassis.
Broadcast Topology		Broadcasts the current chassis chain topology, configuring the current attributes on the physical

Operation	Keys/Shortcut	Description
		chain.
IxRouter		Opens the IxRouter window. For more information on IxRouter window function for IxExplorer, see *IxRouter Window*. For more information on Protocols available, see the *IxNetwork User Guide*.
Rename	Second select on name or Rename pop-up option	Change the name of the chassis chain
Generate Tcl Script		Activates the ScriptGen feature and allows for the generation of Tcl configuration script. See ScriptGen for details.
Run Tcl Script		Allows to run a Tcl script froma list of scripts. See Run Tcl Script for more information.
Diagnostics		The Diagnostics Collection Utility collects log information from the chassis and from the client computer and wraps it into a comclicked (.zip) file named ixoslogs-YYYYMMDDHHMM.zip. The file can be sent to Ixia Technical Support. See Collect Diagnostic Logs.
Properties	Alt+Enter	Invokes the Chassis Chain Properties dialog. See *Chassis Chain Properties*.

Icon Colors

The color of the icon for the Chassis changes during system operation. The colors correspond to the states described in the following table:

Table:Chassis Status Icon States

Color	Meaning
Red	The chassis is not visible from the host running the IxExplorer software. This may be transitory as the software initializes, or due to an un-initialized, disconnected, or unpowered chassis. Also, the Ixia ‘server’ software running on the chassis’ processor may not be ready. A red icon can also mean that the IxServer component on the chassis is not properly licensed. See the Getting Started Guide for more information on licensing.
Yellow	The chassis has been found and information is being read from the

Color	Meaning
	chassis into the IxExplorer software. The chassis may not be used for transmission or capture yet. The indicator may remain yellow if there is a version mismatch between the chassis and the IxExplorer software.
Green	The chassis is fully initialized and available for transmission and capture.
Gray	The chassis is disabled in the chassis' properties sheet, or there is an incompatibility between the versions of IxExplorer software, IxServer software, or HAL software.
Purple/Clear	The chassis and client have mismatching software, and cannot connect. The icon becomes purple when selected, and clear when not selected.
Half Green/Half White	The chassis and client have mismatching software, but still can connect. This occurs for minor software mismatches (in the case of a service pack update).
Concentric Circles around any icon	The chassis is operating using GPS timing.

Chassis Detail Data

The chassis Details view shows the cards contained in the selected chassis, as shown in the following figure. See *Cards for details on how to modify these properties.*

The elements of the chassis Details view are described in the following table.

Table:Detail Data for Chassis

Column	Description
Name	The card number within the chassis.
Type	The type of card. See the *Ixia Platform Reference Manual* for a list of cards and their characteristics.
Hardware Version	The hardware version number of the card.

Chassis Properties

The *Chassis Properties* dialog allows to modify some of the global chassis properties through several tab pages. The dialog is accessed by right-clicking a Chassis icon and selecting *Properties*. The tab pages included in the dialog are:

- *Chassis Poperties—General*
- *Chassis Properties-Time Source*
- *Chassis Properties—Safety Features*
- *Chassis Properties-Logging and Alerts*
- *Chassis Properties—IxRemoteIp*
- *Chassis Properties—Virtual Ports*

The *Chassis Properties* dialog is shown in *Figure:Chassis Properties Dialog*.

Chassis Properties—General

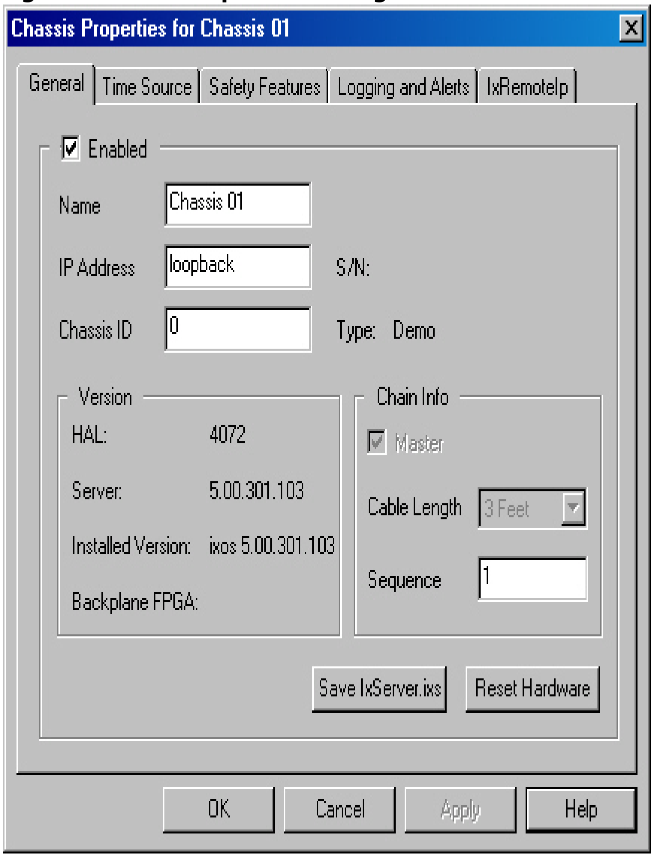
The **General** tab is used to set basic chassis information such as the chassis name, IP address, and ID number in the chassis chain. It is accessed by right-clicking a **Chassis** icon, selecting **Properties** in the menu, and then selecting the **General** tab (this is the default tab displayed).

NOTE This tab page is also displayed when adding a new chassis to a chassis chain. However, only the Name and IP Address fields become active. Further chassis information must be entered after the chassis is added to the chassis chain.

CAUTION If the chassis is part of a chassis chain, it is very important to correctly configure the Chassis Info, to avoid undesired results and timing measurement errors.

The **General** tab is shown in *Figure:Chassis Properties Dialog*.

Figure:Chassis Properties Dialog



The fields and controls in this dialog are described in the following table.

Table:General Chassis Properties Dialog

Field/Control	Description
Enabled	Enables or disables the chassis. A chassis may be automatically disabled if it runs a version of the IxHAL or IxServer software which is incompatible with the IxExplorer operation.
Name	The name of the chassis in the chassis chain.
IP Address	The IP address or computer name assigned to the chassis itself.

Field/Control	Description
Chassis ID	This is the assigned ID of the chassis. It is an arbitrarily assigned number and is used in the timestamp that may be added to transmitted packets. The chassis ID should be unique among all of the chassis in a chassis chain.Instrumentation Box for the process of using the chassis ID as part of a timestamp.
S/N	(Read-Only) The serial number of the chassis.
Type	(Read-Only) The type of chassis. See *Ixia Platform Reference Manual* for a list of chassis and capabilities.
HAL Version	(Read-Only) The software version and build number of the HAL software.
Server Version	The IxServer version.
Installed Version	Installed version of IxOS software.
Backplane FPGA Version	The Backplane FPGA version.
Master	(Read-only) If set, this indicates that this chassis is at the head of a chassis chain. A chassis is a master based on where the time source is coming from. • The chassis is in synchronous mode and no clock cable is connected to the Sync In port. • The chassis is configured to get time from a GPS or CDMA time source. A chassis is a subordinate (not a master) when it has a Sync In cable from another chassis. Available options are: • Master-CDMA • Master-GPS • Master-Internal • Slave
Cable Length	(Read-only) For all but the Master Chassis, this should be set to the length of Ixia-supplied cable which connects this chassis to the previous chassis in the chain. The choices are in increments of three feet. Pick the value to match the length of cable used. CAUTION Sync cables longer than six feet are not supported. Use at your own risk.
Sequence	This indicates where this chassis is placed in the physical chassis chain. NOTE Sequence numbers must be unique in a daisy chain. Within a daisy chain, there cannot be duplicate sequence numbers. The master chassis must have the smallest sequence value in the physical chain. The order of sequence numbers must match the order of chassis (up to 4294967295). The numbers do not have to be sequentially contiguous (1, 2, 3, and so on.) but they must be sequentially increasing in value (1, 5, 8, and so on.).

Field/Control	Description
	NOTE Example of an invalid sequence: 5, 1, 8 (invalid because the master must be the smallest value in the sequence).
Save IxServer.ixs	When clicked, saves the current IxServer configuration to an IxServer.ixs file on the server. The `IxServer.ixs` file is saved automatically when there is a orderly shutdown of IxServer. It may also be saved manually, by using this button, to ensure backup of the configuration without having to shut down the system, such as in service monitoring situations. If some unexpected shutdown occurs, the IxServer configuration is reloaded from the saved *.ixs* file on power-up.
Reset Hardware	When this button is clicked, the chassis resets all the hardware, restarts port CPU, does local processor test, and rewrites the streams. This action does not modify existing port/stream configuration.
Card	Enter the card number of the load module you want to force hot-swap.
Force Hotswap	Simulates the physical removal and reinsertion of a load module by turning off the power on the load module and then bringing it back up 5 seconds later.
Power Management	Select the check box to monitor the cards for inactivity. You can enter the time in minutes after which you want to automatically power off individual cards. The field is enabled when you select the **Power Management** check box.

CAUTION 1. Place your cursor in the area of the text frame ABOVE this cell.

2. Hold down the SHIFT key and press the LEFT ARROW key twice.

3. Copy the selected items, then go back to the body page and paste them in.

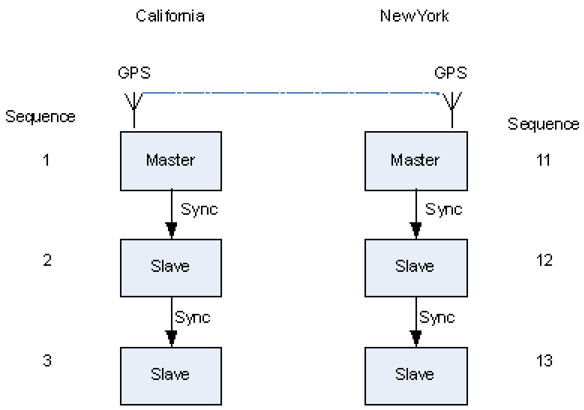
Virtual Chassis Chains

A virtual chassis chain consists of two or more physical chains that are linked together to operate as one. For example, there might be a physical chain in California (with a master and two subordinate chassis) and another physical chain in New York. The two physical chains are linked through a GPS module or by using an Ixia 250 chassis with built-in CDMA. To configure this virtual chassis chain properly, the sequence numbers might have the array shown in the following figure.

Figure:Virtual Chassis Chain Example

Physically, the three California chassis are connected, so their sequence numbers must reflect this fact. The same applies to the three chassis in New York. The sequence numbers need to indicate which chassis is the master (in each physical chain).

NOTE The sequence numbers for the different chains cannot be interleaved. In the example above, the California sequence cannot be 1, 2, 14 because '14' would be part of the range of New York sequence numbers.



Chassis Properties-Time Source

The *Time Source* tab provides facilities that allow for synchronization of independent Ixia chassis and chassis chains located anywhere in the world. The tab is accessed by right-clicking the *Chassis* icon, selecting the *Properties* command, and selecting the *Time Source* tab in the *Chassis Properties* dialog.

Accurate timing can be used to obtain valid latency and other measurements in a live global network. Four scenarios are possible:

- **Independent operation**: Each Ixia chassis chain generates its own timing.
- **Ixia 100**: A one-slot chassis which includes a GPS or CDMA receiver.
- **Ixia AFD1 GPS Receiver**: A chassis is attached to the external Ixia GPS Receiver.
- **Metronome**: Provides time synchronization from multiple external time delivery sources.

IxClock – a separate module which generates a timing signal from multiple sources. It must be connected to an Ixia 400 or 1600 chassis. It is programmed through the *Chassis Properties* dialog of the controlling chassis.

NOTE When chassis are linked together into a chassis chain by sync cables, the time source selected for the Master in the chain is the basis for the timing of ALL chassis in that chain. Any time source selected for an individual subordinate chassis is overridden by the timing supplied from the master chassis.

In the case of the Ixia AFD1 GPS receiver, it functions as the 'master' timing source.

The timing choices are the following:

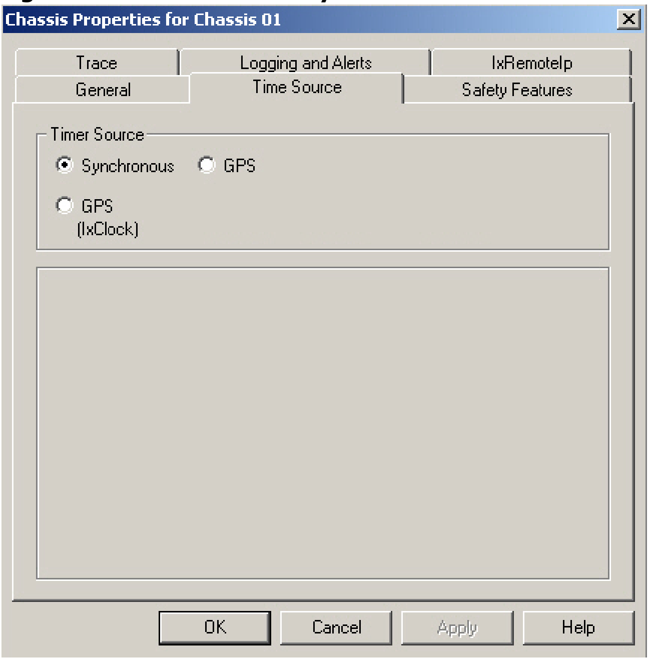
- *Synchronous*—Internal synchronization. If a chassis is used in a stand-alone manner or as master in a chassis chain, it may generate its own start signal. In general, there is insufficient timing accuracy between timing masters for measurements over distance. This is also known as synchronous timing.
- *GPS*—For use with the Ixia 100 GPS-equipped chassis or the Ixia AFD1 GPS receiver. The Ixia 100 requires connection to an external GPS antenna to 'capture' multiple GPS satellites. It maintains accuracy of less than 150 nanoseconds.
  This is also the options used for the external Ixia GPS Receiver.
- *CDMA*—The Code Division Multiple Access (CDMA) cellular network transmits an accurate time signal. It maintains an accuracy of less than 100 microseconds.

- *Metronome*—Metronomes provide time synchronization from multiple external time delivery sources like GPS, ToD, BNC and PTP, and translating that time into the IXIA time delivery interface.

Synchronous

The *Time Source* tab of the *Chassis Properties* dialog is shown in the following figure, with the Synchronous option selected.

Figure:Time Source Tab—Synchronous



The fields and controls in this tab are described in the following table.

Table:Time Source Tab—Synchronous

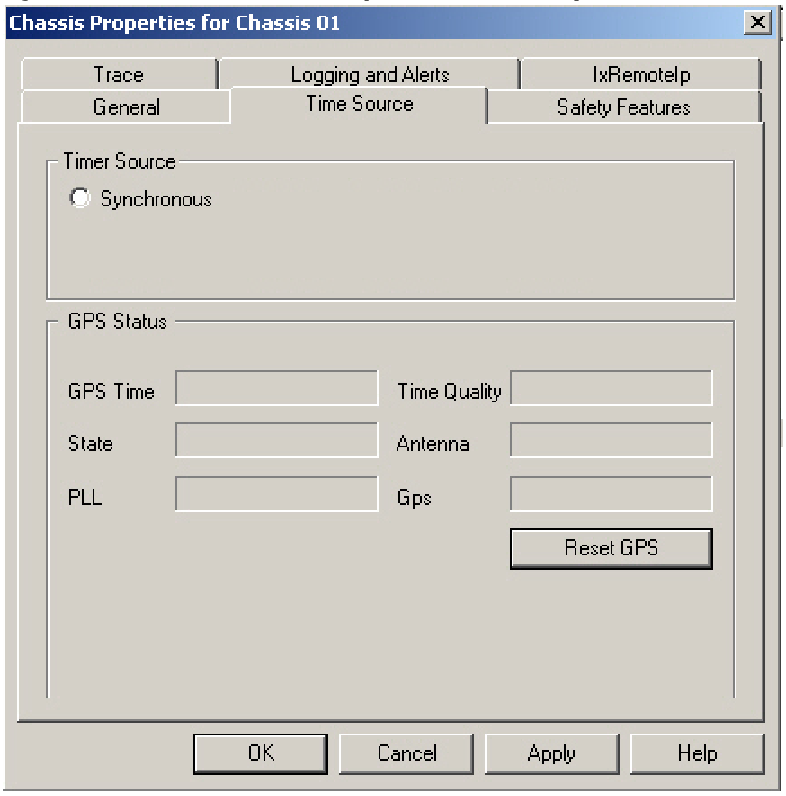
Section	Field/Control	Description
Time Source		Indicates which of the possible timing synchronization sources to use for this chassis.
	Synchronous	Uses the internally generated clock, or clocked from a sync-in line. No global synchronization is performed.
	GPS	For use with IXIA 100 GPS equipped chassis or IXIA AFD1 GPS receiver only, indicates the use of high-precision GPS signals for synchronization.
	PC Clock	Use the clock associated with the chassis' operating system. Depending on the available hardware or software, this may be highly inaccurate.
	CDMA	For use with IXIA 100 CDMA equipped chassis only, indicates the use of the Code Division Multiple Access (CDMA) cellular network which transmits an accurate time signal.

Section	Field/Control	Description
	GPS (IxClock)	Timing is provided autonomously by the IxClock unit by virtue of a permanently connected GPS or a temporary GPS connection reinforced by a rubidium oscillator.
	1PPS (IxClock)	Time of day is set by the GPS unit and the time is maintained by a one pulse per second signal connected to a IxClock connector.
	T1 (IxClock)	Time of day is set by the GPS unit and the time base is maintained by a T1 signal connected to an IxClock connector.
	E1 (IxClock)	Time of day is set by the GPS unit and the time base is maintained by an E1 signal connected to an IxClock connector.

GPS

This option is for use with the IXIA 100 GPS-equipped chassis or the external Ixia AFD1 GPS receiver, and indicates the use of high-precision GPS signals for synchronization. The GPS options of the *Time Source* tab are shown in *Figure:Time Source Tab—GPS (Ixia 100 Chassis)* and *Figure:Time Source Tab—GPS (Ixia AFD1 GPS Receiver).*

Figure:Time Source Tab—GPS (Ixia 100 Chassis)

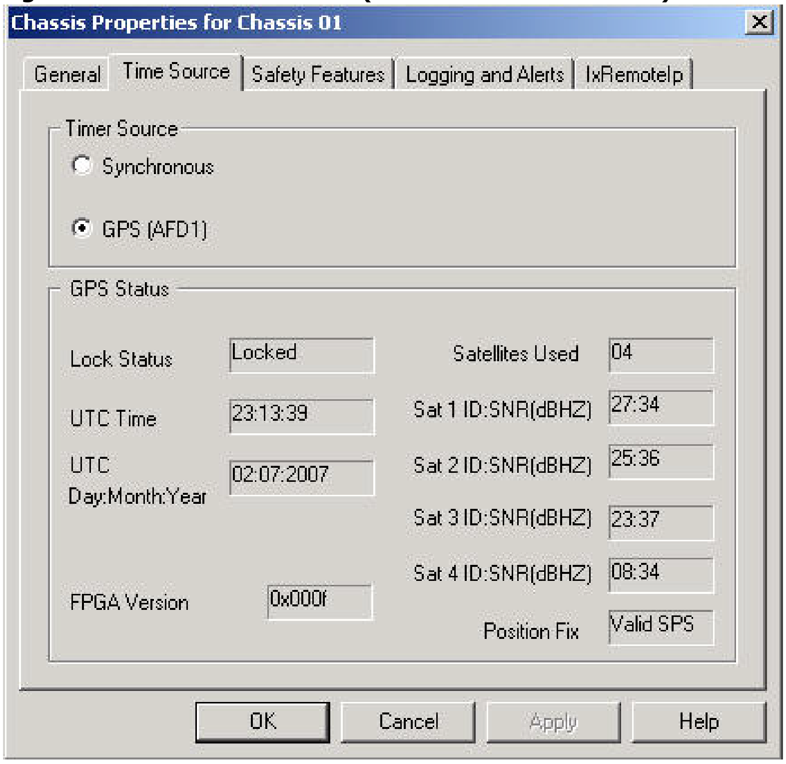


The fields and controls in this tab are described in the following table.

Table:Time Source Tab—GPS (Ixia 100 Chassis)

Section	Field/Control	Description
GPS Status		Indicates the status of the GPS unit. Some of these values are reflected in a series of lights on the front of the chassis. Refer to the *Ixia Platform Reference Manual* for details.
	GPS Time	The current time received from the GPS unit, or 'No Response' if nothing has been received from the GPS unit for a few seconds.
	State	The state of the GPS unit. This value must be 'Ready' or 'Searching' in order for GPS synchronization to be triggered.
	PLL	The state of the GPS's Phased Lock Loop. Either 'OK' or 'Unlocked.' The value must be 'OK' in order for GPS synchronization to be triggered.
	Time Quality	A value from 1 to 4 indicating the Stratum of the GPS connection. Each Stratum level indicates one connection removed from the GPS time source; thus, Stratum 1 is directly connected to a GPS source, while Stratum 4 is three connections removed. The time accuracy for each Stratum is as follows: • Stratum 1—within 100 ns of absolute GMT. • Stratum 2—within 1 us of absolute GMT • Stratum 3—within 10 us of absolute GMT • Stratum 4—within 100 us of absolute GMT
	Antenna	Select 'OK,' 'Open,' or 'Short.' The value must be 'OK' in order for GPS synchronization to be triggered.
	GPS	The state of the GPS unit, either 'Locked' or 'Unlocked.' 'Locked' is displayed when enough satellites have been detected. The value must be 'Locked' in order for GPS synchronization to be triggered.
	Reset GPS	Sends a reset signal to the GPS hardware, causing it to reacquire satellites.

Figure:Time Source Tab—GPS (Ixia AFD1 GPS Receiver)



The fields and controls in this tab are described in the following table.

Table:Time Source Tab—GPS (Ixia GPS Receiver)

Section	Field/Control	Description
GPS Status		Indicates the status of the GPS unit. Some of these values are reflected in a series of lights on the front of the chassis. Refer to the *Ixia Platform Reference Manual* for details.
	Lock Status	Either locked or unlocked. Locked means that the Chassis is in synchronization with the time source provided by the GPS receiver. In the locked state, the chassis can be added to a Virtual chassis chain consisting of one or more GPS locked chassis and other chassis connected to these chassis as subordinates. Unlocked means the GPS interface is active but the GPS card or external GPS chassis is not able to determine correct time due to lack of access to the GPS satellite system. In the Unlocked state, the virtual chain will not operate when the chassis is connected.
	UTC Time	The current GPS time.
	UTC Day:Month:Year	The current GPS date.

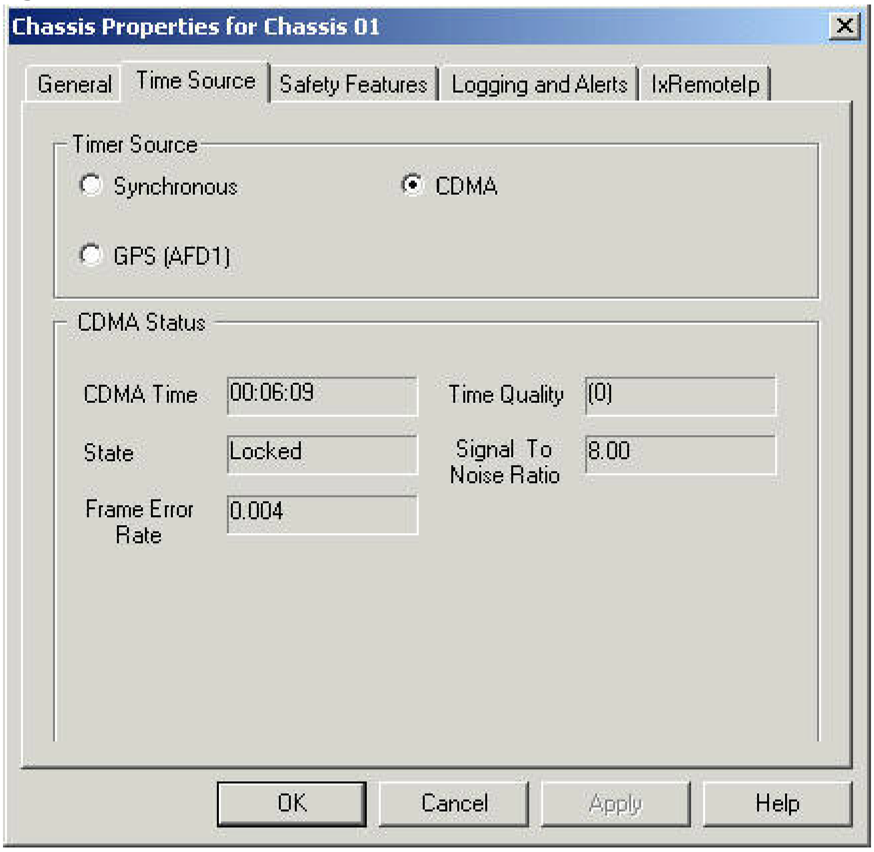
Section	Field/Control	Description
	FPGA Version	The FPGA version of the GPS receiver.
	Satellites Used	The number of satellites being used for time synchronization
	Sat 1 ID - Sat 4 ID	The list of the top four satellites in use. The top four satellites are determined by the highest signal to noise ration.
	Position Fix	Displays the type of GPS being used. Possible values are: • Invalid • Valid SPS • Valid DGPS • Valid PPS

CDMA

This option is for use with the IXIA 100 CDMA-equipped chassis only. CDMA (Code Division Multiple Access) cellular base-stations effectively act as GPS repeaters. The IXIA 100-CDMA has as built-in CDMA receiver with a small antenna on the back of the chassis that receives the CDMA signals passively (it is not necessary to subscribe to any service) and decodes the embedded time signal. Using this approach, the IXIA 100 can be time-synched to GPS with no external antenna on the roof.

The *Time Source* tab with the CDMA option selected is shown in the following figure:

Figure:Time Source—CDMA



The fields and controls for these sections of the dialog are described in the following table.

Table:Time Source Properties Dialog

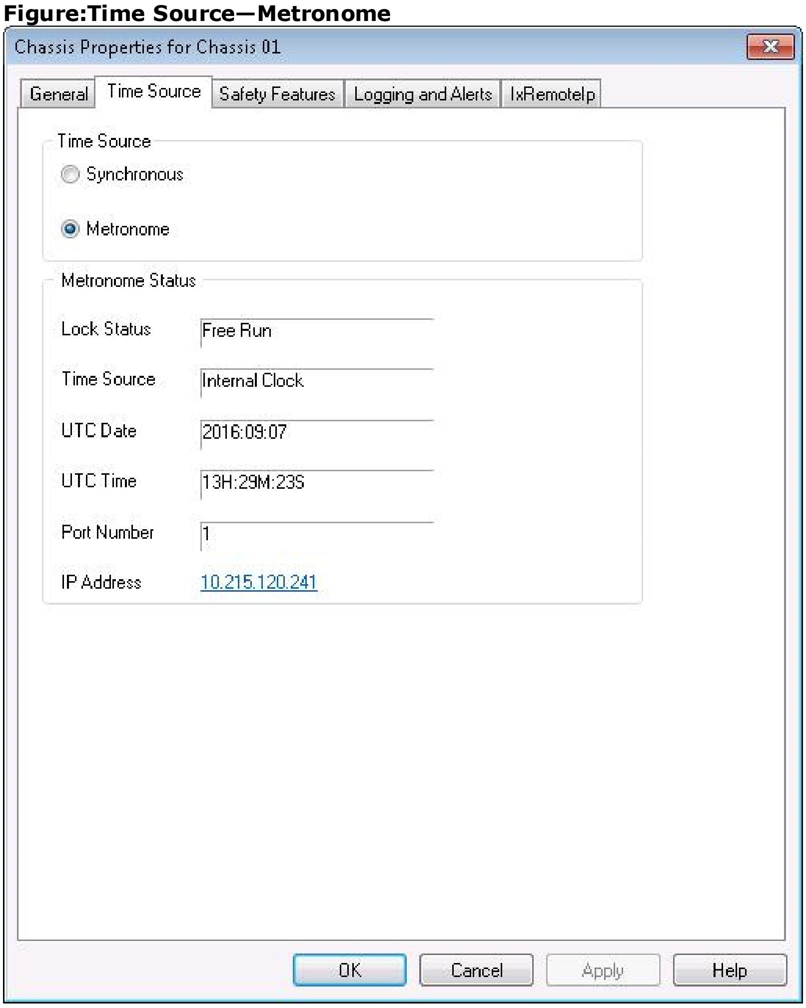
Section	Field/Control	Description
CDMA Status		For use with the Ixia 100 Chassis only. Indicates the status of the CDMA unit. Some of these values are reflected in a series of lights on the front on the chassis. Refer to the *Ixia Platform Reference Manual* for details.
	CDMA Time	The current time received from the CDMA unit or ‘No Response’ if nothing has been received from the CDMA unit for a few seconds.
	State	The state of the CDMA unit, which is one of the following: Acquiring, Signal Detected, Code Locking, Carrier Locking, Locked, or Unknown. The value must be ‘Locked’ in order for CDMA synchronization to be triggered.
	Frame Error Rate	The Frame Error Rate for the Sync Channel. The range is 0.000 to 1.000, where higher values indicate poorer quality. Higher values correlates with lower Signal to Noise ratios.
	Time Quality	A value from 0 to 5 indicating the time quality received from the CDMA unit. 0 is the best quality. A value of 0 or 1 must be displayed in order for CDMA-based synchronization to be triggered.
	Signal to Noise Ratio	The carrier Signal to Noise Ratio (SNR). The typical range is from 2.5 to 11.0, in terms of the Sync Channel symbol rate bandwidth. A higher value is better.
	Reset CDMA	Sends a signal to the CDMA unit to restart the unit and reacquire the CDMA signal.

Metronome

This option is used with the XGS2-SD, XGS2-HS, XGS12-SD and XGS12-HS chassis. Every metronome in the system can provide timing and triggers to eight chassis.

The *Time Source* tab with the Metronome option selected is shown in the following figure:

Figure:Time Source—Metronome



The fields and controls for these sections of the dialog are described in the following table.

Table:Time Source Properties Dialog

Section	Field/Control	Description
Metronome Status		Indicates the status of Metronome. Some of these values are reflected in a series of lights on the front of the chassis. Refer to the *Ixia Platform Reference Manual* for details.
	Lock Status	The status of the Metronome system clock. The possible states are: • Free run - Indicates that the system clock is currently not trying to discipline to any external time references. • Locking - Indicates that a time reference source switch has just taken place and the Metronome system clock is currently in the process of tracking the PLL to the external reference. • Frequency Locked - Indicates that the Metronome system clock is frequency

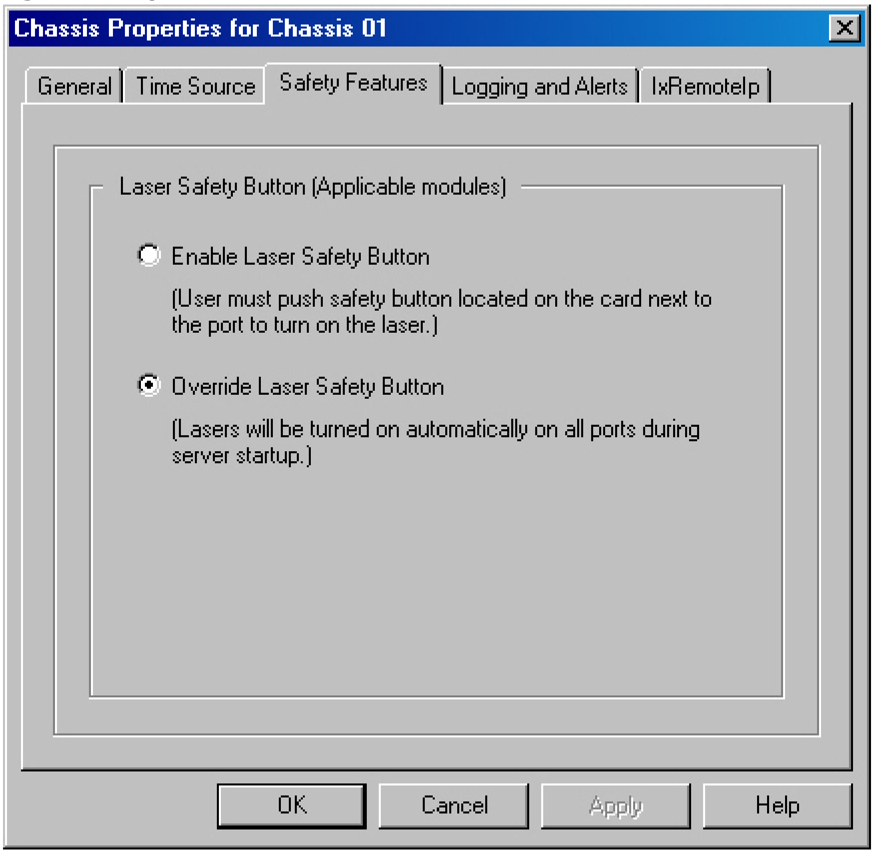
Section	Field/Control	Description
		locked to the external time reference. • Time Locked - Indicates that the Metronome system clock is time locked to the external time reference, which can be any external reference sources. • Holdover - Holds the previous locked clock source and prevents loss of timing.
	Time Source	The type of time synchronization source. Available options are: • Internal Clock • Sync In • GPS • BNC
	UTC Date	The current date from Metronome's clock source.
	UTC Time	The current time from Metronome's clock source.
	Port Number	The Sync Out port number on which the chassis is connected to the Metronome.
	IP Address	The IP address of the Metronome to which the chassis is connected.

Chassis Properties—Safety Features

The *Safety Features* tab controls the use of a safety feature for high powered fiber optics cards. It is accessed by right-clicking the *Chassis* icon in the Tree view, selecting the *Properties* command, and selecting the *Safety Features* tab in the *Chassis Properties* dialog.

The *Safety Features* tab is shown in the following figure:

Figure:Safety Features Tab



The fields and controls of this tab are described in the following table:

Table:Safety Properties Tab

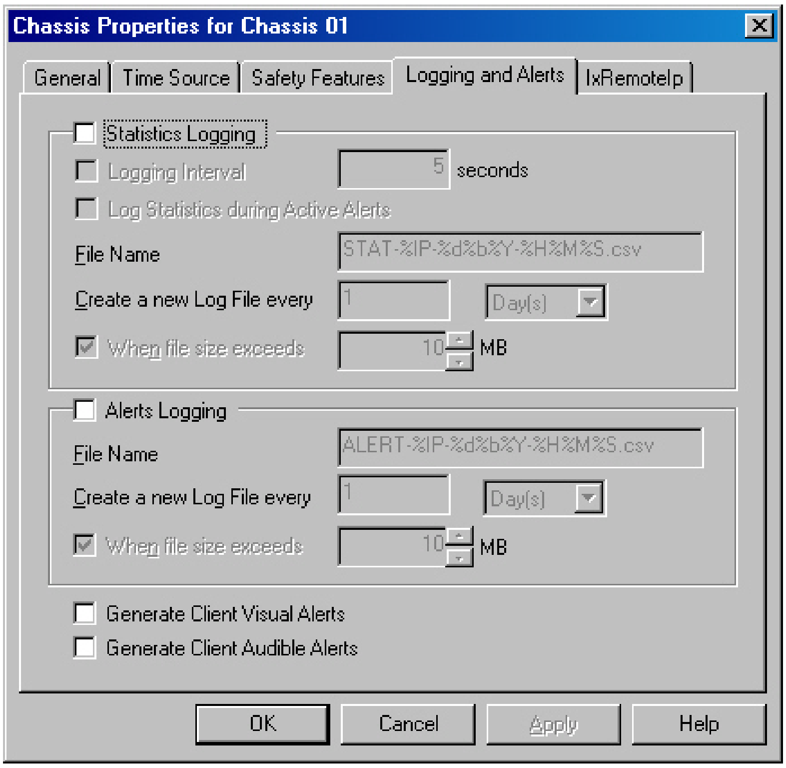
Section	Fields/Controls	Description
Laser Safety Button	Enable Laser Safety Button	You must push the safety button located on the card next to the port to turn on the laser.
	Override Laser Safety Button	The lasers are turned on automatically on all ports of this chassis during server startup.

Chassis Properties—Logging and Alerts

The *Logging and Alerts* tab of the *Chassis Properties* dialog controls the use of statistics logging and alerts for the chassis. The tab is accessed by right-clicking the *Chassis* icon in the Tree view, selecting the *Properties* command, and selecting the *Logging and Alerts* tab in the *Chassis Properties* dialog.

The Logging and Alerts tab is shown in the following figure:

Figure:Logging and Alerts Properties Dialog



Four basic features are enabled in this dialog:

- **Statistics Logging**:Logging of selected statistics at regular intervals.
- **Alerts Logging**: Logging of selected statistics while the statistics is outside of a defined range of values.
- **Generate Client Visual Alerts**:Colored highlighting of statistics that are being monitored. Highlighting occurs within Statistic Views.
- **Generate Client Audible Alerts**: Beeping of the client's PC when an configured alert has been signalled.

The theory of operation for each of these features is described in the Statistics Logging and Alerts sections of the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*. The specification of statistics to be logged or alerted is described in *Statistics Logging and Alerts*.

The fields and controls in this dialog are described in the following table:

Table:Logging and Alerts Dialog

Section	Field/Control	Description
Statistics Logging		If this check box is selected, Statistics Logging is enabled for the chassis.
	Logging Interval	If this check box is selected, then statistics are logged at a regular interval. The value entered in the field (in seconds), is the logging interval. If the check box is cleared, then no repetitive logging occurs.
	Log Statistics during Active Alerts	If this check box is selected, then statistics logging occurs during active alert periods.

Section	Field/Control	Description
		That is, while a particular statistic generates an alert, its value is logged to the log file. The logging rate is between one and two times per second, depending on the card type.
	File Name	Sets the file name of the statistics log file. *File Naming Conventions* for further details.
	Create a new Log File every	This setting indicates how often to create a new log file to hold logged data. Set this time to a value that helps to find appropriate log files on the chassis.
	When file size exceeds	If this check box is selected, when the file size value (in MB) entered in the field is reached, it triggers the creation of a new log file. Set this value to a size that is convenient for copying, viewing, and archiving.
Alerts Logging		If this check box is selected, Alerts Logging is enabled for this chassis.
	File Name	Sets the file name of the alert log file. *File Naming Conventions* for further details.
	Create a new LogFile every	This setting indicates how often to create a new log file to hold logged data for alert conditions. Set this time to a value that helps to find appropriate log files on the chassis.
	When file size exceeds	If this check box is selected, when the file size value (in MB) entered in the field is reached, it triggers the creation of a new log file. Set this value to a size that is convenient for copying, viewing and archiving.
Generate Client Visual Alerts		If this check box is selected, visible alerts are generated on the client station(s). Alerts are sent to all clients connected to any chassis in the chassis chain.
Generate Client Audible Alerts		If this check box is selected, audible alerts are generated on the client station(s). Alerts are sent to all clients connected to any chassis in the chassis chain.

File Naming Conventions

The file names used for either the statistics log file or alert log file may be formatted to include information related to the date, time and other parameters. These values are preceded by a '%' symbol and are described in detail in *Table:Event Logging Properties*. The file name should contain the name of the chassis or some other distinguishing string so that log files from multiple chassis may be copied and coordinated in a single disk directory. In the example shown in the following figure, the name of the chassis is used. A

.csv extension is always added to the name of the file, which should not contain a dot ('.') character.

The log files may be placed on the chassis' local disk or on a disk on the local network associated with the chassis. The different methods for specifying file location are shown in the following table:.

Table:File Specification Formats

File Specification	Description
Simple file name: *Stat-regression3-%d%b%Y-%H%M%S*	The file is placed on the chassis' disk in the same directory used for the installation of the Ixia software, usually *c:\Program Files\Ixia\IxOS\version X*.
Absolute path name: *d:\logs\Stat-regression3-%d%b%Y-%H%M%S*	The file is placed at the absolute location on the chassis' disk. The file specification must start with a <drive letter> and a colon (':').
Network path name: *\\server\share\logs\Stat-regression3-3-%d%b%Y-%H%M%S*	The file is placed on the network location indicated by the Microsoft UNC (Universal Naming Convention) specification. Proper file sharing privileges must have been set up on the target server.

Logged File Format

Statistics files are formatted with commas separating all fields. The first line of the file contains headings that describes the fields in the first line of statistics logged for a port. If each port logs the same statistics, then the headings describes all of the logged data. If not, then some other means of interpreting the logged data must be used.

Figure:Statistics Log File Sample shows an example of a statistics log file, as interpreted by Microsoft Excel. Excel reads the file and uses the commas embedded in the file to define new cells.

Figure:Statistics Log File Sample

	A	B	C	D	E	F	G	H
1	Time (UTC)	Chas	Card	Port	Frames Sent Rate	Moving Average	Valid Frames Received Rate	Moving Average
2								
3	08Nov2000-22:18:33	0	4	1	0	0	0	0
4	08Nov2000-22:18:33	0	4	1	1135090	94591	15514098	1292841
5	08Nov2000-22:18:34	0	4	1	2087651	260679	44750392	4914303
6	08Nov2000-22:18:34	0	4	1	2087788	412938	73989372	10670559
7	08Nov2000-22:18:34	0	4	1	3035985	540685	2087753	552505
8	08Nov2000-22:18:35	0	4	1	2087747	680442	132462844	27889931
9	08Nov2000-22:18:35	0	4	1	2087881	797728	161699856	39040758
10	08Nov2000-22:18:36	0	4	1	2087306	905193	190931080	51698284
11	08Nov2000-22:18:36	0	4	1	2087478	1003716	220166966	65737341
12	08Nov2000-22:18:36	0	4	1	2087700	1094048	248556762	80972292

Statistics values which display as 'Up' and 'Down' in the Statistic View is shown as values of '1' and '0,' respectively. Each logged value or rate is followed by its Moving Average value.

Alert files are also formatted with commas separating all fields. The first line of the file contains headings used for all alert log entries.

Figure:Alert Log File Sample shows an example of an alert log file, as interpreted by Microsoft Excel.

Figure:Alert Log File Sample

	A	B	C	D	E	F	G	H	I	J
1	Time (UTC)	Chas	Card	Port	Stat	Rate	State	Value	Condition	Action
2										
3	08Nov2000-23:20:18	0	4	1	23	1	2	4	CRC Errors Rate > 0	Set Log| Visual| Audible
4	08Nov2000-23:20:18	0	4	1	17	1	1	1345254	Valid Frames Received Rate < 2000000	Set Log| Visual| Audible
5	08Nov2000-23:20:18	0	4	1	23	1	3	0	CRC Errors Rate OK	Set Log| Visual| Audible
6	08Nov2000-23:20:18	0	4	1	17	1	3	2087904	Valid Frames Received Rate OK	Set Log| Visual| Audible
7	08Nov2000-23:20:18	0	4	1	12	1	2	7219	Path REI (FEBE) Rate > 0	Set Log| Visual| Audible
8	08Nov2000-23:20:18	0	4	1	13	1	2	3	Path BIP (B3) Rate > 0	Set Log| Visual| Audible
9	08Nov2000-23:20:18	0	4	1	8	1	2	459509	Line REI (FEBE) Rate > 0	Set Log| Visual| Audible
10	08Nov2000-23:20:18	0	4	1	123	1	3	0	Section BIP Severely Errored Seconds Rate OK	Set Log| Visual| Audible
11	08Nov2000-23:20:19	0	4	1	12	1	3	0	Path REI (FEBE) Rate OK	Set Log| Visual| Audible

The columns used in alert entries are described in *Table:Alert Log Entry Columns*.

Table:Alert Log Entry Columns

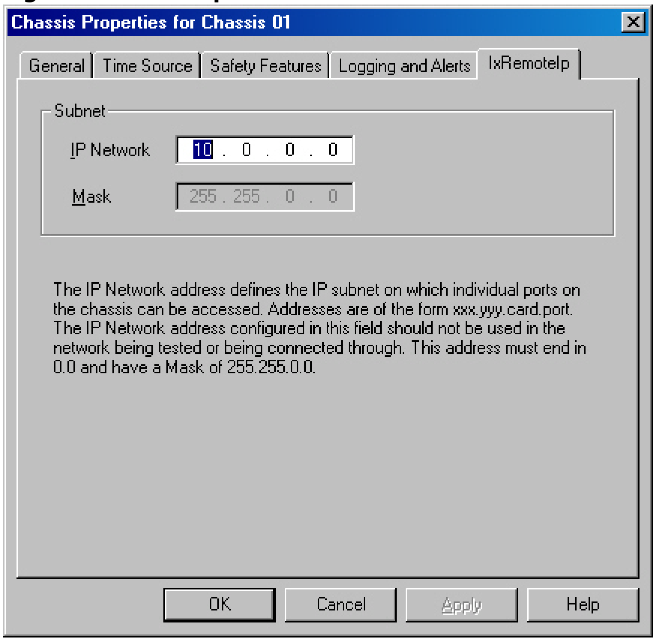
Column	Description
Time (UTC)	The time at which the alert happened.
Chas Card Port	The chassis ID, card number, and port number that generated the alert.
Stat	The Ixia internal statistics number, which is also shown in the condition column.
Rate	If the alert occurred for a **count** variable, then '0' is displayed. If the alert occurred for a **rate** variable, then '1' is displayed.
State	The state associated with the alert event. One of: • **0-clear**. The alert has been acknowledged. • **1-minimum threshold alert**. The value was below the minimum threshold. • **2-maximum threshold alert**. The value was above the maximum threshold. • **3-disabled**. The alert was disabled by a client.
Value	The value of the statistics that generated the alert.
Condition	The alert condition that was triggered.
Action	The action that was performed as a result of the alert. One or more of: • **Log**—Log entries were added to the statistics file for the port while the alert condition was in effect. • **Visual**—A visual alert notification was sent to all connected clients. • **Audible**—An audible alert notification was sent to all connected clients.

Chassis Properties—IxRemoteIp

IxRemoteIp is a feature of a chassis that works with some card types. It provides a means by which individual Ixia chassis may be referenced by individual IP addresses for Ixia products. The tab is accessed by right-clicking the *Chassis* icon in the Tree view, selecting the *Properties* command, and selecting the *IxRemoteIp* tab in the *Chassis Properties* dialog.

The *IxRemoteIp* tab is shown in *Figure:IxRemoteIp Tab*.

Figure:IxRemoteIp Tab



The IP Network address and network mask indicate the IP subnet for the ports on the chassis, and may be configured by you.

The IP Network address that you enter is stored in the registry into a registry key. When you upgrade to a new IxOS version, this address is read from the registry and hence the address is retained between IxOS versions.

NOTE Protocol interfaces should not be created in the same subnet as the IxRemoteIP (the IxRemoteIP subnet default is 10.0.0.0/16). Creating protocol interfaces in this subnet causes problems and odd behavior.

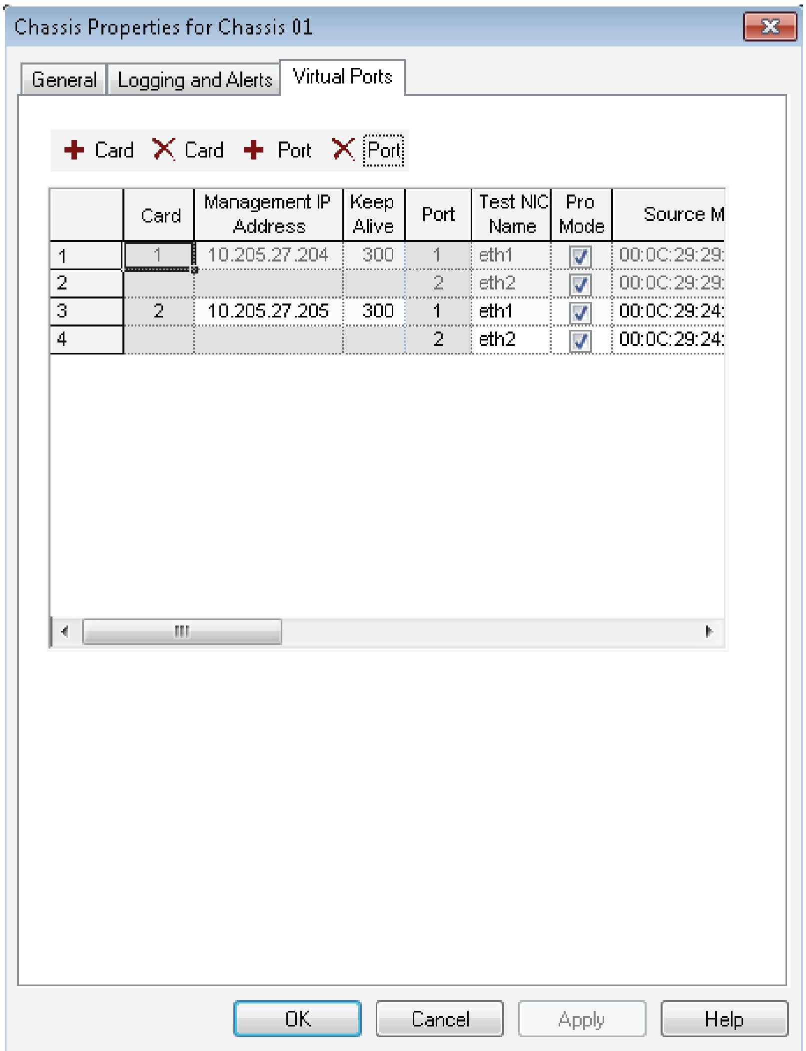
Protocol Interface Wizard Types for more information on creating protocol interfaces.

Chassis Properties—Virtual Ports

The *Virtual Ports* tab of the *Chassis Properties* dialog is available for virtual machines and is accessed by right-clicking the *Chassis* icon in the Tree view, selecting the *Properties* command, and selecting the *Virtual Ports* tab in the *Chassis Properties* dialog.

The *Virtual Port* tab is shown in the following figure:

Figure: Virtual Ports Dialog



The fields and controls in this dialog are described in the following table:

Table: Virtual Ports Dialog

Section	Field/Control	Description
	Card	The card number.
	Management IP Address	Management IP address of the Linux machine with the IxVM software agent installed.
	Keep Alive	The keep-alive timeout in seconds. Each IxVM card has a keep-alive mechanism between the virtual chassis and the virtual card. In case either of these two components do not send or receive a keep-alive message for a certain amount of time, then the virtual card will disconnect from the virtual chassis.
	Port	The name of the port on the IxVM card to be used for traffic generation and measurement
	Test NIC Name	Name of the virtual interface that will be

Section	Field/Control	Description
		used as a traffic generator. Virtual interface must be created before adding the port.
	Pro Mode	Denotes the promiscuous or non-promiscuous mode in which a virtual port is added to a virtual card.
	Source MAC	The first source MAC address to be generated for the stream.
	Link MTU	MTU value of test interface from a virtual machine. The minimum value is 1500 and the maximum value is 9000 and should be changed mainly when there are control plane frames bigger than 1500.
	Ext. Type	Select the extended card type in the list. Options include the following: • IxVM • RackSim
	Line Speed (Mbps)	Select the line speed. Options include the following: • 100MBPS • 1000MBPS: 1 Gb speed • 10000MBPS: 10 Gb speed
+ Card		Adds a virtual load module.
X Card		Removes a virtual load module.
+ Port		Adds a port to the load module.
X Port		Removes a port from the load module.

You can add or remove a virtual load module and also add a port to load module by clicking the respective Card and Port buttons.

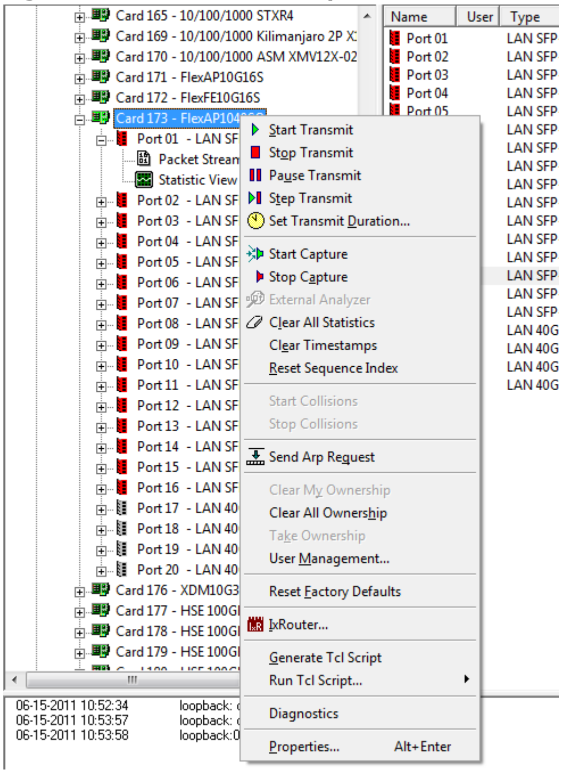
Cards

A card, also referred to as an interface load module, holds one or more ports. Each port on a card generally has the same characteristics. Cards always appear in the tree below a chassis and always contain Port definitions. The population of ports beneath a card happens automatically as the software queries the chassis for its contents. The position of the cards in the tree is shown in *Figure:Card Level of the Explore Network Resource Window* along with the pop-up menu available by clicking the right mouse button.

Tree Operations

The tree operations for a card are accessed by right-clicking the Card icon in the Tree view. The menu is shown in *Figure:Card Level of the Explore Network Resource Window*.

Figure:Card Level of the Explore Network Resource Window



The operations available at the card level of the tree are described in *Table:Card Level Operations*. Port operations apply to all ports on the card.

Table:Card Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand or contract tree elements beneath the current level.
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A 'Start Transmit' or 'Step Transmit' operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted.
Set Transmit Duration		Sets a specific time period for transmission. Selecting this icon opens the *Set Transmit Duration* dialog, as described in *Set Transmit Duration*.
Start Capture		Enables the start of data capture operations. NOTE Capture feature is disabled in XDM10G32S load module.

Operation	Keys/Shortcut	Description
Stop Capture		Disables data capture operations. **NOTE** Capture feature is disabled in XDM10G32S load module.
External Analyzer		Launches a third party packet analyzer. The type of analyzer launched is determined by the settings in the *External Analyzer tab*, as described in *External Analyzer Option*. This button is only active when the analyzer type is specified in *External Analyzer* tab.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations* for details.
Clear Timestamps		Clears the global time value used in timestamps which may be included in each frame. Refer to *Instrumentation Box* for details.
Reset Sequence Index		When Sequence checking is in use, this resets the sequence number for the selected ports back to 0. Refer to the section on Sequence Checking Operation in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.
Start Collisions		Enables collision generation for received data, if programmed for the ports and enabled.
Stop Collisions		Stops collision generation.
Send ARP Request		Send an ARP packet requesting addresses. The first IP address found in the streams for each port is used for the ARP request. ARP must be enabled in the IxRouter window for at least one port on this card. **NOTE** ARP feature is not supported in XDM10G32S load module.
Clear My Ownership		The current user's ownership for all ports on the selected card owned by the user is cleared.
Clear All Ownership		The ownership for all ports on the

Operation	Keys/Shortcut	Description
		selected card is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with all ports on the selected card. A warning message may be displayed if a port is owned by another user.
User Management		A dialog is displayed, allowing centralized, per chassis control of port ownership.
Reset Factory Defaults		Resets the card to default factory card configuration, leaves one default stream (if applicable), and changes the card mode to the factory default (if applicable). NOTE Resetting the card to factory default settings will not clear the timestamps. To clear the timestamps, you have to click **Clear Timestamps** option.
IxRouter		Opens the IxRouter window. For more information on IxRouter window function for IxExplorer, *IxRouter Window*. For more information on protocols available, see the *IxNetwork User Guide*.
Generate Tcl script		Activates the ScriptGen feature and allows for the generation of Tcl configuration script. *ScriptGen* for details.
Run Tcl Script		Allows to run a Tcl script from a list of scripts. *Run Tcl Script...*or more information.
Diagnostics		Opens the Ixia Diagnostics Collection Utility dialog. You can collect log information from the chassis and from the client computer and wrap it into a comclicked (.zip) file named ixoslogs- YYYYMMDDHHMM.zip. See *Collect Diagnostic Logs*.
Properties	Alt + Enter	Opens a separate dialog for the properties related to the type of card in

Operation	Keys/Shortcut	Description
		use. See *Card Properties*.

Card Detail Data

For each port on the card the Details view shows the following elements in *Table:Detail Data for Card*, as shown in *Figure::Detail Data for Card*. See the section on *Ports* *for information on modifying these properties.*

Table:Detail Data for Card

Column	Description
Name	The port number within the card. The accompanying icon and color indicate the state of the port.*Ports* *for an explanation of the icons and colors.*
User	The login name of the user that has taken ownership of the port.
Type	The type of port. See *Ixia Platform Reference Manual* for a list of cards and their ports' characteristics.
Link State	Either up or down, depending on whether the port is connected to another device or not and an Ethernet link has been negotiated.
Line Speed	The data rate of the port(s) on the card.
Duplex Mode	(for Ethernet and Unframed BERT modules) Whether the port is operating in half or full duplex mode.
State	Running or not running. If you take ownership of the Port from IxExplorer or TCL, the *State* is 'Running'. If you do not take ownership or release ownership of ports, *State* and *Duration* are empty.
Duration	Duration shows the time of the current State in days / hrs / min format. See definition of *State*, above.

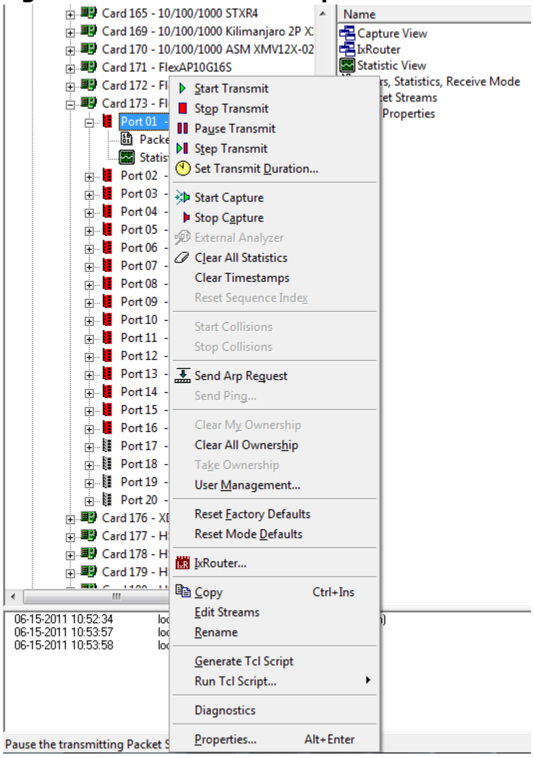
Ports

One or more ports are supported on each card, as shown in *Figure:Port Level of the Explore Network Resource Window*, along with the pop-up menu available by right-clicking the mouse when a port is selected.

Tree Operation

The tree operations for a chassis are accessed by right-clicking the Port icon in the Tree view. The menu is shown in *Figure:Port Level of the Explore Network Resource Window*.

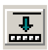
Figure:Port Level of the Explore Network Resource Window



The operations available at the port level of the tree are described in *Table:Port Level Operations*.

Table:Port Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand or contract tree elements beneath the current level.
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A 'Start Transmit' or 'Step Transmit' operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted.
Set Transmit Duration		Sets a specific time period for transmission. Selecting this icon opens the *Set Transmit Duration* dialog, as described in *Set Transmit Duration*.
Start Capture		Enables the start of data capture operations. NOTE Capture feature is disabled in XDM10G32S load module.
Stop Capture		Disables data capture operations. NOTE Capture feature is disabled in

Operation	Keys/Shortcut	Description
		NOTE XDM10G32S load module.
External Analyzer		Launches a third party packet analyzer. The type of analyzer launched is determined by the settings in the *External Analyzer tab*, as described in *External Analyzer Option*. This button is only active when the analyzer type is specified in *External Analyzer* tab.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations* for details.
Clear Timestamps		Clears the global time value used in timestamps which may be included in each frame. Refer to *Instrumentation Box* for details.
Reset Sequence Number		When Sequence checking is in use, this resets the sequence number back to 0. Refer to the section on Sequence Checking Operation in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.
Start Collisions		Enables collision generation for received data, if programmed for the port and enabled.
Stop Collisions		Stops collision generation.
Send ARP Request		Send an ARP packet requesting the addresses for the selected port. The first IP address found in the stream for the port is used for the ARP request. ARP must be enabled in the IxRouter window for the port. NOTE ARP feature is disabled in XDM10G32S load module.
Send Pause Control		Sends a single Pause Control Frame. The characteristics of the frame are specified in a dialog identical to that used during frame data specification.See *Pause Control*.
Send Ping...		Opens the *Ping* dialog. Allows to specify a destination address, clear the ARP table, and send a PING packet from an interface which has been configured on the selected port.

Operation	Keys/Shortcut	Description
		NOTE An INTERFACE must be created in the Interfaces window of the IxRouter window, before the Ping option can be used. Refer to ICMP/PINGv4. NOTE Ping feature is disabled in XDM10G32S load module.
Clear My Ownership		The current user's ownership for the selected port is cleared.
Clear All Ownership		The ownership for the selected port is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with the selected port. A warning message may be displayed if the port is owned by another user. NOTE In **XDM10G32S** load module, all 32 ports use the same CPU. If ownership is taken of one port, the ownership of the remaining 31 ports in the card is automatically transferred to the same user. Multi-user ownership of the ports is not allowed in this load module. The 'Take Ownership' option is disabled on the remaining ports once one port is transferred ownership.
User Management		A dialog is displayed, allowing centralized, per chassis control of port ownership.
Reset Factory Defaults		Resets the port to default factory port configuration, leaves one default stream (if applicable), and changes the port mode to the factory default (if applicable). NOTE Resetting the card properties to factory default settings will not clear the timestamps. To clear the timestamps, you have to click **Clear Timestamps** option.
Reset Mode Defaults		Resets the port to default factory port

Operation	Keys/Shortcut	Description
		configuration and leaves one default stream (if applicable). This option does NOT reset the port mode (if applicable).
IxRouter		Opens the IxRouter window. For more information on IxRouter window function for IxExplorer, see *IxRouter Window* For more information on protocols available, see the *IxNetwork User Guide*.
Copy	 Ctrl+Ins	Copies a number of port characteristics so that they may be pasted onto other ports. Refer to the section on *Port Copying Operations* Port Copying Operations *for a further explanation.*
Edit Streams		Invokes the *Frame Data/Streams* dialog for the port.*Stream and Flow Control* and Frame Data Structure for details.
Rename		Allows a name to be added to the port or edited.
Generate Tcl Script		Activates the ScriptGen feature and allows for the generation of Tcl configuration script. See *ScriptGen* for details.
Run Tcl Script		Allows to run a Tcl script from a list of scripts. See *Run Tcl Script...* for more information.
Diagnostics		Opens the Ixia Diagnostics Collection Utility dialog. You can collect log information from the chassis and from the client computer and wrap it into a comclicked (.zip) file named ixoslogs- YYYYMMDDHHMM.zip. See *Collect Diagnostic Logs*.
Properties		Allows the properties for a port to be adjusted. For a full explanation of the port properties that may be modified, • *Port Properties — 10/100/1000 Ethernet Family* • *Port Properties–POS and ATM Families* • *Port Properties–10 GE and UNIPHY Families*

Icon Colors

NOTE

Port icons for Power over Ethernet (PoE) ports are different than regular port icons. *PoE Port Icons* and Appendix 3, *PoE Port Icons* for more information.

Port icons are displayed in the Resources window, and can alert you to different port states. The icon associated with each port varies in color with the state of the port, as described in *Table:Port Icon Color Codes*.

Table:Port Icon Color Codes

Color	Description
Red	Link is down on port.
Green	Link is up on port.
Yellow	Link is in loopback mode.
Gray	Link is unavailable because is it busy or is an unsupported port type.
Blue	Link is in OAM loopback mode and traffic is paused.

In addition, the port icon varies according the type of activity occurring on the port during testing, as described in *Table:Port Icons*.

Table:Port Icons

Icon	Description
	Port capture is progress; the trigger has been matched and the buffer is not yet full.
	The port is transmitting.
	The port is both transmitting and capturing.
	The port is in echo mode. For more information about echo mod-e,Echo.

PoE Port Icons

PoE port icons look slightly different than regular port icons. They also do not signal trans-mission or capture. *Table:PoE Port Icon Colors* below shows PoE port icons and what their colors signify.

Table:PoE Port Icon Colors

Icon Color	Description
	Green—port is tested and calibrated, and ready to emulate a Powered Device (PD).
	Gray—port is the middle of the testing/calibration process.
	Red—port has failed one or more of the calibration tests. It will not accept Power Sourcing Equipment (PSE) input.

Testing statistics can be viewed in the IxServer main window. For more information on the IxServer main window, see the *IxServer User Guide*.

PoE ports can be retested or recalibrated using the *Card Properties* dialog. For more information on the *Card Properties* dialog, *Card Properties*.

Port Detail Data

The Port Details list for a port selected in the Resources tree has elements that allow further programming of the port's operation, as shown in *Figure::Detail Data for Port* and described in *Table:Detail Data for Port* .

Any of these details may be changed while the element is selected in the Tree view, or in the Details view in the right-hand panel.

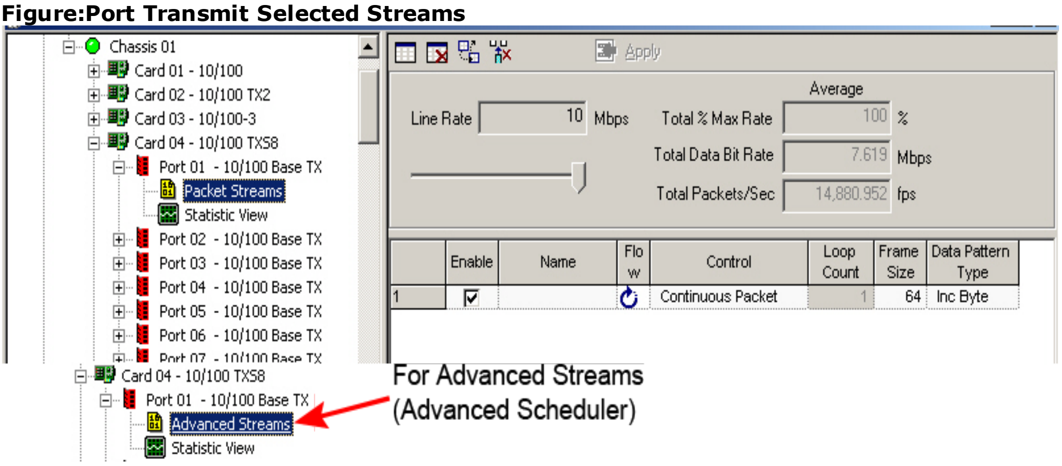
Table:Detail Data for Port

Name	Description
Capture View	Displays data for data captured on the port. *Capture View* for full details.
IxRouter	Displays the IxRouter window that allows the configuration of the Protocol Server that controls IP/ARP addressing, BGP, OSPF, ISIS, RSVP, RIP, RIPng, IGMP, PIM-SM, and so forth, testing. Refer to the *IxNetwork User Guide* for additional information.
Statistic View	Displays statistics for captured data for the port.*Statistic View* for details.
Filters, Statistics, Receive Mode	Displays a dialog which allows programming of the criteria for data capture, filtering, statistics gathering and asynchronous stream activation.*Filter Properties* for full details
Packet Streams or Packet Flows or Advanced Streams	Displays a dialog which allows programming of packet contents and stream formation.*Stream and Flow Control* and Frame Data Structure for details.
Port Properties	Allows the properties for a port to be adjusted. For a full explanation of the port properties that may be modified *Port Properties — 10/100/1000 Ethernet Family*,*Port Properties–POS and ATM Families* and*Port Properties–10 GE and UNIPHY Families*.
BERT	Only for BERT-capable modules in BERT mode. Displays the BERT configuration dialogs.
VSR Statistics	Only for VSR-capable modules. Displays the *VSR Statistics* dialogs.

Special Streams Operations

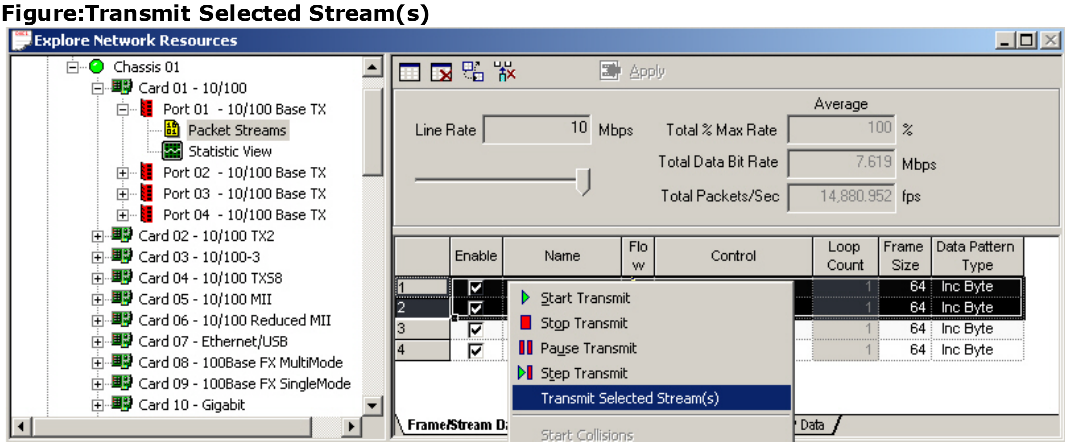
As shown in *Figure:Port Transmit Selected Streams*, Packet Streams (or Packet Flows or Advanced Streams depending on the configuration of the port) and Statistic View are shown below the Port Level in the tree. If Packet Streams/Flows is selected, then the detail data for the port shows the defined streams/flows for the port. From this display, a number of operations related to streams/flows are possible (*Stream and Flow Control*.)

Figure:Port Transmit Selected Streams



One particular operation is particularly valuable—the ability to execute a selected subset of streams/flows. To perform this operation, select the streams/flows in the table, and then use the *Transmit Selected Stream(s)* pop-up menu option. The normal application of streams is interrupted, and each of the selected streams/flows is applied once. This is illustrated in *Figure:Transmit Selected Stream(s)*.

Figure:Transmit Selected Stream(s)



In addition, the detail data for the port displays an editable spreadsheet for the actual transmitted data. This data may be edited from this display, as described in *Stream Editing*.

NOTE Transmit Selected Streams:

Do not use the configured frame rate.

Do not obey continuous transmission settings.

Do not enable the transmit arrow on the port icon.

This function is intended for debug purposes during port configuration development.

Port Copying Operation

A number of the features of a port may be copied to any number of other ports. The Port Copy Wizard consists of four screens which are presented here to demonstrate the entire port copying operation. The Port Copy Wizard is accessed by right-clicking a port and selecting *Copy* from the menu.

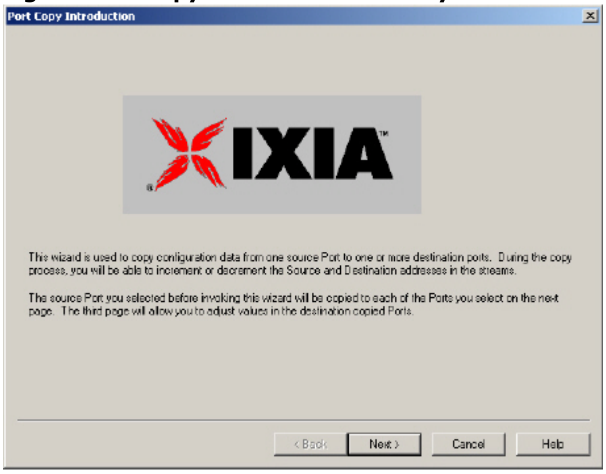
The four dialogs in the wizard are:

- *Port Copying Introduction Dialog—Introductory instructions.*
- *Port Copy Select Port Dialog—Selects the ports to copy to.*
- *Port Copy Options Dialog—Selects the features of the port to copy.*
- *DA/SA Port Copy Address Adjustment Dialog—An optional dialog that allows DA/SA dynamic adjustments.*

Port Copying Introduction Dialog

When invoked with a single port selected, the Port Copy operation starts by displaying a *Port Copy Introduction* screen, shown in *Figure:Port Copy Wizard Introductory Screen*.

Figure:Port Copy Wizard Introductory Screen

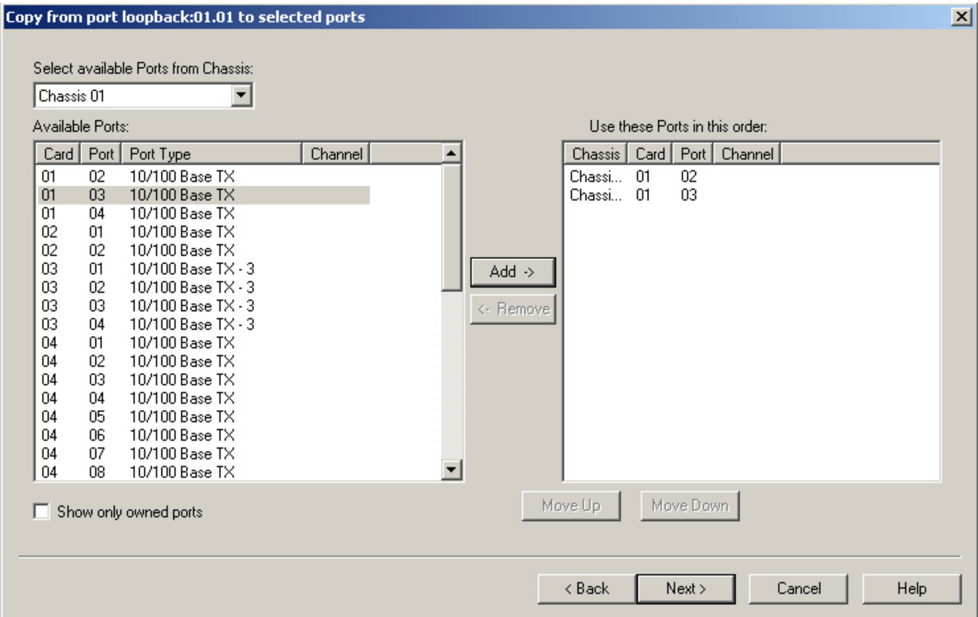


When the *Next* > button is clicked, a chooser dialog is presented with a list of ports of the same type as the original port. *Port Copy Select Port Dialog*

Port Copy Select Port Dialog

The *Select Port* dialog is a 'chooser' dialog with a list of ports of the same type as the original port. On the left side of the window, highlight the desired ports using either the shift-click or control-click methods, and then click the *Add* button to place them in a list on the right side of the window. This dialog is shown in *Figure:Choose Ports Dialog for Port Copying*.

Figure:Choose Ports Dialog for Port Copying

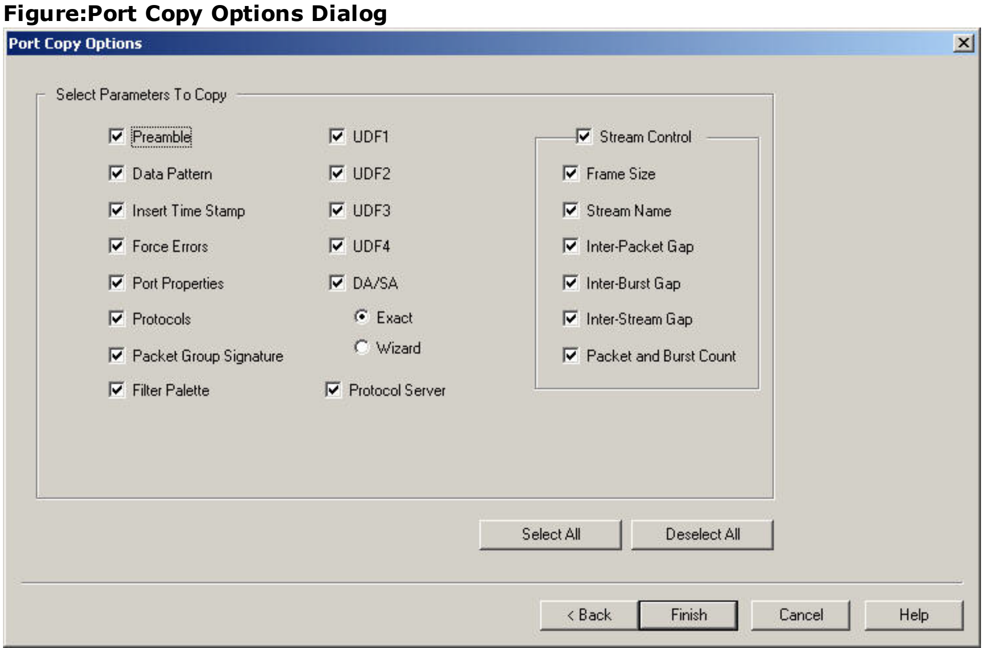


When the *Next >* button is clicked, the *Port Copy Options Dialog is presented allowing the selection of which features of the port are to be copied.*

Port Copy Options Dialog

The *Port Copy Options* dialog allows the selection of which features of the port are to be copied. This dialog is shown in *Figure:Port Copy Options Dialog*.

Figure:Port Copy Options Dialog



The options available in this dialog are described in *Table:Port Copy Options Dialog*.

Table:Port Copy Options Dialog

Option	Description
Preamble	If selected, the Preamble settings from the port's *Frame Data* dia-

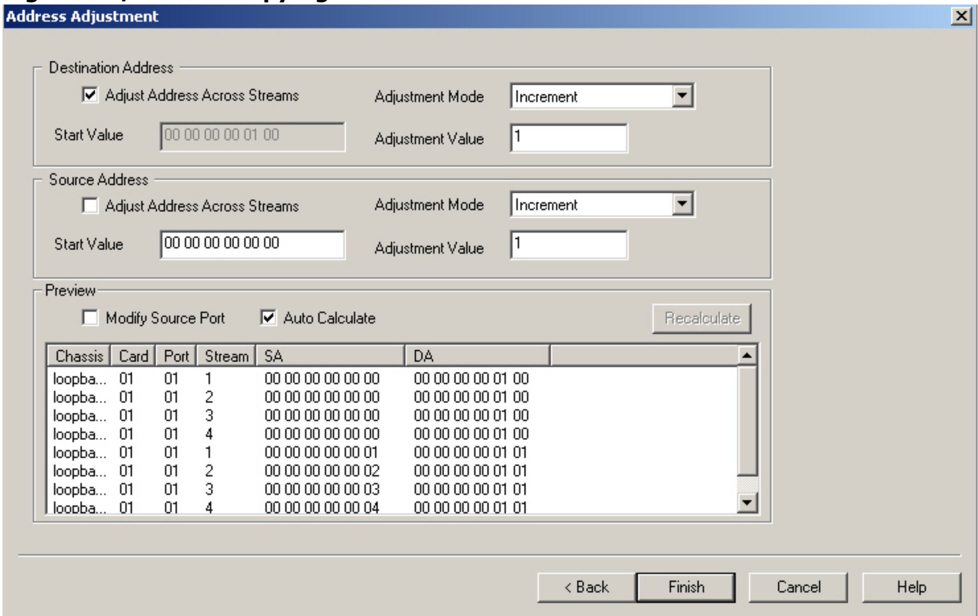
Option	Description
	log are copied.
Data Pattern	If selected, the Data Pattern settings from the port's *Frame Data* dialog are copied.
Insert Time Stamp	If selected, the Insert settings from the port's *Frame Data* dialog are copied.
Force Errors	If selected, the Force Errors settings from the port's *Frame Data* dialog are copied.
Port Properties	If selected, the Port's Properties are copied.
Protocols	If selected, the Protocols settings from the port's *Frame Data* dialog are copied.
Packet Group Signature	If selected, the definition of the packet group signature from the *Frame Data* dialog is copied.
Filter Palette	If selected, the settings from the port's *Filter Properties* dialog are copied.
UDF 1, 2, 3, 4	If selected, the UDF 1, 2, 3 or 4 settings from the port's *Frame Data* dialog are copied.
DA/SA	If selected, the DA/SA settings from the port's *Frame Data* dialog are copied. Two choices are available for setting DA/SA values: • **Exact**—The DA/SA values are copied exactly. • **Wizard**—A further wizard allows the DA and SA values to vary algorithmically; these are described below. If the DA/SA Wizard selection is made, then the *DA/SA Port Copy Address Adjustment Dialog* is presented.
Protocol Server	If selected, the settings from the *IxRouter* dialog are copied.
Stream Control	If selected, the stream type selection from the port's *Stream Control* dialog are copied along with other items not covered by the next six elements.
Frame Size	If selected, the Frame Size settings from the port's *Frame Data* dialog are copied.
Stream Name	If selected, the Name settings from the port's *Stream Control* dialog are copied.
Inter-Packet Gap	If selected, the Inter-Packet Gap settings from the port's *Stream Control* dialog are copied.
Inter-Burst Gap	If selected, the Inter-Burst Gap settings from the port's *Stream Control* dialog are copied.
Inter-Stream Gap	If selected, the Inter-Stream Gap settings from the port's *Stream Control* dialog are copied.
Packet and Burst Count	If selected, the packet and burst counts from the port's *Stream Control* dialog are copied.
Select All	If this button is used, all options are selected.
Deselect All	If this button is used, all options are cleared.

NOTE Port statistics and alert setup information is always copied, regardless of the selections made in this dialog.

DA/SA Port Copy Address Adjustment Dialog

If the DA/SA Wizard is selected in the Port Copy Options dialog, the DA/SA Port Copy *Address Adjustment* dialog is shown in *Figure:DA/SA Port Copying Wizard*.

Figure:DA/SA Port Copying Wizard



This wizard allows Source and Destination Addresses to be modified so that an entire system may be tested based on the programming of a small number of ports. The DAs and SAs may be assigned across ports so that ports 'talk' to each other. Addresses associated with the source port (being copied from) are copied with modifications to all the destination ports (being copied to).

There are a number of copy modes that differ based on the values of the *Adjust Address Across Streams* setting in each dialog. These modes are summarized in *Table:DA/SA Address Adjustment Modes*.

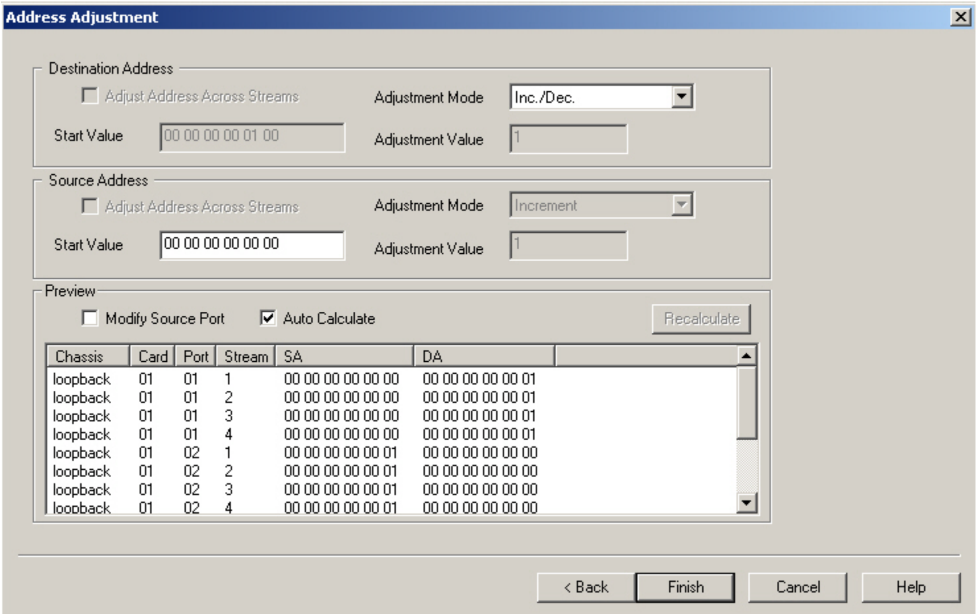
Table:DA/SA Address Adjustment Modes

Mode	Usage without ***Adjust Address Across Streams*** (default)	Usage with ***Adjust Address Across Streams***
Increment/Decrement	The Start Value is initially copied from the source port and may be user modified. This value is incremented/decremented by the Adjustment Value amount and assigned consecutively to each stream of each destination port, in order.	The Start Value is initially copied from the source port and cannot be modified. This value is incremented/decremented by the Adjustment Value amount and assigned consecutively to all streams of each destination port, in order.
Idle	The Start Value is initially copied from the source port and may be modified. This value is assigned to all streams of each destination port.	No difference.

Mode	Usage without *Adjust Address Across Streams* (default)	Usage with *Adjust Address Across Streams*
Inc./Dec.	Modifies both the DA and SA values. See further explanation below.	No difference.

The Increment/Decrement mode manipulates both the SA and DA at the same time so that pairs of ports, including the source port, talk to each other. For example, in the figure below, Card 1-Port 1 is being copied to Card 1 Port 2. Note in the Preview display shown in *Figure:Address Adjustment for Inc./Dec*. Mode how each pair of ports has each other's Source Address as their Destination address and vice versa.

Figure:Address Adjustment for Inc./Dec. Mode



Note that the *Start Value* field for the Source Address shows the only variable address in this case, and that values all increment by one.

Three additional controls located within the Preview box are described in *Table:Port Copy Preview Controls*.

Table:Port Copy Preview Controls

Control	Description
Modify Source Port	If selected, the source port (being copied from) is modified at the same time as the destination ports, based on the Start Value.
Auto-Calculate	If selected, the values displayed in the Preview box are automatically updated as different selections are made.
Recalculate	If *Auto-Calculate* is cleared, this button is enabled. When selected, it updates the Preview box with correct values

Port Groups

Port Groups are collections of ports which may be used as a convenience in several places. The ports that are used in a port group may be drawn from any card in any chassis in any chassis chain. The position of the Port Groups in the tree is shown in *Figure: Port Group*

Level of the Explore Network Resource Window, along with the pop-up menu available by clicking the right mouse button.

Tree Operations

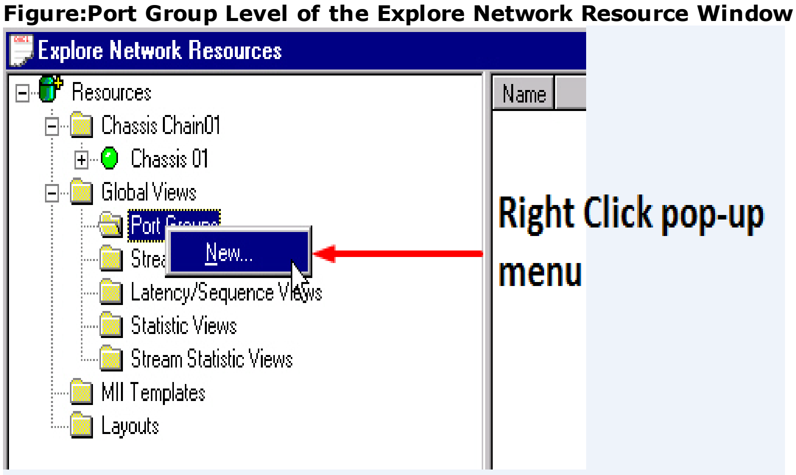
There are two sets of tree operations for Port Groups:

- Port Group top level (folder)—Allows for the creation of new Port Groups (*Tree Operation for Port Group Folder*).
- Port Group level—Used to manage existing Port Groups (*Tree Operation for Port Groups*).

Tree Operation for Port Group Folder

The tree operations for the Port Groups top level are accessed by right-clicking the Port Groups icon in the Tree view. The menu is shown in *Figure:Port Group Level of the Explore Network Resource Window*.

Figure:Port Group Level of the Explore Network Resource Window



The operations available at the Port Groups level of the tree are described in *Table:Port Groups Level Operations*.

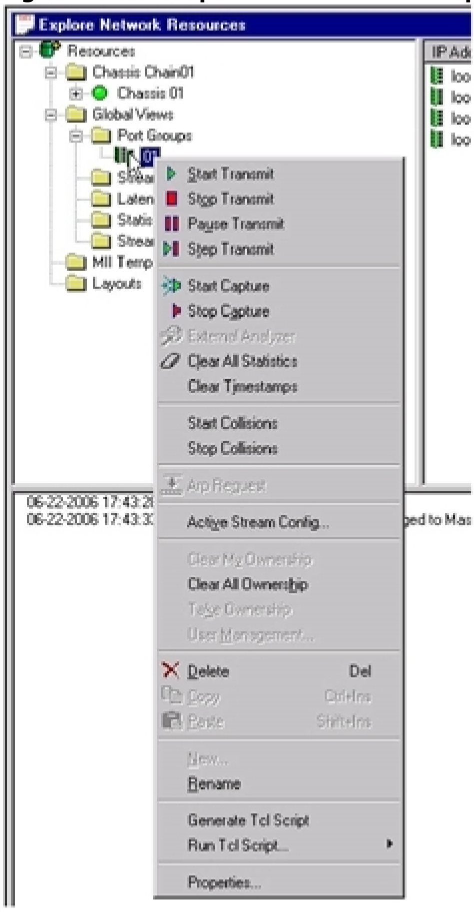
Table:Port Groups Level Operations

Operation	Keys/Shortcut	Description
New		Displays the *Select Port* dialog, where available ports are selected to create a new Port Group. See *Select Port Dialog* for additional information. The name of the new port group is the next sequential number available. This may be renamed.

Tree Operation for Port Groups

The tree operations for individual Port Groups are accessed by selecting the Port Groups icon in the Tree view, then right-clicking a specific Port Group from a list of Port Groups. The menu is shown in *Figure:Port Group Definition Level—Explore Network Resource Window*.

Figure:Port Group Definition Level—Explore Network Resource Window



Port operations are performed on all ports in the selected port group. The operations available at the Port Groups level of the tree are described in the *Table:Port Group Level Operations*.

Table:Port Group Level Operations

Operation	Keys/Shortcut	Description
Expand/Contract tree	Double-click label, click ⊟ or ⊞	Expand or contract tree elements beneath the current level.
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A 'Start Transmit' or 'Step Transmit' operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted on all of the ports contained in the selected port group.
Start Capture		Starts data capture.
Stop Capture		Stops data capture.

Operation	Keys/Shortcut	Description
External Analyzer		Launches a third party packet analyzer. The type of analyzer launched is determined by the settings in the *External Analyzer tab*, as described in *External Analyzer Option*. This button is only active when the analyzer type is specified in *External Analyzer* tab.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations* for details.
Clear Timestamps		Clears the global time value used in time stamps which may be included in each frame. Refer to *Instrumentation Box* for details.
Start Collisions		Enables collision generation for received data, if programmed for the ports and enabled.
Stop Collisions		Stops collision generation.
Arp Request		Send an ARP packet requesting the addresses for the ports associated with the port group. The first IP address found in the stream for each port is used for the ARP request.
Active Stream Config		Allows one of several parameters to be varied across the ports in the port group.
Clear My Ownership		The current user's ownership for the ports associated with the port group is cleared.
Clear All Ownership		The ownership for the ports associated with the port group is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with the ports associated with the port group. A warning message may be displayed if the port is owned by another user.
Delete	 Del	Deletes the selected port group, after answering 'Yes' to a confirmation dialog.
Rename Port Group		Enables editing of the port group name.
Generate Tcl Script		Activates the ScriptGen feature and allows for the generation of Tcl con-

Operation	Keys/Shortcut	Description
		figuration script. *ScriptGen* for details.
Run Tcl Script		Allows to run a Tcl script from a list of scripts. See *Run Tcl Script...* for more information.
Properties		Displays the *Select Port* dialog which allows the selection/modification of which ports are members of the port group. See *Select Port Dialog* for additional information.

Port Group Detail Data

The Details view for the Port Groups level lists all of the user-defined port groups. If a specific Port Group is selected, then ports within the Port Group are listed.

For each port, the Details view shows the elements listed in *Table:Detail Data for Port Groups*.

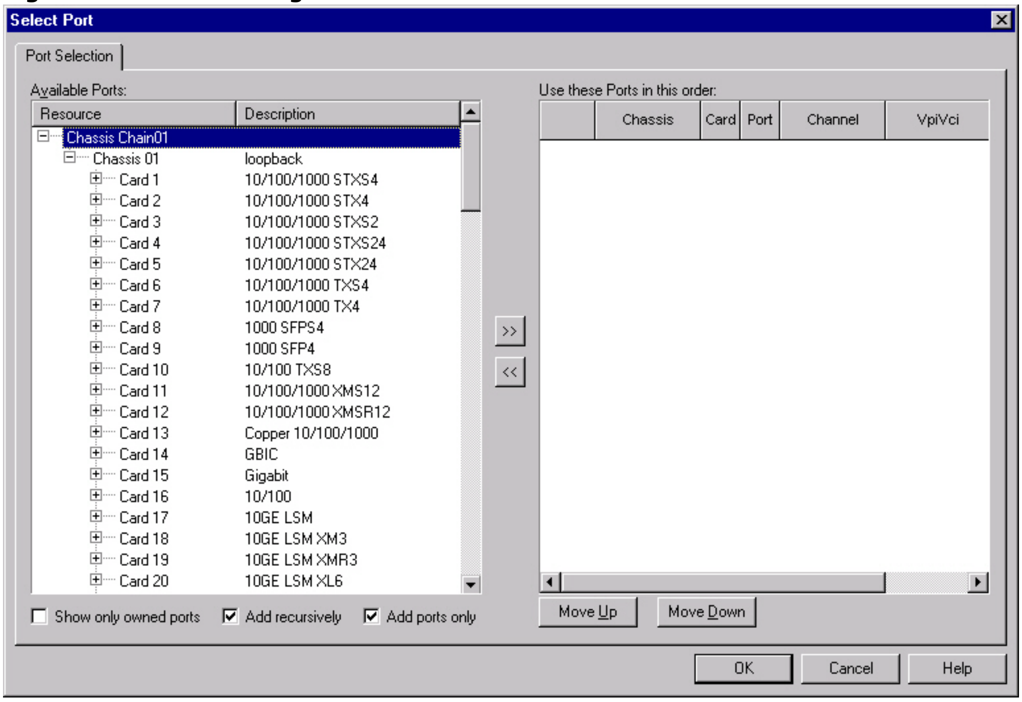
Table:Detail Data for Port Groups

Column	Description
IP Address	The IP address of the chassis where the port is located.
Chassis	The number of the chassis in the chassis chain where the port is located.
Card	The card number in the chassis where the port is located.
Port	The number of the port in the card.

Select Port Dialog

The *Select Port* dialog is pictured in *Figure:Select Port Dialog*. This dialog allows ports to be assigned to a Port Group and Stream Group, as well as to Packet Group Statistic Views and Statistic Views. It is also used for selecting the source port for automatic Stream Generation.

Figure:Select Port Dialog



The elements of this dialog are described in *Table:Port Group Properties (Select Port) Dialog Controls*.

Table:Port Group Properties (Select Port) Dialog Controls

Element	Description
Available Ports	Displays the list of ports that are not currently members of the port group. For each port, the name of the chassis, card number, and port number are displayed. If applicable, Channel and VPI/VCI are displayed.
Use these Ports in this Order	Displays the list of ports that are currently selected for the port group. For each port, the name of the chassis, card number, and port number are displayed. If applicable, Channel and VPI/VCI are displayed.
Show only owned ports	If selected, only ports for which you have taken ownership are displayed in the *Available Ports* list.
Add recursively	The Add recursively check box enables the capability for adding groups of ports at one time. Select the Add recursively check box. Then select/highlight a higher level item in the list: Card (load module), Chassis, or Chassis Chain. Click the >> (Add) button, and all of the ports listed under that higher level item are added to the list of active ports in the right pane.
Add ports only	Selecting this check box limits the view to port information only.
Move Up	This button moves the selected port up one place in the port list order.
Move Down	This button moves the selected port down one place in the port list order.
>> (Add)	Click this button to add ports to the port group. Select one or more ports from the Available Ports list before clicking the *Add* button.

Element	Description
	Ports can also be added by doubling clicking them.
<< (Remove)	Click this button to remove ports from the port group. Select one or more ports from the Use these Ports in this Order list before clicking the *Remove* button. Ports can also be removed by double-clicking them

Stream Groups

The Stream Groups view allows for grouping together streams in the chassis for group operation. The position of the Stream Groups view in the Resources tree, along with the pop-up menu that is available by clicking the right mouse button, is shown in *Figure:Packet Group Statistic Views Level of the Explore Network Resource Window*.

Tree Operations

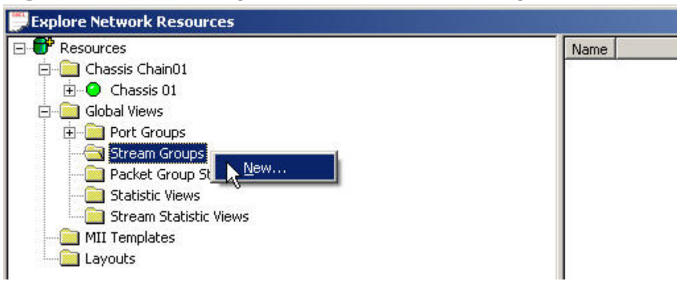
The tree operations of Stream Groups view are accessed by right-clicking the *Stream Groups* icon, as shown in *Figure:Stream Groups View Level of the Explore Network Resource Window*.

There are two sets of tree operations for Stream Groups:

- Port Group top level (folder)—Allows for the creation of new Port Groups (*Tree Operation for Stream Groups Folder*).
- Port Group level—Used to manage existing Port Groups (*Tree Operation for Stream Groups)*.

Tree Operation for Stream Groups Folder

Figure:Stream Groups View Level of the Explore Network Resource Window



The operations available at the Stream Groups View level of the tree are described in *Table:Stream Group View Level Operations.*

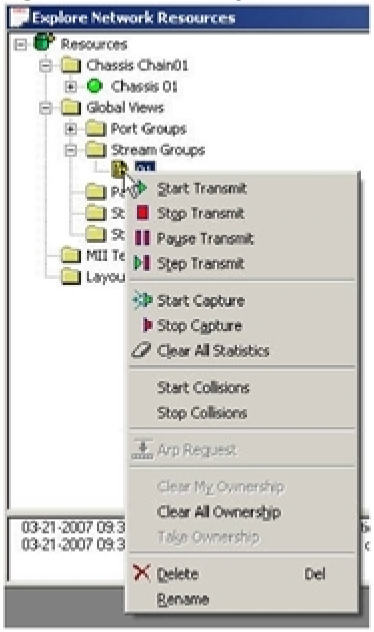
Table:Stream Group View Level Operations

Operation	Keys/Shortcut	Description
New		Displays the *Select Port* dialog, where available ports are selected to create a new Stream Group. See *Select Port Dialog* for additional information. Creates a new Stream Group with a name in the form 'NN', where NN is the next available number.

Tree Operation for Stream Groups

The tree operations for individual Stream Groups are accessed by selecting the Stream Groups icon in the Tree view, then right-clicking a specific Stream Group from a list of Stream Groups. The menu is shown in *Figure:Stream Group Definition Level—Explore Network Resource Window*.

Figure:Stream Group Definition Level—Explore Network Resource Window



Stream operations are performed on all streams in the selected stream group. The operations available at the Stream Groups level of the tree are described in the *Table:Stream Groups Level Operations*.

Table:Stream Groups Level Operations

Operation	Keys/Shortcut	Description
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A 'Start Transmit' or 'Step Transmit' operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted on all of the ports contained in the selected Stream Group.
Start Capture		Starts data capture.
Stop Capture		Stops data capture.
Clear All Statistics		Clears all statistics. Refer to *Statistics Operations* for details.
Start Collisions		Enables collision generation for

Operation	Keys/Shortcut	Description
		received data, if programmed for the ports and enabled.
Stop Collisions		Stops collision generation.
Arp Request		Send an ARP packet requesting the addresses for the ports associated with the Stream Group. The first IP address found in the stream for each port is used for the ARP request.
Clear My Ownership		The current user's ownership for the ports associated with the Stream Group is cleared.
Clear All Ownership		The ownership for the ports associated with the Stream Group is cleared. A warning message may be displayed if a port is owned by another user.
Take Ownership		The current user's login is associated with the ports associated with the Stream Group. A warning message may be displayed if the port is owned by another user.
Delete	 Del	Deletes the selected Stream Group, after answering 'Yes' to a confirmation dialog.
Rename		Enables editing of the stream group name.

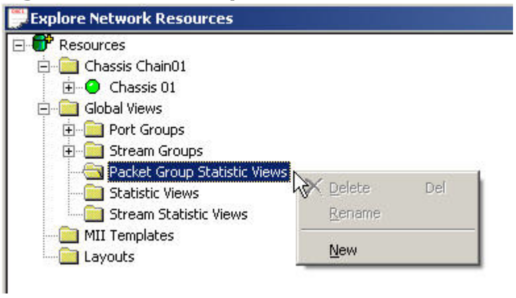
Packet Group Statistic Views

The Packet Group Statistic Views allows for the collection and analysis of latency data. For ports which support sequence checking based on user-defined thresholds, sequence checking data is also displayed in this view. The position of the Packet Group Statistic Views in the Resources tree, along with the pop-up menu that is available by clicking the right mouse button, is shown in *Figure:Packet Group Statistic Views Level of the Explore Network Resource Window*.

Tree Operations

The tree operations of Packet Group Statistic Views are accessed by right-clicking the *Packet Group Statistic Views* folder, as shown in *Figure:Packet Group Statistic Views Level of the Explore Network Resource Window.*

Figure:Packet Group Statistic Views Level of the Explore Network Resource Window



The operations available at the Packet Group Statistic Views level of the tree are described in *Table:Packet Group Statistic View Level Operations.*

Table:Packet Group Statistic View Level Operations

Operation	Keys/Shortcut	Description
Delete	 Del	Deletes an existing Packet Group Statistic View.
Rename		Allows editing of the name of the Packet Group Statistic View.
New		Displays the *Select Port* dialog, where available ports are selected to create a new Packet Group Statistic View. *Select Port Dialog* for additional information. Creates a new Packet Group Statistic View with a name in the form 'NN', where NN is the next available number.

Packet Group Statistic Detail Data

The details pane for a Packet Group Statistic View displays a list of Packet Group Statistic View groups with the details described in *Table:Detail Data for Packet Group Statistic View*, as shown in.

Table:Detail Data for Packet Group Statistic View

Name	Usage
Name	The name of the Packet Group Statistic View.
Number of Ports	The number of ports in the Packet Group Statistic View.
File Name	The file associated with the packet group where settings are kept. These are stored in the directory *Latency Views* beneath the directory where IxExplorer was installed.
Last Modified	The date and time that the Packet Group Statistic View settings or data was last modified.

Statistic Views

The Statistic Views allow a statistics display for a set of ports. The ports that are used in a Statistic View may be drawn from any card in any chassis in any chassis chain. The position of the ports in the tree is shown in *Figure:Statistic Views Level of the Explore Network*

Resource Window, along with the pop-up menu available by clicking the right mouse button.

Tree Operations

Accessing the tree operations for Statistic Views is done by right-clicking the *Statistic View* icon in the Tree view, as shown in *Figure:Statistic Views Level of the Explore Network Resource Window*.

Figure:Statistic Views Level of the Explore Network Resource Window

The operations available at the Statistic Views level of the tree are described in *Table:Statistic Views Level Operations*.

Table:Statistic Views Level Operations

Operation	Keys/Shortcut	Description
Delete	 Del	Deletes an existing Statistic View.
Rename		Change the name of a Statistic View.
New		Displays the *Select Port* dialog, where available ports are selected to create a new Statistic View. *Select Port Dialog* for additional information. Creates a new Statistic View with a name of the form 'NN', where NN is the next available number.

Detail Data

The details pane for a Statistic View displays a list of Statistic View groups. The column headings are described in *Table:Detail Data for Statistic View*.

Table:Detail Data for Statistic View

Columns	Description
Name	The name of the Statistic View group.
Number of Stats	The number of statistics displayed in the view.
Number of Ports	The number of ports in the Statistic View group.

Properties associated with the Statistic Views are associated with *Options*.

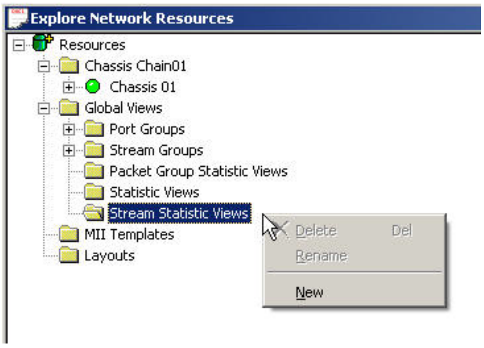
Stream Statistic Views

The Stream Statistic View allows to view statistics for a particular stream. The streams that are used in a Stream Statistic View may be drawn from any port and card in any chassis in any chassis chain. The position of the ports in the tree is shown in *Figure:Stream Statistic View*, along with the pop-up menu available by clicking the right mouse button.

Tree Operation

The Tree operations for Stream Statistic Views are accessed by right-clicking the *Stream Statistic View* icon in the Tree view, as shown in *Figure:Stream Statistic View*.

Figure:Stream Statistic View



The operations available at the Stream Statistic Views level of the tree are described in *Table:Stream Statistic Views Level Operations*.

Table:Stream Statistic Views Level Operations

Operation	Keys/Shortcut	Description
Delete	 Del	Deletes an existing Stream Statistic View.
Rename		Change the name of a Stream Statistic View.
New		Displays the *Select Port* dialog, where available ports are selected to create a new Stream Statistic View.*Select Port Dialog* for additional information. Creates a new Stream Statistic View with a name of the form NN, where NN is the next available number.

Detail Data

The details pane for a Stream Statistic View displays a list of Stream Statistic View groups.

Properties associated with the Stream Statistic Views can be controlled with *Options.*

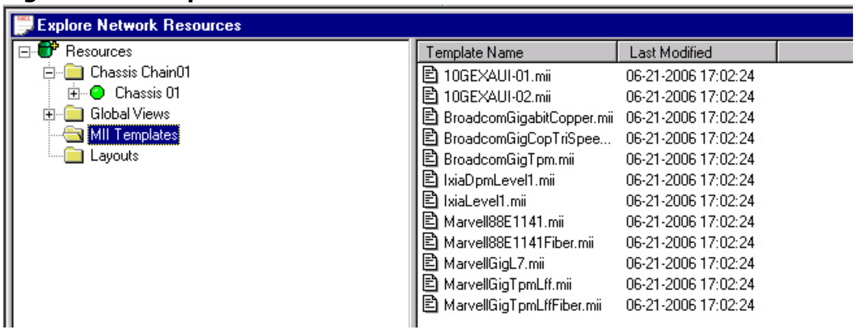
Stream Statistic Views are described in detail in *Stream Statistic Views*.

MII Templates

The MII template files control the correspondence between ports and Media Independent Interface (MII) register values. The creation and editing of MII templates is described in *MII Register Files*.

The MII template files control is shown in *Figure:MII Templates*.

Figure:MII Templates



Detail Data

The elements shown in the details pane of the MII Template are described in *Table:MII Template Details View*.

Table:MII Template Details View

Columns	Description
Template Name	Shows the MII Template file name.
Last Modified	Shows the date on which the file was last modified.

Layouts

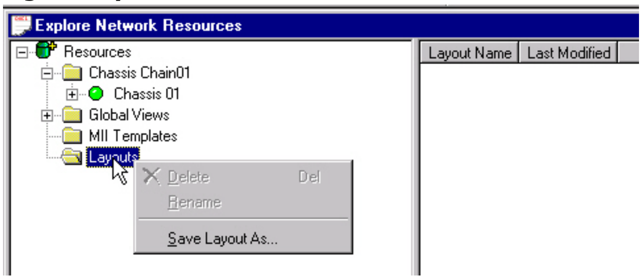
The Layouts folder allows to save and store IxExplorer view formats for future retrieval. A layout can be saved as a *.lay* file and then recalled by double-clicking the file.

For example, you save a layout where the Statistic Views, Packet GroupViews, and MII Templates are all open in the GUI as `layout1.lay`. Normally when IxExplorer is shutdown and reopened, you have to manually open all of these views. With a *.lay* file, simply click the file and all of the previously open views are automatically reopened.

Tree Operation

The Tree operations of Layouts are accessed by right-clicking the *Layouts* icon in the Tree view, as shown in *Figure:Layouts View*.

Figure:Layouts View



The operations available at the Statistic Views level of the tree are described in *Table:Layouts Level Operations*.

Table:Layouts Level Operations

Operation	Keys/Shortcut	Description
Delete	 Delete	Deletes an existing Layout View.
Rename		Change the name of a Layout View.
Save Layout As...		Save a layout with a specific name. This saved layout appears in the right window of the dialog.

Data Detail

The elements in the details pane, as shown in *Table: Detail Data for Statistic View*, are described in *Table:Detail Data for Layout View*.

Table:Detail Data for Layout View

Columns	Description
Layout Name	The name of the Layout View.
Last modified	The date of the last modification to this Layout View.

Tools Menu Functions

The Tools menu functions provide access to various chassis controls and global features. The following is a list of the operations in the Tools menu:

- *Tcl Consol*—Allows for the creation of Tcl scripts.
- *Run Tcl Script...*—Allows for the implementation of existing Tcl scripts.
- *Chassis Shutdown/Reboot Dialog*—Shuts down the chassis.
- *Options*—Opens the *IxExplorer Options* dialog.
- *IxOS Upgrade*—Starts the IxOS remote client upgrade process.

Tcl Console

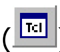
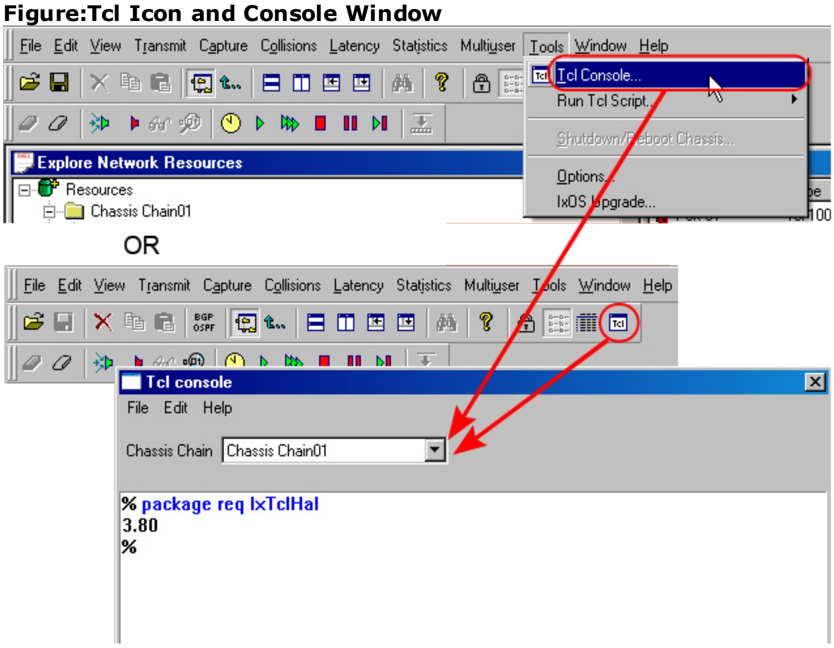
The Tcl console allows to create a Tcl script. The Tcl console is opened by selecting *Tools > Tcl Console* in the menu options, or by clicking the *Tcl* icon () in the toolbar. Both are shown in *Figure:Tcl Icon and Console Window*.

Figure:Tcl Icon and Console Window



Tcl applications can now be entered into the window and applied to a selected Chassis Chain (from a pull-down list). For information on Tcl and Ixia Tcl applications, see the Ixia Tcl Development Guide.

Previously created Tcl applications can also be edited or run using the *File > Source...* menu options in the Tcl window.

NOTE When sourcing a script from the Tcl Console to a file, if the Exit command is used in the script, it shuts down IxExplorer.

Run Tcl Script

The *Run Tcl Scrip* option allows to select a Tcl script from a list of scripts. Tcl scripts can be used to perform operations that would otherwise be difficult or tedious to do manually.

Ixia provides a number of scripts that can be used on the chassis, card, or port level. This feature can be accessed in one of two ways:

- By right-clicking a chassis, card, or port in the resources window, then selecting the *Run Tcl Script* menu option, or
- By selecting *Run Tcl Script* from the *Tools* menu.

The available scripts are shown in another pop-up menu. The scripts in this list are stored in the directory *C:\Program Files\Ixia\TclScripts\IxExplorer\Macros\Port*. Scripts that are added to this directory are displayed when selecting the *Run Tcl Script* option.

The *Run Tcl Script* menu option is shown in *Figure:Run Tcl Script Option*.

Figure:Run Tcl Script Option

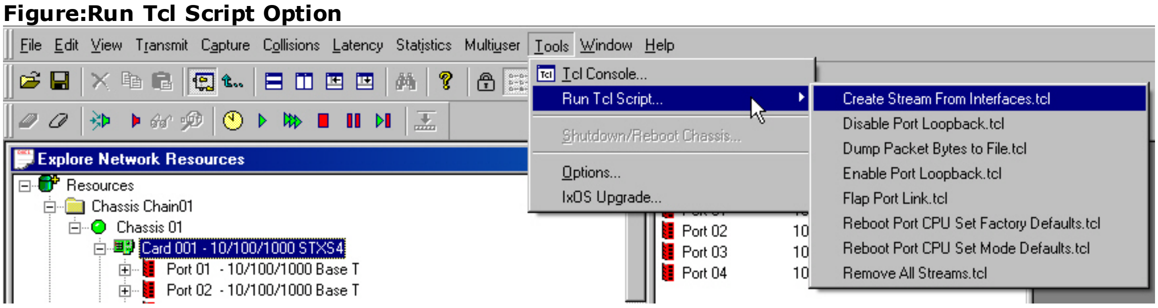


Table:Ixia Resource Tcl Scripts lists the Ixia provided scripts, and describes their functions. Users can create their own scripts and add them to the directory for use.

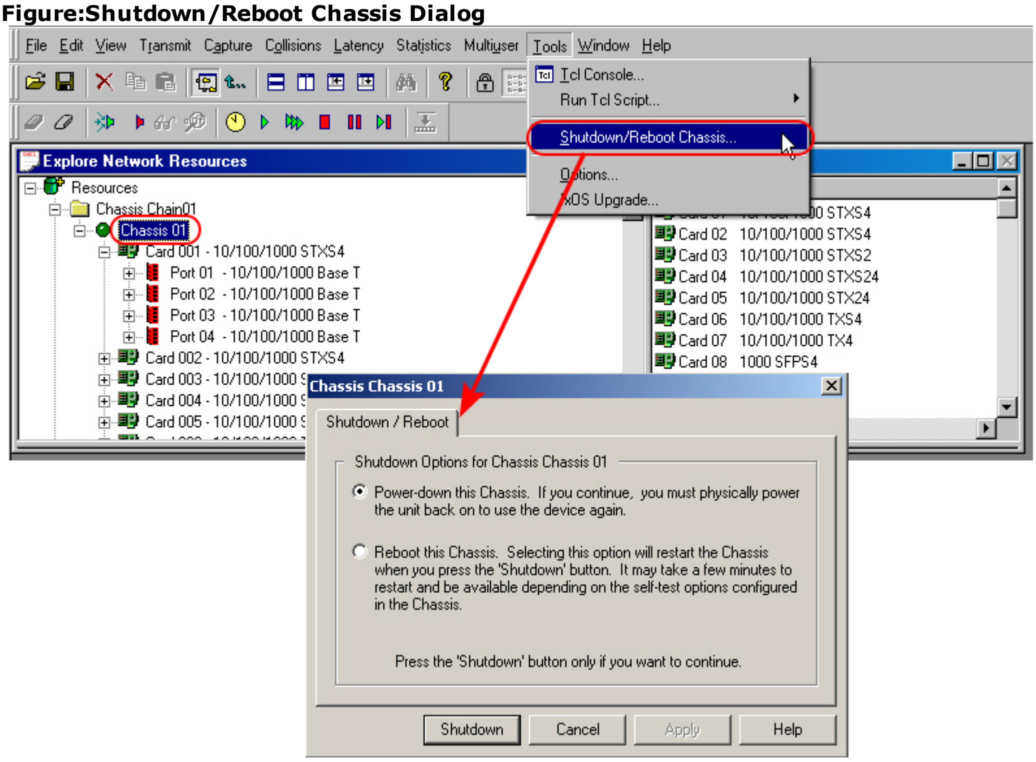
Table:Ixia Resource Tcl Scripts

Script	Description
Create Stream from Interfaces.tcl	Running this script creates a stream from a previously configured interface file on the selected port or ports.
Disable Port Loopback.tcl	Running this script takes the port or ports out of loopback mode.
Dump Packet Bytes to File.tcl	Running this script dumps the packet content info to a text file for the selected port streams.
Enable Port Loopback.tcl	Running this script puts the port or ports into loopback mode.
Flap Port Link.tcl	Running this script sends the selected port or ports into diagnostic loopback mode, then returns it to operational status.
Reboot Port CPU Set Factory Defaults.tcl	Running this script restarts the CPU on the selected port or ports, and resets the factory defaults as described in *Table:Port Level Operations*.
Reboot Port CPU Set Mode Defaults.tcl	Running this script restarts the CPU on the selected port or ports, and resets the mode defaults as described in *Table:Port Level Operations*.
Remove All Streams.tcl	Running this script removes all created streams for the selected port or ports.

Chassis Shutdown/Reboot Dialog

When a Chassis is selected/highlighted in the Resources window, the *Shutdown/Reboot Chassis...* option is available in the *Tools* submenu, as shown in *Figure:Shutdown/Reboot Chassis Dialog*.

Figure:Shutdown/Reboot Chassis Dialog



The choices in this dialog are described in *Figure:Display Format Tab*.

Table:Shutdown/Reboot Chassis Dialog

Section	Control	Description
Shutdown Options for Chassis *Chassis name*	Power-down this Chassis.	If selected, the unit must be physically powered back on to use the device again. Selecting this option turn off the Chassis when the *Shutdown* button is clicked.
	Reboot this Chassis.	Selecting this option restarts the Chassis when the *Shutdown* button is clicked. It may take a few minutes to restart and be available depending on the self-test options configured in the Chassis.
	Shutdown	Click the *Shutdown* button ONLY to continue with the shutdown or restart of the Chassis.
	Cancel	Click the *Cancel* button to close this dialog without shutting down or restarting the Chassis.

Options

The global Options properties are available from the main IxExplorer menu bar, *Tools* > *Options* dialog, which allows for the configuration of certain GUI general parameters. The *Options* dialog consists of several tabs:

- *General*—Controls some of the global settings.
- *Display Format*—Controls the manner in which the information is displayed.
- *Units*—Controls what units are used when displaying transmit and receive bits.

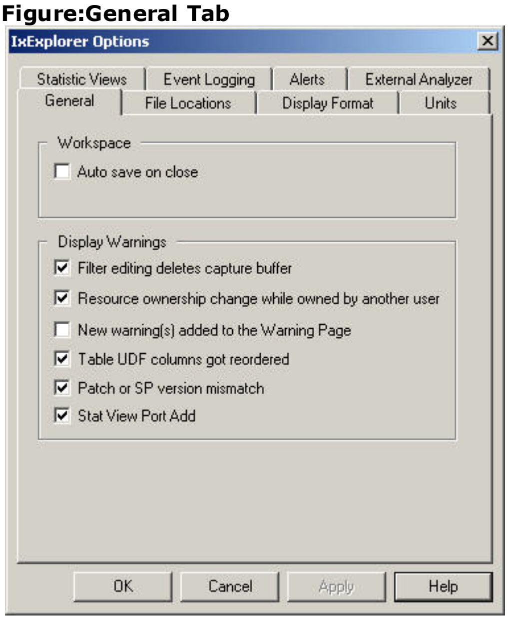
- *Statistic Views*—Controls the way Statistic Views are displayed.
- *Event Logging*—Controls the logging of events and errors.
- *Alerts*—Controls the handling of audible and visual alerts.
- *External Analyzer Option*—For exporting captured data to a 'sniffer' or other external analyzer program.

General

The *General* tab controls some global IxExplorer GUI settings, such as configuration save options and display warnings. The tab is accessed by selecting *Tools* > *Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *General* tab (this is the default display tab).

The *General* tab of the *IxExplorer Options* dialog is shown in *Figure:General Tab*.

Figure:General Tab



The fields and controls in this tab are described in *Table:General Properties*.

Table:General Properties

Field/Control	Description
Auto save on close	Causes the current workspace to be saved every time IxExplorer is exited.
Filter editing deletes capture buffer	Causes a warning to be displayed when any of the filtering (trigger or filter) properties are edited, indicating that the capture buffer is to be erased.
Resource ownership change while owned by another user	Causes a warning to be displayed when the ownership of a port not owned by the current user is changed.
New warnings added to the Warning Page	Causes a warning when a message has been added to the Warnings/Information page of the *Stream Properties* dialog.
Table UDF columns got reordered	Causes a warning if the Table UDF columns have been reordered.
Patch or SP version mis-	Causes a warning when their is a mismatch between the ver-

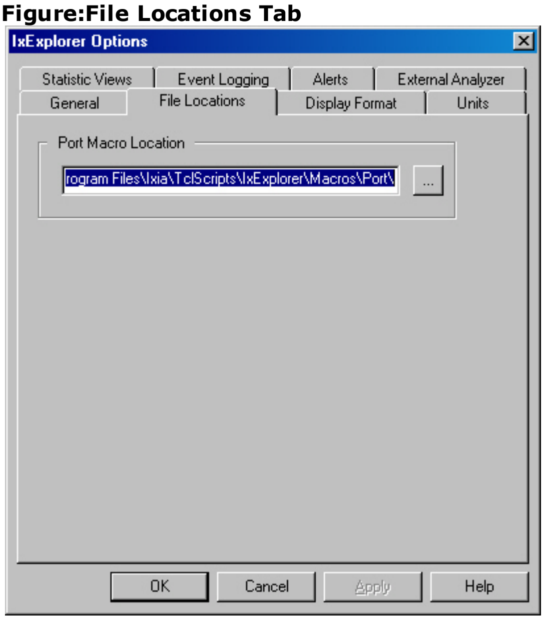
Field/Control	Description
match	sion or service pack of IxServer and IxExplorer.
Stat View Port Add	Displays a warning about deletion of existing user defined columns when a port is added in Statistic View.

File Locations

The File Locations tab sets the default location for port macros. The tab is accessed by selecting *Tools > Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *File Locations* tab.

The *File Locations* tab in the *IxExplorer Options* dialog is shown *Figure:File Locations Tab*.

Figure:File Locations Tab



The fields and controls in this tab are described in *Table:File Locations Properties*.

Table:File Locations Properties

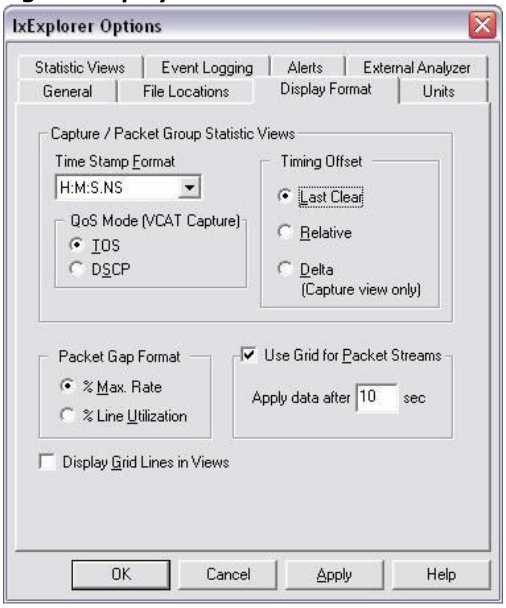
Field/Control	Description
Port Macro Location	A path to the directory where the port macros are kept. Use the browse  button to select a new directory.

Display Format

The *Display Format* tab controls the look of the GUI for various functions such as Capture and Packet Group Statistic Views. The tab is accessed by selecting *Tools > Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *Display Format* tab.

The *Display Format* tab of the *IxExplorer Options* dialog is shown in *Figure:Display Format Tab*

Figure:Display Format Tab



The fields and controls in this tab are described in *Table:Display Format Properties*. When captured data is displayed, the selections control the manner in which the information is displayed.

Table:Display Format Properties

Field/Control	Description
Time Stamp Format	This choice controls the general format of time values that are displayed. The choices are: • H:M:S.NS—hours:minutes:seconds:nanoseconds. • H:M:S:MS:US:NS—hours:minutes:seconds:milliseconds:microseconds:nanoseconds. • S.NS—seconds:nanoseconds. • Raw—exclicked as multiples of the basic system clock. Note: If Raw format is selected, then only the Timing Offset *Last Clear* option is enabled.
Timing Offset	This choice controls which type of time value is displayed. The choices are: • Last Clear—This option shows the time since the last clearing of timestamps. Note: This is the only enabled option if *Raw* format is selected. • Relative—The time is displayed relative to the beginning of first capture. The first capture is displayed as 0 and the last capture as *last capture* minus *first capture*. (Disabled if *Raw* format is selected.) • Delta—The time is displayed relative to the immediately preceding timestamp. The timestamp of the most recent capture minus the timestamp of the immediately preceding capture. (Disabled if *Raw* format is selected.) NOTE Delta option is not supported in Latency Stat View.
QoS Mode	The mode Quality of Service mode employed on captured packets.

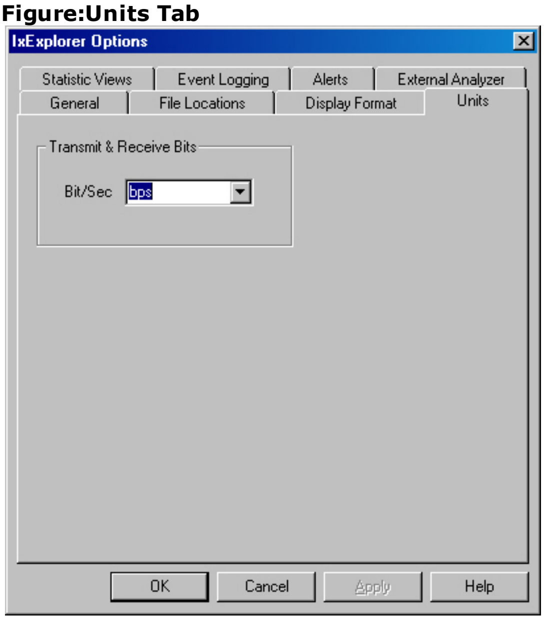
Field/Control	Description
(VCAT Capture)	Select the option button for the desired type, either Type of Service (ToS), or Differentiated Services Code Point (DSCP) value.
Packet Gap Format	This option controls the manner in which Inter-Packet Gaps are programmed. The two choices are: • % Max Rate—The percentage of the maximum rate obtainable. From 1 to 100%. • % Line Utilization—The maximum line utilization, considering overhead periods and bytes. The percentage is always lower than 100% due to these overheads.
Use Grid for Packet Streams	When packet streams/flows/advanced streams are displayed in the right hand IxExplorer panel, a spreadsheet (grid) representation is used. This allows for interactive stream and flow editing using spreadsheet manipulation techniques.See *Stream Editing*.
Apply data after ___ sec	This option controls the amount of delay time for changes in the Stream Editing grid to be applied. The default is 10 seconds.
Display Grid Lines in Views	Causes grid lines to appear in the Details view of the main window.

Units

The *Units* tab page in the *IxExplorer Options* dialog is used to control the type of units being measured when setting the rate control. The rate control is set on the *Stream Control* tab page. For more information on stream control, *Stream and Flow Control*. The tab is accessed by selecting *Tools* > *Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *Units* tab.

The *Units* tab page is shown in *Figure:Units Tab*.

Figure:Units Tab



The *Bit/Sec* menu in the Transmit & Receive Bits section allows the selection of one of the following rates:

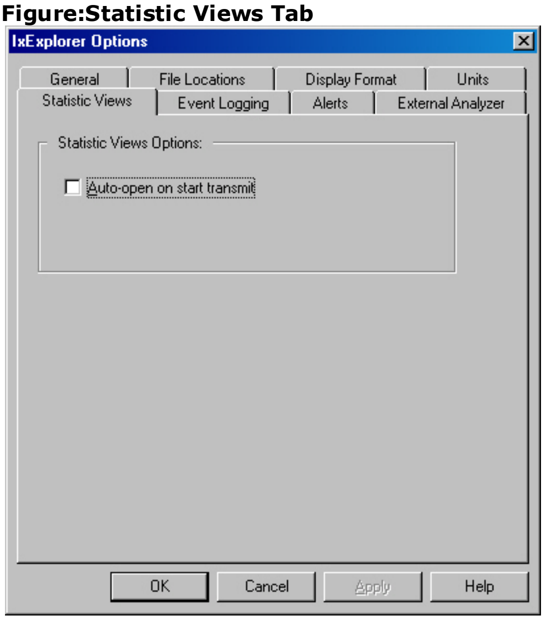
- bps—bits per second.
- Kbps—Kilobits per second.
- Mbps—Megabits per second.
- Gbps—Gigabits per second.

Statistic Views

The *Statistic Views* tab sets the default behavior of Statistic Views. The tab is accessed by selecting *Tools > Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *Statistic Views* tab.

The *Statistic Views* tab in the *IxExplorer Options* dialog is shown in *Figure:Statistic Views Tab*.

Figure:Statistic Views Tab



The fields and controls in this tab are described in *Table:Statistic Views Properties*.

Table:Statistic Views Properties

Field/Control	Description
Auto open on start transmit	If this option is selected, then a Statistic View which contains all of the transmitting ports is displayed when a start transmit operation is applied. It uses or creates a Statistic View which is named based on the means by which the transmission is started. The format is <chassis>:CC:PP, where <chassis> is the IP address or name of the chassis, CC is the card number and PP is the port number. PP is '00' if an entire card or chassis is used. CC is '00' if an entire chassis is used.

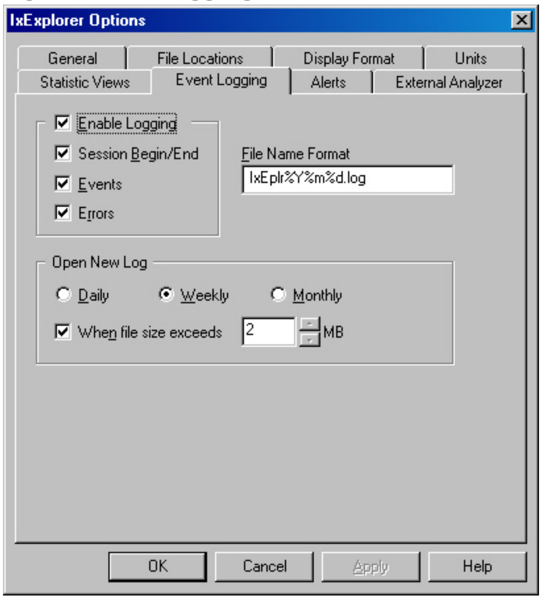
Event Logging

The *Event Logging* tab controls the behavior of logging functions in IxExplorer. The tab is accessed by selecting *Tools > Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *Event Logging* tab.

The *Event Logging* tab in the *IxExplorer Options* dialog is shown in *Figure:Event Logging Tab*.

NOTE Event log files are also created when you switch from one IxOS version to another (in a multi-version environment).

Figure:Event Logging Tab



The fields and controls in this tab are described in *Table:Event Logging Properties*.

Table:Event Logging Properties

Section	Field/Control	Description
Enable Logging		This check box must be selected in order for any event to be logged.
	Session Begin/End	If selected, the time period for each use of IxExplorer is logged.
	Events	If selected, enables logging of events.
	Errors	If selected, enables logging of errors.
File Name Format		Indicates the name under which the various log files are kept. The event files are logged into the same directory in which the Ixia IxExplorer was loaded (usually c:\Program Files\Ixia\IxOS\version X). The name may contain any of the following character sequences, which are substituted with actual values when each log file is created: • %Y: The four digit year number (for example, *2002*). • %m: The two digit month number. For example, *01* for January. • %d: The two digit day number within the month. • %a: The abbreviated weekday name.

Section	Field/Control	Description
		• %A: The full weekday name. • %b: The abbreviated month name. • %B: The full month name. • %c: The date and time appropriate for the locale. • %H: The hour in 24-hour format. • %I: The hour in 12-hour format. • %j: The day of the year as a decimal number. • %M: The minute as a decimal number. • %p: The AM/PM indicator. • %S: The second as a decimal number. • %U: The week of the year as a decimal number. • %w: The weekday as a decimal number. • %W: The week of the year as a decimal number • %x: The date representation for the current locale • %y: The two digit year number (for example, *99).* • %z,%Z: The time-zone name or abbreviation. • %%: The percent sign.
Open New Log	Daily/Weekly/Monthly	A new log is started on a daily, weekly or monthly basis, depending on the selection.
	When file size exceeds __ MB	If this is selected, a new log is also started when the size of a log file exceeds a specified size.

Alerts

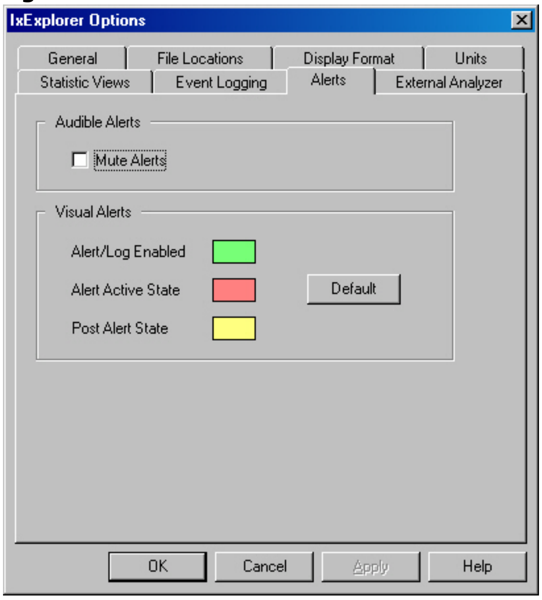
The *Alerts* tab in the *IxExplorer Options* dialog controls the handling of audible and visual alerts as a whole. The tab is accessed by selecting *Tools* > *Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *Alerts* tab.

By default, audible alerts are broadcast through the Windows software (‘Exclamation’ sound) when Logging and Alerts has been enabled on a port, and there is an error (red) condition for a Statistics parameter. The volume setting can be modified by going to the *Windows Start* > *Settings* > *Control Panel* > *Sounds and Multimedia* > *Sounds*, and moving the slider bar. If this modification is not sufficient, you may choose to use external speakers.

Refer to the section on Statistics Logging and Alerts in the ‘Theory of Operation: General’ chapter of the *Ixia Platform Reference Manual* for more information.

The *Alerts* tab is shown in *Figure:Alerts Tab*.

Figure:Alerts Tab



The fields and controls in this tab are described in *Table:Alerts Properties*.

Table:Alerts Properties

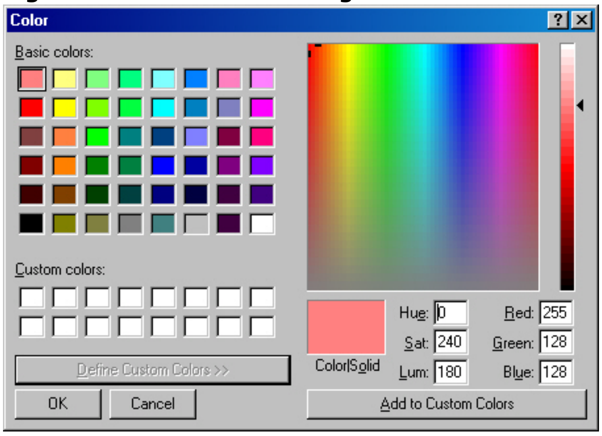
Section	Field/Control	Description
Audible Alerts	Mute Alerts	If cleared, when the (red) 'Alert Active State' is shown for one or more parameters in the Statistic View, a repeated, audible alarm sound is broadcast on the PC client station. If selected, all audible alarms are muted.
Visual Alerts		When user-selected statistics are configured for alerts, the cells in Statistic View (spreadsheet mode) are color-coded. Colors for the different alert status levels are defined in this dialog. Left-click one of the color blocks to display the *Color* dialog, shown in *Figure:Color Selection Dialog for Alert Status with Custom Colors*.
	Alert/Log Enabled	This color indicates that logging and/or alerts has been enabled for the statistic, and no alerts are active (or have been active, with acknowledgment pending). The default color is green.
	Alert Active State	This color indicates that this statistic has been enabled for alerts to be sent when out-of-range conditions occur, and that an alert is active. The default is red.
	Post Alert State	This color indicates that an alert was active, but that conditions are currently within the valid range and an acknowledgment is pending. The default is yellow.

Alert Color Selection Dialog

The *Alert Color Selection* dialog is used to control the color of alerts. It is accessed by double-clicking an alert color in the *Alerts* tab (shown in *Figure:Alerts Tab*).

The *Color* dialog for alert status colors is shown in *Figure:Color Selection Dialog* for Alert Status with Custom Colors. It can be expanded to provide access to custom colors by selecting the *Define Custom Colors >>* button.

Figure:Color Selection Dialog for Alert Status with Custom Colors



License Management

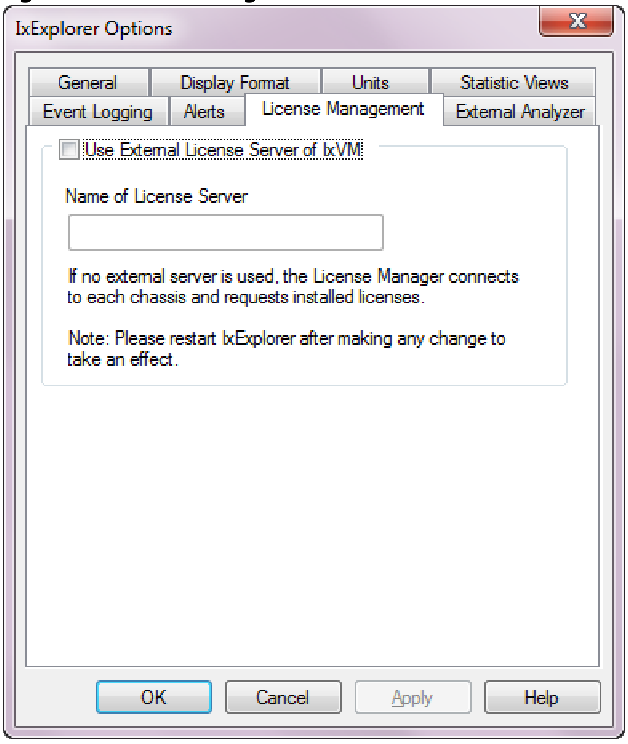
License management technique is the means by which Ixia ensures that its software is licensed and used appropriately. This allows Ixia customers to centralize and monitor their software usage.

For IxOS, only IxServer is licensed. The IxExplorer client can be installed anywhere, as many times as needed, without a license.

The *License Management* tab of the *IxExplorer Options* dialog allows to select the usage of the external license server of IxVM. If you do not use this server, the License Manager requests installation licenses for each chassis.

The *License Management* tab is shown in *Figure:License Management Tab*.

Figure:License Management Tab



The fields and controls in this tab are described in *Table:License Management Tab*.

Table:License Management Tab

Field/Control	Description
Use External License Server of IxVM	Select the check box to use the external IxVM license server for server licenses.
Name of License Server	The name of the external license server.

External Analyzer Option

The *External Analyzer* tab of the *IxExplorer Options* dialog allows to select a program to use as an external analyzer. The tab is accessed by selecting *Tools > Options* in the menu bar to open the *IxExplorer Options* dialog, then selecting the *External Analyzer* tab.

These settings apply when an *External Analyzer* tab is used to export the output file from the analyzer program to a sub-directory in the Ixia Program Files directory. This is done using the *External Analyzer* icon () located in the IxExplorer toolbar, or the External Analyzer right-click menu option in any chassis chain, chassis, card, or port. This menu option is described in the sections listed below:

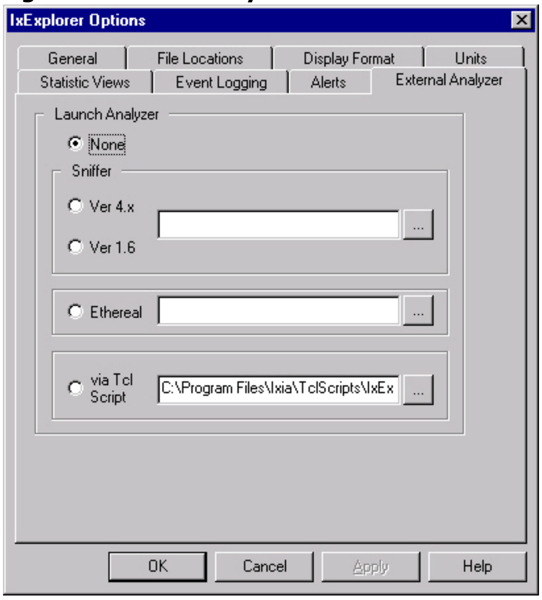
- *Chassis Chains*
- *Chassis*
- *Cards*
- Ports

The External Analyzer menu option is also part of the Port Groups right-click menu, as described in the section listed below:

- *Port Groups*

The *External Analyzer* tab is shown in *Figure:External Analyzer Tab*.

Figure:External Analyzer Tab



The fields and controls in this tab are described in *Table:External Analyzer Tab*.

Table:External Analyzer Tab

Section	Field/Control	Description
Analyzer	None	No external network protocol analyzer program is used.
	Sniffer®	The Sniffer® network protocol analyzer program is used. Select the version to be used: • Ver 4.x • Ver 1.6
	Ethereal	The (free) Ethereal network protocol analyzer program is used.
	via Tcl Script	A specified Tcl Script is used.
	...	Click this button to open the 'Cfg' sub-directory of the Ixia Program directory. Select a file, which is displayed in the field to the left.

IxOS Upgrade

This option is used to upgrade the IxExplorer client to match the version of IxServer on a chassis. You are prompted to select the *IxOS Upgrade* option when the IxExplorer client and IxServer are out of synchronization.

See *Automatic Update Feature* in the *IxOS Getting Started Guide*, for more information on the *IxOS Upgrade* option.

ScriptGen

ScriptGen (Generate Tcl Script) is a tool that may be used to generate a Tcl script that reflects the current configuration of Ixia ports. It is intended to be used after ports have been successfully configured using IxExplorer, IxAutomate (previously IxScriptmate), the Tcl API, the C++ API or other tool. The generated Tcl script can be used to recreate a port setup as the basis for a new Tcl test. ScriptGen may be used on both Windows-based and Unix-based computers.

ScriptGen generates a complete Tcl program into an output file. All aspects of a port's configuration is reflected in the output.

Generate Tcl Script is a right-click menu option for:

- Chassis, as shown in *Chassis*.
- Cards, as shown in *Cards*.
- Ports, as shown in *Ports*.

When using ScriptGen, all ports below the selected tree level is included in the generated script.

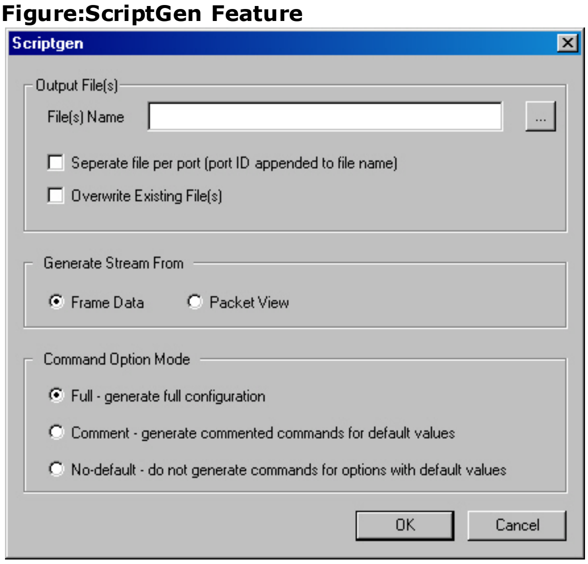
NOTE Port ownership can affect ScriptGen's file creation, in the following manner:

If the first port is explicitly owned by a user, then all ports in the set of ports to be scripted must either be owned by that user or be 'unowned.'

If the first port is 'unowned,' then all ports in the set must be 'unowned.'

The *ScriptGen* dialog is shown in *Figure:ScriptGen Feature*.

Figure:ScriptGen Feature



The controls shown in the *ScriptGen* dialog are explained in *Table:ScriptGen Usage*.

Table:ScriptGen Usage

Section	Control/Field	Usage
Output File(s)		Controls how the Tcl script is generated.
	File(s) name	The name of the output file to generate the output into. The name of the *.tcl* file should be changed for each port used.

Section	Control/Field	Usage
	...	This button allows to browse for a location to save the file.
	Separate file per port	If selected, the output for each port is saved as a separate file. The file name is an amalgam of the name indicated in the Output File Name and the chassis, slot, and port.
	Overwrite Existing File(s)	If selected, the saved file or files overwrites any files with the same name. If not selected, the output is not saved, and a warning displays in the trace window.
Generate Stream From		Determines if the stream is generated from the *Frame Control* dialog, or the *Packet View* dialog. For information on Frame Control, *Frame Data Structure* For information on Packet View,*Packet View*.
	Frame Data	Generate stream from Frame Data.
	Packet View	Generate stream from Packet View.
Command Option Mode		Sets how much of the default information should be included in the script.
	Full	Generates a script that includes all control information, whether it is default configuration or not.
	Comment	Generates a script that includes all control information, but all default configuration is set as a comment. Commented information does not affect card, port, or stream behavior.
	Non-Default	Generates a script that only includes non-default configuration information.

NOTE When using ScriptGen with Port Groups, ports in the same Port Group from different chassis chains cause the ScriptGen option to fail. Likewise, ports from chassis that have the same chassis ID causes the ScriptGen option to fail.

Chapter 4 - Stream and Flow Control

Any Ixia port can generate large numbers of packets during the course of a pattern transmission. Streams are the means by which these packets are organized and generated. Stream configuration controls how many packets are generated, the ordering of the packets, and the gaps between the packets.

The following major sections cover the use of the Stream Control functions:

- *Types of Data Transmission*
- *Types of Packet Streams*
- *Stream Properties Dialog*
- *Stream Editing*
- *Stream Grid–GFP Tab*
- *DCC Packet Streams and Packet Flows*
- *ATM Streams*
- *Changing Streams Without Interruption*

Types of Data Transmission

The Ixia system uses a sophisticated model for the programming of transmitted data. The main types of data transmission on Ixia ports are described in the following sections:

- *Packet Streams*
- *Packet Flows*
- *Advanced Streams*

For configuration and transmission of packet streams, refer to the following sections:

- *Frame Data Tab* is the means by which the contents of frames (packets) are formed.
- *Stream Properties Dialog* dictates how a set of streams is applied.
- *Stream Editing* describes how related streams can be grouped into sets which are used for pattern application or for triggered applications.

For DCC Packet Streams, Advanced Streams, and Packet Flows:
DCC Packet Streams and Packet Flows for additional information.

For ATM Streams:
ATM Streams for additional information.

For GFP Streams:
Stream Grid–GFP Tab for additional information.

Packet Streams

This model is supported by the Ixia load modules, where dedicated hardware can be used to generate up to 255 *streams*. The entire set of streams may be repeated indefinitely or for a count of times. The variability within the packets is necessarily generated algorithmically.

For ports that support more than one option, the *Transmit Mode* for each port must be set to indicate whether it will use streams, flows, or advanced streams. The programming of packet streams or packet flows uses the same programming model, with a few exceptions related to continuous bursts of packets. Since the model is so similar in both cases, we refer to both packet streams and packet flows as 'streams.' Individual streams are related to each other by their basic types.

Packet Flows

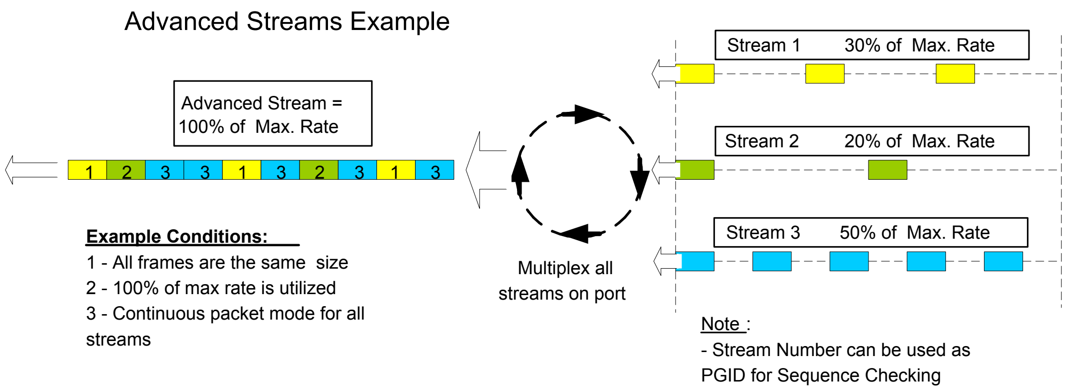
For some load modules, the transmitted data model is also supported through software, in which case the data is referred to as *flows*. Up to 15,872 unique packets may be generated by flows on ports that support this option. Because the flows are programmed in advance by the software, there can be more defined flows than streams. Flows can also transmit data configurations, which cannot be algorithmically described in streams. Flows may be created and edited in one of two ways, in the same manner as streams or (for some load modules) through a spreadsheet format flow image editor. The flow image editor saves the results in a disk file for later use.

Advanced Streams

A third type of stream configuration is called *Advanced Streams,* which involves interleaving of all defined streams for a port into a single, multiplexed stream. Each stream is assigned a percentage of the maximum rate. The frames of the streams are multiplexed so that each stream's long-term percentage of the total transmitted data rate is as-assigned. When the sum of all of the streams is less than 100% of the data rate, idle bytes are automatically inserted into the multiplexed stream, as appropriate.

Advanced Stream Scheduler is available for a number of different load modules; consult the *Ixia Platform Reference Manual*. Advanced stream configuration is explained in *Stream Control for Advanced Streams*.

Figure:Example of Advanced Stream Generation



Types of Packet Streams

The types of packet streams which can be configured in the *Stream Control* tab are illustrated in the following sections:

- *Continuous Packet Stream*
- *Continuous Burst Stream*
- *Stop After Stream*
- *Advance to Next Stream*
- *Return to ID*
- *Return to ID for Count*

Continuous Packet Stream

A Continuous Packet stream is one in which an infinite number of packets are generated, with a programmable Inter-Packet Gap (IPG). Packets are generated until a 'Stop Transmit' operation is performed. Continuous packets are **not** available for use with packet flows. The continuous packet stream is illustrated in *Figure:Continuous Packet Stream Sequence.*

Figure:Continuous Packet Stream Sequence

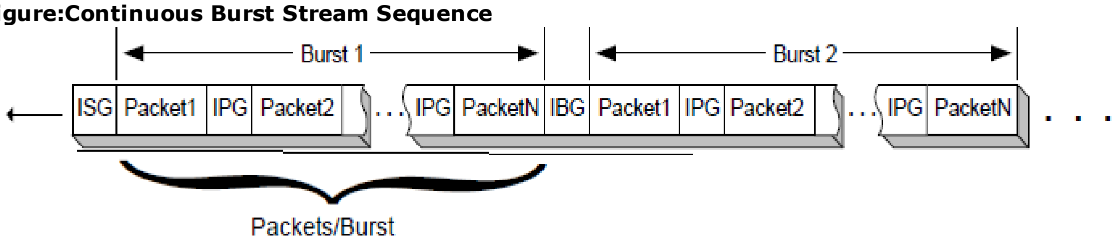
The elements of the stream are controlled by various sections of the *Stream Control* and *Frame Data* tabs, and are described in the following sections:

- Inter-Stream Gap (ISG)-*Inter-Stream Gap/Stream Gap.*
- Packet-Frame Data Tab.
- Inter-Packet Gap (IPG)-*Rate Control/Inter-Packet Gap.* ***Note**: An IPG does not follow the last packet.*

Continuous Burst Stream

A Continuous Burst stream is one in which an infinite number of bursts of packets are generated, with programmable inter-packet gaps (IPG) and inter-burst gaps (IBG). Bursts are generated until a Stop Transmit operation is performed. Continuous bursts are not available for use with flows. A continuous burst stream is illustrated in *Figure: Continuous Burst Stream Sequence.*

Figure:Continuous Burst Stream Sequence



NOTE An example of a stream with a finite number of bursts is shown in *Figure:Single*

NOTE *Stream Sequence with a Finite Number of Bursts.*

The elements of the stream are controlled by various sections of the *Stream Control* and *Frame Data* tabs, and are described in the following sections:

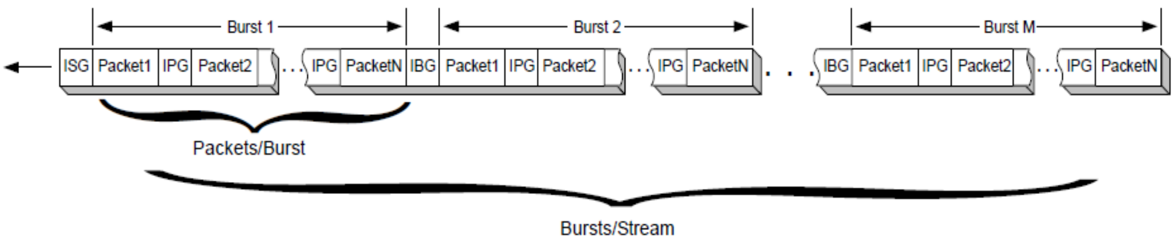
- Inter-Stream Gap (ISG): *Inter-Stream Gap/Stream Gap*.
- Packet: *Frame Data Tab*.
- Inter-Packet Gap (IPG): *Rate Control/Inter-Packet Gap*.
- Packets/Burst: *Basic Stream Controls*.
- Inter-Burst Gap (IBG): *Inter-Burst Gap/Burst Gap*.

NOTE An IBG does not follow the last packet in a stopped continuous burst stream or finite burst stream.

General Stream Structure

A stream in which a finite number of bursts is supported is illustrated in *Figure:Single Stream Sequence with a Finite Number of Bursts.*

Figure:Single Stream Sequence with a Finite Number of Bursts



The elements of the stream are controlled by other boxes and dialogs and are described in the following sections:

- Inter-Stream Gap (ISG): *Inter-Stream Gap/Stream Gap*.
- Packet:*Frame Data Tab*.
- Inter-Packet Gap (IPG): *Rate Control/Inter-Packet Gap*.
- Packets/Burst: *Basic Stream Controls*.
- Inter-Burst Gap (IBG): *Inter-Burst Gap/Burst Gap*.
- Bursts/Stream: *Basic Stream Controls*.

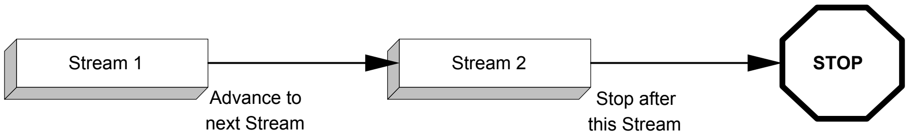
Stop After Stream

This option is used to generate a stream which is the *last* stream to be transmitted for a set of streams. Advancing from one stream to another is covered in *Advance to Next Stream*.

Advance to Next Stream

This option is used to transmit a stream and then proceed to the next stream in the set of streams. Stopping after a stream is covered in *Stop After Stream*. *The sequencing of streams is illustrated in Figure:Advance to Next Stream Sequence.*

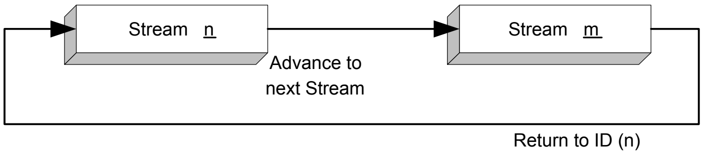
Figure:Advance to Next Stream Sequence



Return to ID

This option is used to transmit a stream and then return to a previously transmitted stream configuration (within the set of defined streams) for the next stream transmission. The set of streams is transmitted until a Stop Transmit is processed. Advancing between streams and stopping after a stream is covered in *Stop After Stream* and *Advance to Next Stream. The sequencing of streams is illustrated in Figure:Return to ID Stream Sequence.*

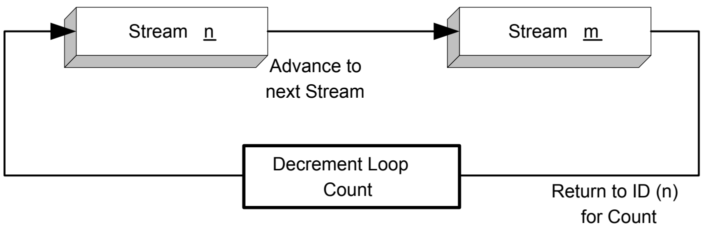
Figure:Return to ID Stream Sequence



Return to ID for Count

This option is used to transmit a stream and then proceed to a previous stream (located by its stream ID) in the set of streams, forming a loop for transmitting the included subset of streams for a programmable number of times. Advancing between streams and stopping after a stream is covered in previous sections. The sequencing of streams is illustrated in *Figure:Return to ID for Count Sequence.*

Figure:Return to ID for Count Sequence



Stream Properties Dialog

The *Stream Properties* dialog is displayed by double-clicking a row in the Packet Stream-s/Flows grid window, or by right-clicking a port and selecting the *Edit Streams* option in the menu. Within the dialog, the *Stream Control* tab allows you to control the type and con-figuration of individual streams or flows.

There are several variations of the *Stream Control* tab, based on the type of load module, described in the following sections:

- *Stream Control Tab for 10/100 Modules*
- *Stream Control Tab for Gigabit Modules*

- *Stream Control for Standard POS Modules*
  - Also applies to optional DCC packet streams.
  - Does not apply to POS 622 (OC-12c/OC-3c POS) modules.
- *Stream Control for POS 622 Modules*
- *Stream Control for 10 Gigabit Modules*
- *Stream Control for TXS Ethernet Modules*
- *Stream Control for Xcellon-Flex Modules*
- *Stream Control for Lava, Multis, Novus, and Novus-R Modules*
- *ATM Streams*

For the Advanced Stream Scheduler, refer to:

- *Stream Control for Advanced Streams*

For information on the GFP Stream Queue grid, refer to:

- *Stream Grid–GFP Tab*

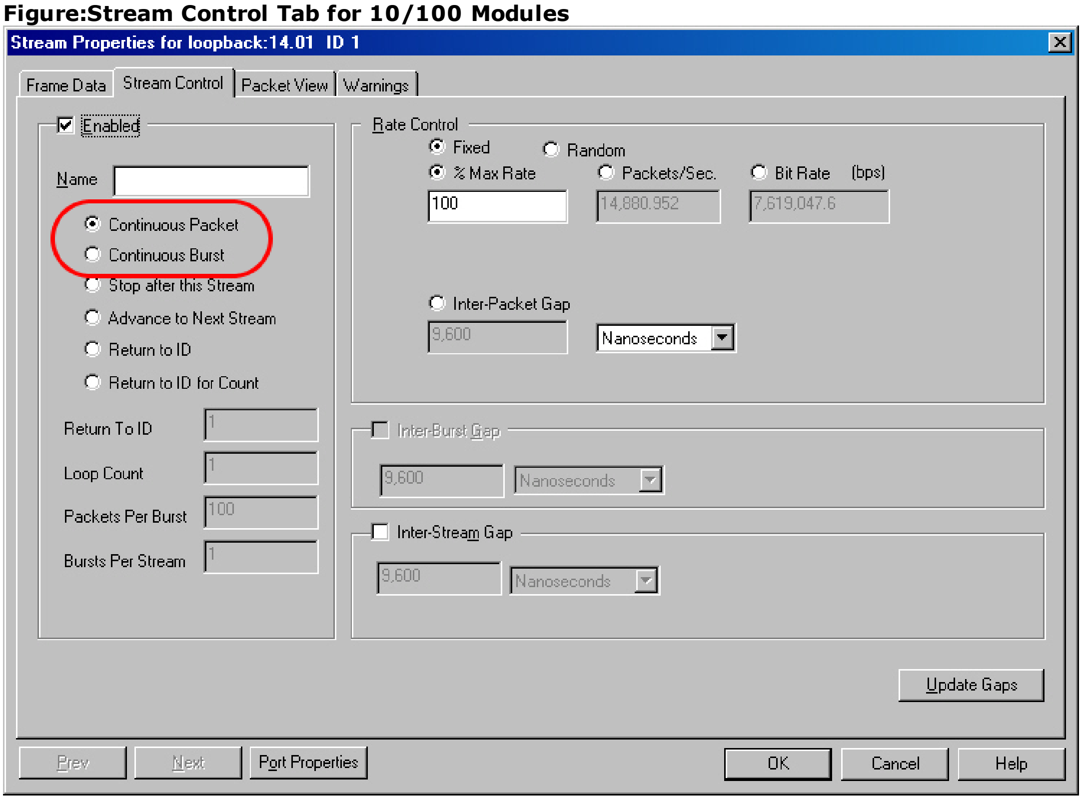
For ATM Stream Control, refer to:

- *Stream Control for ATM*

Stream Control Tab for 10/100 Modules

The *Stream Control* tab for 10/100 modules is shown in *Figure:Stream Control Tab for 10/100 Modules*. The options within the dotted frame are not supported for Packet Flows. Refer to *General Structure of Stream Control Tab* for information on the content of the tab.

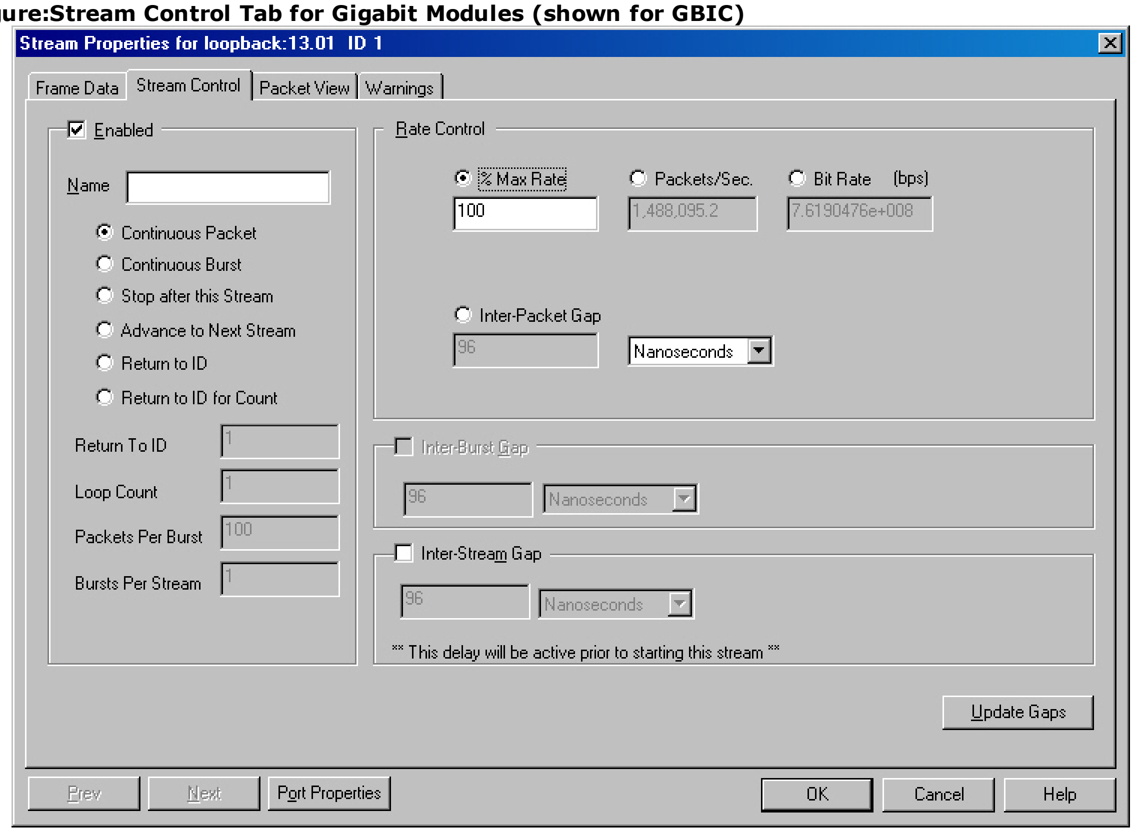
Figure:Stream Control Tab for 10/100 Modules



Stream Control Tab for Gigabit Modules

The *Stream Control* tab for Gigabit modules is shown in *Figure:Stream Control Tab for Gigabit Modules (shown for GBIC).* Refer to General Structure of Stream Control Tab for information on the content of the tab.

Figure:Stream Control Tab for Gigabit Modules (shown for GBIC)

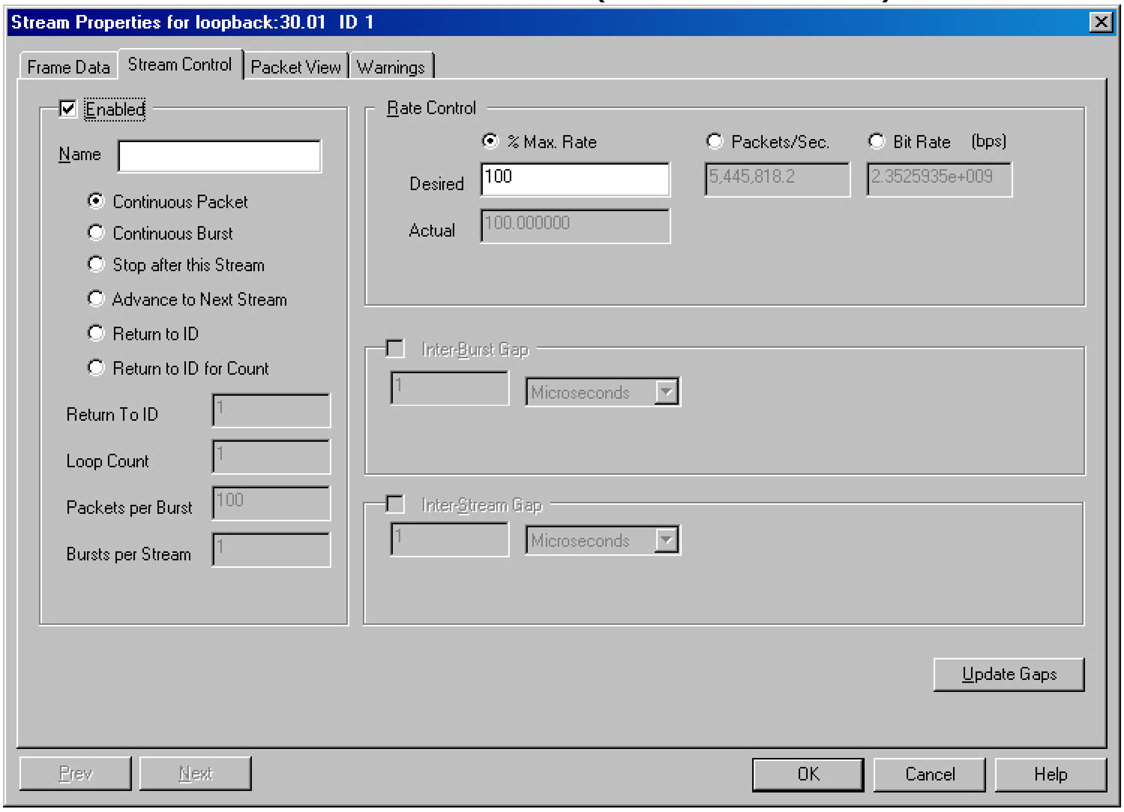


Stream Control for Standard POS Modules

The *Stream Control* tab for standard Packet over SONET (POS) modules is shown in *Figure:Stream Control Tab for Standard POS Modules (shown for OC-48c POS).* Refer to *General Structure of Stream Control Tab* for information on the content of the tab.

NOTE **for DCC:**
This tab is also used to set up DCC Packet Streams for the optional DCC feature. For additional information on DCC packet streams DCC Packet Streams and Packet Flows.

Figure:Stream Control Tab for Standard POS Modules (shown for OC-48c POS)

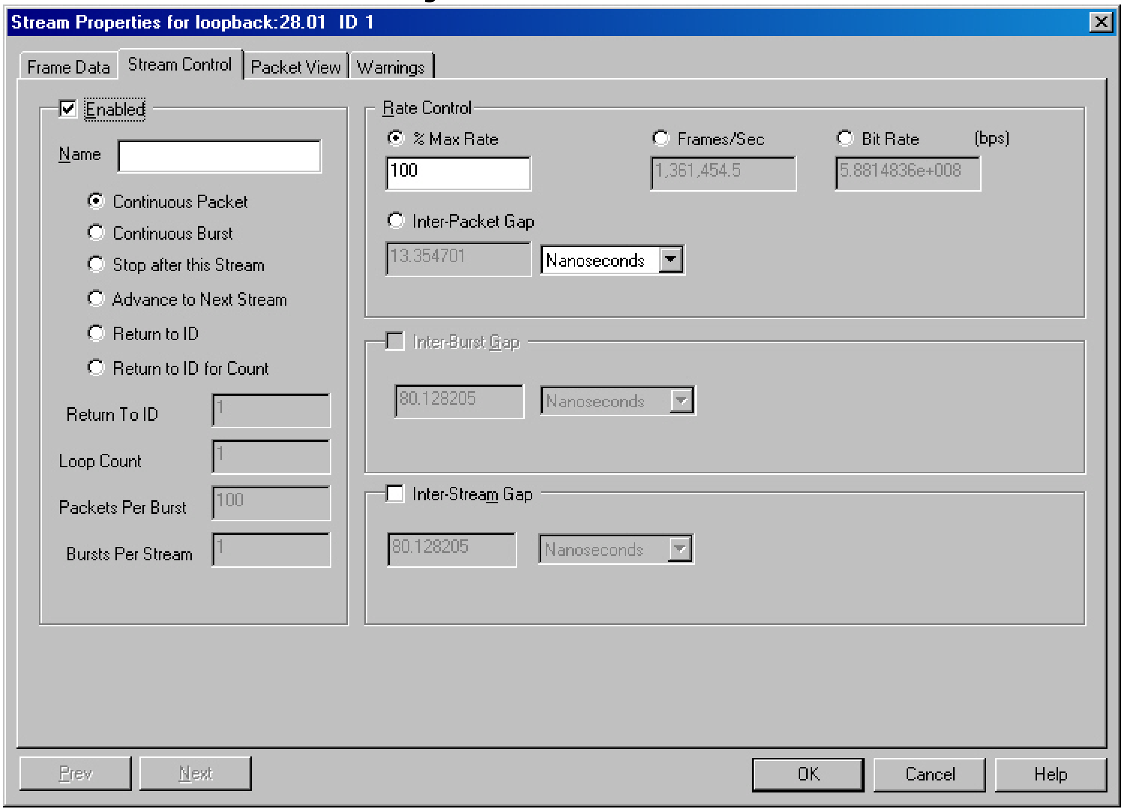


Stream Control for POS 622 Modules

The *Stream Control* tab for POS 622 (OC-12c/OC-3c POS) modules combines aspects of both TXS Ethernet and standard POS modules *Stream Control* tabs. Refer to *General Structure of Stream Control Tab* for information on the content of the tab.

The POS 622 *Stream Control* tab is shown in *Figure:POS 622 Stream Control Tab Page.*

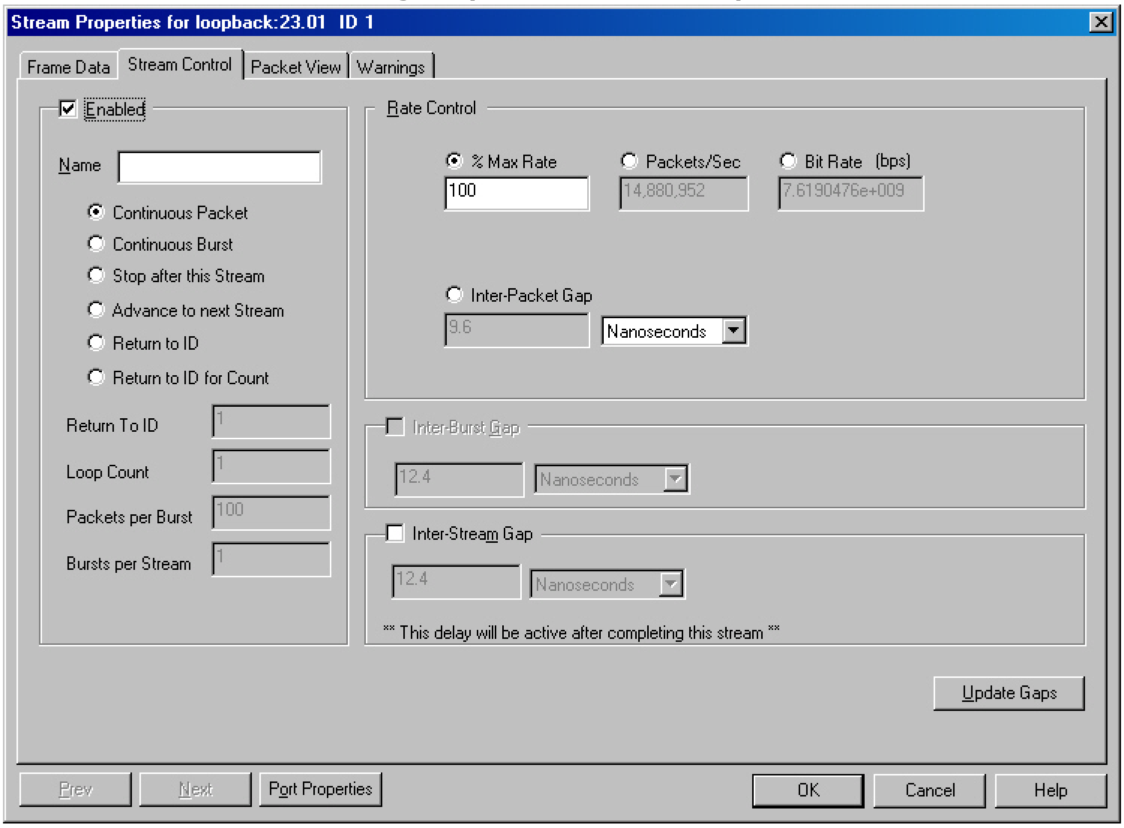
Figure:POS 622 Stream Control Tab Page



Stream Control for 10 Gigabit Modules

The *Stream Control* tab for 10 Gigabit modules is shown in *Figure:Stream Control Tab for 10 Gigabit (shown for 10GE WAN).*Refer to General Structure of Stream Control Tab for information on the content of the tab.

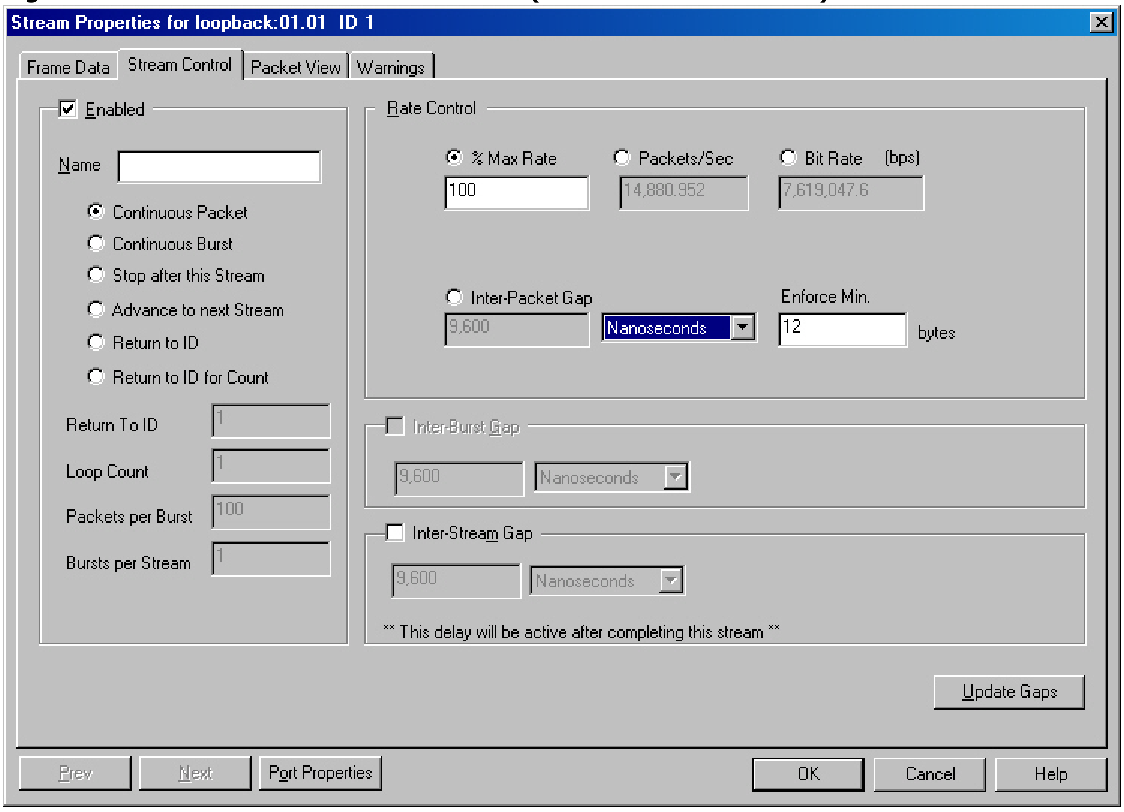
Figure:Stream Control Tab for 10 Gigabit (shown for 10GE WAN)



Stream Control for TXS Ethernet Modules

The *Stream Control* tab for the TXS family of modules (10/100 TXS8, 10/100/1000 TXS4, and 1000 SFPS4) is shown in *Figure:Stream Control Tab for TXS Modules (shown for 1000 SFPS4).* Refer to *General Structure of Stream Control Tab* for information on the contents of the tab.

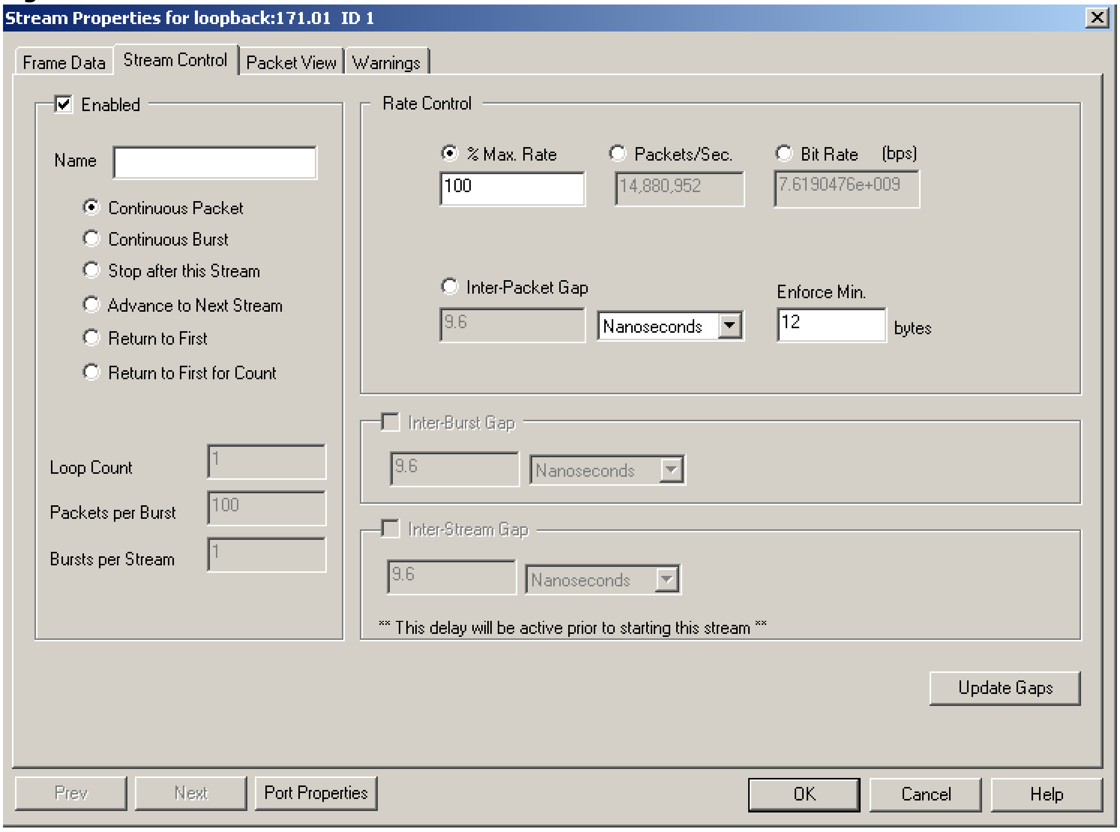
Figure:Stream Control Tab for TXS Modules (shown for 1000 SFPS4)



Stream Control for Xcellon-Flex Modules

The *Stream Control* tab for the Xcellon-Flex family of modules (FlexAP10G16S and FlexFE10G16S) is shown in *Figure:Stream Control Tab for Xcellon-Flex Modules.*Refer to *General Structure of Stream Control Tab* for information on the contents of the tab.

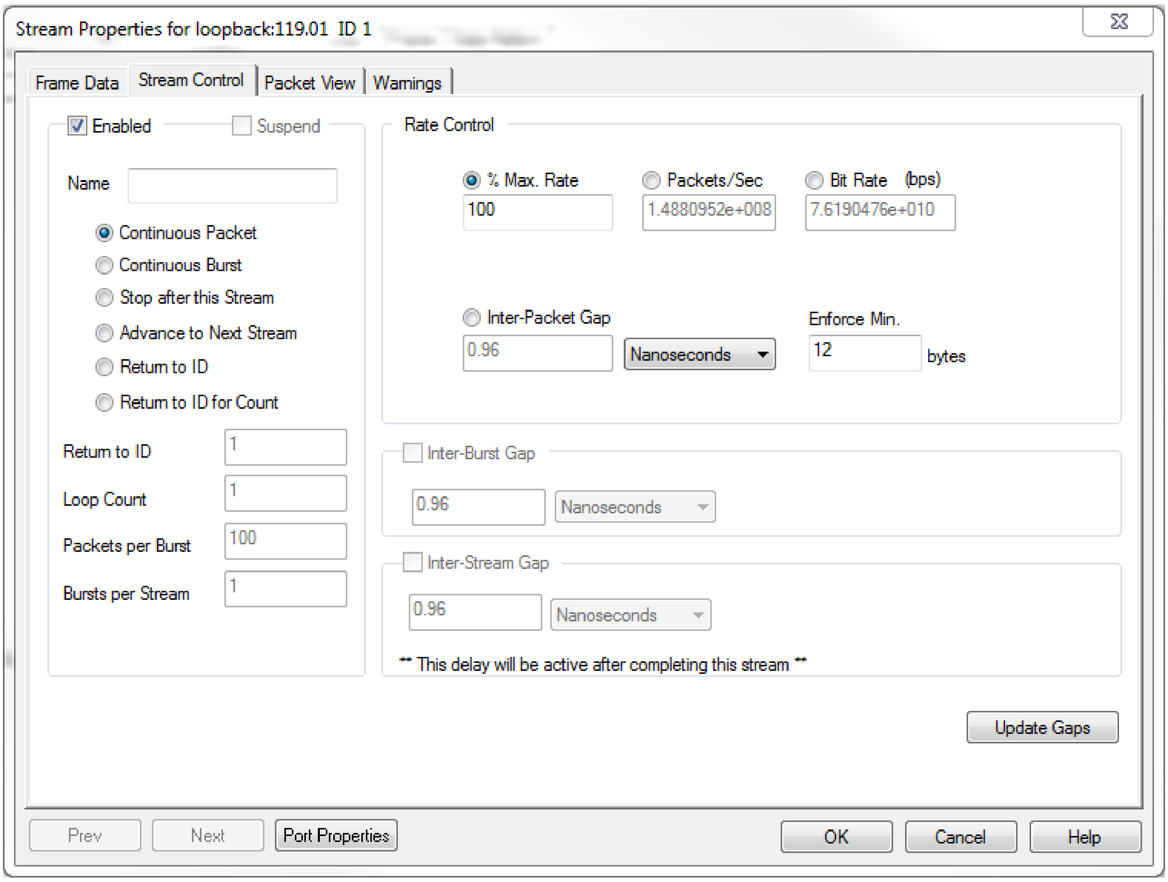
Figure:Stream Control Tab for Xcellon-Flex Modules



Stream Control for Lava, Multis, Novus, and Novus-R Modules

The *Stream Control* tab for Lava, Multis, Novus, and Novus-R modules is shown as follows: Refer to *General Structure of Stream Control Tab* for information on the contents of the tab.

Figure:Stream Control Tab for Lava, Multis, Novus, and Novus-R Modules



General Structure of Stream Control Tab

The sections within the *Stream Control* tab control all aspects of stream formation. The general division is:

Basic Stream Controls	Within the left section of the tab. Controls the basic type of each stream as well as the counts for packets, bursts and loop counts. You may assign a name to each stream for reference purposes.
Rate Control/Inter-Packet Gap	Controls the time interval between packets.
Inter-Burst Gap/Burst Gap	Controls the time interval between bursts of packets.
Inter-Stream Gap/Stream Gap	Controls the time interval before each stream.
Update Gaps Button	When the values/units for parameters in the *Stream Control* tab are changed, press the *Update Gaps* button. This results in an update of the other related parameters.
Port Properties Dialog	Controls a number of basic port properties. This dialog is discussed in the following chapters: • Chapter 18,*Port Properties — 10/100/1000 Ethernet Family* • Chapter 19,*Port Properties–POS and ATM Families* • Chapter 20,*Port Properties–10 GE and UNIPHY Families* • Chapter 21,*Port Properties–40/100 GE Family*
Next/Prev	Displays the *Stream Control* tab for the Next or Previous stream.

Basic Stream Controls

The basic stream controls for all types of load modules are included in the *Enabled* box on the left hand side of the *Stream Control* tab, as shown in *Figure:Basic Stream Controls.*

Figure:Basic Stream Controls

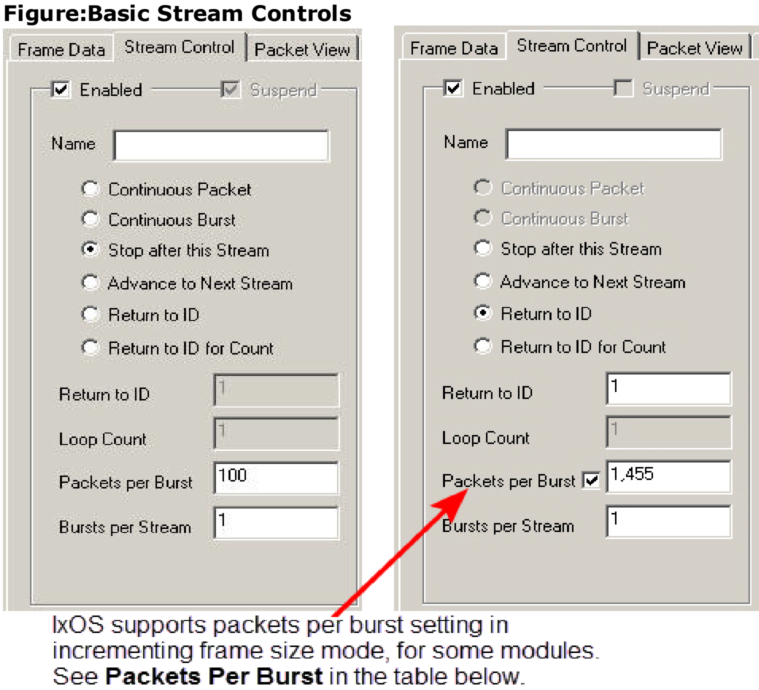


Figure:Basic Stream Controls—Flex Module

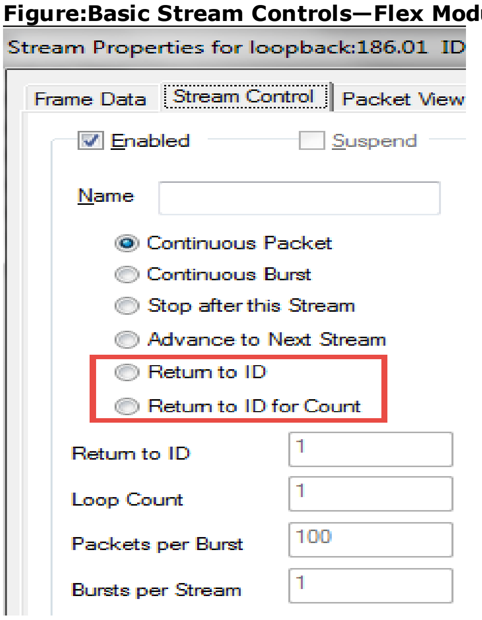
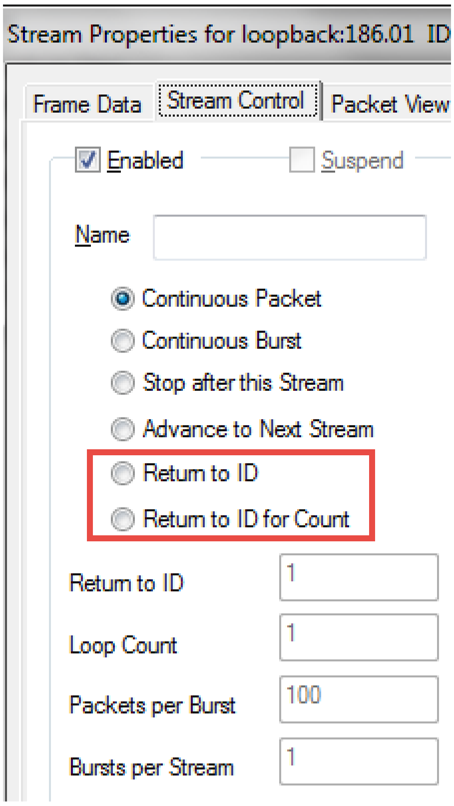


Figure:Basic Stream Controls—Multis Module



The fields and controls in this box are described in *Table:Basic Stream Controls.*

Table:Basic Stream Controls

Field/Control	Description
Enabled	A stream must be enabled in order for it to be used. Up to 255 streams may be defined per port. Disabled streams are skipped over when the port transmits.
Suspend	Select check box to suspend selected stream(s). Uncheck to resume. This will cause the traffic to stop and restart. *Changing Streams Without Interruption* for details.
Name	This is a user-assigned name for the stream. This name need not be unique.
Continuous Packet	Designates a type of stream that sends out a continuous sequence of packets with the same inter-packet gap between packets. Continuous Packet mode may not be used with flows. *Continuous Packet Stream*.
Continuous Burst	Designates a type of stream that sends out a continuous set of packet bursts. Continuous Burst mode may not be used with flows. See **Note** below for information on maximum burst count. *Continuous Burst Stream*.
Stop after this Stream	Designates that this stream is the end of a sequence of streams. *Stop After Stream*.
Advance to next	Designates that the next stream is to be transmitted after the cur-

Field/Control	Description
Stream	rent stream is complete. *Advance to Next Stream*.
Return to First	Designates that the stream identified (with a Stream ID) in the *Return To First* field is to be used after the first stream is complete.
Return to First for Count	Designates that the stream identified in the *Return To First* field is to be used after the first stream is complete. The loop is repeated for number of times specified in the Loop Count parameter.
Return to ID	Designates that the stream identified (with a Stream ID) in the *Return To ID* field is to be used after the current stream is complete. *Return to ID*.
Return to ID for Count	Designates that the stream identified in the *Return To ID* field is to be used after the current stream is complete. The loop is repeated for number of times specified in the Loop Count parameter. *Return to ID for Count*.
Loop Count	The count used in a stream loop. Indicates the number of times that the stream identified in the *Return to ID* field is transmitted. *Return to ID for Count*.
Packets per Burst	Specifies the number of packets in each burst. Some load modules support packets per burst setting in incrementing frame size mode.Using the Packet/Burst Setting in Incrementing Frame Size Mode (Chapter 5) for information.
Bursts per Stream	Specifies the number of bursts in each stream. See **Note** below for information on maximum burst count.

NOTE **Maximum Memory for Stream Data Xcellon**-Multis load modules have 64KB memory per resource group for stream data. As the value list, frame size, and other stream properties become more complex, the maximum number of streams decrease.

NOTE **Maximum Burst Count** This field applies to burst counts on multi-speed load modules. The maximum burst count is different for different speeds on multi-speed load modules. If the value in the burst count field is larger than the maximum when the speed is changed, the value is changed to the new maximum. Refer to the *Ixia Platform Reference Manual* for the per speed limits.

Rate Control/Inter-Packet Gap

The rate control and inter-packet gap are controlled by the setting the Rate Control section of the *Stream Control* tab, shown in *Figure:Stream Control—Rate Control and Inter-Packet Gap, Fixed Mode (shown for Standard 10/100 Ethernet Module)* for 10/100 and Gigabit modules. The tab for standard Packet over SONET modules is discussed in *Rate Control for Standard POS Modules*.

NOTE

On older load modules, streams require a minimum period for setup which is equal to the time required to send 5 packets. When running at wire speeds, a stream with less than 5 packets may generate a trailing IPG before the start of transmission of the following stream. Flows do not exhibit this limitation. Also, using a long inter-frame gap that exceeds the timeout value of a protocol causes the protocol to fail.

Setting the inter-packet gap and the rate control is discussed in the following sections:

- *Rate Control/Inter-Packet Gap*
- *Rate Control for Standard POS Modules*

Rate Control/Inter-Packet Gap

The Rate Control and Inter-Packet Gap (IPG) can be set for 10/100 and Gigabit Ethernet modules, 10 Gigabit modules, and POS 622 (OC-12c/OC-3c POS). The sections for setting the IPG are described in the following sections:

- *Rate Control/IPG for Standard 10/100 Ethernet*
- *Rate Control/IPG for Standard Gigabit, 10 Gigabit Ethernet, and POS 622 Modules*
- *Rate Control/IPG for TXS Ethernet Modules*
- *Rate Control/IPG for FC Modules*

Rate Control/IPG for Standard 10/100 Ethernet

Figure:Stream Control—Rate Control and Inter-Packet Gap, Fixed Mode (shown for Standard 10/100 Ethernet Module)

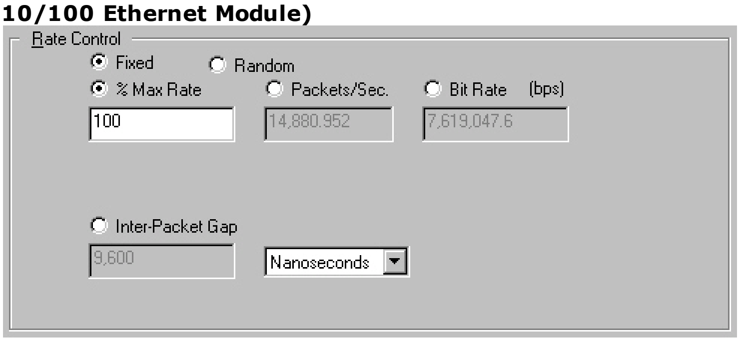
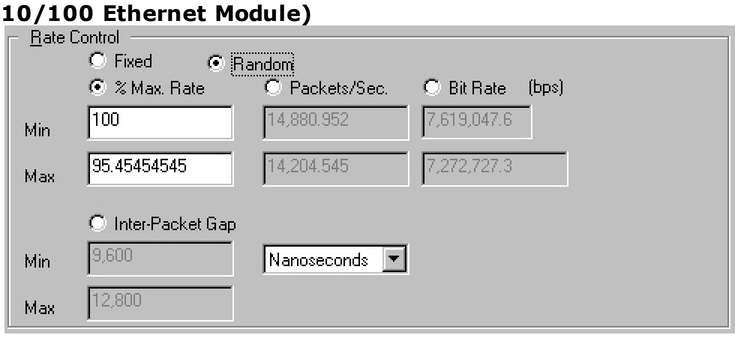


Figure:Stream Control—Rate Control and Inter-Packet Gap, Random Mode (shown for Standard 10/100 Ethernet Module)



The inter-packet gap controls allow to specify the gap between packets. The gap can be specified in terms of time, desired packets/second, or percentage of utilization of the max rate. IPGs are inserted between packets, but not at the end of bursts or streams.

The minimum time, maximum time, and resolution varies depending on the load module type. Refer to *Ixia Platform Reference Manual* for a full description. The fields and controls in this box are described in *Table:Inter-Packet Gap Controls for Ethernet Modules.*

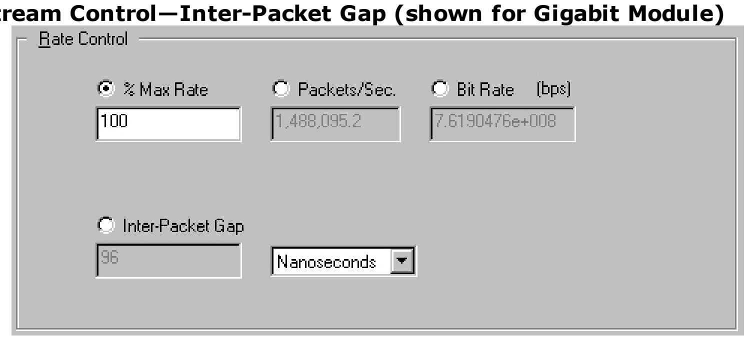
Table:Inter-Packet Gap Controls for Ethernet Modules

Section	Field/Control	Description
Choice of Generation Type	Fixed	When selected (as opposed to the *Random* selection), all inter-packet gaps are a constant value specified by the *Value* row.
	Random	When selected (as opposed to the *Fixed* selection), the size of inter-packet gaps is randomly generated within the range of values specified in the *Min* and *Max* rows.
% Max Rate		For fixed IPGs, this specifies the percentage of time to be used for packet transmission versus total transmission time. The actual inter-packet gap time is configured to allow that utilization. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the percentage utilization within a burst; except for *Continuous Packet* type streams the percentage is lower due to inter-burst and Inter-Stream gaps. The use of *% Max Rate* is controlled by *Options*.
Packets/Sec		For fixed IPG's, this specifies the intended number of packets to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets transmitted per second within a burst; except for *Continuous Packet* type streams the actual packets per second is lower due to inter-burst and inter-stream gaps.
Bit Rate (bps)		The bit rate of the stream, in bits per seconds.
Inter-Packet Gap		This specifies the amount of time between packets within a burst. The time must be specified in multiples of the indicated time units.
Bit Rate		(Read-only) The bit rate of the stream, in bits per seconds.
Units		Selects the time units used for the *Inter-Packet Gap* column. The choices available depend on the type of load module: • Nanoseconds (default) • Microseconds • Milliseconds • Seconds

Section	Field/Control	Description
		• Clock Ticks: The length of a clock tick varies by load module type. Refer to the *Ixia Platform Reference Manual* for values. • Bytes
Min Gap **(For Use with Random IPGs ONLY)**	% Max Rate	For random IPGs, this specifies the lower end of the range of percentage utilization to be generated. See *% Max Rate* above for a full explanation of this field. The use of *% Max Rate* is controlled by *Options*.
	Packets/Sec	For random IPGs, this specifies the lower end of the range of packets per second to be generated. See *Packets/Sec* above for a full explanation of this field.
	Bit Rate	The bit rate of the stream, in bits per seconds.
	Inter-Packet Gap	For random IPGs, this specifies the lower end of the range of time values to be generated. See *Inter-Packet Gap* above for a full explanation of this field.
Max Gap **(For Use with Random IPGs ONLY)**	% Max Rate	For random IPGs, this specifies the upper end of the range of percentage utilization to be generated. See *% Max Rate* above for a full explanation of this field. The use of *% Max Rate* is controlled by *Options*.
	Packets/Sec	For random IPGs, this specifies the upper end of the range of packets per second to be generated. See *Packets/Sec* above for a full explanation of this field.
	Bit Rate	(Read-only) The bit rate of the stream, in bits per seconds.
	Inter-Packet Gap	For random IPGs, this specifies the upper end of the range of time values to be generated. See *Inter-Packet Gap* above for a full explanation of this field.

Rate Control/IPG for Standard Gigabit, 10 Gigabit Ethernet, and POS 622 Modules

Stream Control—Inter-Packet Gap (shown for Gigabit Module)



The Inter-Packet Gap Box controls allow to specify the gap between packets. The gap can be specified in terms of time, desired packets/second, or percentage utilization/Max Rate. IPGs are inserted between packets, but not at the end of bursts or streams.

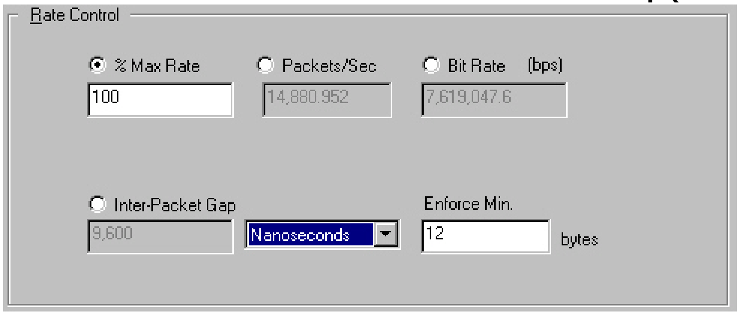
The fields and controls in this box are described in *Table:Inter-Packet Gap Controls for Gigabit and 10 Gigabit Modules.*

Table:Inter-Packet Gap Controls for Gigabit and 10 Gigabit Modules

Section	Field/Control	Description
% Max Rate		For fixed IPGs, this specifies the percentage of time to be used for packet transmission versus total transmission time. The actual inter-packet gap time is configured to allow that utilization. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the percentage utilization within a burst; except for *Continuous Packet* type streams the percentage is lower due to inter-burst and Inter-Stream gaps. The use of *% Max Rate* is controlled by Options.
Packets/Sec		For fixed IPGs, this specifies the intended number of packets to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets transmitted per second within a burst; except for *Continuous Packet* type streams the actual packets per second is lower due to inter-burst and inter-stream gaps.
Bit Rate		The bit rate of the stream, in bits per seconds.
Inter-Packet Gap		This specifies the amount of time between packets within a burst. The time must be specified in multiples of the indicated time units.
Units		Selects the time units used for the *Inter-Packet Gap* column. The choices available depend on the type of load module: • Nanoseconds (default) • Microseconds • Milliseconds • Seconds • Clock Ticks: The length of a clock tick varies by load module type. Refer to the *Ixia Platform Reference Manual* for values. • Bytes

Rate Control/IPG for TXS Ethernet Modules

Figure:Stream Control—Rate Control and Inter-Packet Gap (shown for TXS Module)



The Inter-Packet Gap Box allows to specify the gap between packets. The gap can be specified in terms of time, desired packets/second, or percentage utilization/Max Rate. IPGs are inserted between packets, but not at the end of bursts or streams.

The fields in this box are described in *Table:Inter-Packet Gap for TXS Ethernet Modules.*

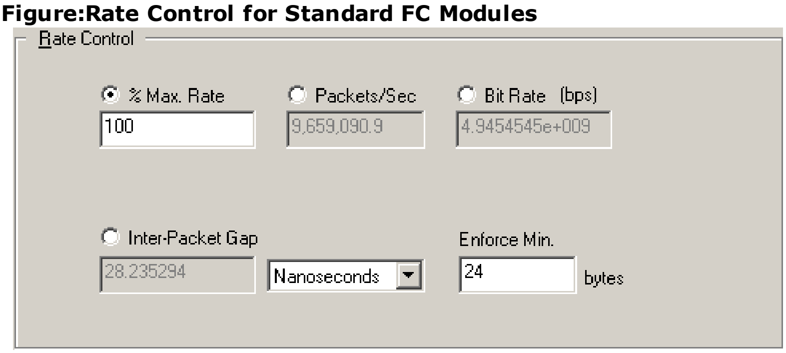
Table:Inter-Packet Gap for TXS Ethernet Modules

Section	Field/Control	Description
% Max Rate		For fixed IPGs, this specifies the percentage of time to be used for packet transmission versus total transmission time. The actual inter-packet gap time is configured to allow that utilization. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the percentage utilization within a burst; except for *Continuous Packet* type streams the percentage is lower due to inter-burst and Inter-Stream gaps. The use of %Max Rate is controlled by *Options*.
Packets/Sec		For fixed IPGs, this specifies the intended number of packets to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets transmitted per second within a burst; except for *Continuous Packet* type streams the actual packets per second is lower due to inter-burst and inter-stream gaps.
Bit Rate		The bit rate of the stream, in bits per seconds.
Inter-Packet Gap		This specifies the amount of time between packets within a burst. The time must be specified in multiples of the indicated time units.
Units		Selects the time units used for the *Inter-Packet Gap* column. The choices available depend on the type of load module: • Nanoseconds (default) • Microseconds

Section	Field/Control	Description
		• Milliseconds • Seconds • Clock Ticks: The length of a clock tick varies by load module type. Refer to the *Ixia Platform Reference Manual* for values. • Bytes
Enforce Min Gap		(For TXS family of modules only.) (In bytes) Sets the smallest inter-packet gap (IPG) that is allowed. The default is 12 bytes.

Rate Control/IPG for FC Modules

Figure:Rate Control for Standard FC Modules



The Inter-Packet Gap box allows to specify the gap between packets. The gap can be specified in terms of time, desired packets/second, or percentage utilization/Max Rate. IPGs are inserted between packets, but not at the end of bursts or streams.

The fields in this box are described in *Table:Inter-Packet Gap for FC Modules.*

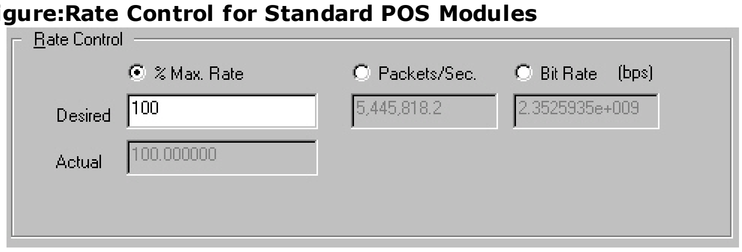
Table:Inter-Packet Gap for FC Modules

Section	Field/Control	Description
% Max Rate		For fixed IPGs, this specifies the percentage of time to be used for packet transmission versus total transmission time. The actual inter-packet gap time is configured to allow that utilization. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the percentage utilization within a burst; except for *Continuous Packet* type streams the percentage is lower due to inter-burst and Inter-Stream gaps.
Packets/Sec		For fixed IPGs, this specifies the intended number of packets to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets transmitted per second within a burst; except for *Continuous Packet* type streams the actual

Section	Field/Control	Description
		packets per second is lower due to inter-burst and inter-stream gaps.
Bit Rate		The bit rate of the stream, in bits per seconds.
Inter-Packet Gap		This specifies the amount of time between packets within a burst. The time must be specified in multiples of the indicated time units.
Units		Selects the time units used for the *Inter-Packet Gap* column. The choices available depend on the type of load module: • Nanoseconds (default) • Microseconds • Milliseconds • Seconds • Bytes
Enforce Min.		(In bytes) Sets the smallest inter-packet gap (IPG) that is allowed. The minimum IPG can be set at 24 bytes for FC modules.

Rate Control for Standard POS Modules

Figure:Rate Control for Standard POS Modules



Rate control is available for standard Packet over SONET modules controls the average rate of transmitting packets. Rate control is also available for, which is described in *Stream Control for POS 622 Modules*

NOTE

POS 622 modules use *Inter-Packet Gap* (IPG) fields instead of *Rate Control* fields. For information on setting POS 622 module IPG, *Rate Control/Inter-Packet Gap*.

The fields and controls in this box are described in *Table:Rate Controls for Standard (POS) Modules.*

Table:Rate Controls for Standard (POS) Modules

Field/Control	Description
% Max Rate	Allows the average packet rate to be exclicked as a percentage of the maximum rate.
Actual	An automatic calculation of the actual packet rate, based on the capabilities of the port, exclicked as a percentage of the maximum rate.

Field/Control	Description
Packets Per Second	An automatic calculation of the number of packets per second based on the Packet Rate.
Bit Rate	The bit rate of the stream, in bits per seconds.

Inter-Burst Gap/Burst Gap

Inter-Burst Gaps (IBGs)/Burst Gaps are inserted between packet bursts, but not at the end of bursts or streams. The minimum and maximum time and resolution vary, depending on the load module type. (Refer to *Ixia Platform Reference Manual*.)

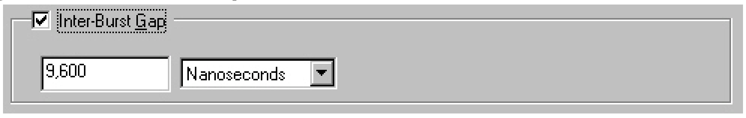
The gap interval between packet bursts within a stream is defined differently for Ethernet-type and POS modules. These types are explained in the following sections:

- *Inter-Burst Gap (IBG)*
- *Inter-Stream Gap/Stream Gap*

Inter-Burst Gap (IBG)

The gap between bursts of transmitted packets is controlled by the Inter-Burst Gap (IBG) box, as shown in *Figure:Inter-Burst Gap.*

Figure:Inter-Burst Gap



The fields and controls in this box are described in *Table:Inter-Burst Gap Controls for Ethernet-Type Modules.*

Table:Inter-Burst Gap Controls for Ethernet-Type Modules

Field/Control	Description
Inter-Burst Gap	Select this box to enable the generation of inter-burst gaps.
Value–Time **or** Value–Time/Bytes	This specifies the amount of time between bursts within a stream. The time must be specified in multiples of the indicated time units. For 10 Gigabit, 10/100/1000 TXS8, 1000 SFPS4, and 10/100/1000 TXS4 modules, the gap can be specified in bytes instead of time units.
Units	Selects the time units used for the *Time* column. The choices available depend on the type of load module: • Nanoseconds (not available on standard POS modules) • Microseconds • Milliseconds • Seconds • Clock Ticks: The length of a clock tick varies by load module type. Refer to the *Ixia Platform Reference Manual* for values (not available on standard POS modules). • Bytes (not available for standard POS or POS 622 modules)

Inter-Stream Gap/Stream Gap

Inter-Stream Gaps precede nearly all types of streams, even Continuous Packet and Continuous Burst streams. Advanced Streams are not preceded by inter-stream gaps, and for 10 Gigabit ports, the inter-stream gap is active AFTER the stream rather than before. The minimum and maximum time and resolution varies depending on the load module type (refer to the *Ixia Platform Reference Manual*).

The gap interval between streams is defined differently for Ethernet-type and POS modules. These types are described in the following sections:

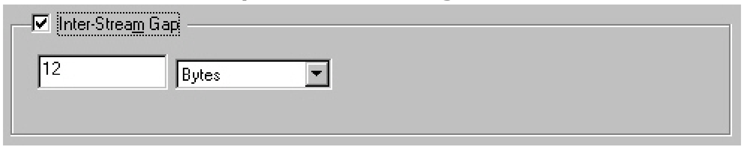
- *Inter-Stream Gap (ISG) for Ethernet-Type and POS 622 Modules*
- *Stream Gap for Standard POS Modules*

NOTE No Inter-Stream Gap (ISG) is used for Advanced Streams.

Inter-Stream Gap (ISG) for Ethernet-Type and POS 622 Modules

The gap before an Ethernet or POS 622 stream is controlled by a setting in the Inter-Stream Gap box, as shown in *Figure:Inter-Stream Gap for 10/100, Gigabit, and POS 622 Modules.*

Figure:Inter-Stream Gap for 10/100, Gigabit, and POS 622 Modules



The fields and controls in this box are described in *Table:Inter-Stream Gap Controls for 10/100 Ethernet, Gigabit, and POS 622 Modules.*

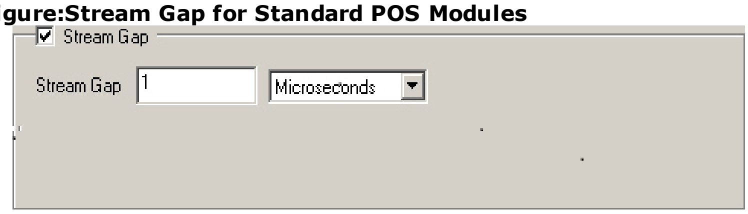
Table:Inter-Stream Gap Controls for 10/100 Ethernet, Gigabit, and POS 622 Modules

Field/Control	Description
Inter-Stream Gap	If selected, enables generation of the inter-stream gap.
Units	Selects the time units used for the *Time* field. The choices available depend on the type of load module: • Nanoseconds • Microseconds • Milliseconds • Seconds • Clock Ticks: The length of a clock tick varies by load module type. Refer to the *Ixia Hardware Manual* for values. • Bytes (not available for POS 622).
Time **or** Time/Bytes	This specifies the amount of time between streams. The time must be specified in multiples of the indicated time units. For 10 Gigabit, 10/100/1000 TXS8, 1000 SFPS4, and 10/100/1000 TXS4 modules, the gap can be specified in bytes instead of time units.

Stream Gap for Standard POS Modules

The Stream Gap for Packet over SONET Modules controls the amount of time before another stream is applied. The Stream Gap box is shown in *Figure:Stream Gap for Standard POS Modules.*

Figure:Stream Gap for Standard POS Modules



The fields and controls in this box are described in *Table:Stream Gap Controls for Packet over SONET Modules.*

Table:Stream Gap Controls for Packet over SONET Modules

Field/Control	Description
Stream Gap	Check this box to enable generation of the inter-stream gap.
Stream Gap	This specifies the amount of time between streams. The time must be specific in multiples of the simulated time units.
(Time units)	Selects the time units for the *Time* column. The choices are: • Microseconds • Milliseconds • Seconds

Stream Control for Advanced Streams

The Advanced Stream Scheduler feature, which is available on a number of modules, as detailed in the *Ixia Platform Reference Manual*, interleaves all of the individually configured streams for the port. This allows to configure a number of streams which are concurrently active. They transmit packets in an interleaved fashion.

Refer to *Advanced Streams* for additional information on Advanced Streams.

There are two different tabs for advanced stream configuration, depending on the type of module, and these are described in the following sections:

- *Advanced Streams for Standard POS and POS 622 Modules*.
- *Advanced Streams for Ethernet Modules* .
  (10GE, 10/100 TXS8, 10/100/1000 TXS4, 1000 SFPS4, 10GE XDM10G32S)

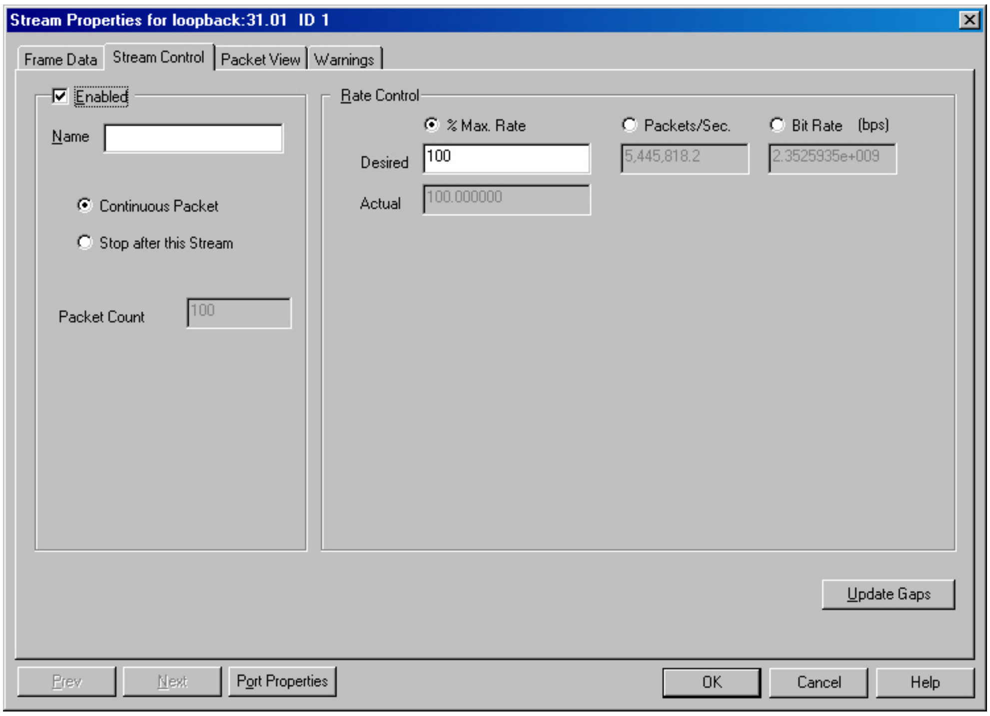
NOTE For DCC Advanced Streams *Advanced Streams for Standard POS and POS 622 Modules*.

Advanced Streams for Standard POS and POS 622 Modules

For standard Packet over SONET (POS) and POS 622 module advanced streams, the desired packet rate, as a percentage of the Maximum rate, can be configured for each of the streams. The *Stream Control* tab for POS Advanced Streams is shown in *Figure:Stream Control for Advanced Streams—POS.*

NOTE **DCC** tab is also used to set up DCC Advanced Streams for the optional DCC feature. For additional information on DCC packet streams *DCC Packet Streams and Packet Flows*.

Figure:Stream Control for Advanced Streams—POS



The fields and controls in this tab are described in *Table:Stream Control for Advanced Streams—POS.*

Table:Stream Control for Advanced Streams—POS

Section	Field/Control	Description
(Stream info)	Enabled	Check this box to enable the use of the stream configured in this tab.
	Name	(Optional) A user-assigned name for this stream.
	(Type of stream transmission)	Choose one of: • **Continuous Stream**: The configured stream is repeated until a Stop Transmit is sent. • **Stop After This Stream**: Transmission stops after this stream is sent. The length of the stream is determined by the value entered into the *Packet Count* field.
	Packets Count	The total number of packets to be sent in this configured stream.
Packet (rate)	% Max Rate	Default is 100%. The percentage of the available bandwidth requested for use by this stream is set in the *Desired* field, while (Read-only) the

Section	Field/Control	Description
		actual percentage of the available bandwidth used by this stream is shown in the *Actual* field.
	Actual	(Read-only) The actual percentage of the available bandwidth used by this stream.
	Packets per Second	The packet rate, based on the actual percentage of the available bandwidth used.
	Bit Rate (bps)	The bit rate of the stream, in bits per seconds.
Update Gaps		When this button is clicked, values that are entered into the fields for the inter-packet gap are reflected in the read-only fields.

Advanced Streams for Ethernet Modules

For module families which support advanced streams, the desired packet rate (as a percentage of the maximum rate) can be configured for each of the streams. In addition, a minimum inter-packet gap is required.

Module families for which this is true include these:

- LSM10GE
- LM1000(S)TXS4/24
- LSM1000XMS12
- LSM1000XMV4/8/12/16-01
- LSM1000XMVDC4/8/12/16
- LSM1000XMVDC4-NG
- ASM1000XMV12X
- LM622-MR POS
- MSM 2.5G/10G
- XDM10G32S

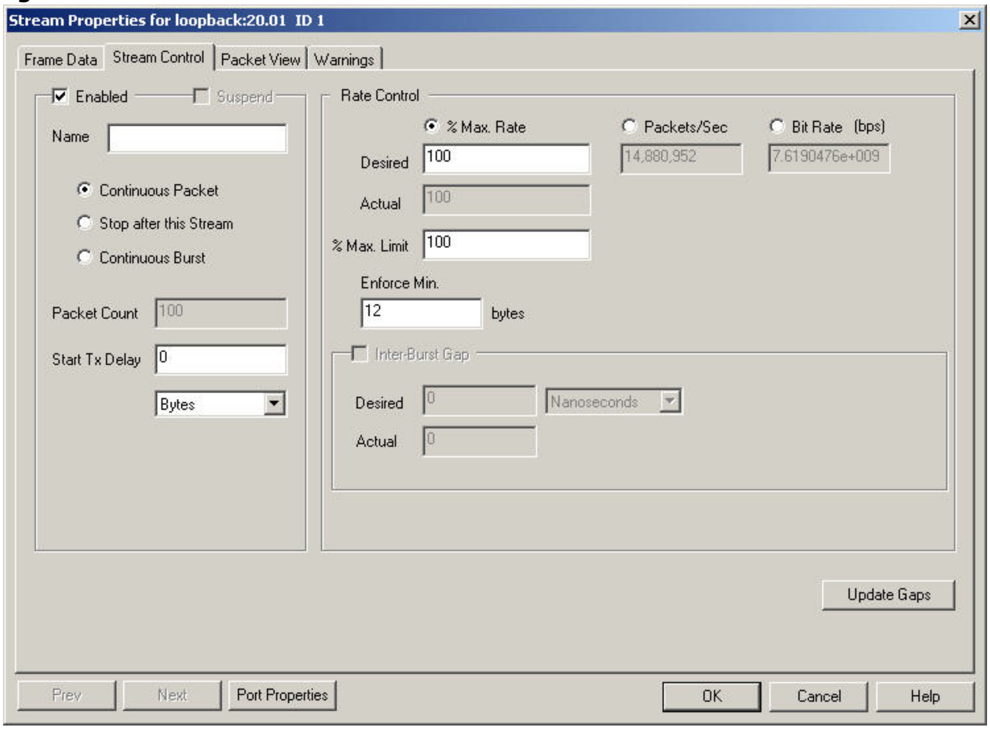
Each stream in the Advanced Stream Scheduler in Continuous Burst mode has its own Inter-Burst Gap and Packet Count. The Inter-Burst Gap and Start Tx Delay share the same counter. The Packet Count is used to count the packets per burst.

For information on the corresponding data rates for various module types, see the *Ixia Platform Reference Manual*.

When FCoE protocol is implemented on a NGY module, and the selected flow control type is Priority-based (PFC), the Stream Control tab of the Advanced Streams properties includes the assignment of a PFC Queue. Priority-based Flow Control for information.

The *Advanced Stream* tab for 10GE and TXS Ethernet modules is shown in *Figure:Advanced Streams—Ethernet.*

Figure:Advanced Streams—Ethernet



The fields and controls in this tab are described in *Table:Advanced Streams—Ethernet.*

Table:Advanced Streams—Ethernet

Section	Field/Control	Description
(Stream info)	Enabled	If selected, enables the use of the stream configured in this tab.
	Name	(Optional) A user-assigned name for this stream.
	(Type of stream transmission)	Choose one of: • **Continuous Packet**: The configured packet stream is repeated until a Stop Transmit is received. • **Stop After This Stream**: Transmission stops after this stream is sent. The transmit duration of the stream (packets transmitted) is determined by the value entered into the *Packet Count* field. • **Continuous Burst**: Sends out a continuous set of packet bursts. If selected, the Start Tx Delay option is automatically synchronized with the Inter-Burst Gap setting. (See Start Tx Delay, below.) *Continuous Burst* mode may not be used with flows. See **Note** following *Table: Basic Stream Controls* for information on maximum burst count.
	Packet Count	The total number of packets to be sent in this configured stream.

Section	Field/Control	Description
	Start Tx Delay	(Not applicable to POS modules) Entering a number in this field delays the start of the scheduled stream by the entered number (initially bytes). It is possible to change the value of the delay by selecting a value type in the pull-down menu directly below this field. Value options are: • Nanoseconds • Microseconds • Milliseconds • Seconds • Bytes (default) Once a number is entered, selecting a new value converts the delay time number from the original format to reflect the new value. NOTE If Continuous Burst mode is selected, Start Tx Delay is disabled and Inter-Burst Gap is enabled. The setting for Start Tx Delay automatically duplicates the Inter-Burst Gap setting. The two are synchronized.
Packet (rate)	% Max Rate	Default is 100%. The percentage of the available bandwidth requested for use by this stream is set in the *Desired* field, while the actual percentage of the available bandwidth used by this stream is shown in the *Actual* field (read-only). This is the IEEE-defined full speed line rate (theoretical speed) for Ethernet port.
	% Max Limit	The maximum rate the stream can attain when its rate is dynamically adjusted (in stream editor grid). Example: You set the %Max Limit to 50%, then the stream rate can be dynamically changed to any rate from 0% to 50% in the stream editor grid. The stream rate cannot be changed to 80%.
	Packets per Second	The packet rate, based on the actual percentage of the available bandwidth used.
	Bit Rate (bps)	The bit rate of the stream, in bits per second.
	Enforce Min. Gap (bytes)	Default is 12 bytes.
Inter-Burst Gap	Desired Actual	*Inter-Burst Gap/Burst Gap. For definitions, Table: Inter-Burst Gap Controls for Ethernet-Type Modules.*

Section	Field/Control	Description
		NOTE If Continuous Burst mode is selected, Start Tx Delay is disabled and Inter-Burst Gap is enabled. The setting for Start Tx Delay automatically duplicates the Inter-Burst Gap setting. The two are synchronized.
Update Gaps		When this button is clicked, values that are entered into the fields for the inter-packet gap are reflected in the read-only fields.

Update Gaps Button

When one of the Inter-Packet Gap quantities, *Time, Packets/Sec*, or *% Util (% Max Rate)* is changed, the use of this button causes the other parameters to be correspondingly updated.

Port Properties Button

The *Port Properties* button opens the *Port Properties* dialog for the port being configured for stream control. Refer to the following chapters for further details:

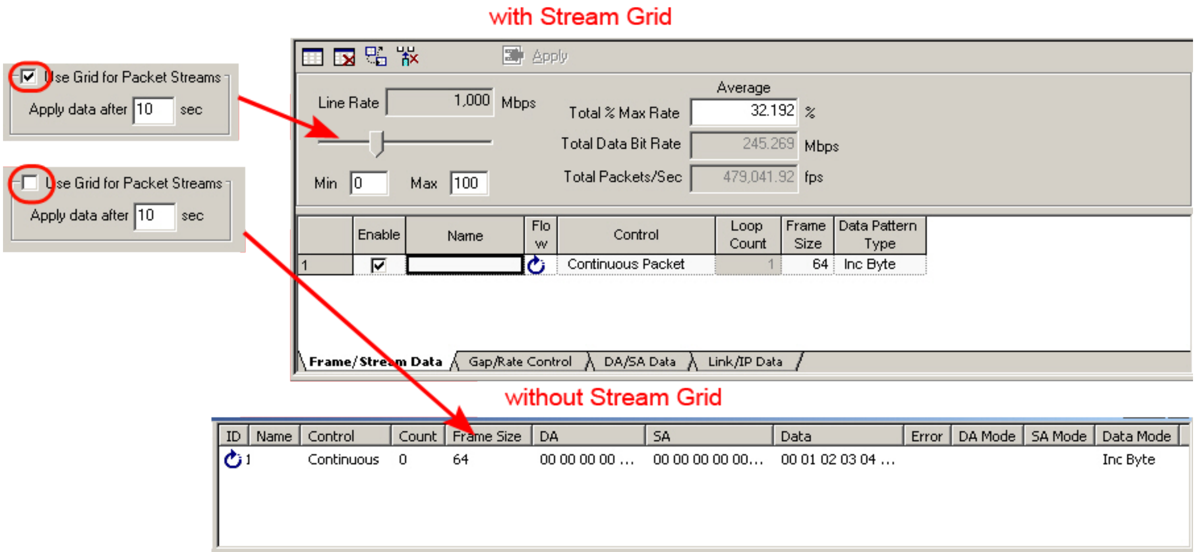
- Chapter 18,*Port Properties — 10/100/1000*
- Chapter 19,*Port Properties–POS and ATM Families*
- Chapter 20,*Port Properties–10 GE and UNIPHY Families*

Stream Editing

Stream editing is the primary means of configuring Packet Streams and Flows. Stream editing requires that the *Use Grid for Packet Streams option* of the *Tools > Options > Display* menu be selected.See Display Format*. If this option is not enabled, the Packet Stream information is displayed in list format, as shown in Figure:Packet Stream Displays.*

NOTE For information on ATM Stream Editing, see *ATM Stream Queue Grid*.

Figure:Packet Stream Displays



The stream editing grid provides a spreadsheet representation of the packet contents, allowing direct viewing and configuration. Various spreadsheet operations are available to create useful sequences of packets.

Data within the spreadsheet may be configured in two ways:

- Entered directly into the spreadsheet, or
- Entered in the standard Frame Data tab in the Stream Properties page.*Frame Data Structure*.

Stream editing is described in the following sections:

- *Stream Editing Window*
- *Stream Display Options*
- *Stream Data Manipulation*

NOTE Auto Apply Feature:

It is important to remember that each time a change made to a row in the stream configuration grid, and 'Enter' is clicked or the cursor is clicked in that row again, the 'Auto Apply' function is started.

This function runs for 10 seconds before the actual change is made, and this countdown is displayed in the header of the window. During the 10 seconds, the *Apply* button can be selected to apply the changes immediately (the 10-second countdown stops).

During the 10 seconds, the Auto Apply can be stopped by clicking the cursor in the row again.

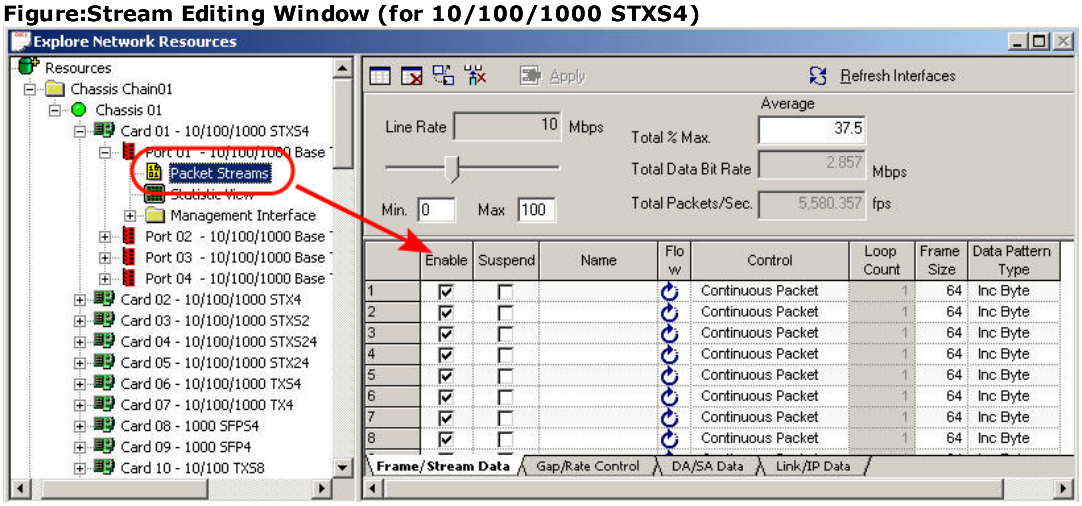
Stream Editing Window

Stream editing is enabled whenever the '... Streams' or '... Flows' item is selected (clicked) for a port in the Explore Network Resources tree, as shown in *Figure:Stream*

Editing Window (for 10/100/1000 STXS4). This window allows to configure multiple streams on a port at one time. Each of the streams or flows occupies a row in the table. This window is used for editing both normal scheduler streams and Advanced Scheduler streams.

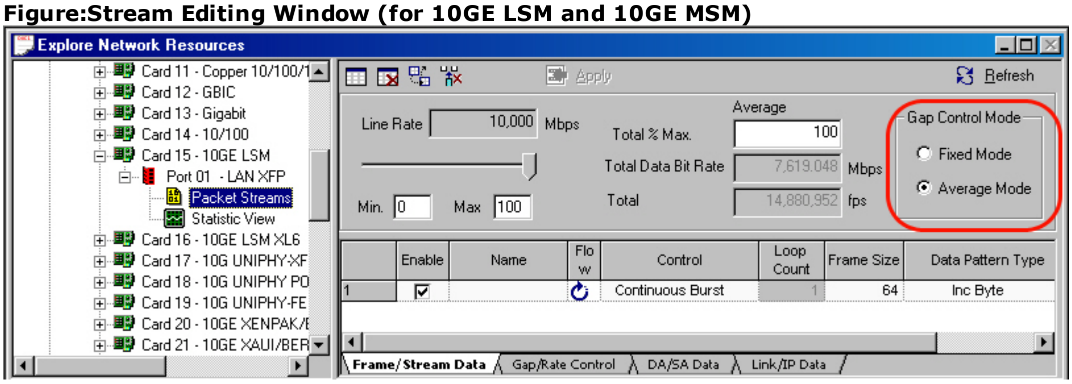
NOTE DCC Packet Streams and Packet Flows for information on editing DCC Packet Flows and Streams.

Figure:Stream Editing Window (for 10/100/1000 STXS4)



The 10GE LSM and 10G MSM modules (when in LAN or WAN mode) have one additional feature in the Stream Editing window called *Gap Control Mode*. This is shown in *Figure:Stream Editing Window (for 10GE LSM and 10GE MSM).*

Figure:Stream Editing Window (for 10GE LSM and 10GE MSM)



- For information on the Header fields, *Stream Editing Window Header*.
- For information on the Stream Edit Views/Columns, *Stream Display Options. (Each of the possible frame data and stream control data items represents a column in the display.)*
- For information on customizing the windows and use of the pop-up menu *Customizing the Stream Edit Window*.
- For simplified examples using the Stream Editing window, *Stream Editing Example—Normal Scheduler* and *Stream Editing Example—Advanced Scheduler*.

Stream Editing Window Header

The fields in the Stream Editing window header control global settings, and are described in *Table:Stream Editing Window—Header Fields (Global Settings).*

Table:Stream Editing Window—Header Fields (Global Settings)

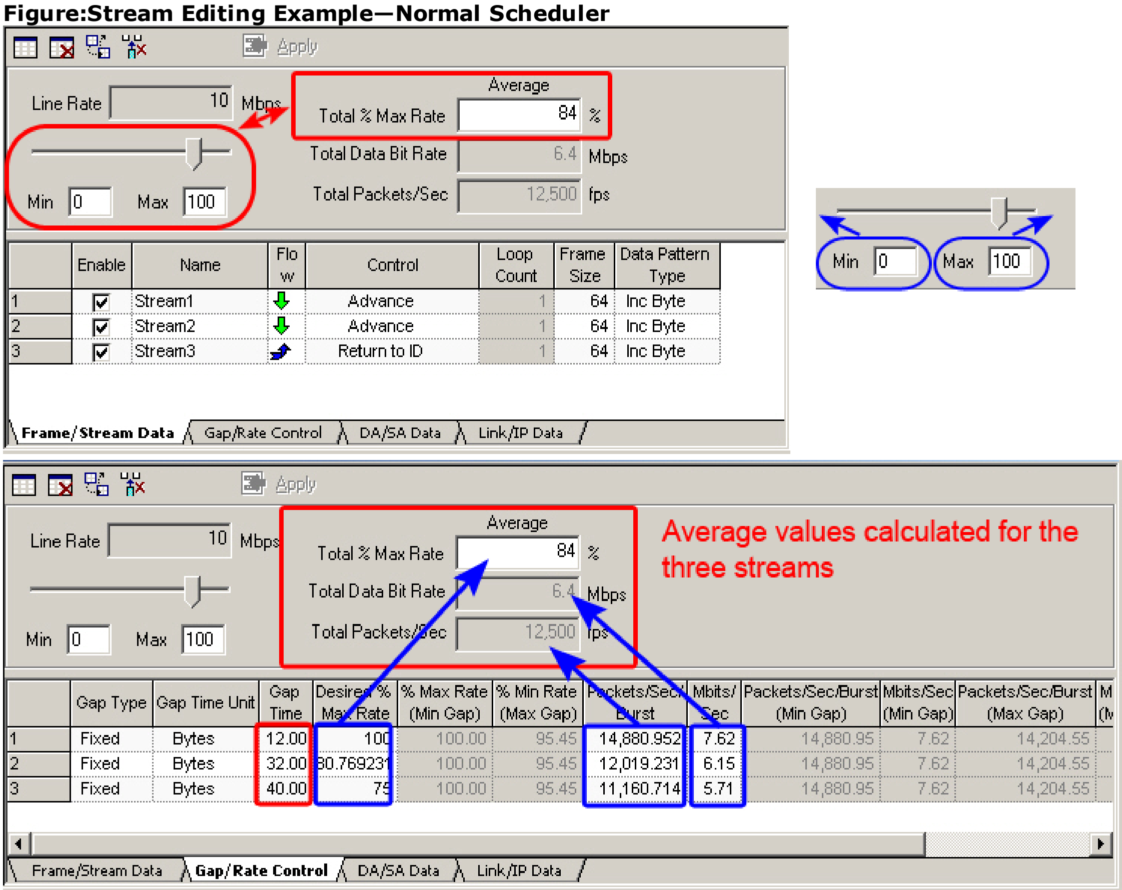
Field/Control	Description
Line Rate	(Read-Only) The maximum possible line speed (in Megabits per Second) for this port.
Slider Bar	(Linked with the *Total % Max Rate* field) The value in the *Total % Max Rate (Average)* field reflects the setting of the slider bar. Changes in that field causes the setting of the slider bar to change. Click the pointer and drag it to the percentage value of the *Total % Max Rate* to set. CAUTION If the slider is set to '0,' all ratio settings for the individual streams in this window are lost. The slider bar or *Total % Max Rate* field can be used to change the line rate of stream(s) without interrupting traffic *Changing Streams Without Interruption*.
Min.	This is the minimum setting possible for the Slider Bar (in %). The default is 0%, but you may enter a different value to set the lower end of a different range, for greater accuracy in setting rate values.
Max.	This is the maximum setting possible for the Slider Bar (in %). The default is 100%, but you may enter a different value to set the higher end of a different range, for greater accuracy in setting rate values.
Total % Max Rate	This value is based on the **maximum possible** portion of the line rate that is used for transmitting data bits on this type of port. (This value can be changed by using the slider bar or by entering a value directly into this field.) • For **Normal Scheduler** streams, this value may be averaged over the *Desired % Max Rates* for the various streams (depending on the types of streams). For a Continuous Packet or Continuous Burst stream, this is equal to the *Desired % Max Rate* for that selected stream. • For **Advanced Scheduler** streams, this value is the sum of the *Desired % Max Rates* for the various streams. If the sum of the rates entered is greater than 100%, the 'Oversubscribed' warning banner appears. A value of 100% means that 100% of the **maximum possible data bit rate** for that port is used. The calculation of the data bit rate does not include gap bytes, SONET overhead bytes, and so on. CAUTION **CAUTION:** If the value in this field is set to '0', all

Field/Control	Description
	CAUTION ratio settings for the individual streams in this window is lost. The *Total % Max Rate* field or the slider bar can be used to change the line rate of stream(s) without interrupting traffic.*Changing Streams Without Interruption*.
Total Data Bit Rate	(Read-Only) This is the total rate (in Megabits per Second) at which data bits are transmitted on this port. This value is dependent on stream configuration settings, such as Inter-Packet Gap, and so forth. For example, setting the IPG to a larger value, while keeping the other variables unchanged, decreases the data bit rate. For a Continuous Packet stream, this is equal to the 'Mbits/Sec' for that stream. For other stream control types and sequences of streams, this value may be an average of the 'Mbits/Sec' values for the streams. For **Ethernet** ports, the calculation of this value includes the data bits in the frames, but excludes the bits in the preamble. For **SONET** ports, the calculation of this value includes the data bits in the frames, but excludes SONET Overhead bits and bits in the Flag byte.
Total Packets/Sec	This is the total number of packets that are transmitted each second on this port, based on the value for the *Total Data Bit Rate* divided by the number of bits in the packets. For a Continuous Packet stream, this is equal to the 'Packets/Sec/Burst' for that stream. For other stream control types and sequences of streams, this value may be an average of the 'Packets/Sec/Burst' values for the streams.
Gap Control Mode	(For 10GE LSM and 10GE MSM modules only.) Controls the inserted packet gap behavior for the stream, as defined by IEEE. The options are: • Fixed Mode: Gap is adjusted to conform so that packets plus the gap are a multiple of 4. The value set is a minimum enforced gap. • Average Mode: Gap is adjust during each transmission so that packets plus gaps are a multiple of 4, plus or minus three bytes. This conforms to the Idle Deficit Count method defined in IEEE 802.3ae, so as to keep the average gap to the requested value.

Stream Editing Example—Normal Scheduler

A simple example for use of the stream editing window in normal stream scheduler mode is shown in *Figure:Stream Editing Example—Normal Scheduler.* This example is for a 10/100 TXS8 Ethernet module, operating at 10 Mbps. Three streams are configured, all using default values except for the gap size, which has been configured with a different size gap for each stream. The Gap Type is *Fixed*, so all of the columns associated with Min and Max Gaps for Random gaps are dimmed and unavailable. The 8-byte (default) preamble bits and the gap bytes are not included in the calculation for the Total Data Bit Rate (Average). The *Min* and *Max* values fields for the *Total % Max Rate* slider bar are kept at the defaults of 0% and 100%, respectively.

Figure:Stream Editing Example—Normal Scheduler

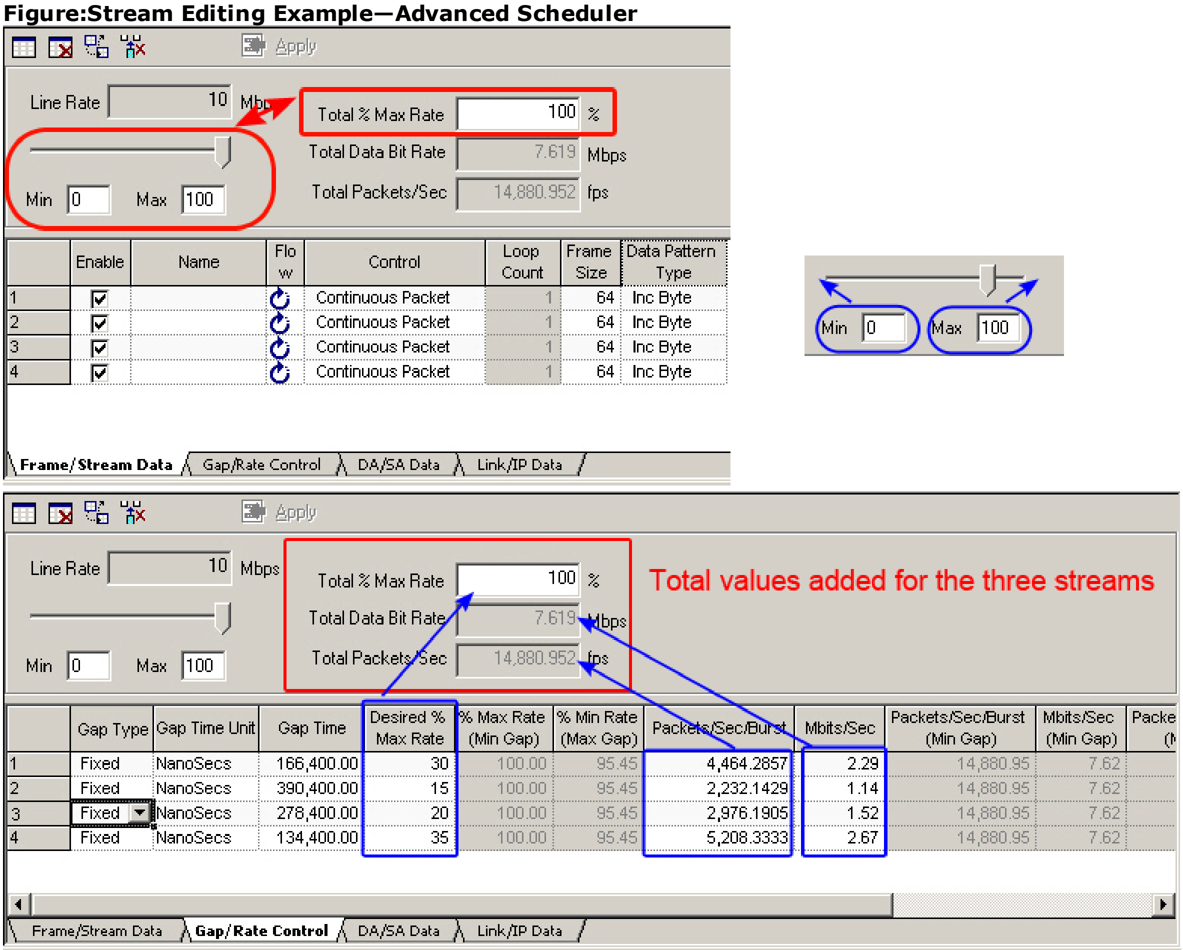


Stream Editing Example—Advanced Scheduler

A simple example for use of the stream editing window in Advanced Stream Scheduler mode is shown in *Figure:Stream Editing Example—Advanced Scheduler.* This example is for a 10/100 TXS8 Ethernet module, operating at 10 Mbps. Four streams are configured, all using default values except for the *Desired % Max Rate* for each individual stream. The sum of the % max rates equals 100%. The Gap Type is *Fixed*, so all of the columns associated with *Min* and *Max* gaps for random gaps are dimmed and unavailable. The 8-byte (default) preamble bits and the gap bytes are not included in the calculation for the *Total Data Bit Rate* (Average).

The *Min* and *Max* values for the *Total % Max Rate* slider bar are kept at the defaults of 0% and 100%, respectively. If the *Total % Max Rate* slider bar or edit box are changed, it causes the desired rates for all of the stream to change proportionately, maintaining the percent ratio between the streams to remain constant. The exception to the maintained ratio is when any stream's modified percentage exceeds the capacity of the hardware for gap times.

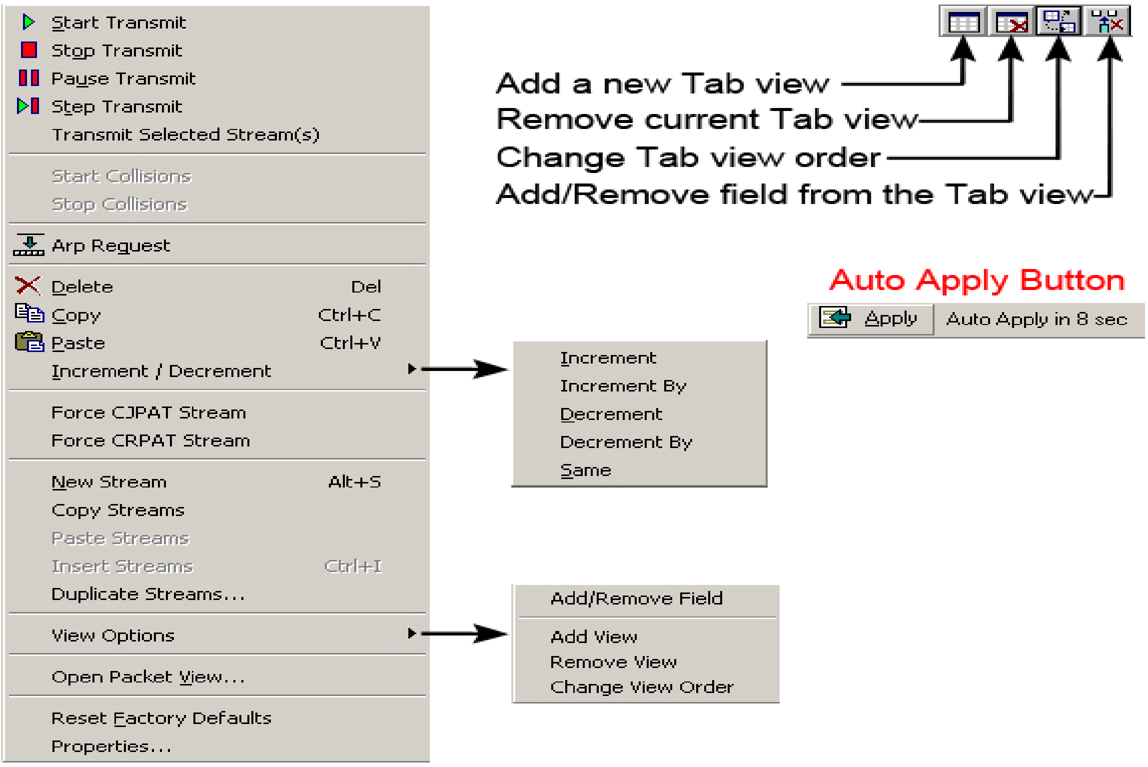
Figure:Stream Editing Example—Advanced Scheduler



Customizing the Stream Edit Window

The particular columns to be displayed may be selected. A selection of columns is called a 'view,' and multiple views may be created. The creation of multiple views and selection of columns, as well as other operations is accomplished through the pop-up menu and the menu bar, shown in *Figure:Stream Editing Pop-Up Menu and Menu Bar (shown for 10GE LAN).*

Figure:Stream Editing Pop-Up Menu and Menu Bar (shown for 10GE LAN)

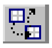


The menu choices available in the pop-up menu and menu bar are described in *Table:Stream Editing Pop-Up Menu Choices.*

Table:Stream Editing Pop-Up Menu Choices

Command	Keys/Shortcuts	Description
Start Transmit		Starts the transmission of data.
Stop Transmit		Stops the transmission of data.
Pause Transmit		Temporarily pauses the transmission of data. A 'Start Transmit' or 'Step Transmit' operation continues after a pause.
Step Transmit		After a pause, causes a single packet to be transmitted.
Transmit Selected Stream (s)		Starts transmit on the selected/highlighted stream(s).
Start Collisions		Enables collision generation for received data, if programmed for the port and enabled.
Stop Collisions		Stops collision generation.
ARP Request		Send an ARP packet requesting addresses. The first IP address found in the streams for each port is used for the ARP request.
Delete		The selected row(s) are deleted.

Command	Keys/Shortcuts	Description
	Del	
Copy	 Ctrl+C	Copies the selected rectangle of cells to the clipboard.
Paste	 Ctrl+V	Pastes the contents of the clipboard onto the currently selected cells. Note that this pasting operation always succeeds, but may not necessarily make sense. For example, pasting stream names onto loop counts results in an enormous number being pasted. In general, like numeric representations may be cut and pasted to produce the expected results.
Force CJPAT Stream		(For 10GE modules only) Forces the configuration values for the selected stream to the values specified by IEEE 802.3ae Annex A, for Continuous Jitter Test Pattern (CJPAT) testing.
Force CRPAT Stream		(For 10GE modules only) Forces the configuration values for the selected stream to the values specified by IEEE 802.3ae Annex A, for Continuous Random Test Pattern (CRPAT) testing.
Increment/Decrement > Increment Increment By... Decrement Decrement By... Same		These options are available when any rectangle is selected within the spreadsheet. The values within the selected cells are automatically manipulated. *Stream Data Manipulation*.
New Stream	Alt+S	A new stream is inserted after the last currently selected cell.
Copy Streams...		If one or more rows (streams) are selected, these are copied to the clipboard.
Paste Streams...		If one or more rows (streams) are selected, the contents of the clipboard replace these rows.
Insert Streams	Ctrl+I	Used with the copy option, when one or more streams are copied to the clipboard. Insert the cursor into a row in the list of streams, and select Insert Streams. The streams are inserted in the list, with one row per stream, immediately below the row with the

Command	Keys/Shortcuts	Description
		cursor.
Duplicate Streams...		The currently selected rows (streams) are duplicated following the current selection. A dialog prompts for the number of times to duplicate the stream(s).
View Options > Add View		Opens the *Add/Remove Field* dialog. *Stream Display Options* for more information.
View Options > Remove View		The current view is removed. The last view may not be removed.
View Options > Change View Order		The order of the views may be changed through the use of the dialog. *Change View Order Option* for a description of this dialog.
View Options > Add/Remove Field		Offers the dialog shown in *Stream Display Options, which allows selection of the fields (columns) displayed in the current view.*
Open Packet View...		The *Packet View* dialog, as described in *Packet View Tab*, is invoked to display the first packet associated with the selected stream.
Reset Factory Defaults		Resets to the factory default values.
Properties... (or Double-click row in the stream grid)		Displays the *Stream Control* dialog for the currently selected stream. It is described in *Stream Properties Dialog*.

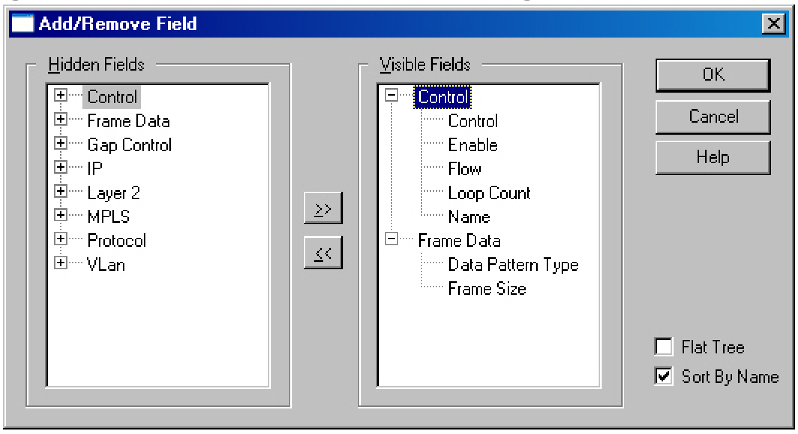
Stream Display Options

The fields (columns) that are displayed in the spreadsheet are controlled by the pop-up menu option, *View Options > Add/Remove Field.*

NOTE For the *Add/Remove Field* dialog for Logging and Alerts, *Add/Remove Field Option*.

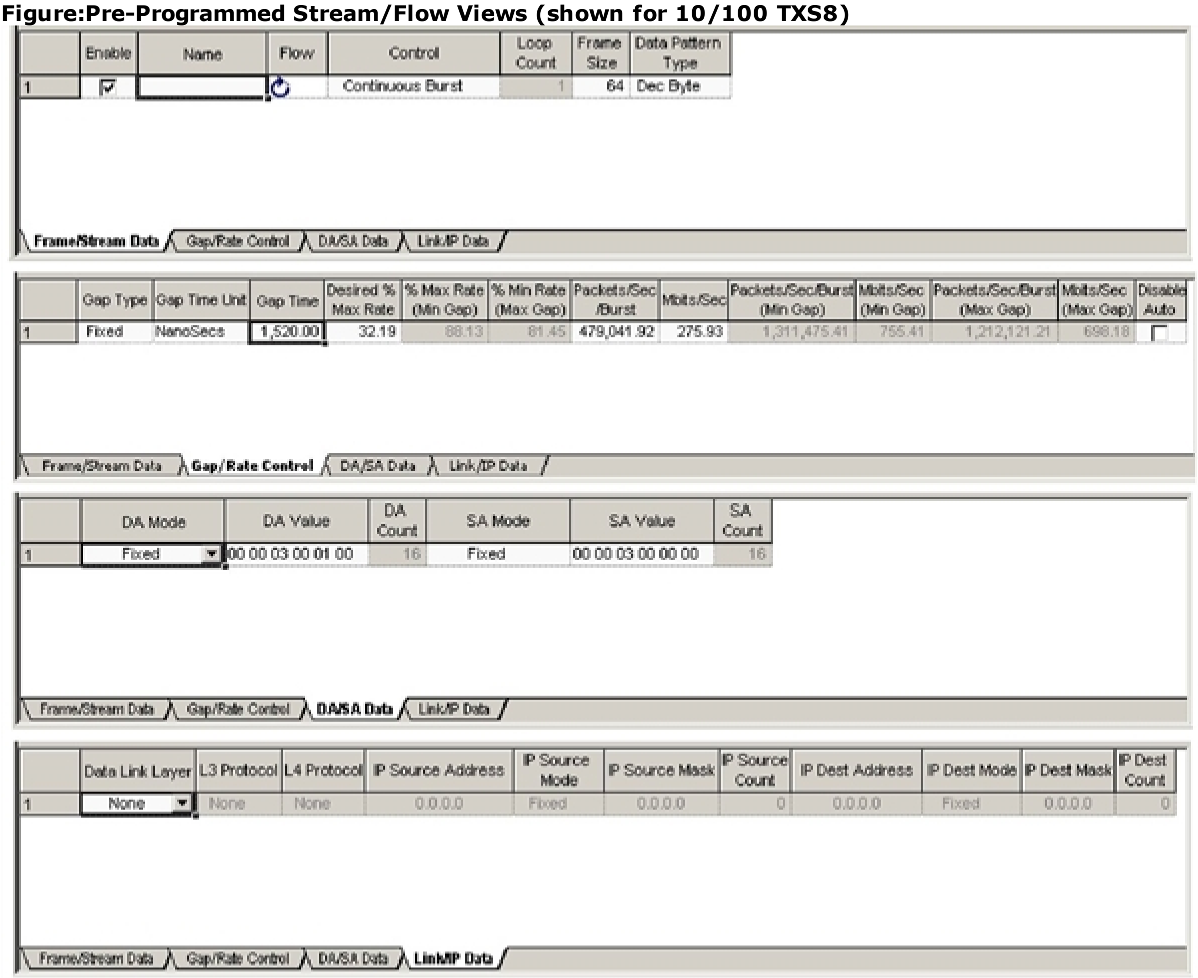
Selecting this option opens the *Add/Remove Field* dialog which is shown in *Figure:Stream Edit—Add/Remove Field Dialog.*

Figure:Stream Edit—Add/Remove Field Dialog



To create or modify a customized spreadsheet view, use the >> arrow to move a *Hidden Field* to the *Visible Fields* list and << to move a *Visible Field* to the *Hidden Fields* list. The columns in a view may be moved by selecting a column in the spreadsheet and moving it to its new location (using the mouse click-and-drag method). A red line indicates where it will be placed when the mouse button is released. Four views are pre-programmed. (For POS modules, only the Frame/Stream Data and Gap/Rate Control views are available.) These views are shown in *Figure:Pre-Programmed Stream/Flow Views (shown for 10/100 TXS8)* and described in *Table:Columns Available for Pre-Programmed Views.*

Figure:Pre-Programmed Stream/Flow Views (shown for 10/100 TXS8)



The columns available for each of the four pre-programmed views are:

Table:Columns Available for Pre-Programmed Views

View	Columns Available
Frame/Stream Data	Enable Name Flow Control Loop Count Frame Size Data Pattern Type
Gap/Rate Control	Gap Type Gap Time Units Gap Time Desired % Max Rate % Max Rate (Min Gap) % Min Rate (Max Gap) Packets/Sec/Burst Bits/Sec Packets/Sec/Burst (Min Gap) Bits/Sec (Min Gap) Packets/Sec/Burst (Max Gap) Bits/Sec (Max Gap) Disable Auto
DA/SA Data	DA Mode DA Value DA Count SA Mode SA Value SA Count
Link/IP Data	Data Link Layer L3 Protocol L4 Protocol IP Source Address IP Source Mode IP Source Mask IP Source Count IP Dest Address IP Dest Mode IP Dest Count

The available columns and their usage are shown in *Table:Stream Edit Available Fields.Not all of the fields available in the Stream Properties Dialog or* Frame Data Structure are available in the spreadsheet view. The table below shows the fields listed in the default order for the Add/Remove Field dialog, which is Sort by Name and presents the fields alphabetically in a multilevel tree.

Table:Stream Edit Available Fields

Category	Field	Type	Description
Control	Allow Auto Delete	check box	Allows for auto deletion of a stream if selected.

Category	Field	Type	Description
			If streams are generated from IxRouter-/IxNetwork, and Allow Auto Delete is selected, then existing streams are first deleted, then created. If auto delete is not selected, then streams are appended to existing streams.
	Bursts Per Stream	Integer	If stream control is set to other than Continuous packet or burst, this is the # of bursts in the stream. *Basic Stream Controls*.
	Control	Choices	Indicates what happens after the stream is applied. Choose one of: • Continuous Packet • Continuous Burst • End • Advance • Return to ID • Return For Count *Basic Stream Controls*.
	Enable	check box	Enables or disables the stream. *Basic Stream Controls*.
	Flow	Read-only icon	Indicates what happens after the stream is applied. Choose one of: —Continuous packet/burst —End —Advance —Return to ID —Return for Count *Basic Stream Controls*.
	Loop Count	Integer	If *Control* is set to *Return for Count*, this is the number of times to loop back. *Basic Stream Controls*.
	Name	Text	The name of the stream. *Basic Stream Controls*.
	Packets Per Burst	Integer	If *Control* is other than *Continuous packet*, this is the number of packets in each burst. *Basic Stream Controls*.
	Return To ID	Integer	If *Control* is set to one of *Return for ID* or

Category	Field	Type	Description
			Return for Count, this is the stream ID to return to while looping. Basic Stream Controls.
Frame Data	Data Pattern Data	Hex value - 4-octet	The data pattern associated with the selected data pattern type. Data Pattern Box.
	Data Pattern Type	Choice	The type of data pattern to apply to the body of a frame. Choose one of: • Inc Byte • Inc Word • Dec Byte • Dec Word • Random • Repeating • Fixed • ARP/Discovery Data Pattern Box. *The patterns associated with the Repeating, Fixed, and ARP/Discovery choices must be set through the Frame Data tab, which may be invoked by double-clicking anywhere in the row.*
	Forced Error	Choice	The type of error to insert in the packets in the stream. Choose one of: • No Errors • Alignment • Dribble Bit • Bad CRC • No CRC Force Errors Box.
	Frame Size	Integer	If *Size Type* is set to *Fixed*, then this field is used to set the size of each frame. Frame Size.
	Frame Size Type	Choice	The manner in which the frame size is set for generated packets. Choose one of: • Fixed • Random

Category	Field	Type	Description
			• Increment • Auto *Frame Size*. NOTE For **OC-48c POS, OC-192c POS,** and **10GE** modules, only one stream of incrementing frame size can be created per group of streams. Overall, up to 254 non-incrementing frame size streams, plus one incrementing frame size stream, may be configured concurrently for a port on one of these modules.
	Max Frame Size	Integer	If *Size Type* is set to *Random* or *Increment*, then this is the largest frame size that is generated. *Frame Size*.
	Min Frame Size	Integer	If *Size Type* is set to *Random* or *Increment*, then this is the smallest frame size that is generated. *Frame Size*.
	Preamble Size	Integer	The size, in bytes, of the preamble. *Preamble Size Box*.
Signature (sub-category)	Data Integrity Signature	check box	(Only displayed if available for the load module type.) If selected, data integrity values are inserted for each outbound packet. *Instrumentation Box*.
	Packet Group Signature	check box	If selected, this indicates that transmitted packets will have a packet group signature and packet group ID inserted into the packet. If selected, timestamp is also implied. *Instrumentation Box*.
	Sequence Signature	check box	If selected, sequence numbers are inserted in each outbound packet. *Instrumentation Box*.
	Time Stamp	check box	If selected, indicates that the six bytes before the FCS should hold a 48-bit timestamp with a 20ns resolution from the start of packet stream application.

Category	Field	Type	Description
			Instrumentation Box.
UDF1 through UDF4 (sub-category)	For Data 1-4: UDF__ Bit Mask 1 - 4	Mask	For counter 1, 2, 3, or 4, a correspondingly large set of bit values which control whether each value is held at 0, 1, or allowed to change ('X'). Chapter 7,*Frame Data–User Defined Fields (UDF)* .
	UDF __ Init Value 1 - 4	Integer	The initial value for the Counter 1, 2, 3, or 4, as masked by the Bit Mask Value. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	UDF __ Mode 1 - 4	Choice	Up or Down controls the direction of counting for Counter 1, 2, 3, or 4. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Counter Type	Integers (variable)	The use and division of the 32-bit counter. The choices cover all possible counter lengths and combinations. For example: '8', '16', '24' and '32' indicate single counters of their respective lengths, '8x16' indicates an 8-bit counter followed by a 16-bit counter, and '8x8x16' indicates an 8-bit counter followed by an 8-bit counter followed by a 16-bit counter. This causes the appropriate number of counters to be displayed in the remainder of the tab (up to 4). Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Continuously Counting	check box	If the Continuous Counting box is selected, then the counter will continuously count. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Enable	check box	Must be selected for the particular UDF to be active. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Offset	Integer	The offset from the start of the frame. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Random	check box	If selected, the counter values changes randomly. Chapter 7,*Frame Data–User Defined Fields (UDF)*.

Category	Field	Type	Description
	Repeat Count	Integer	If the *Continuous Counting* box is not selected, then the value in the *Repeat Count* field is used to control the number of times that the counter increments. When the Repeat Count is exhausted, the value resets to 0 and counting is continued. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Bit Mask 1 - 4	Mask	For counter 1, 2, 3, or 4, a correspondingly large set of bit values which control whether each value is held at 0, 1, or allowed to change (‘X’). Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Init Value 1 - 4	Integer	The initial value for the Counter 1, 2, 3, or 4, as masked by the Bit Mask Value. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
	Mode 1 - 4	Choice	Up or Down controls the direction of counting for Counter 1, 2, 3, or 4. Chapter 7,*Frame Data–User Defined Fields (UDF)*.
Gap/Rate Control	% Max Rate (Min Gap)	Integer	This is the minimum size of the generated random gaps as a percentage of the maximum rate possible. Either this field or the *Packets/Sec (Min Gap)* field may be used to make this setting; the other one reflects the calculated value. *Rate Control/Inter-Packet Gap*.
	%Min Rate (Max Gap)	Integer	This is the maximum size of the generated random gaps as a percentage of the maximum rate possible. Either this field or the *Packets/Sec (Max Gap)* field may be used to make this setting; the other one reflects the calculated value. *Rate Control/Inter-Packet Gap*.
	Actual % of Max Rate		This is the percentage of the maximum rate that is being used by stream traffic, not

Category	Field	Type	Description
			including the gaps.
	Bits/Sec		**(For *Gap Type-Fixed* only)** The Data Bit Rate for this stream, specified in bits per second.
	Bits/Sec (Max Gap)		**(For *Gap Type-Random* only)** The Data Bit Rate for this stream, specified in bits per second, when the maximum value for the random gap is being used.
	Bits/Sec (Min Gap)		**(For *Gap Type-Random* only)** The Data Bit Rate for this stream, specified in bits per second, when the minimum value for the random gap is being used.
	Desired % of Max Rate	Integer	Allows to set a percentage of the maximum line rate that stream traffic should be sent at.
	Disable Auto Scale	check box	When it is selected, this check box disables the ability to change the gap time if you change the line rate for a particular stream. The rate for the stream will not change if the global rate for all streams changes.
	Gap Time	Integer	**(For *Gap Type-Fixed* only)** This is the size of the fixed gap in *Gap Time Units*. Either this field or the *% Max Rate,* or the *Packets/Sec* field may be used to make this setting; the others reflect the calculated value. *Rate Control/Inter-Packet Gap*.
	Gap Time Unit	Choice	The time unit used with the Gap Time value. Choose one of: • NanoSecs • MicroSecs • MilliSecs • Seconds • Clock Ticks (if available) • Bytes (if available)
	Gap Type	Choice	The type of Inter-Packet Gap generation. Choose one of: • **Fixed**: Gaps are all of a fixed size, as determined by the *Time Units, Gap Time* and *Gap Time* columns. • **Random**: Gaps are randomly gen-erated within the range specified by *%*

Category	Field	Type	Description
			Max Rate (Min Gap) and *% Max Rate (Max Gap)*. *Rate Control/Inter-Packet Gap*.
	Inter-Burst	Inter-Burst Enable	Enables the generation of inter-burst gaps. See *Inter-Burst Gap/Burst Gap*.
		Inter-Burst Gap Time	If the *Inter-Burst Enable* box is selected, then this is the size of the inter-burst gap, exclicked in *Gap Unit* units. See *Inter-Burst Gap/Burst Gap*.
		Inter-Burst Gap Time Unit	The units used to specify the *Gap Time*. The available choices depend on the type of module. Choose one of: • NanoSecs • MicroSecs • MilliSecs • Seconds • Clock Ticks (if available) • Bytes (if available) See *Rate Control/Inter-Packet Gap*.
	Inter-Stream	Inter-Stream Enable	Enables the generation of inter-stream gaps. See *Inter-Stream Gap/Stream Gap*.
		Inter-Stream Gap Time	The size of the inter-stream gap, exclicked in *Gap Unit* units. See *Inter-Stream Gap/Stream Gap*.
		Inter-Stream Gap Time Unit	The units used to specify the *Gap Time*. Choose one of: Choose one of: • NanoSecs • MicroSecs • MilliSecs • Seconds • Clock Ticks (if available) • Bytes (if available) See *Rate Control/Inter-Packet Gap*
	Packets/Sec/Burst	Integer	**(For *Gap Type-Fixed* only)** This is the number of packets to generate

Category	Field	Type	Description
			each second. Either this field or the *Gap Time*, or the *% Max Rate* field may be used to make this setting; the others reflects the calculated value. See *Rate Control/Inter-Packet Gap*.
	Packets/Sec/Burst (Max Gap)	Integer	If the value for *Gap Type* is *Random*, then this is the maximum size of the generated random gaps as a number of packets per second. Either this field or the *% Max Rate (Max Gap)* field may be used to make this setting; the other one reflects the calculated value. See *Rate Control/Inter-Packet Gap*.
	Packets/Sec/Burst (Min Gap)	Integer	If the value for *Gap Type* is *Random*, then this is the minimum size of the generated random gaps as a number of packets per second. Either this field or the *% Max Rate (Min Gap)* field may be used to make this setting; the other one reflects the calculated value. See *Rate Control/Inter-Packet Gap*.
	Time Units	Choice	The units used to specify the *Gap Time*. Choose one of: • NanoSecs • MicroSecs • MilliSecs • Seconds • Clock Ticks *Rate Control/Inter-Packet Gap*.
IP	IP Dest Address	IP Address	For those layer 3 protocols that require IP addresses, this is the starting destination IP address for packets in this stream. See *Source and Destination IPv4 Addresses*.
	IP Dest Count	Integer	Available only for *Incr.* or *Decr. Host* and *Incr.* or *Decr. Network* options. This is count of increments/decrements until the address is reset to the *IP Dest Address* value and counting starts again. See *Source and Destination IPv4 Addresses*.
	IP Dest Mask	IPv4 or IPv6	(Not available for IPv6)

Category	Field	Type	Description
		Address Mask	Used with the IP Destination Address to create a range of addresses.
	IP Dest Mode	Choice	The means of generating subsequent IP addresses as in *IP Source Mode.* See *Source and Destination IPv4 Addresses*.
	IP Source Address	IP Address	For those Layer 3 protocols that require IP addresses, this is the starting source IP address for packets in this stream. See *Source and Destination IPv4 Addresses*.
	IP Source Count	Integer	Available only for *Incr.* or *Decr. Host* and *Incr.* or *Decr. Network.* This is count of increments/decrements until the address is reset to the *IP Source Address* value and counting starts again. *Source and Destination IPv4 Addresses*.
	IP Source Mask	IPv4 or IPv6 Address Mask	(Not available for IPv6) Used with the IP Destination Address to create a range of addresses.
	IP Source Mode	Choice	The means of generating subsequent IP addresses. Choose one of: • Fixed • Incr. Host • Decr. Host • Cont. Incr. Host • Cont. Decr. Host • Incr. Network • Decr. Network • Cont. Incr. Net • Cont. Decr. Net • Random • Custom Mask Increment • Custom Mask Decrement • Custom Mask Continuous Increment • Custom Mask Continuous Decrement • Custom Mask Random See *Source and Destination IPv4 Addresses*.

Category	Field	Type	Description
IPv4 DSCP (IP Sub-category)			Controls the configuration of the DSCP header information.
	IP DSCP Assured Forwarding Class Selector	Choice	Allows to select the DSCP Assured Forwarding class for the stream traffic. The options are: • Class 1 • Class 2 • Class 3 • Class 4
	IP DSCP Assured Forwarding Precedence	Choice	Allows to select the DSCP Assured Forwarding Precedence for the stream traffic. The options are: • Low Drop Precedence • Medium Drop Precedence • High Drop Precedence
	IP DSCP Class Selector	Choice	Allows to select the DSCP Class for the stream traffic. The options are: • Class 1 = 001000 • Class 2 = 010000 • Class 3 = 011000 • Class 4 = 100000 • Class 5 = 101000 • Class 6 = 110000 • Class 7 = 111000
	IP DSCP Custom	Binary notation	Allows to set a custom binary value for the DSCP header information.
	IP DSCP Mode	Choice	Allows to select the DSCP mode for the stream traffic. The options are: • Default • Class Selector • Assured Forwarding • Expedited Forwarding • Custom
	IP DSCP Enable	check box	Enables the DSCP protocol.
IPv4 TOS (IP Sub-category)			These settings are for the Type of Service (TOS) bits in the IPv4 header.
	IP TOS Bit3 (Delay)		Choose one of: • 0 - Normal

Category	Field	Type	Description
			• 1 - Low
	IP TOS Bit4 (Throughput)		Choose one of: • 0 - Normal • 1 - Low
	IP TOS Bit5 (Reli-ability)		Choose one of: • 0 - Normal • 1 - Low
	IP TOS Bit6 (Cost)		Choose one of: • 0 - Normal • 1 - Low
	IP TOS Bits0-2 (Precedence)		Choose one of: • 000 - Routine • 001 - Priority • 010 - Immediate • 011 - Flash • 100 - Flash Override • 101 - CRITIC/ECP • 110 - Internet Control • 111 - Network Control
	IPv4 TOS Enable	check box	Enables the TOS feature
IPv6 specific (IP Sub-cat-egory)			These settings are used to configure the IPv6 specific fields in the IPv6 header.
	IPv6 Dest. Step Size	Integer	Sets the step size when incrementing or decrementing the IPv6 Destination Address.
	IPv6 Flow Label	Integer	Labels a sequence of packets for which it requests special handling by IPv6-capable routers. Routers that do not support this function must set this field to zero when cre-ating, forwarding, or receiving the packet.
	IPv6 Hop Limit	Integer	The Hop limit is decremented by 1 by each node that forwards the packet. When the value reaches 0, the packet is discarded.
	IPv6 Next Header	Integer	Identifies the type of the next extension header. When value = 59, means ‘No Next Header.’
	IPv6 Payload Length	Integer	Length of the IPv6 payload, which is the length of the entire packet which follows the IPv6 header (in octets). The payload includes any extension headers.
	IPv6 Source Step	Integer	Sets the step size when incrementing or

Category	Field	Type	Description
	Size		decrementing the IPv6 SourceAddress.
	IPv6 Traffic Class	Integer	Identifies the class or priority of the IPv6 packet.
Layer 2	DA Count	Integer	If *DA Mode* is either *Increment* or *Decrement*, then this is the number of times that the address increments before being reset and started again. See *DA/SA Property Sheet*.
	DA Mask	4-octet address (hex)	The mask associated with the DA mask.
	DA Mode	Choice	The type of destination MAC address generation. Choose one of: • Increment • Continuous Inc. • Decrement • Continuous Dec. • Fixed • Random • ARP/Discovery See *DA/SA Property Sheet*.
	DA Value	MAC Address	The first destination MAC address to be generated for the stream. DA/SA Property Sheet
	SA Count	Integer	If *SA Mode* is either *Increment* or *Decrement*, then this is the number of times that the address increments before being reset and started again. See *DA/SA Property Sheet*.
	SA Mask	4-octet address (hex)	The mask associated with the SA mask.
	SA Mode	Choice	The type of source MAC address generation. Choose one of: • Increment • Continuous Inc. • Decrement • Continuous Dec. • Fixed

Category	Field	Type	Description
			• Random See *DA/SA Property Sheet*.
	SA Value	MAC Address	The first source MAC address to be generated for the stream. See *DA/SA Property Sheet*
MPLS	MPLS Auto Set 'Bottom of the Stack' Bit	check box	If selected, the Bottom of Stack field above is dimmed and unavailable. The 'S' (bottom of stack) bit is automatically set for the bottom stack entry and reset for all other entries.
	MPLS Auto Set Label	check box	If selected, the Label field is dimmed (inactive). The label values is automatically assigned. If cleared, you can enter a custom value for the label that is highlighted in the MPLS Labels list.
	MPLS Enable	check box	Enables the MPLS specific header information.
	MPLS Type	Choice	Sets the overall packet type for the MPLS data. The options are: • MPLS Unicast • MPLS Multicast
MPLS Label 1/Label 2 (Sub Categories)	Bottom of the Stack	Integer	A single bit that represents the last entry (bottom) of the stack.
	Experimental Use	Integer	A three-bit field that may be used for experimental purposes.
	Label	Integer	The value of the label element of the entry. Several values have specific interpretations which are exclicked to the right of the label value: • 0: IPv4 Explicit NULL Label. Only valid as the one and only entry on the stack, indicating that the entry should be popped and forwarding of the packet should be done based on the IPv4 header. • 1: Router Alert Label. Valid anywhere in the stack except at the bottom. Used to signal an alert to the software associated with the router that finds this at the top of the stack.

Category	Field	Type	Description
			• 2: IPv6 Explicit NULL Label. As in '0', but with IPv6 header interpretation. • 3: Implicit NULL Label. A reserved value used within a router. • 4 to15: Reserved.
	Time To Live	Integer	The TTL field. It is decremented by routers as they process label stack entries.
Protocol	Data Link Layer	Choice	The type of data link encapsulation. Choose one of: • None • Ethernet II • Ethernet SNAP • 802.3 Raw • 802.3 (IPX) See Frame Data–User Defined Fields (UDF).
	L3 Protocol	Choice	This is the Layer 3 protocol to be used. Choose one of: • None • IPv4 • IPv6 • IPv6 Over IPv4 • IPv4 Over IPv6 • IPX • ARP • Pause Chapter 7, *Frame Data–User Defined Fields (UDF)*.
	L4 Protocol	Choice	This is the Layer 4 protocol to be used. Choose one of: • None • TCP • UDP • ICMP • IGMP • RIP • DHCP • OSPF *Frame Data–Protocol Control*.
IGMP (Protocols	IGMP Checksum	Integer	The 16-bit one's complement of the one's complement sum of the 8-octet IGMP mes-

Category	Field	Type	Description
Sub-category)			sage.
	IGMP Group	Dotted decimal	The IP address of the group associated with the message.
	IGMP Max Response Time	Integer	Maximum expected response time.
	IGMP Max Response Time Type	Integer	The type of response time for IGMP.
	IGMP Mode	Choice	Choose one of: • Fixed • Increment • Decrement • Continuous increment • Continuous decrement
	IGMP Repeat Count	Integer	Number of times to repeat the information in the IGMP header.
	IGMP Type	Choice	The IGMP message. Choose one of: • Membership Query • Membership Report • Leave Group (for Version 2 only)
	IGMP Valid Check-sum	Integer	The checksum type for IGMP.
	IGMP Version	Choice	IGMP Version Number. Choose one of: • Unknown • 1 • 2 - the version described in this table. • 3 - changes the composition of this dia-log(The default is Version 2)
Stream Con-trol	Bursts Per Stream	Integer	If stream control is set to other than Continu-ous packet or burst, this is the # of bursts in the stream. *Basic Stream Controls*.
	Control	Choices	Indicates what happens after the stream is applied. Choose one of: • Continuous packet • Continuous burst • End • Advance • Return to ID

Category	Field	Type	Description
			• Return for Count *Basic Stream Controls*.
	Enable	check box	Enables or disables the stream. *Basic Stream Controls*.
	Flow	Read-only icon	This icon matches the Control choice, and indicates what happens after the stream is applied. Choose one of: - Continuous packet/burst - End - Advance - Return to ID - Return for Count *Basic Stream Controls*.
	Loop Count	Integer	If *Control* is set to *Return for Count*, this is the number of times to loop back. *Basic Stream Controls*.
	Name	Text	The name of the stream. *Basic Stream Controls*.
	Packets Per Burst	Integer	If *Control* is set to other than *Continuous packet*, this is the number of packets in each burst. *Basic Stream Controls*.
	Return To ID	Integer	If *Control* is set to one of *Return for ID* or *Return for Count*, this is the stream ID to return to while looping. *Basic Stream Controls*.
Stacked VLAN	CE-VLAN	Group	If selected, displays the Inner Stacked VLAN settings, which are: • CE-VLAN Bit Mask • CE-VLAN CFI • CE-VLAN ID • CE-VLAN ID Count Mode • CE-VLAN Repeat Count • CE-VLAN Step • CE-VLAN Tag Control Info • CE-VLAN Tag Protocol ID • CE-VLAN User Priority
	SP-VLAN	Group	If selected, displays the Outer Stacked

Category	Field	Type	Description
			VLAN settings, which are: • SP-VLAN Bit Mask • SP-VLAN CFI • SP-VLAN ID • SP-VLAN ID Count Mode • SP-VLAN Repeat Count • SP-VLAN Step • SP-VLAN Tag Control Info • SP-VLAN Tag Protocol ID • User Priority
Stacked VLAN Enable		Choice	Enables the Stacked VLAN option.
VLAN	VLAN	check box	Indicates that a VLAN tag is to be added to the header. Edit VLAN.
	VLAN Canonical Format	Choices	The Canonical Format Indicator is a single bit flag value. Choose one of: • Reset • Set
	VLAN ID	Integer	The VLAN ID to be added to the header. Edit VLAN.
	VLAN ID Count Mode	Choices	Used to set the mode by which the VLAN ID (VID) varies. Choose one of: • **Fixed**: The single ID specified in the *VID* field is used. • **Increment**: The ID specified in the *VID* field is used as the start of a number of repeated sequence of VIDs as indicated by the *Repeat Count* field and the *Bit Mask* field. • **Decrement**: The ID specified in the *VID* field is used as the start of a number of repeated sequence of VIDs as indicated by the *Repeat Count* field and the *Bit Mask* field. • **Continuous Increment**: The ID specified in the *VID* field is used as the start of an infinite sequence of VIDs as indicated by the *Bit Mask* field. • **Continuous Decrement**: The ID specified in the *VID* field is used as the

Category	Field	Type	Description
			start of an infinite sequence of VIDs as indicated by the *Bit Mask* field. • **Random**: The VID is varied randomly as indicated by the *Bit Mask* field.
	Repeat Count	Integer	For the Increment and Decrement VLAN ID Count Mode choices, this indicates the number of repeats for the cycle of varied VIDs.
	VLAN User Priority	Integer	The user priority of the tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.

Stream Data Manipulation

Data may be created and moved by a variety of techniques as shown in *Table:Stream Data Manipulation Techniques.* Data within the spreadsheet may be selected as a single cell or as any rectangular area.

Table:Stream Data Manipulation Techniques

Task	Keyboard Shortcut	Menu Option	Description
Delete Row	Del	Delete	Removes the selected row.
Copy Data	Ctrl + C	Copy	Makes a copy of the selected data, which may be copied on top of another location through the use of Paste.
Paste Data	Ctrl + V	Paste	Data copied through Copy replaces the currently selected data. If the copied data is larger than the current selection, the current selection is extended down and to the right to accommodate the size. Data may only be pasted over compatible items.
Move Row(s)			Any number of selected rows may be moved to another place by selecting the row(s) and holding the left mouse button down while moving the cursor to the new position. A red line displays the new location that the rows possess when the mouse button is released.

Additional pop-up options make it possible for a cell to be incremented by a fixed value with respect to the cell just above it. Any rectangular selection involving two or more adjacent rows and one or more adjacent columns may be used. All of the elements in a column may be selected by left-clicking a column heading. The pop-up menu choices that apply are shown in *Table:Stream Increment/Decrement Operations.*

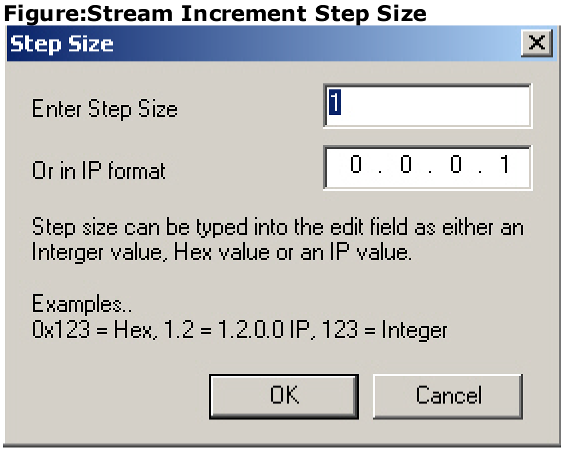
Table:Stream Increment/Decrement Operations

Menu Option	Description
Increment	Each cell is one greater than the cell above.
Increment By...	Each cell is incremented by a specified amount.

Menu Option	Description
Decrement	Each cell is one less than the cell above.
Decrement By...	Each cell is decremented by a specified amount.
Same	Each cell is the same as the cell above.

When *Increment By...* or *Decrement By...* are selected, the *Step Size* dialog is displayed. This dialog is shown in *Figure:Stream Increment Step Size.*

Figure:Stream Increment Step Size

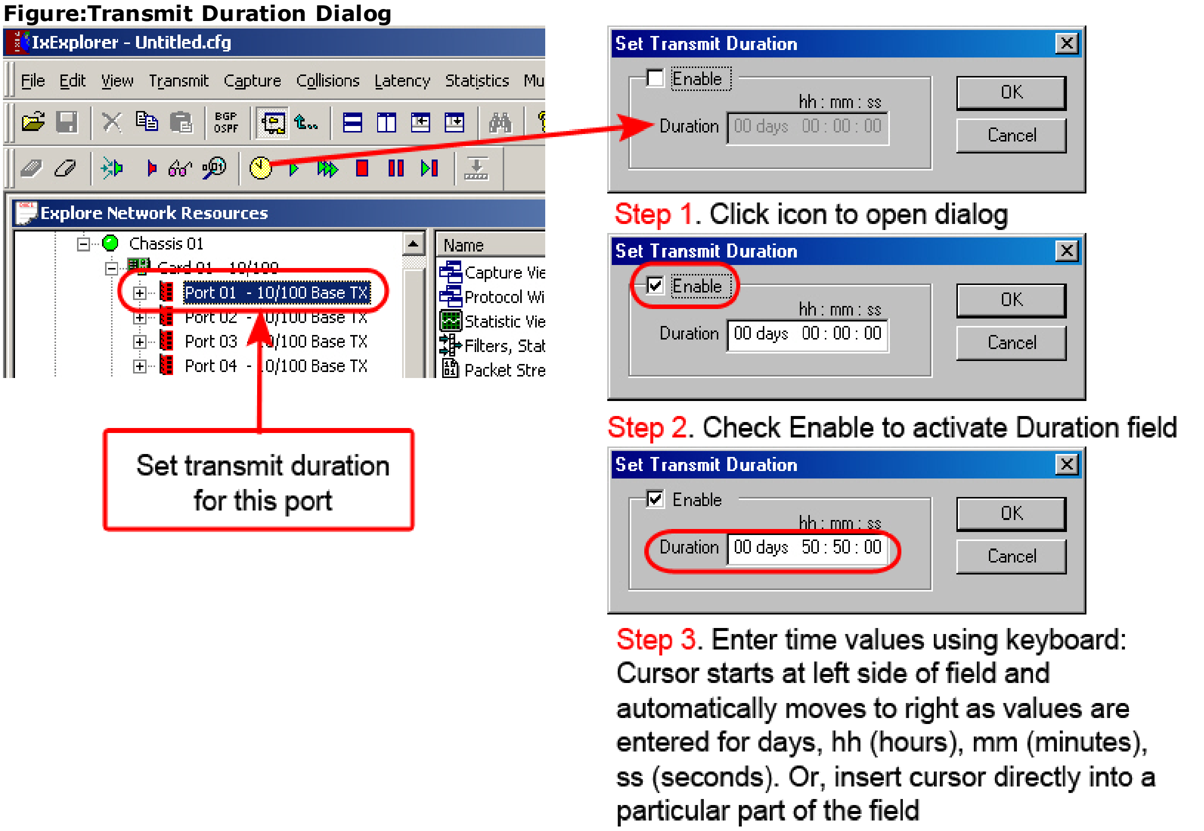


The increment step size used is a 32-bit unsigned quantity, which may be exclicked in decimal, in hexadecimal (with a preceding *0x*) notation, or as an IP address. When the data to be incremented/decremented is larger than 32 bits, only the last 32 bits of data are incremented or decremented.

Set Transmit Duration

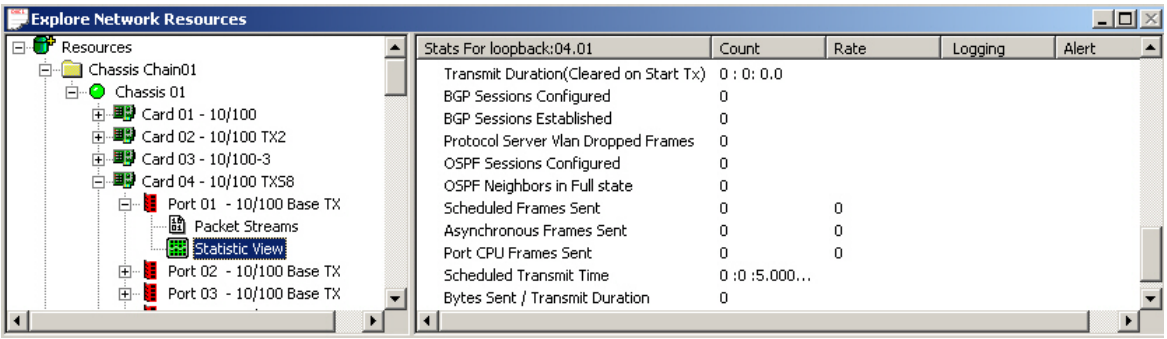
The Set Transmit Duration option allows to set the Scheduled Transmit Duration for stream transmission, as shown in *Figure:Transmit Duration Dialog.* This option is available for the following levels in the Network Resources Tree: Chassis Chain, Chassis, Load Module, Port, and Packet Streams. The time settings are entered directly into the *Duration* field. An example for setting the Transmit Clock for streams on a port is shown in *Figure:Transmit Duration Dialog.*

Figure:Transmit Duration Dialog



The *Scheduled Transmit Duration* is displayed in the Statistic View for the port, as shown in *Figure:Scheduled Transmit Duration in Statistic View,* along with the *Bytes Sent/Transmit Duration* and *Transmit Duration* statistics. This statisitic is only accurate to within one second.

Figure:Scheduled Transmit Duration in Statistic View



Stream Grid–GFP Tab

When employing Generic Framing Procedure (GFP) on OC-48c POS load modules, a separate *GFP Data* tab appears in the Stream Grid window allowing to view and modify the various GFP stream settings. The *GFP Data* tab is only visible if GFP has been selected in Port Properties, as described in Frame Data for GFP.

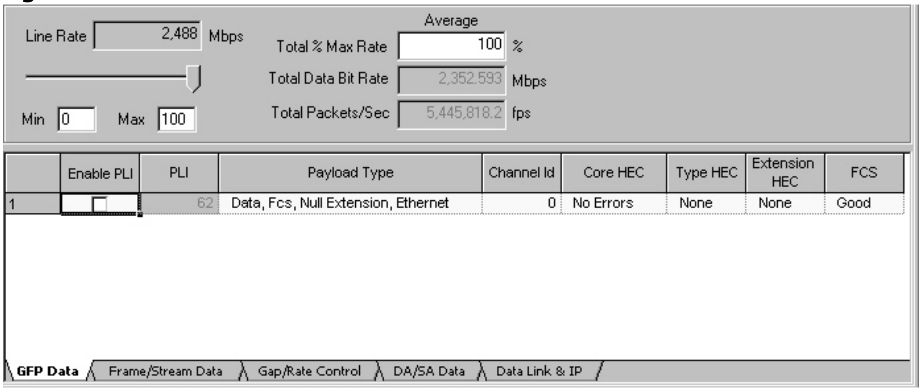
For more in formation on GFP, refer to the GFP - Generic Framing Procedure in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

GFP Data Tab in Stream Grid

The *GFP Data* tab in the Stream Grid is shown in *Figure:GFP Data Stream Grid Tab.*

The tabs other than the *GFP Data* tab are described in *Stream Display Options*.

Figure:GFP Data Stream Grid Tab



The controls in the top half of the Stream Queue grid operate as described in *Stream Editing Window*.

The *GFP Data* tab in the Stream grid options are described in *Figure:GFP Data Tab Display.*

Table:GFP Data Tab Display

Field/Control	Usage
Enable PLI	Enables the Payload Length Indicator (PLI) field in the GFP frame.
PLI	Displays the Payload Length Indicator (PLI). The PLI is a two octet field containing a binary number that represents the number of octets in the GFP Payload Area. The absolute minimum value of the PLI field in a GFP client frame is 4 octets. PLI values 0-3 are reserved for GFP control frame usage. This field is only active when the *Enable PLI* check box is selected.
Payload Type	Displays the selected Payload type. Payload types are enumerated in Frame Data for GFP.
Channel ID	Sets the Channel ID. The Channel ID is an 8-bit binary number used to indicate one of 256 communications channels at a GFP initiation/termination point.
Core HEC	Sets the error type for the Core Header Error Control (cHEC) to *No Errors*, *1 bit Error*, or *Multiple bit Errors*. The cHEC is a two octet field containing a CRC-16 error control code that protects the integrity of the Core Header contents by enabling both single-bit error correction and multi-bit error detection.
Type HEC	Sets the error level for the Type Header Error Control (tHEC). The tHEC is a two octet field containing a CRC-16 error control code that protects the integrity of the Type Field contents by enabling both single-bit error correction and multi-bit error detection.

Field/Control	Usage
Extension HEC	Set the error level for the Extension Header Error Control (eHEC). The eHEC is a two octet field containing a CRC-16 error control code that protects the integrity of the extension header contents by enabling both single-bit error correction (optional) and multi-bit error detection.
FCS	Set the Frame Check Sequence (FCS) to be *Good* (transmitted frame is accurate), *Bad* (transmitted frame contains errors), or absent (not included with the transmitted frame). The GFP Payload FCS is an optional, four octet frame check sequence containing a CRC-32 sequence that protects the GFP Payload Information field contents.

DCC Packet Streams and Packet Flows

The Data Communication Channel (DCC) packets can be used to control and monitor SONET network devices, through the DCC bytes in the Transport Overhead of each SONET frame, which is the traditional link layer for Operation, Administration, and Maintenance (OAM) functions.

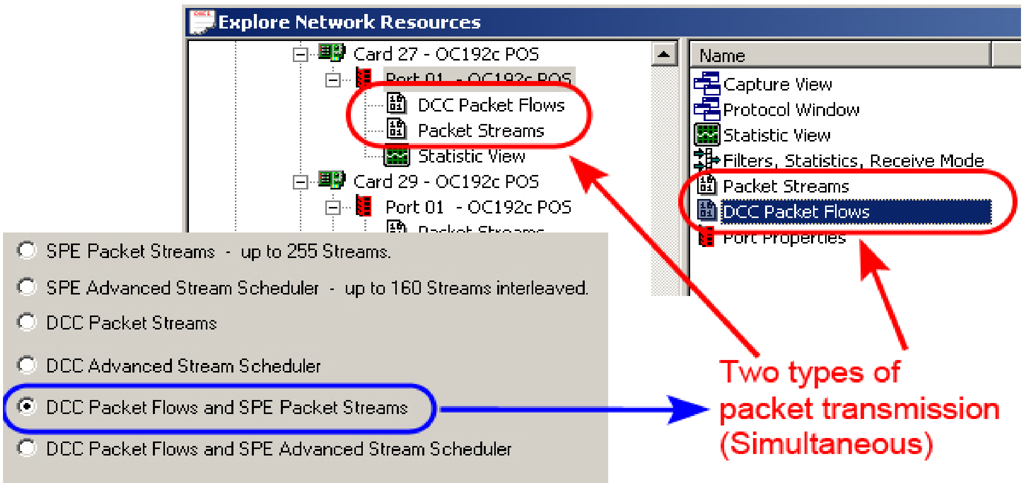
In addition, sending control plane information over the DCC channel allows rapid provisioning of end-to-end connections.

In the port properties for an OC-192c module which supports the optional DCC feature, the *Transmit Modes* tab allows to select DCC Packet Streams or Advanced Streams, or DCC Packet Flows in combination with the standard Synchronous Payload Envelope (SPE) transmission of packet streams or advanced streams.

DCC Packet Flows

When a combination mode with DCC packet flow plus SPE packet or advanced streams is selected in Transmit Modes, **TWO** packet transmission types are listed in the Network Resources tree and Port Details list, as shown in *Figure:DCC Packet Transmission Types.*

Figure:DCC Packet Transmission Types



BOTH transmission types must be configured for this DCC option. The packets in the DCC Packet Flows are transmitted in the SONET frame overhead either over the LOH or SOH.

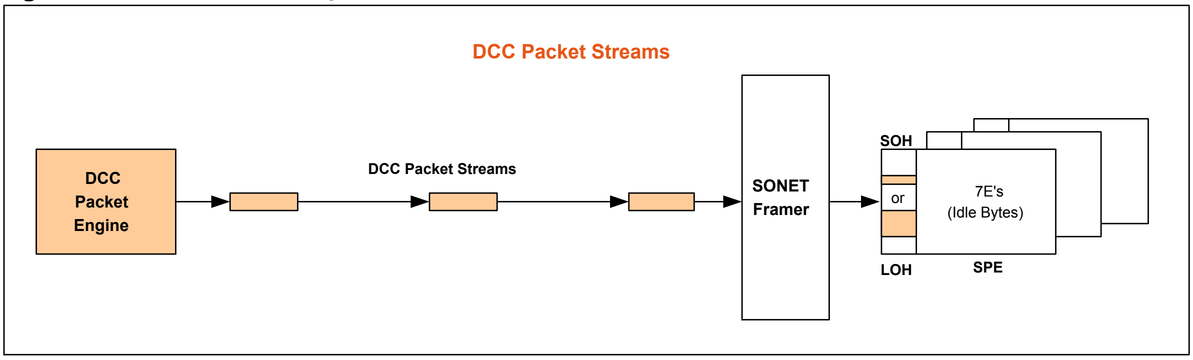
Simultaneously, packets are transmitted in the normal manner, as packet streams or advanced streams, within the SPE payload of the SONET frame. To configure the different transmission types, refer to the sections listed below:

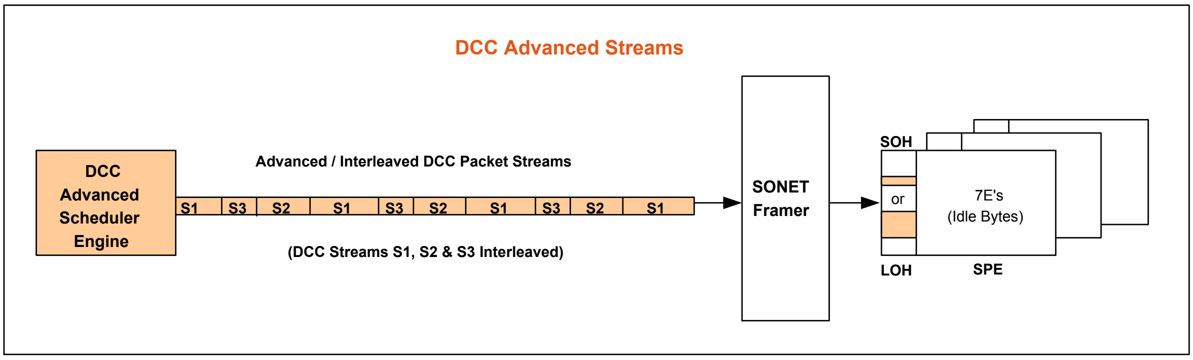
- DCC Packet Streams: *DCC Packet Streams and DCC Advanced Streams*.
- DCC Packet Flows: *DCC Packet Flows*.
- DCC Advanced Stream Scheduler: *DCC Packet Streams and DCC Advanced Streams*.
- SPE (normal) Packet Streams: *Stream Control for Standard POS Modules*.
- SPE (normal) Advanced Streams: *Advanced Streams for Standard POS and POS 622 Modules*.

DCC Packet Streams and DCC Advanced Streams

A simplified diagram illustrating how DCC Packet Streams and DCC Advanced Streams are generated is shown in *Figure:DCC Packet Streams/Advanced Streams.*

Figure:DCC Packet Streams/Advanced Streams





DCC Packet Streams

DCC Packet Streams are configured like normal (SPE) packet streams over SONET, but with a greatly reduced speed. Since only three bytes for SOH, or nine bytes for LOH, per SONET frame are being used to create the DCC channel, the rates are 192 Kbps or 576 Kbps, respectively.

To configure the DCC packet streams, first double-click 'DCC Packet Streams' to display the DCC stream grid. Then double-click a stream entry in the table to display the *Stream Properties* dialog, and select the *Stream Control* tab. Configure the stream properties as for a normal packet stream. *Stream Control for Standard POS Modules* for additional information.

DCC Advanced Streams

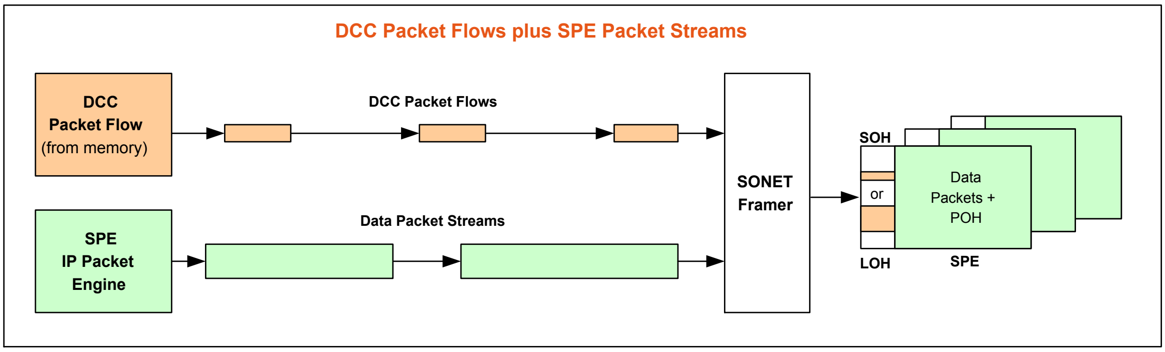
DCC Advanced Streams are configured like normal (SPE) advanced packet streams over SONET, but with a greatly reduced speed. Since only three bytes for SOH, or nine bytes for LOH, per SONET frame are being used to create the DCC channel, the rates are 192 Kbps or 576 Kbps, respectively.

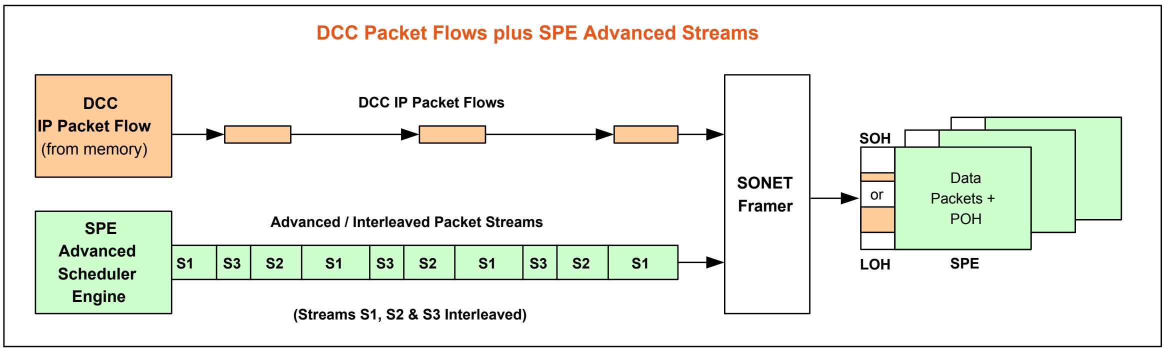
To configure the DCC advanced streams, first double-click *DCC Advanced Streams* to display the DCC stream grid. Double-click a stream entry in the table to display the *Stream Properties* dialog, then select the *Stream Control* tab. Configure the stream properties as for a normal advanced packet stream. *Advanced Streams for Standard POS and POS 622 Modules* for additional information.

DCC Packet Flows

A simplified diagram illustrating how DCC Packet Flows are generated simultaneously with normal (SPE) packet streams and advanced streams is shown in

DCC Packet Flows with SPE Packet Streams/Advanced Streams



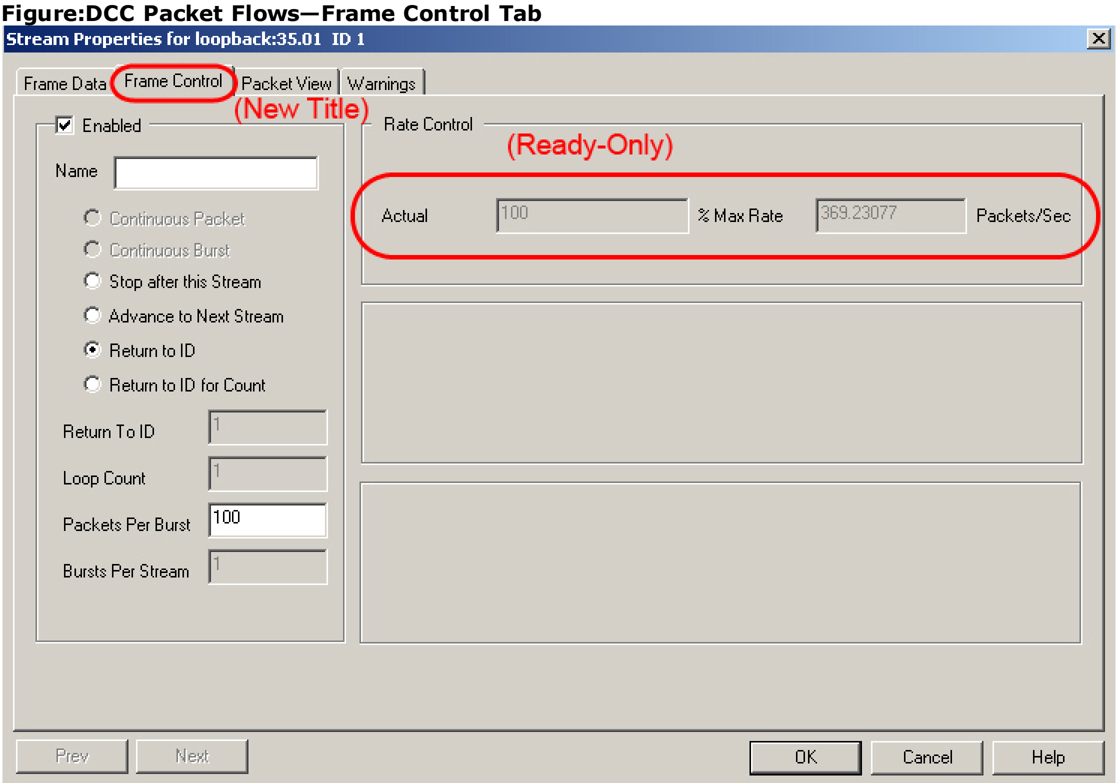


DCC Packet Flows are set up by the Ixia software in a manner similar to that used for packet flows on 10/100 modules. The IP flow packets are created by the software, and then saved in memory until time for transmission. The flow packets are then sent on a *Start Transmit*, but with a greatly reduced speed compared to the full OC-192c rate. Since only three bytes for SOH, or nine bytes for LOH, per SONET frame are being used to create the DCC channel, the rates are 192 Kbps or 576 Kbps, respectively.

To configure the DCC packet flows, first double-click *DCC Packet Flows* to display the DCC stream grid. Double-click a flow entry in the table to display the *Stream Properties* dialog. A modified version of the *Stream Control* tab is available for stream configuration. The tab is renamed to *Frame Control* to more accurately reflect the type of configuration, as shown in *Figure:DCC Packet Flows—Frame Control Tab.*

Stream Control for Standard POS Modules and *Instrumentation Box* for additional information.

Figure:DCC Packet Flows—Frame Control Tab



In general, for various applications of this tab, the same terminology is used in configuring either packet streams or flows, for example, 'Advance to Next Stream.'

The fields and controls in this tab are described in *Table:DCC Packet Flows—Frame Control Tab.*

Table:DCC Packet Flows—Frame Control Tab

Section	Field/Control	Description
Basic Stream Controls	Enabled	A packet flow must be enabled in order for it to be used. Disabled flows are skipped over when the port transmits.
	Name	This is an arbitrary, user-defined label assigned to the packet flow. The name need not be unique.
(Transmission Sequence)	(Continuous Packet)	*(Not available)*
	(Continuous Burst)	*(Not available)*
	Stop after this Stream	Designates that this stream (flow) is the last of a sequence of streams (flows). *Stop After Stream*.
	Advance to Next Stream	Designates that the next stream (flow) is to be transmitted after transmission of the current stream is complete. *Advance to Next Stream*.

Section	Field/Control	Description
	Return to ID	Designates that the stream (flow) whose ID number is shown in the *Return To ID* field is to be transmitted after transmission of the current stream (flow) is complete. It is used for continuous transmission. Choose *Return to ID* for continuous packet/burst. See *Return to ID*.
	Return to ID for Count	Designates that the stream (flow) whose ID number is shown in the *Return To ID* field is to be (re-)transmitted a number of times after transmission of the current stream (flow) is complete. This loop is repeated for the number of times specified in the *Loop Count* field. See *Return to ID for Count*.
	Return to ID	The ID number of the stream (flow) that is to be (re-)transmitted after transmission of the current stream (flow) is complete. See *Return to ID*. This value is forced to 1 for DCC Packet Flows.
	Loop Count	Active only when *Return to ID for Count* mode is selected above. The count used in a stream (flow) loop. It indicates the number of times to retransmit the stream (flow) identified in the *Return to ID* field. See *Return to ID for Count*.
	Packets Per Burst	Specifies the number of packets in the burst. NOTE Since the number of bursts per stream is forced to 1 for DCC Packet Flows, this value specifies the **total number of packets in this flow.**
	Bursts Per Stream	Specifies the number of bursts in the stream (flow). This value is forced to 1 for DCC Packet Flows.
Rate Control	% Max Rate	(Read-only) The percentage of the maximum bit rate.
	Packets/Sec	(Read-only) The number of packets per second that corresponds to the % Max Rate.

ATM Streams

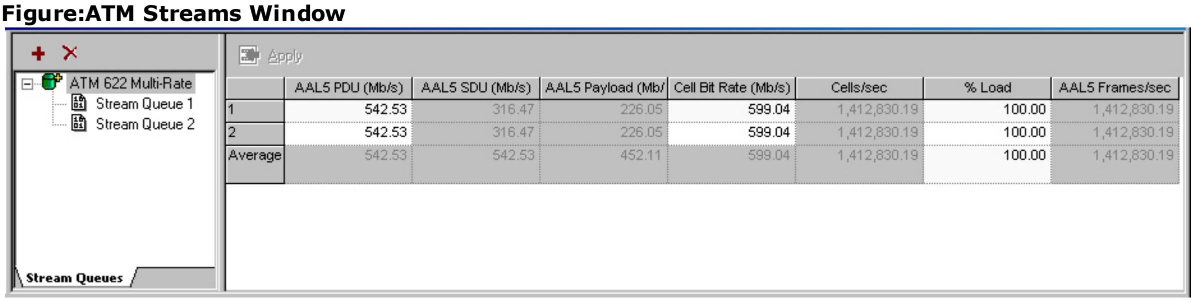
ATM Streams Window

When the Packet Streams item is selected, the ATM Streams window is displayed, as shown in *Figure:ATM Streams Window.*

NOTE Stream control for the POS 622 module is described in *Stream Control for POS 622 Modules*.

Up to 15 Stream Queues, each consisting of multiple streams, may be configured for each port. Up to 4,096 transmit streams can be defined per port, divided among multiple stream queues or all assigned to a single queue. These stream queues are transmitted in parallel.

Figure:ATM Streams Window



The fields and controls in this dialog are described in *Table:ATM Packet Stream View.*

Table:ATM Packet Stream View

Section	Field/Control	Description
Header		Add an entry.
		Deleted selected entry(ies).
		Click to apply the changes which have been made in the window. NOTE If this option is not clicked after changes are made, the Auto-Apply timer applies the changes automatically after 10 seconds have passed.
Stream Queue grid	AAL5 PDU (Mb/s)	The rate of AAL5 CSPS-PDU data in Megabits per second.
	AAL5 SDU (Mb/s)	The rate of AAL5 CSPS-SDU data in Megabits per second.
	AAL5 Payload (Mb/s)	The rate of AAL5 payload data in Megabits per second.
	Cell Bit Rate (Mb/sec)	The rate exclicked in Megabits per second.
	Cells/sec	The rate exclicked in (53-byte) cells per second. For each individual stream queue, the cell rate is specified only on the Summary page.
	% Load	Each Stream Queue can be assigned a load of up to 100% of line rate.
	AAL5 Frames/Sec	The rate exclicked in AAL5 Frames (PDUs) per second.
Average		The averages for the values in the column.

ATM Stream Queue Grid

When a Stream Queue in the list under the port is selected, the Stream Queue grid is displayed (with five sub-tabs) for a list of streams, as shown in *Figure:ATM Stream Queue Grid–ATM Data* through *Figure:ATM Stream Queue Grid–Link/IP Data.*

Although up to 4,096 transmit streams can be defined per port—divided among multiple stream queues or all assigned to a single queue—only a total of 127 entries can be actively monitored on an individual stream level. So the check box *Statistic* in the ATM Data grid is used to select the streams that are monitored. In the example below, Stream 1 and Stream 4 of Stream Queue 3 are enabled, while Streams 2 and 3 are not. (This discussion continues at topic *Per Stream Statistic View*.)

When you add a new stream, the default state of the *Statistic* check box is enabled. But once the number of entries that can be monitored reaches 127, adding a new stream results in entries with the *Statistic* check box cleared. At the maximum state, no additional statistics can be monitored until you explicitly free up some previously selected entries, by clearing them.

Figure:ATM Stream Queue Grid–ATM Data

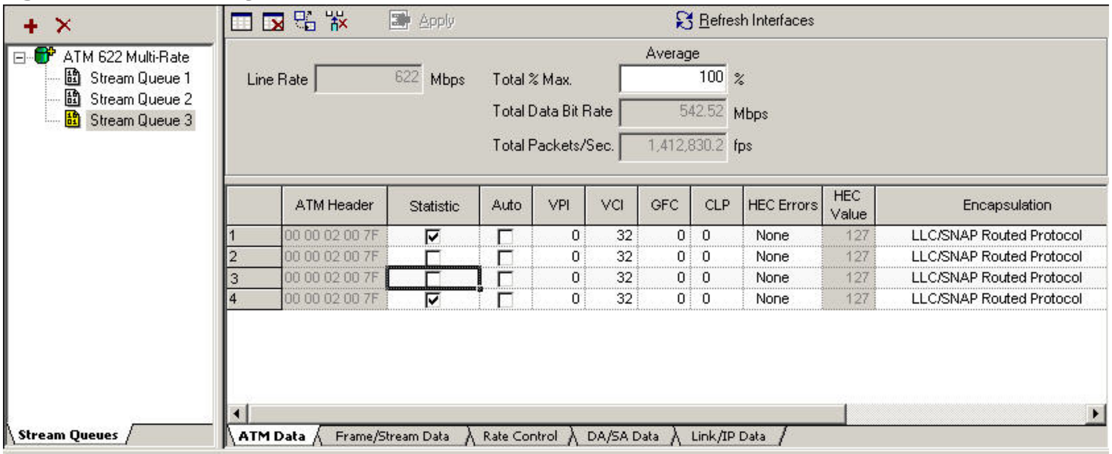


Figure:ATM Stream Queue Grid–Frame/Stream Data

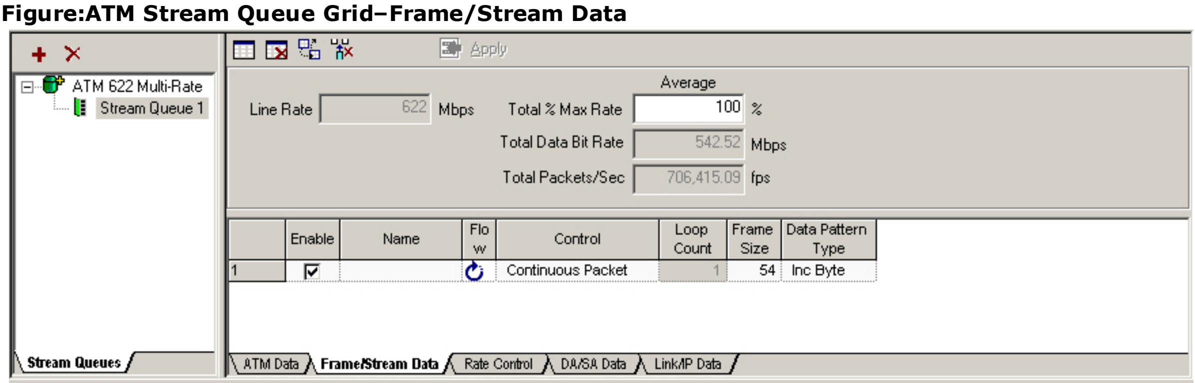


Figure:ATM Stream Queue Grid–Rate Control

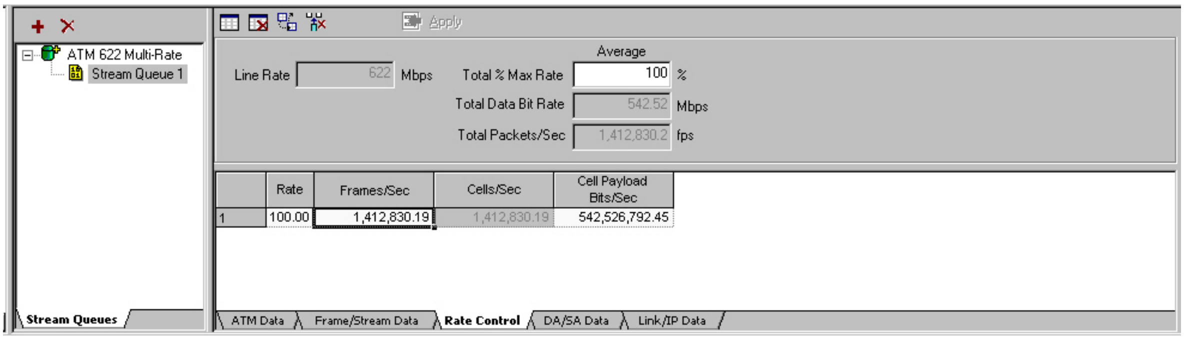


Figure:ATM Stream Queue Grid–DA/SA Data

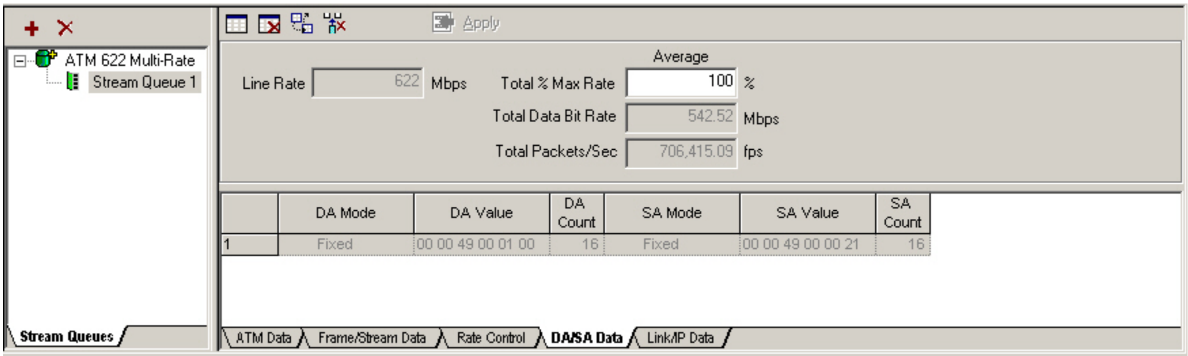
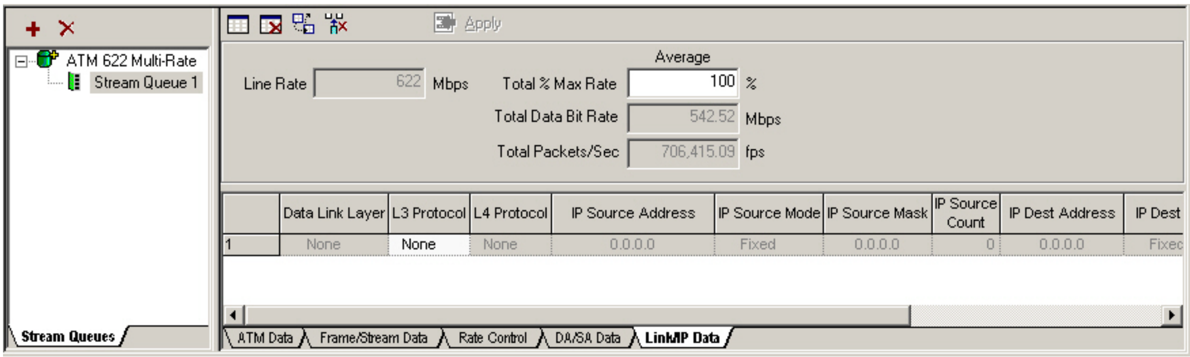


Figure:ATM Stream Queue Grid–Link/IP Data



The fields and controls in these dialogs are described in *Table:ATM Stream Queue Grid.*

Table:ATM Stream Queue Grid

Section/View	Field/Control	Description
Header	Line Rate	(Read-only) Line Rate of the OC-3c/OC-12c port (in Mbps).
	Average -Total % Max Rate	(in %) The average of the user defined data rates for the VCs (as a percentage).
	Average - Total Data Bit Rate	(Read-only) (in Mbps) The average of the data rates for the VCs (with data rates automatically calculated from the user settings for percentage of Max Rate) (in Mbps).
	Average - Total Packets/Sec	(Read-only) (in Mbps) The average of the data rates for the VCs (with packet rates automatically calculated from the user settings for percentage of Max Rate) (in Mbps).

Section/View	Field/Control	Description
ATM Data	ATM Header	Displays the bytes in the 5-byte ATM Cell header.
	Statistic	If selected, transmit statistic for this stream is monitored
	Auto	If selected, the VPI and VCI are read-only and the values are automatically assigned (0/32). If not selected, you can assign the VPI and VCI.
	VPI	Virtual Path Identifier for this stream.
	VCI	Virtual Circuit/Connection Identifier for this stream.
	GFC	Generic Flow Control, for device control signalling. Uncontrolled equipment uses a setting of 0000 (Null value).
	CLP	Cell Loss Priority setting for this stream queue/VC. Used for setting discard priority level for ATM cells. A CLP value = 0 has higher priority than a CLP value = 1.
	HEC Errors	Header Error Correction Errors. Choose the number of bit errors to insert in the HEC byte: • None (errors not inserted) • 1 Bit • 2 Bits • 3 Bits • 4 Bits • 5 Bits • 6 Bits • 8 Bits
	HEC Value	(Read-only) The decimal value corresponding to the HEC Error setting in the field to the left. It is the calculated HEC value with the HEC error setting applied. (It changes with the VPI/VCI.)
	Encapsulation	The type of RFC 2684 multiplexing encapsulation used. Choose one of: • LLC/SNAP Routed Protocol • LLC Bridged Ethernet/802.3 • LLC Bridged Ethernet/802.3 no FCS • VC MUX Routed Protocol • VC MUX Bridged Ethernet/802.3 • VC MUX Bridged Ethernet/802.3 no FCS
	User Management	Bit 1 of the *PT* field.

Section/View	Field/Control	Description
		This bit has to do with user management and indicates if the ATM cell is a control or data cell. 0 - ATM data cell 1 - ATM control cell
	Congestion	Bit 2 of the *PT* field. This bit indicates Congestion/No Congestion. Choose one of: 0 - Congestion Not Experienced 1 - Congestion Experienced
	Last Cell	Bit 3 of the *PT* field. This bit indicates if this is the last ATM cell of the frame. [ATM User to ATM user indication (AUU) = 0 for the first and intermediate ATM cells. AUU = 1 for the last ATM cell.]
	Force AAL5 Error	Option to force an error in the AAL5 frame CRC. Choose one of: • No Error • Bad CRC
Frame/Stream Data	Enable	Enables the use of the options in this sub-view. These choices are described more fully in the *ATM Stream Control* tab and *Frame Data* sections.
	Name	The user-defined name for this stream queue/VC.
	Flow	(Displays an icon associated with the selection in the *Control* field to the right.)
	Control	The type of stream control to use for this ATM stream. Choose one of: • Continuous Packet • Continuous Burst • End • Advance • Return to ID* • Return For Count* These options are discussed more fully in *Stream Control for ATM*. NOTE An ATM stream cannot be set to *Return to ID* or *Return For Count*

Section/View	Field/Control	Description
		NOTE unless it is the last stream in the queue. If it is not the last stream, it is automatically forced to *Advance* stream mode. Also, *Return to ID* can only be set to '1'. If the user enters any other value, it is forced to a value of '1'.
	Loop Count	Applies to Return for Count control mode. Enter the number of loops for the stream queue/VC.
	Frame Size	The size of the frame, in bytes.
	Data Pattern Type	The type of data pattern used in the payload of the frame. Choose one of: • Inc Byte • Inc Word • Dec Byte • Dec Word • Random • Repeating • Fixed
Rate Control	Rate	The setting on this stream queue/VC for the percentage of the maximum available rate.
	Frames/Sec	The average number of frames per second transmitted by this stream, based on the set *Rate*.
	Cells/Sec	(Read-only) The average number of full ATM cells per second transmitted by this stream, based on the set *Rate*.
	Cell Payload Bits/Sec	The average number of cell payload bits per seconds transmitted by this stream, based on the set *Rate*.
DA/SA Data	DA Mode	The type of destination MAC address generation. Choose one of: • Increment • Continuous Inc. • Decrement • Continuous Dec. • Fixed • Random • ARP/Discovery
	DA Value	The first destination MAC address to be generated for the stream.

Section/View	Field/Control	Description
	DA Count	(Read-only) If *DA Mode* is either *Increment* or *Decrement*, then this is the number of times that the address increments before being reset and started again.
	SA Mode	The type of source MAC address generation. Choose one of: • Increment • Continuous Inc. • Decrement • Continuous Dec. • Fixed • Random
	SA Value	The first source MAC address to be generated for the stream.
	SA Count	(Read-only) If *SA Mode* is either *Increment* or *Decrement*, then this is the number of times that the address increments before being reset and started again.
Link/IP Data	Data Link Layer	(Read-only) The type of data link encapsulation. One of: • None • Ethernet II • Ethernet SNAP • 802.3 RAW • 802.3 (IPX) Reflects the setting in the *Frame Data* tab Protocols section.
	L3 Protocol	This is the Layer 3 protocol to be used. Choose one of: • None • IPv4 • IPv6 • IPv6 Over IPv4 • IPv4 Over IPv6 • IPX • Arp • Pause
	L4 Protocol	This is the Layer 4 protocol to be used. Choose one of: • None

Section/View	Field/Control	Description
		• TCP • UDP • ICMP • IGMP • RIP • DHCP • OSPF
	IP Source Address	For those Layer 3 protocols that require IP addresses, this is the starting source IP address for packets in this stream queue.
	IP Source Mode	The means of generating subsequent IP addresses. Choose one of: • Fixed • Incr. Host • Decr. Host • Cont. Incr. Host • Cont. Decr. Host • Incr. Network • Decr. Network • Cont. Incr. Net • Cont. Decr. Net • Random • Custom Mask Increment • Custom Mask Decrement • Custom Mask Continuous Increment • Custom Mask Continuous Decrement • Custom Mask Random
	IP Source Mask	The mask associated with the SA address
	IP Source Count	If the *IP Source Mode* is any of the choices except *Fixed* or *Random*, this is count of increments/decrements until the address is reset to the *IP Source Address* value and counting starts again.
	IP Dest Address	For those layer 3 protocols that require IP addresses, this is the starting destination IP address for packets in this stream.
	IP Dest Mode	The means of generating subsequent IP addresses. Choose one of: • Fixed

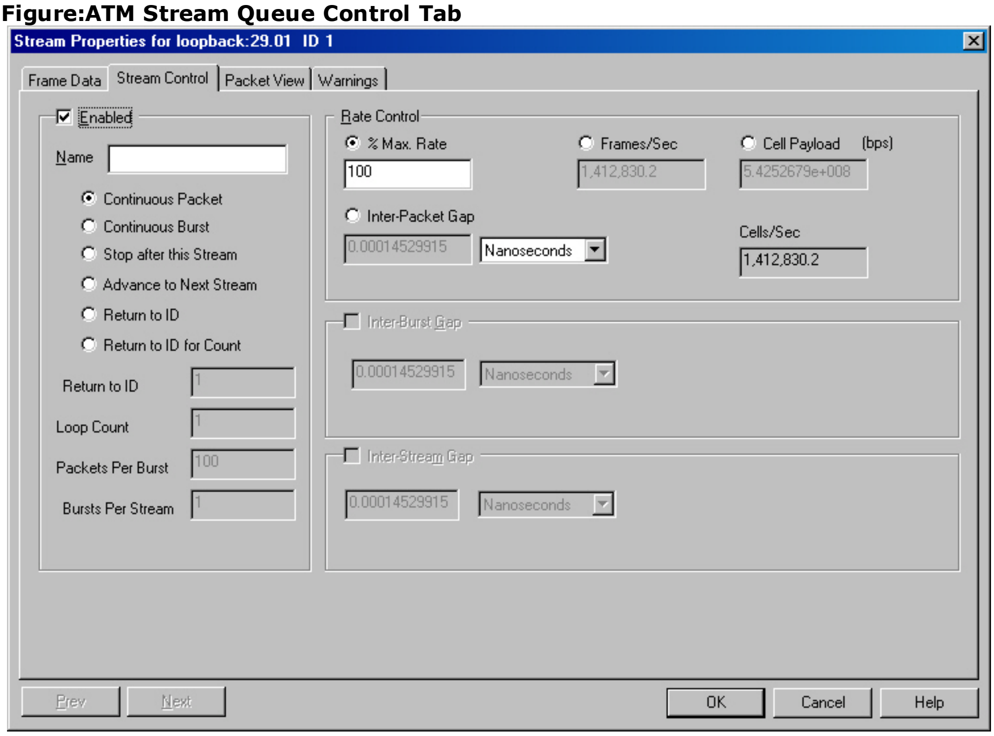
Section/View	Field/Control	Description
		• Incr. Host • Decr. Host • Cont. Incr. Host • Cont. Decr. Host • Incr. Network • Decr. Network • Cont. Incr. Net • Cont. Decr. Net • Random • Custom Mask Increment • Custom Mask Decrement • Custom Mask Continuous Increment • Custom Mask Continuous Decrement • Custom Mask Random
	IP Dest Mask	The mask associated with the DA address.
	IP Dest Count	If the *IP Dest Mode* is any of the choices except *Fixed* or *Random*, this is count of increments/decrements until the address is reset to the *IP Dest Address* value and counting starts again.

Stream Control for ATM

The *Stream Control* tab for an individual ATM Stream Queue is shown in *Figure:ATM Stream Queue Control Tab.*

NOTE For POS 622 (OC-12c/OC-3c POS) module *Stream Control* tab descriptions, Stream Control for POS 622 Modules.

Figure:ATM Stream Queue Control Tab



The fields and controls in this box are described in *Table:Basic Stream Controls.*

Table:ATM Stream Control Tab

Section	Field/Control	Description
Basic Stream Controls	Enabled	A stream must be enabled in order for it to be used. Up to 255 streams may be defined per port. Disabled streams are skipped over when the port transmits.
	Name	This is a label assigned to the stream. The name need not be unique.
	Continuous Packet	A type of stream that sends out a continuous sequence of packets with the same inter-packet gap between packets. *Continuous Packet* mode may not be used with flows.
	Continuous Burst	A type of stream that sends out a continuous set of packet bursts. *Continuous Burst* mode may not be used with flows. **Note**following *Table:Basic Stream Controls* for information on maximum burst count.
	Stop after this Stream	Designates that this stream is the end of a sequence of streams.
	Advance to Next Stream	Designates that the next stream is to be transmitted after the current stream is complete.
	Return to ID	Designates that the stream identified (with a Stream ID) in the *Return To ID* field is to be used after the current stream is complete. NOTE An ATM stream cannot be set to

Section	Field/Control	Description
		NOTE *Return to ID* unless it is the last stream in the queue. If it is not the last stream in the queue, it is forced to *Advance to Next Stream*.
	Return to ID for Count	Designates that the stream identified in the *Return To ID* field is to be used after the current stream is complete. The loop is repeated for number of times specified in the Loop Count parameter. NOTE An ATM stream cannot be set to *Return to ID for Count* unless it is the last stream in the queue. If it is not the last stream in the queue, it is forced to *Advance to Next Stream*.
	Return To ID	The stream ID that runs after the current stream has run.
	Loop Count	The count used in a stream loop. Indicates the number of times that the stream identified in the *Return to ID* field is transmitted.
	Packets Per Burst	Specifies the number of packets in each ATM burst.
	Bursts Per Stream	Specifies the number of bursts in this ATM stream.
Rate Control		Rate control for ATM modules controls the average rate of transmitting packets/sec. Each Stream Queue may operate at 100% of Max Rate.
	% of Max Rate	This specifies the intended number of packets to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets transmitted per second within a burst; except for *Continuous Packet* type streams the actual packets per second is lowered due to inter-burst and inter-stream gaps.
	Frames/Sec	This specifies the intended number of frames to be transmitted per second. The actual inter-packet gap time is configured to allow that packet rate. The actual rate may be adjusted slightly to allow for the clock rates associated with each type of port (see *Inter-Packet Gap* below). This value only relates the packets

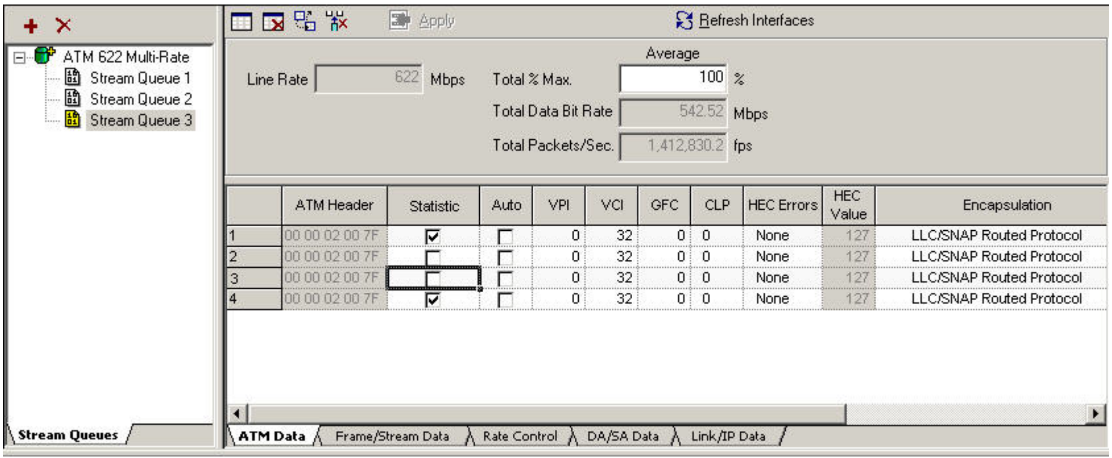
Section	Field/Control	Description
		transmitted per second within a burst; except for *Continuous Packet* type streams the actual packets per second is lowered due to inter-burst and inter-stream gaps.
	Cell Payload (bps)	The average number of cell payload bits per seconds transmitted by this stream.
	Inter-Packet Gap	This specifies the amount of time between packets within a burst. The time must be specified in multiples of the indicated time units.
	Time	This specifies the amount of time between packets. The time must be specified in multiples of the indicated time units.
	Units	Selects the time units used for the *Time* field. The choices are: • Nanoseconds • Microseconds • Milliseconds • Seconds • Cells
	Cells/Sec	(Read-only)
	Inter-Burst Gap	Check this box to enable the generation of inter-burst gaps.
	Time	This specifies the amount of time between bursts within a stream. The time must be specified in multiples of the indicated time units.
		Selects the time units used for the *Time* column. The choices are: • Nanoseconds • Microseconds • Milliseconds • Seconds • Cells
	Inter-Stream Gap	If selected, enables generation of the inter-stream gap.
	Time	This specifies the amount of time between streams. The time must be specified in multiples of the indicated time units.
	Units	Selects the time units used for the *Time* field. The choices available depend on the type of load module: • Nanoseconds • Microseconds • Milliseconds

Section	Field/Control	Description
		• Seconds • Cells

Per Stream Statistic View

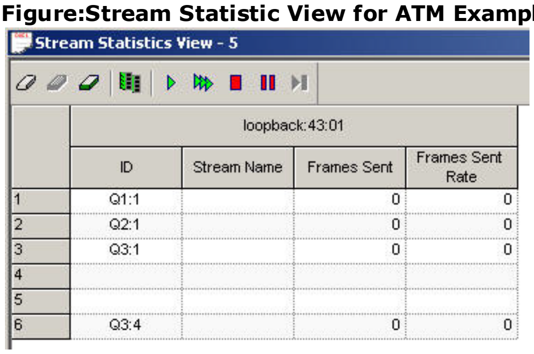
When in Per Stream Tx Stats mode, you can create a *Stream Statistic View* for that port. The per stream statistic view is only available when the ATM port is in Per Stream Tx Stats mode and not in Per VPIVCI mode (on the ATM Data tab, shown in *Figure:ATM Stream Queue Grid–ATM Data.* For a general discussion of Stream Statistic View, *Stream Statistic View*.

Figure:ATM Stream Queue Grid–ATM Data



An example of the Stream Statistic View is shown in *Figure:Stream Statistic View for ATM Example.*The entries for Q3:2 and Q3:3 are blank because they are disabled in the Stream configuration (shown above). The Stream Statistic View reflects the latest state of the streams automatically in real-time (that is, you can add or delete a stream, toggle the *Statistics* check box, and immediately see the changes reflected in this view).

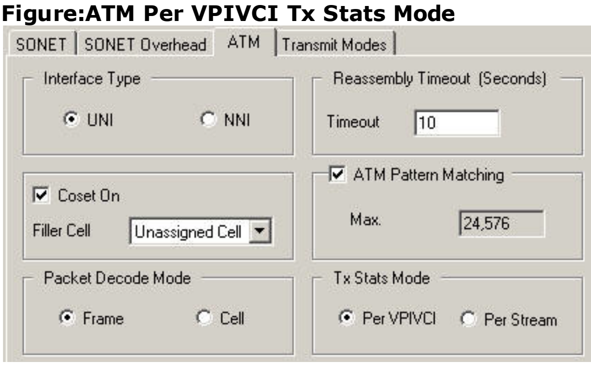
Figure:Stream Statistic View for ATM Example



Per VPIVCI Statistic View

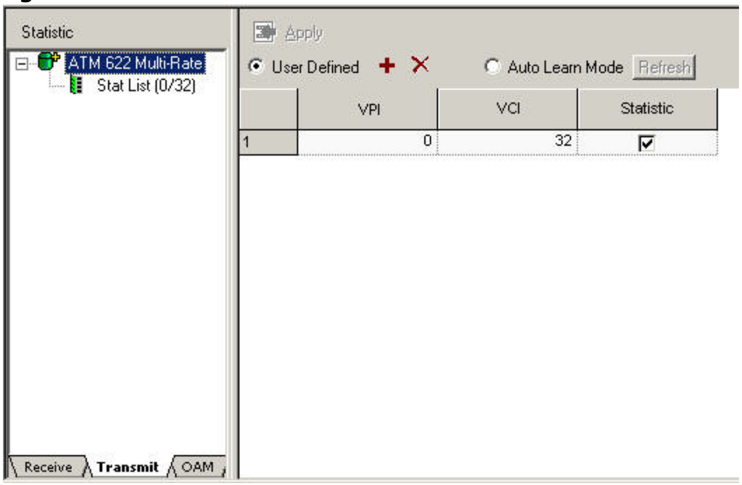
To configure stream entries for Per VPIVCI monitoring, configure the port property to Per VPIVCI mode (Tx Stats) as shown in *Figure:ATM Per VPIVCI Tx Stats Mode.*

Figure:ATM Per VPIVCI Tx Stats Mode



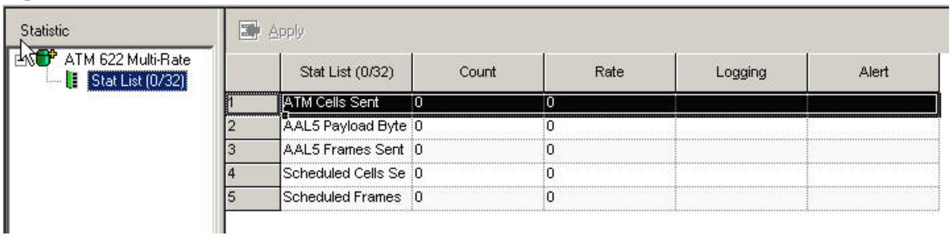
Then under the VPI/VCI Registration, configure the particular VPI/VCI entry to monitor, in addition to enabling the Tx *Statistic* check box, as shown in *Figure:ATM Per VPIVCI Tx Stats Mode.*

Figure:ATM Per VPIVCI Tx Stats Mode



Then the particular VPIVCI StatList becomes available, as shown in *Figure:ATM Per VPIVCI Tx StatList.*

Figure:ATM Per VPIVCI Tx StatList



Changing Streams Without Interruption

This feature applies to these load modules:

- LM1000(S)TX(S)2/4/24
- LM1000SFP(S)4
- LSM1000XMS(R)12
- ASM1000XMV(R)16

- MSM10G1
- LSM10G(L)1, LSM10GXL6
- LSM10GXM(R)3
- NGY LSM10GXM4(R), LSM10GXM8(R)

Both Packet and Advanced streams can be suspended and then resumed, and the Total % Line Rate can be changed, without affecting the overall traffic. When streams are suspended/resumed or adjusted for Total % Line Rate using the Stream Editing grid, the changes take effect without stopping/restarting traffic.

NOTE Use only the Stream Editing grid to make these changes. Changing streams from the Stream Properties page does **not** work the same way, and traffic **is** interrupted..

Packet Streams

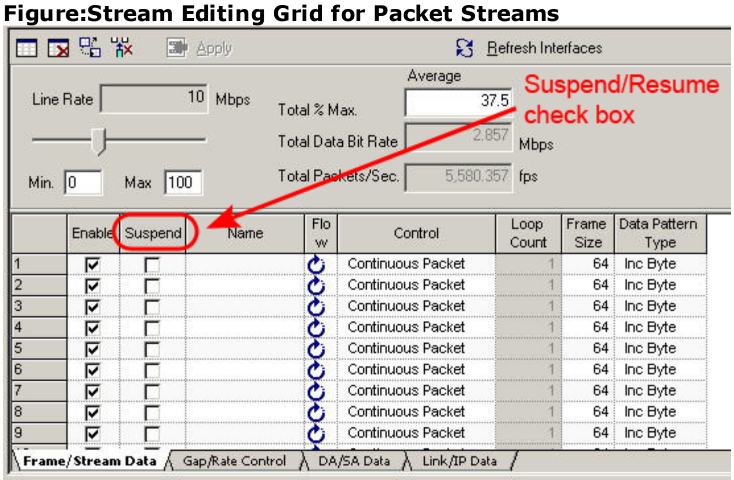
Suspend/Resume

Packet streams (also known as basic or sequentially scheduled streams) can be suspended and resumed during transmission. However, if new streams are added, the stream traffic must stop and restart after the new configuration is loaded. When a packet stream is suspended and then resumed, a persistent UDF continues to count from where it left off when the stream was suspended.

If a currently active stream is suspended, it runs to completion and not execute again until it is resumed.

The Stream Editing grid features a Suspend check box, as shown in *Figure:Stream Editing Grid for Advanced Streams.* Select the check box to suspend the stream, then click again (deselect) to resume traffic on that stream. After suspending or resuming one or more streams, you must click **Apply** or wait for the Apply timer to expire, for the change to take effect. Changes to multiple streams are processed one-by-one.

Figure:Stream Editing Grid for Packet Streams



Rate Change

The Total % Line Rate can be changed using either the slider or the Total % Line Rate field. When Total % Line Rate is changed, rates on all streams (on the port) are affected.

When changing the rate on a packet stream, the rate change takes effect after the next packet for the stream is scheduled.

After changing the rate of one or more streams, you must click **Apply** or wait for the Apply timer to expire, for the change to take effect. Changes to multiple streams are processed one-by-one.

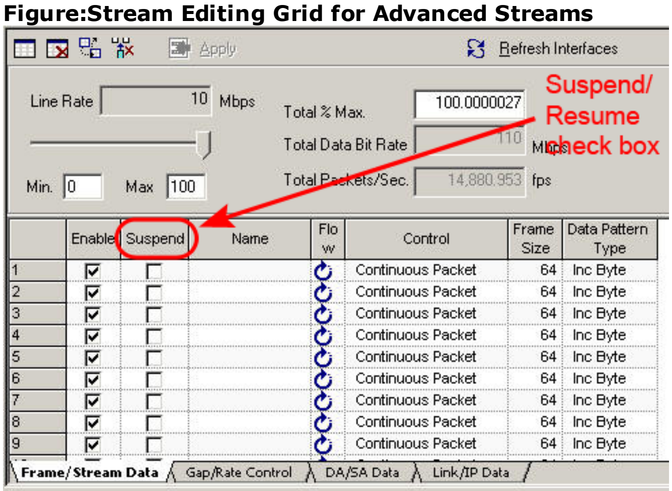
Advanced Streams

Suspend/Resume

Advanced streams (also known as concurrently scheduled streams) can be suspended and then resumed without interrupting traffic on other streams. However, new streams cannot be added without stopping and restarting traffic. When a running stream is suspended, it will not transmit packets until it is resumed. When a stream is suspended and then resumed, the stream continues from where it left off with regard to its packet count, UDFs, and so on.

The Stream Editing grid features a Suspend check box, as shown in *Figure:Stream Editing Grid for Advanced Streams.* Select the check box to suspend the stream, then click again (deselect) to resume traffic on that stream. After suspending or resuming one or more streams, you must click **Apply** or wait for the Apply timer to expire, for the change to take effect. Changes to multiple streams are processed one-by-one.

Figure:Stream Editing Grid for Advanced Streams



Rate Change

Like the Packet streams, when changing the rate on a Concurrent stream, the rate change takes effect after the next packet for the stream is scheduled. Each stream has a maximum rate so that the software can determine if it should go into a fast or slow counter in the hardware. For details, Advanced Streams for Ethernet Modules.

The Total % Line Rate can be changed using either the slider or thse Total % Line Rate field. When Total % Line Rate is changed, rates on all streams (on the port) are affected.

After changing the line rate of one or more streams, you must click **Apply** or wait for the Apply timer to expire, for the change to take effect. Changes to multiple streams are processed one-by-one.

Transparent Dynamic Rate Change

If selected (in the Transit Modes tab of Port Properties), this allows rate change across counters, for this port, without stopping transmit.

NOTE

The behavior of Transparent Dynamic Rate Change is not intuitive.

Turn ON Transparent Dynamic Rate Change (in Transmit Modes, Port Properties), then switch to Advanced Streams, Gap/Rate Control tab. You see there is no limit (all are at 100%) in Max Limit % Line Rate.

Then if you return to Port Properties / Transmit Modes and turn OFF the TDRC, and then go back to the Gap/Rate Control tab, you see there is a limit; only the first 16 streams are at 100%.

At that point, if you return to Transmit Modes and again turn ON the TDRC, and then go back to Gap/Rate Control tab, you expect to see all streams at 100% (no limit), but in fact the status is unchanged—there is still a limit. This is a case of not being able to UNDO the effect of turning OFF, by turning ON again.

Chapter 5 - Frame Data–Basic Frame Structure

Frame Data Structure

The *Frame Data* tab in the *Stream Properties* dialog provides control over all aspects of packets transmitted by the Ixia hardware. These frames are also referred to as datagrams or packets in some contexts. Many frames may be generated in the processing of a stream. Many of the controls available allow the specification of a series of values applied to subsequent frames.

This chapter discusses basic frame data structure. For other parts of frame data construction, see:

- *Frame Data–Protocol Control*
- *Frame Data–User Defined Fields (UDF)*

The *Frame Data* tab is described in *Frame Data Tab*. The controls available in the *Frame Data* tab correspond to the manner in which the Ixia hardware formats frames. Two main types of frames are Ethernet frames and SONET frames, described in the following sections:

- *Ethernet Frames*
- *SONET Frames*

The main components of the *Frame Data* tab are described in the following sections (some of these components are described in other chapters):

- (For Ethernet ONLY) *Preamble Size Box* and *The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see Ixia Platform Reference Manual. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count value displayed in the field includes the SFD.*
- (For SONET ONLY) *Min Flags Box*
- *Data Pattern Box*
- *Frame Size*
- *Instrumentation Box*
- *Force Errors Box*
- *DA/SA Property Sheet*

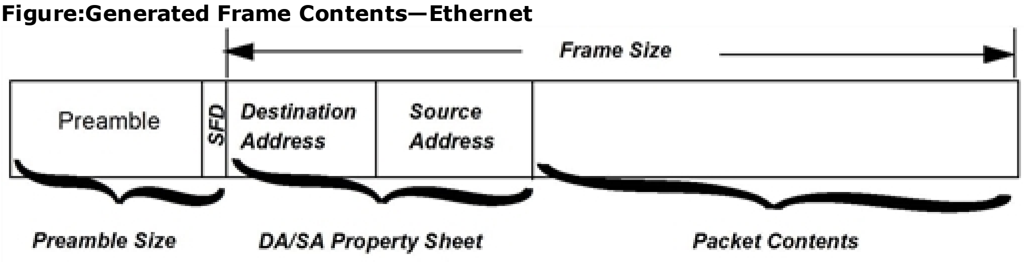
In addition, this chapter includes special sections on the *Frame Data* tab for the following features:

- *Frame Data for GFP*
- *Frame Data for ATM/POS 622*

Ethernet Frames

Every Ethernet frame has a basic structure as shown in *Figure:Generated Frame Contents—Ethernet*.

Figure:Generated Frame Contents—Ethernet



The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. For 10 Gigabit Ethernet cards, the preamble is 8 bytes long and has a value of 0x55 (though some of the preamble bytes may be modified by you). The permissible preamble size varies between cards, see the *Ixia Platform Reference Manual*. The length of the Preamble is controlled by the *Frame Data for Ethernet Modules*. *The Preamble is followed by the SFD—Start Frame Descriptor, which has a value of 0xAD (0xD5 for 10 Gigabit Ethernet cards). The SFD is considered as part of the preamble and is included in the preamble size calculation.*

The DA (Destination Address) and SA (Source Address) fields follow. They hold MAC addresses and are 6 bytes each. These values may contain a constant value, a random value, or may increment or decrement. The contents of these two fields is controlled by the fields of the *DA/SA Property Sheet*.

The Packet Contents are programmed by five types of data generators. The list below indicates the order in which the generators are applied. The data created by each generator overwrites data created by earlier generators, if they overlap. The data generators are:

1. Protocols: Controlled by the *Protocols* sub-tab, described in *Chapter 6, Frame Data–Protocol Control. The protocol generator allows for the formatting of protocol specific headers. Specific IP protocols, such as UDP, are supported in more detail. Protocol header fields start at offset 12 in the frame, immediately following the DA and SA fields.*
2. Data Patterns: Controlled in the *Data Pattern Box*. *The data patterns may be simple algorithmic values, random values, repetitions of fixed patterns or arbitrary sets of data retrieved from a disk. Data patterns start after the DA/SA fields and any protocol headers that are generated.*
3. UDF1, UDF2, UDF3, UDF4, and UDF5 (availability of UDF5 depends on type of module): These User Data Fields (UDFs) are not normally permitted to overlap and are controlled by the *User Defined Field* sub-tabs, as described in *Chapter 7,Frame Data–User Defined Fields (UDF). In the case of the Ixia ATM and Ethernet TXS modules, there are five UDFs. Each UDF controls a 32-bit counter. In general, each UDF may be positioned anywhere between the end of DA or SA fields and the end of the frame, although some modules allow the UDF to start at the beginning of the frame. See the Ixia Platform Reference Manual for information on the UDF types supported by each module.*
4. Frame Identity Record (FIR): This 6-byte quantity is Ixia hardware-generated data which can be used to uniquely identify each frame and is controlled by the *Instrumentation Box*. *The FIR record is usually positioned at the end of the packet, or just before the FCS, if it is present (though some modules allow for the manipulation of this position).*

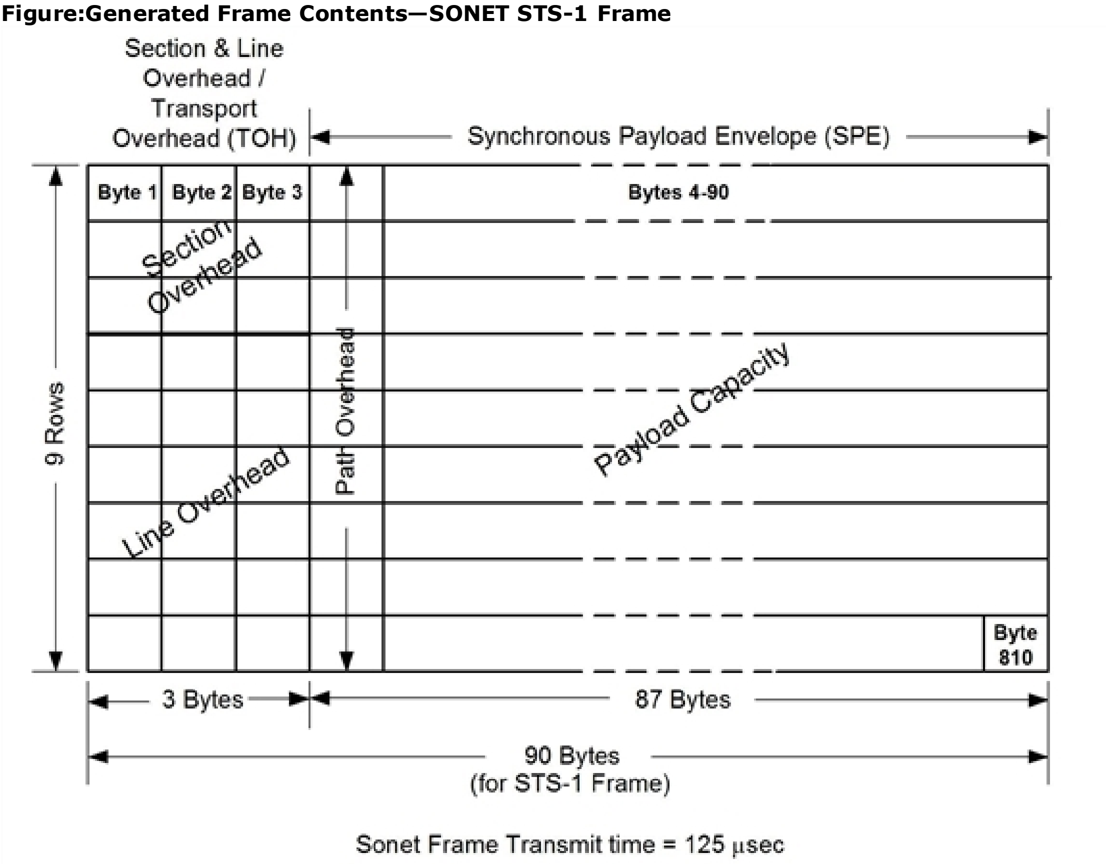
5. Frame Check Sequence (FCS): This four-byte quantity is controlled by the *Force Errors Box*. *It may be used to insert a normal CRC checksum, omit the checksum, or simulate various errors. If included, it is always positioned at the end of the frame.*

SONET Frames

A Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) frame is based on the Synchronous Transport Signal-1 (STS-1) frame, whose structure is shown in *Figure:Generated Frame Contents—SONET STS-1 Frame*. Transmission of SONET Frames of this size correspond to the Optical Carrier level 1 (OC-1).

An OC-3c, consists of three OC-1/STS-1 frames multiplexed together at the octet level. OC-12c, OC-48c, and OC-192c, are formed from higher multiples of the basic OC-1 format. The suffix ‘c’ indicates that the basic frames are concatenated to form the larger frame.

Figure:Generated Frame Contents—SONET STS-1 Frame



The contents of the SONET STS-1 frame are described in *Table:SONET STS-1 Frame Contents*.

Table:SONET STS-1 Frame Contents

Section	Description
Section Overhead (SOH)	Consists of 9 bytes which include information relating to performance monitoring of the STS-n signal, and framing.
Line Overhead (LOH)	Consists of 18 bytes which include information relating to performance monitoring of the individual STS-1s, protection switching information, and line alarm indication signals.

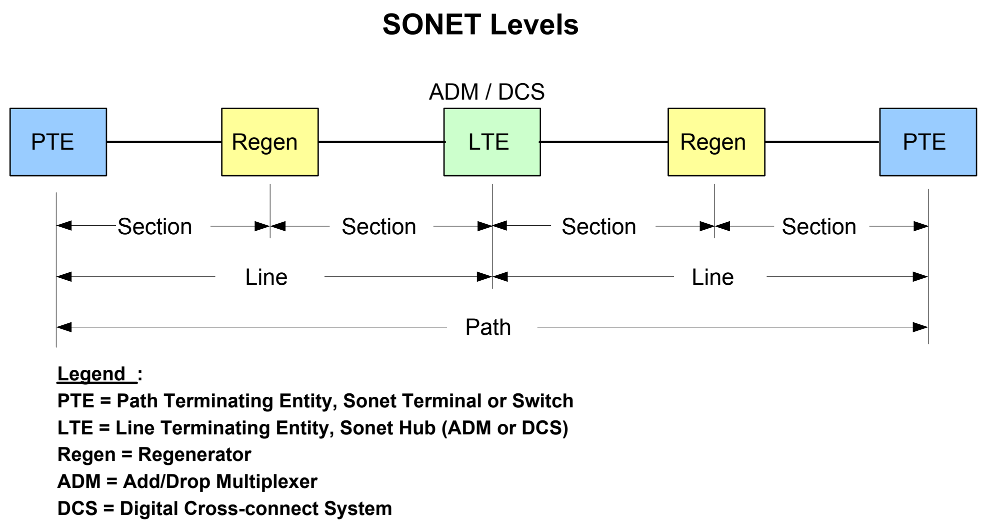
Section	Description
Transport Overhead (TOH)	Consists of a combination of the Section Overhead and Line Overhead sections of the STS-1 frame.
Path Overhead (POH)	Part of the Synchronous Payload Envelope (SPE), contains information on the contents of the SPE, and handles quality monitoring.
Synchronous Payload Envelope (SPE)	Contains the payload information, the packets which are being transmitted, and includes the Path Overhead bytes.
Payload Capacity	Part of the SPE, and contains the packets being transmitted.

The SONET STS-1 frame is transmitted at a rate of 51.84 Mbps, with 49.5 Mbps reserved for the frame payload. A SONET frame is transmitted in 125 microseconds, with the order of transmission starting with Row 1, Byte 1 at the upper left of the frame, and proceeding by row from top to bottom and from left to right.

SONET Levels

The section, line, and path overhead elements are related to the manner in which SONET frames are transmitted, as shown in *Figure:Example Diagram of SONET Levels and Network Elements*.

Figure:Example Diagram of SONET Levels and Network Elements



See Port Properties for DCC for additional information on the optional SONET Data Communication Channel (DCC) feature available on OC-192c POS modules.

Frame Data Tab

NOTE For information on protocol construction of frame data structure, Chapter 6,*Frame Data–Protocol Control*.

To access the *Frame Data* tab, double-click in a stream/flow entry in the *Packet Streams/Packet Flows/Advanced Streams* window, then select the *Frame Data* tab. Alternatively, right-click a port in the Resources window, and select *Edit Streams* from the displayed menu. The *Frame Data* tab varies for different types of load modules. The major types are:

- *Frame Data for Ethernet Modules*—which includes 10/100, 10/100/1000, Gigabit, and 10 Gigabit modules.
- *Frame Data for SONET/POS Modules*—which includes OC-12c/OC-3c, OC-48c, and OC-192c POS load modules.
- *Frame Data for FCM*—which includes FCMGXM4 and FCMGXM8 load modules.
- *Frame Data for Flex*—which includes FlexAP10G16S and FlexFE10G16S load modules.
- *Frame Data for XDM10G32S*—which includes XDM10G32S load module.
- *Frame Data for Lava 40GE/100GE*- which includes Lava AP40GE/100GE 2P and Lava AP40GE/100GE 2RP
- *Frame Data for Xcellon-Multis, Novus, and Novus-R*- which includes Xcellon-Multis, Novus QSFP28, and Novus-R QSFP28 load modules

For information on implementation of SONET-related special features in the *Frame Data* tab, see the following sections:

- *Frame Data for DCC*
- *Frame Data for SRP*
- *Frame Data for RPR*
- *Frame Data for GFP*
- *Frame Data for ATM/POS 622*

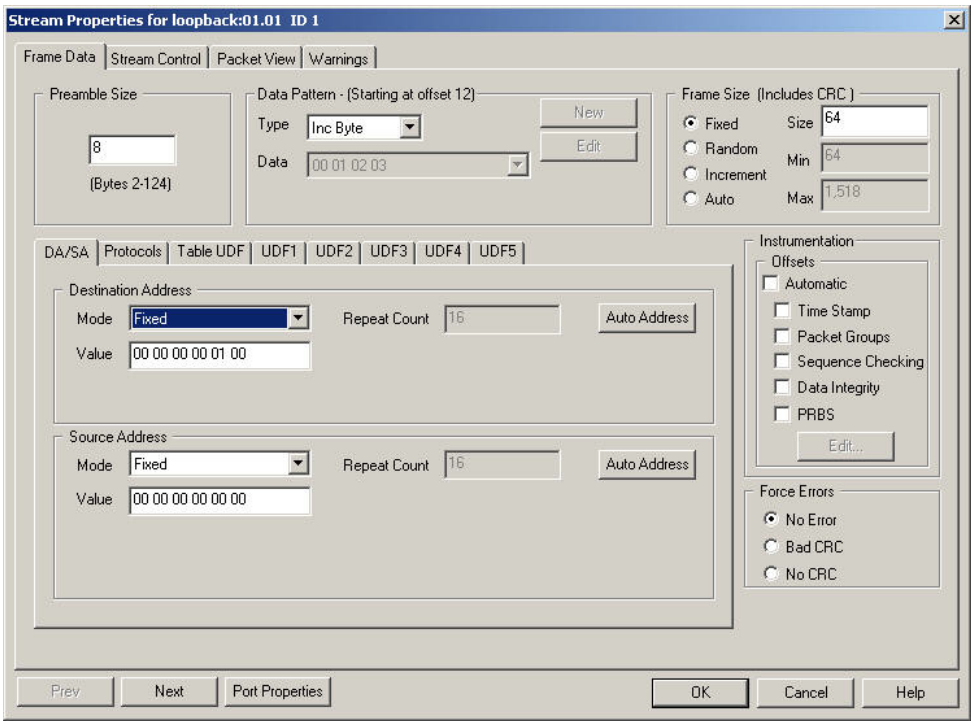
Frame Data for Ethernet Modules

The Ethernet load modules have two main versions of *Frame Data* tabs:

- *10/100/1000 Ethernet Frame Data Tab*—The *Frame Data* tab for 10/100, Copper 10/100/1000, and Gigabit load modules is shown in *Figure:Frame Data for 10/100, 10/100/1000, 10/100 TXS8, and Gigabit Modules (shown for 10/100/1000)*.
- *10 Gigabit Frame Data Tab*—The *Frame Data* tab for 10 Gigabit modules is shown in *Figure: Frame Data for 10 Gigabit Modules*.

10/100/1000 Ethernet Frame Data Tab

Figure:Frame Data for 10/100, 10/100/1000, 10/100 TXS8, and Gigabit Modules (shown for 10/100/1000)



NOTE

These cards—10/100, 10/100/1000, 10/100 TXS8, and Gigabit modules—do not support PRBS. However, the following cards DO support PRBS:

LM1000STXS4 family

LM1000TXS4 family

LM1000SFPS4 family

OLM1000STXS24 family

LSM1000XMS12 family

LSM1000XMV family (not in Data Center Mode)

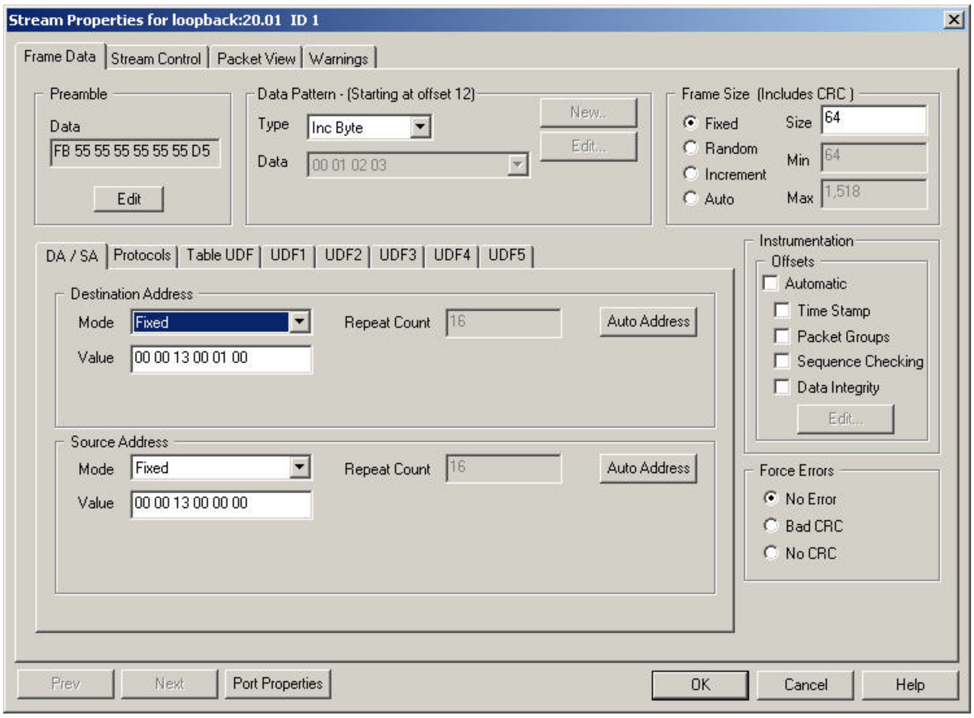
ASM1000XMV12

LSM10G1 and 10GL1

NGY LSM10GXM family (not in Data Center Mode).

10 Gigabit Frame Data Tab

Figure:Frame Data for 10 Gigabit Modules



NOTE Some 10 Gigabit Ethernet modules do not have an UDF 5 sub-tab.

Frame Data

The labeled boxes within the *Frame Data* tab control the formation of frames. The division of functionality is described below.

Controls Related to General Structure

- Preamble:
  - *Preamble Size Box*—for 10/100, 10/100 TXS8, and Gigabit. Controls the size of the preamble, including the SFD.
  - The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see Ixia Platform Reference Manual. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count value displayed in the field includes the SFD.—for 10 Gigabit modules. Displays the size and content of the preamble.
- *Frame Size*—controls the size of frames, not including the preamble and SFD.
- *Port Properties button*—opens the *Port Properties* dialog which controls a number of basic port parameters. See the following chapters for more information on the *Port Properties* dialog:
  - Chapter 18,*Port Properties — 10/100/1000 Ethernet Family*
  - Chapter 19,*Port Properties–POS and ATM Families*
  - Chapter 20,*Port Properties–10 GE and UNIPHY Families*

Packet Contents

The packet contents are controlled by the various property sheets and dialog boxes. The list below corresponds to the order of placement of data within a packet:

- *DA/SA Property Sheet—configures Destination and Source MAC addresses.*
- Protocols Section (as described in Chapter 6,Frame Data–Protocol Control)—protocol headers formatted for both data link and network/
transport layers, including the IP and IPX protocols.
- *Data Pattern Box—determines data values which may cover the remainder of the frame.*
- The User Defined Fields (as described in Chapter 7,Frame Data–User Defined Fields (UDF))—programming of configurable 32-bit counters.
- *Instrumentation Box—insertion of a timestamp, packet group signature, sequence signature, and data integrity signature.*
- *Force Errors Box—control over the CRC in the Frame Check Sequence field at the end of each frame, as well as the creation of alignment and dribble bit errors.*

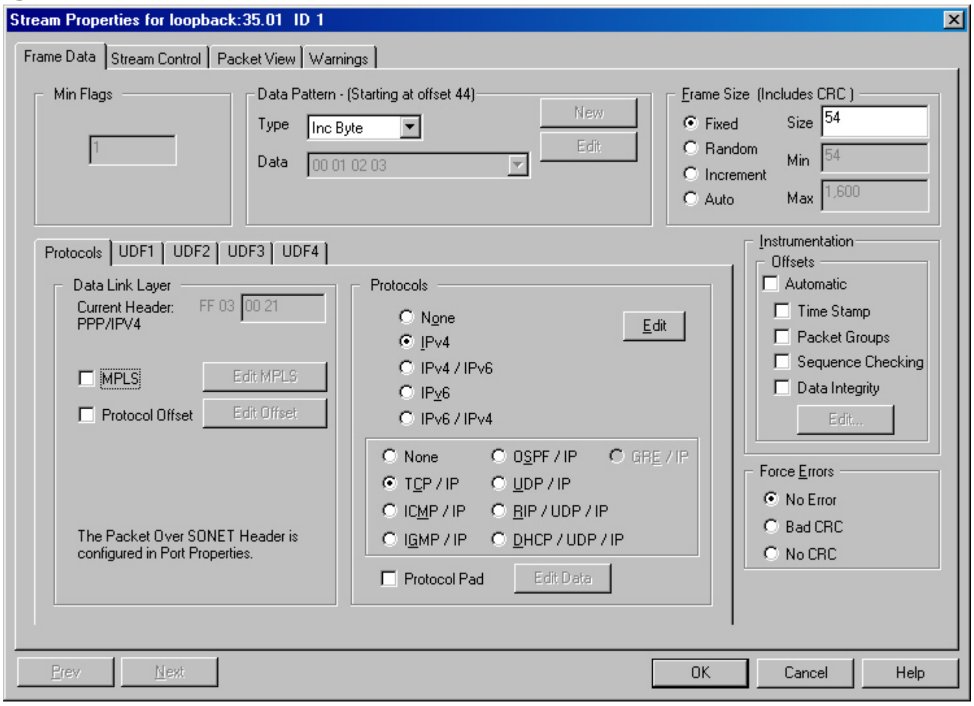
Each tab is shown separately, along with a description of its usage.

Frame Data for SONET/POS Modules

The *Frame Data* tab for Packet over SONET Modules is shown in Figure: Frame Data for Packet over SONET Modules—Overview.

NOTE For POS 622 (OC-12c/OC-3c POS) see *POS 622 Frame Data*.

Figure:Frame Data for Packet over SONET Modules—Overview



NOTE Some modules also have Table and UDF 5 sub-tabs (that is, 10GE MSM) when in WAN or OC-192c Transmit mode.

The labeled boxes within the tab control the formation of frames. The division of functionality is:

Controls Related to General Structure

- *Min Flags Box*—controls the minimum number of empty 'flag' frames sent between good POS packets.
- *Frame Size—controls the size of frames.*
- *Port Properties*—press the *Port Properties* button to display the set of *Port Properties* dialogs, which control a number of basic port parameters for the currently selected load module. See the following chapters for more information:
  - Chapter 18,Port Properties — *10/100/1000 Ethernet Family*
  - Chapter 19,Port Properties–*POS and ATM Families*
  - Chapter 20,Port Properties–*10 GE and UNIPHY Families*

Packet Contents

The packet contents are controlled by the various property sheets and dialog boxes. The list below corresponds to the order of placement of data within a packet:

- *DA/SA Property Sheet—configures Destination and Source MAC addresses.*
- Protocols Section (as described in Chapter 6,Frame Data–Protocol Control)—protocol headers formatted for both data link and network/ transport layers, including the IP and IPX protocols.
- *Data Pattern Box—determines data values which may cover the remainder of the frame.*
- The User Defined Fields (as described in Chapter 7,Frame Data–User Defined Fields (UDF))—programming of configurable 32-bit counters.
- *Instrumentation Box—insertion of a timestamp, packet group signature, sequence signature, and data integrity signature.*
- *Force Errors Box—control over the CRC in the Frame Check Sequence field at the end of each frame, as well as the creation of alignment and dribble bit errors.*

Frame Data Sections

Each section of the *Frame Data* tab is shown separately below, along with a description of its usage:

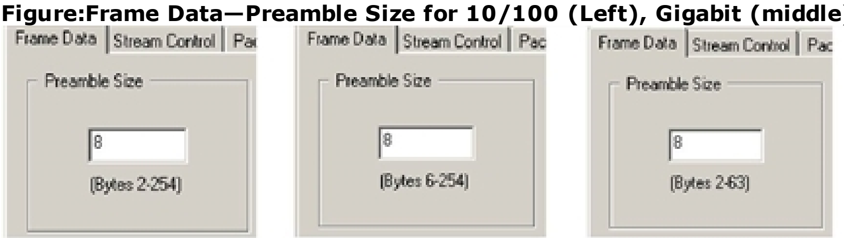
- *Preamble Size Box*
- *The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see Ixia Platform Reference Manual. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count value displayed in the field includes the SFD.*
- *Min Flags Box*
- *Frame Size*
- *DA/SA Property Sheet*
- *Data Pattern Box*
- Protocols section, as described in Chapter 6,Frame Data–Protocol Control

- User Defined Fields, as described in Chapter 7,Frame Data–User Defined Fields (UDF)
- *Instrumentation Box*
- *Force Errors Box*

Preamble Size Box

The Preamble Size box is shown in *Figure:Frame Data—Preamble Size for 10/100 (Left), Gigabit (middle), and 10/100 TXS8 (right)*.

Figure:Frame Data—Preamble Size for 10/100 (Left), Gigabit (middle), and 10/100 TXS8 (right)



The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see *Ixia Platform Reference Manual*. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count value displayed in the field **includes** the SFD.

Preamble Data Box for 10 Gigabit Modules

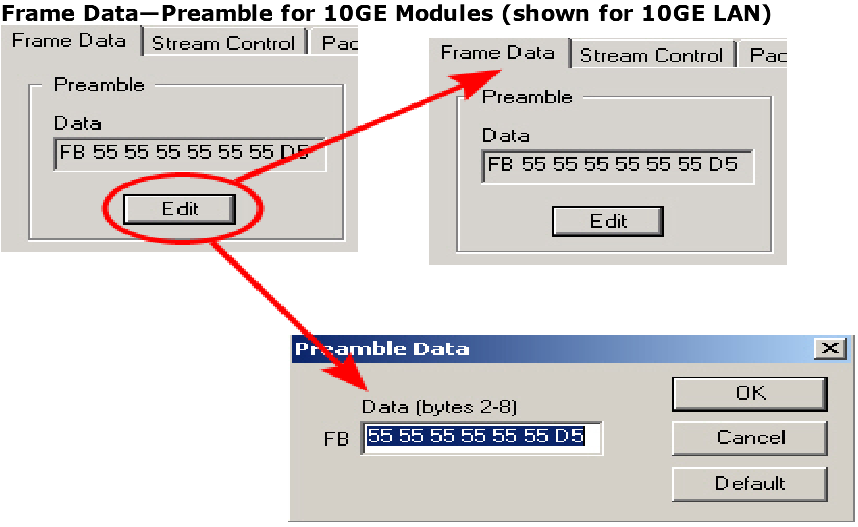
The Preamble Data box for 10 Gigabit Modules contains a read-only field displaying the 8 bytes in the preamble of the 10 Gigabit Ethernet frame. This field reflects the setting that is made in the *Preamble Data* dialog. The length of the preamble for 10 Gigabit modules is fixed at 8 bytes, but some of the bytes can be configured by you. The number of configurable bytes in the dialog depends on the setting for the Transmit start-of-frame detection mode in the *Preamble* tab of the *Port Properties* dialog.

SFD and Byte Count Modes

For SFD Detect Mode, Bytes 2 through 7 are configurable. For Byte Count Mode, Bytes 2 through 8 are configurable.

10GE LAN, 10GE XAUI, 10GE XENPAK, 10GE LSM, 10GE MSM, and 10GE WAN modules support both modes. See *10GE Port Properties-Preamble* for additional information. Also see *10GE Port Properties-Preamble* for additional information. The default values are displayed in the screen captures below. To return to these default values, press the *Default* button.

Frame Data—Preamble for 10GE Modules (shown for 10GE LAN)



Preamble Data Box for 40/100 GE Modules

The Preamble Data box for 40/100 Gigabit Modules contains a read-only field displaying the 8 bytes in the preamble of the 40/100 Gigabit Ethernet frame. This field reflects the setting that is made in the Preamble Data dialog. The length of the preamble for 40/100 Gigabit modules is fixed at 8 bytes, but some of the bytes can be configured only. You can configure Data from (2-8) bytes in the Preamble Data dialog.

Byte Count Modes

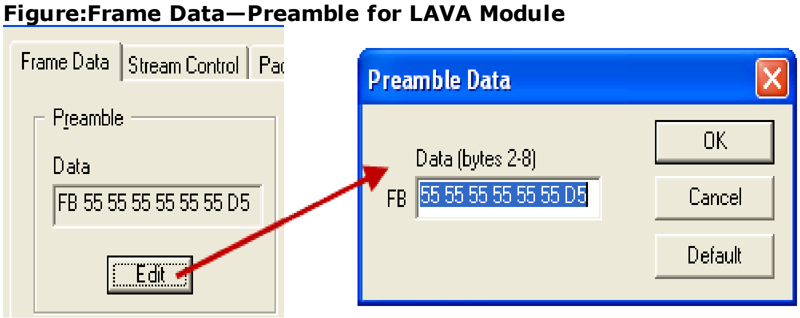
For Byte Count Mode, Bytes 2 through 8 are configurable. 40/100 GE supports this mode. *10GE Port Properties–Preamble* for additional information.

The Preamble box and the Preamble Data dialog are shown in Figure 5-8. The default values are displayed in the screen captures below. To return to these default values, press the Default button.

Lava AP40/100 GE— Preamble

The Lava AP40/100 GE Preamble tab allows you to select the option so that you can view Preamble in Packet View. The preamble precedes the frame, but is not part of the frame itself. The Preamble dialog box of Lava AP40/100 GE module is shown in the following figure:

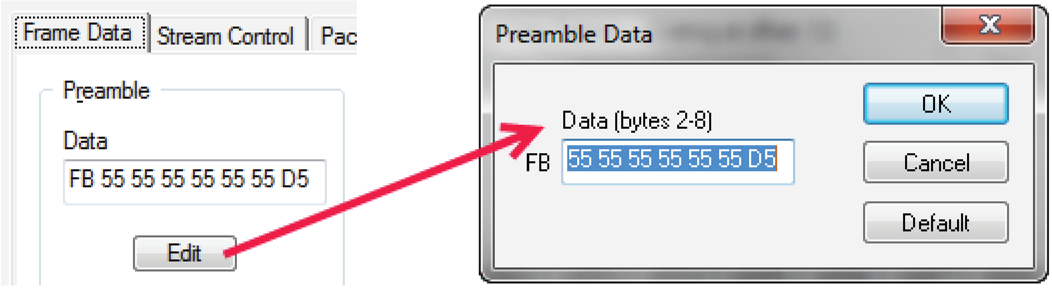
Figure:Frame Data—Preamble for LAVA Module



Xcellon-Multis— Preamble

The Xcellon-Multis Preamble tab allows you to select the option so that you can view Preamble in Packet View. The preamble precedes the frame, but is not part of the frame itself. The Preamble dialog box of Xcellon-Multis module is shown in the following figure:

Frame Data—Preamble for Xcellon-Multis Module



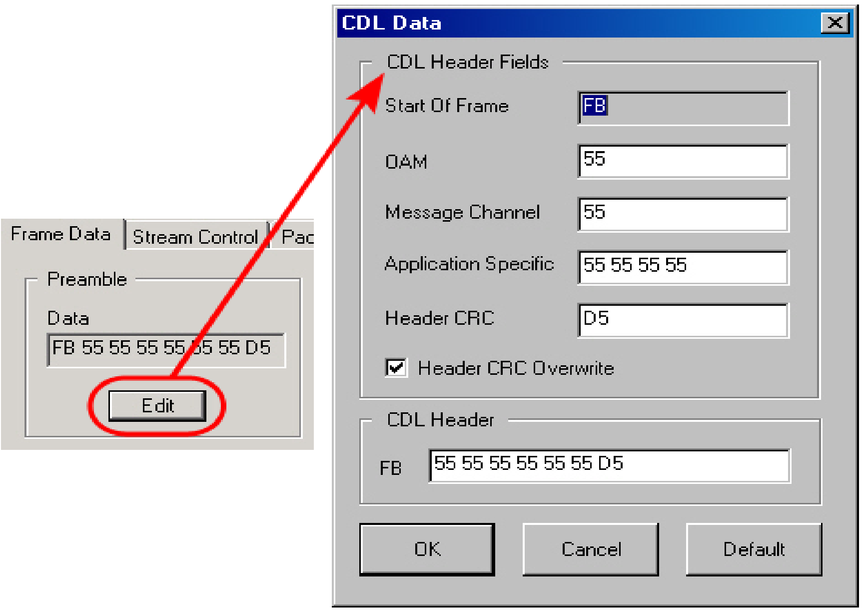
Cisco CDL Preamble Mode

10GE LAN, 10GE XAUI, 10GE XENPAK, 10GE WAN, and 10GE WAN UNIPHY modules all support the Cisco CDL preamble format.

Figure:Frame Data—Preamble for Cisco CDL shows the *CDL Data* dialog box. This dialog box is enabled by selecting the *Cisco CDL* check box on the *Preamble* tab of the *Port Properties* dialog, as described in *Port Properties for 10 Gigabit Modules*.

The default values are displayed in the screen capture below. To return to these default values, press the *Default* button. Bytes 1 through 6 are configurable. Byte 7 (the Header CRC) is also configurable but is not considered part of the CDL Data.

Figure:Frame Data—Preamble for Cisco CDL



The configurable CDL fields are discussed in *Table:CDL Configurable Fields*.

Table:CDL Configurable Fields

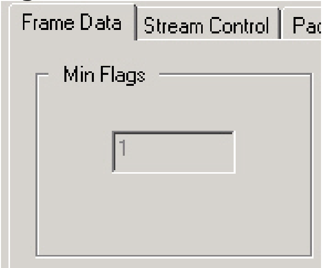
Section	Field/Control	Description
CDL Header	Start of Frame	Signifies the start of the CDL frame. This field is not

Section	Field/Control	Description
Fields		configurable.
	OAM	One byte, in Hex, specifying the Operation, Administration, and Maintenance field.
	Message Channel	One byte, in Hex, specifying the message channel.
	Application Specific	Four bytes, in Hex, specifying the application specific data.
	Header CRC	The Cyclical Redundancy Check checksum for the CDL header. This field is only configurable if the *Header CRC Overwrite* button is selected.
	Header CRC Overwrite	Allows the use to overwrite the calculated CRC.
CDL Header		This field shows the combination of all the CDL fields, modified as described above.

Min Flags Box

The *Min Flags* field is shown in *Figure:Frame Data—Min Flags for POS Modules*.

Figure:Frame Data—Min Flags for POS Modules

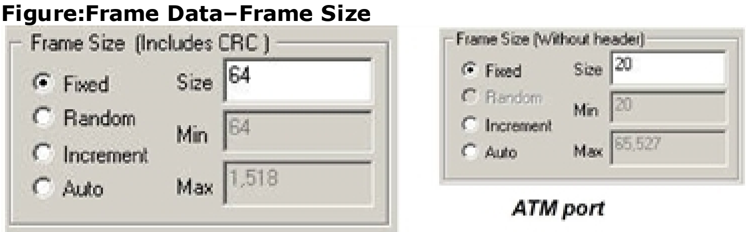


This section is read-only at the current time, and reflects the fact that at least one empty 'flag' frame is sent between transmitted SONET frames.

Frame Size

The Frame Size section is shown in *Figure:Frame Data–Frame Size*.

Figure:Frame Data–Frame Size



Four basic options are available to set the size of frames. The frame size ranges for different port types varies. The size includes everything following the SFD, through the FCS field. The frame size may be one of the following types. (See **Note** below for maximum frame size on OC-12c ports.)

- **Fixed**—sets all frames to a constant size, specified in bytes in the *Size* field.

NOTE For ATM ports, the default setting for *Fixed* frame size is 20 bytes. Frame sizes for ATM less than 43 bytes do not run at the full line rate.

- **Random**—sets frames to have random sizes, varying between the specified *Min* and *Max* lengths, in bytes. For information on the 'Weighted Random Frame Size' feature, *Weighted Random Frame Size*.
- **Increment**—sets frames to have a set of incrementing sizes, between the specified *Min* and *Max* lengths, in bytes. The typical increment is 1 byte. For some load modules, a user-defined increment step can be configured. *Frame Size User-Defined Increment Step* for additional information.
  For some load modules, IxOS supports packets per burst setting in incrementing frame size mode. *Using the Packet/Burst Setting in Incrementing Frame Size Mode* for additional information.
- **Auto**—sets the frame size to the minimum required for the protocols selected, data fields, and UDFs selected.

The Random and Increment settings are not enabled for settings of *IPX* selections in the *Protocols* box. Since the range of frame sizes varies between cards, refer to *Ixia Platform Reference Manual*.

NOTE For **OC-48c POS, OC-192c POS,** and **10GE** modules, only one stream of incrementing frame size can be created per group of streams.

Overall, up to 254 non-incrementing frame size streams, plus one incrementing frame size stream, may be configured concurrently for a port on one of these modules.

This does not apply to newer load modules in the LSM and MSM series, which support 256 incrementing streams.

NOTE For **OC-12c POS** ports:

1) When any type of Data Pattern other than 'Fixed' is selected in the Data Pattern box, the maximum allowable Frame Size is 15,257 bytes for older POS modules. For the POS 622, the maximum frame size is 65,535 bytes.

2) The minimum frame size for POS 622 is 12 bytes. For older POS modules (OC12 POS card), the minimum frame size is 34 bytes.

2) For **asynchronous** streams:

With a PPP header, but without PPP negotiation enabled, the maximum frame size is 1508 bytes (with CRC-32) or 1506 bytes (with CRC-16).

With a PPP header, and with PPP negotiation enabled, the maximum frame size is 3200 bytes or PPP-negotiated MTU, whichever is less.

With a Cisco HDLC header, the maximum frame size is 3,200 bytes.

NOTE With a Frame Relay header, the maximum frame size is 1,500 bytes.

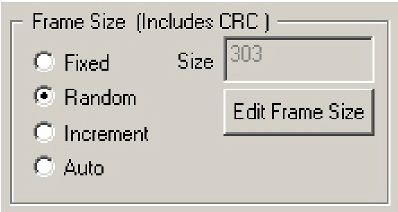
NOTE For **ATM** ports:
Each ATM Stream Queue can have maximum 16 streams of Incremented Frame Sizes; other streams are forced to Fixed Frame Size.

When using Incremented Frame Size with ATM ports with IP/TCP/UDP, the checksums are inaccurate. A warning message to this effect alerts you when Increment Frame Size is selected.

Weighted Random Frame Size

The Weighted Random Frame Size feature is accessed by first selecting the *Random* frame size option, as shown in *Figure:Weighted Random Frame Size—Uniform Distribution*. Clicking the *Edit Frame Size* button displays the *Weighted Random Frame Size* dialog.

Figure: Accessing Weighted Random Frame Size



This feature is used to configure different possible modes of generating random frame sizes for a particular stream. The *Weighted Random Frame Size* dialog lists the four available Random Modes. Each of the different Random Modes displays a different dialog format, as described in the following sections:

- *Weighted Random Frame Size—Uniform Distribution*
- *Weighted Random Frame Size—Weight Pairs*
- *Weighted Random Frame Size—Predefined Distributions*
- *Weighted Random Frame Size—Quad Gaussian*

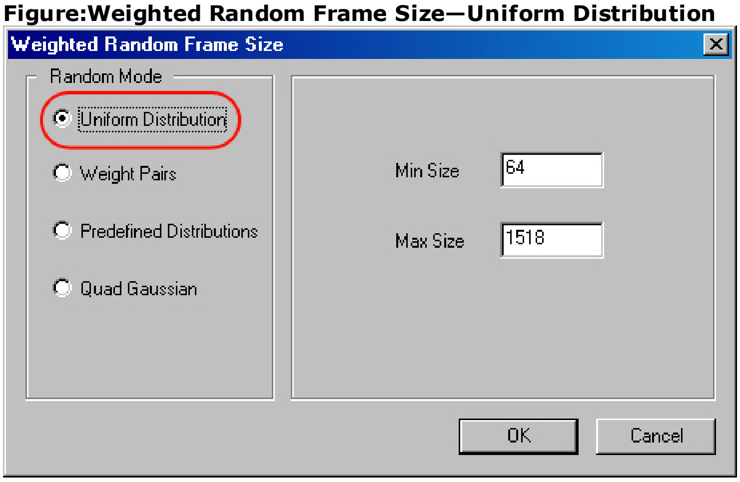
For the middle two types (Weight Pairs and Predefined Distribution), the weights for all of the frame sizes are added up. Each frame size is then given a proportion of the total number of frames, as dictated by its weight value. For example, one of the pre-programmed distributions is (64:7, 594:4, 1518:1). In this case, the total of the weights is 12 (7+4+1). Frames are randomly generated such that 64-byte frames are 7/12 of the total, 594-byte frames are 4/12 of the total, and 1518-byte frames are 1/12 of the total.

NOTE Code uses uniform distribution and relies on it being uniform. However, as with any other probability distribution, the sample distribution is close to theoretical only if the size of the sample is large. So what is described herein is approximate weight distribution—the approximation is better with bigger sample size (that is, larger number of frames). When the number of frames is very low (less than 100) the transmitted frames may not come close to the ratio described herein.

Weighted Random Frame Size—Uniform Distribution

The Uniform Distribution Random Mode version of the dialog box is shown in *Figure:Weighted Random Frame Size—Uniform Distribution*. This is identical to the standard implementation of the random frame size feature. A uniform set of random values between a minimum and a maximum value are generated. The minimum and maximum frame size values are defined by you.

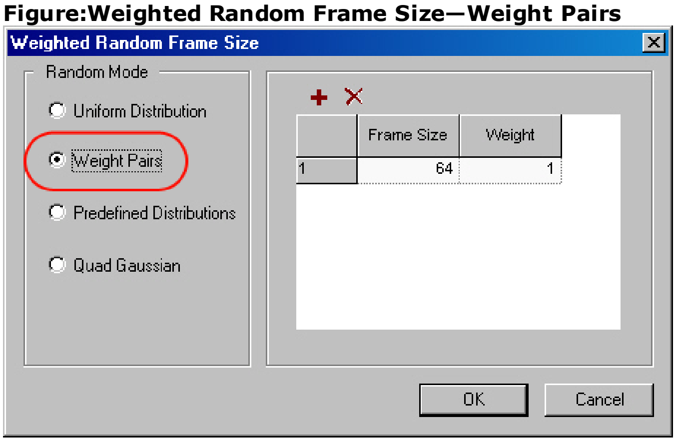
Figure:Weighted Random Frame Size—Uniform Distribution



Weighted Random Frame Size—Weight Pairs

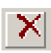
The Weight Pairs Random Mode version of the dialog is shown in *Figure:Weighted Random Frame Size—Weight Pairs*. This dialog allows to custom-program a distribution for a stream. Frame sizes may be any value valid for the port. Weights may be any value, such that the total of all of the weights is less than 2,048.

Figure:Weighted Random Frame Size—Weight Pairs



The fields and controls in this dialog are described in *Table:Weighted Random Frame Size—Weight Pairs*.

Table:Weighted Random Frame Size—Weight Pairs

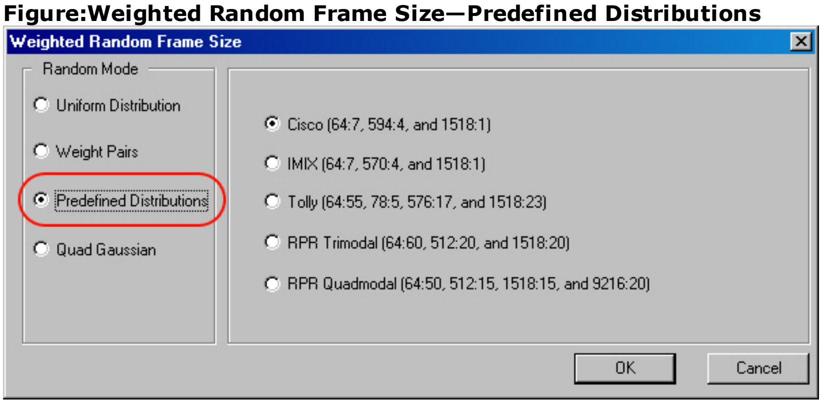
Section	Field/Control	Description
(Header)		Click to add a Weight Pair to the table below.
		Click to delete the selected Weight Pair from the table below.

Section	Field/Control	Description
(Table)	Frame Size	(in bytes) The size of the frame for this Weight Pair.
	Weight	A user-defined, 32-bit integer (weight) assigned to the corresponding frame size in this Weight Pair.

Weighted Random Frame Size—Predefined Distributions

The Predefined Distributions Random Mode version of the dialog is shown in *Figure:Weighted Random Frame Size—Predefined Distributions*. The right pane of the dialog lists the available types of pre-programmed distributions, corresponding to standard traffic models found in various applications.

Figure:Weighted Random Frame Size—Predefined Distributions



The selections available in this version of the dialog are described in *Table:Weighted Random Frame Size—Predefined Distributions*.

Table:Weighted Random Frame Size—Predefined Distributions

Predefined Distribution	Description
Cisco	A pre-programmed distribution, according to Cisco standards: 64:7, 594:4, and 1518:1.
IMIX	A pre-programmed distribution, according to IMIX standards: 64:7, 570:4, and 1518:1.
Tolly	A pre-programmed distribution, according to Tolly testing group standards: 64:55, 78:5, 576:17, and 1518:23.
RPR Trimodal	A pre-programmed distribution: 64:60, 512:20,and 1518:20.
RPR Quadmodal	A pre-programmed distribution: 64:50, 512:15, 1518:15, and 9216:20.

Support for IMIX on Xdensity card

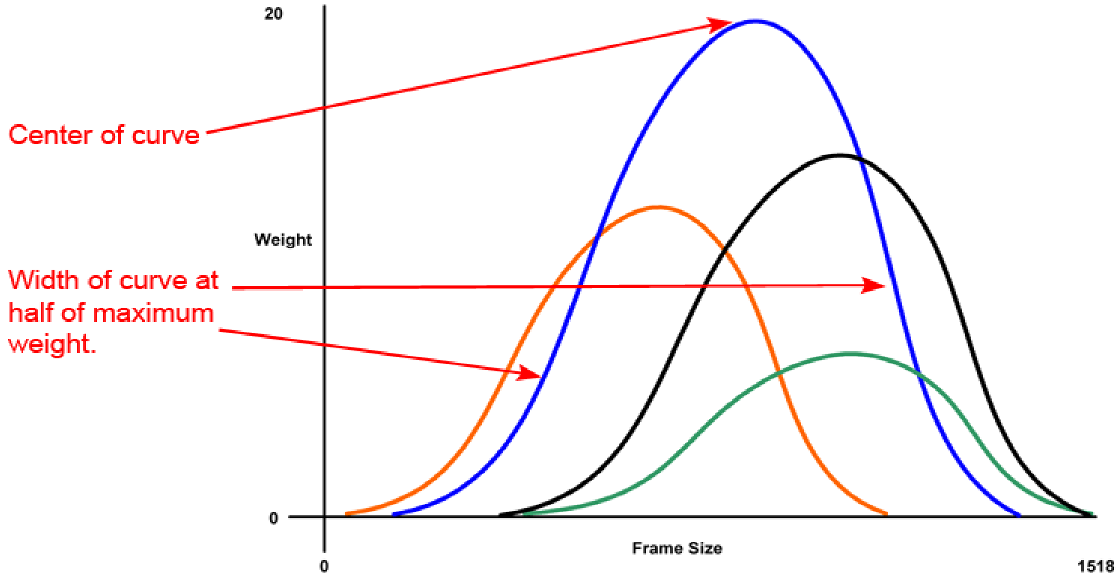
Only predefined distributions are supported in Xdensity card. These include 5 varieties (mentioned in the above table) which are supported on existing load modules. Weighted Pairs and Quad Distribution is not supported. This feature is supported for normal and data center mode.

Weighted Random Frame Size—Quad Gaussian

Quad Gaussian is the superposition of four gaussian distributions. You can specify the center (or mean), width of half maximum, and weight of each gaussian distribution. The distribution is then normalized to a single distribution and generates the random numbers according to the normalized distribution.

The graph in *Figure:Quad Gaussian Distribution* demonstrates how Quad Gaussian Weighted Random Frame Size works.

Figure:Quad Gaussian Distribution

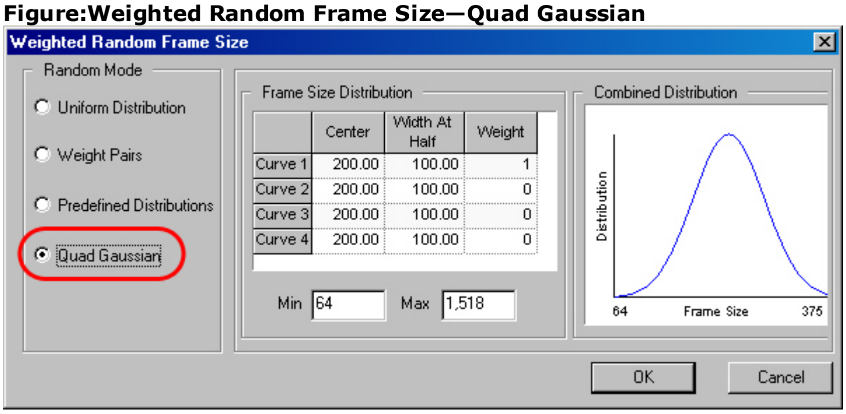


The graphic above shows four Gaussian distributions, reflected as weight over frame size. The frame size represented at the top of the curve is the frame size most likely to be transmitted, while the frame sizes at the beginning and end of each curve are the least likely to be transmitted.

The four curves are combined into a single distribution by the port. It is not necessary to use all four curves; one, two, or three curves can be generated as well as four.

The dialog in *Figure:Weighted Random Frame Size—Quad Gaussian* displays the configuration options for Quad Gaussian Weighted Random Frame Size.

Figure:Weighted Random Frame Size—Quad Gaussian



The Quad Gaussian Configuration controls are discussed in *Table:Quad Gaussian Configuration Controls*

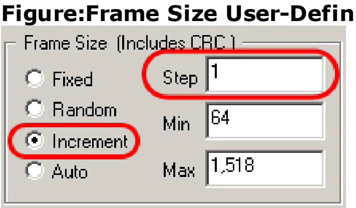
Table:Quad Gaussian Configuration Controls

Frame Size Min	The minimum frame size in bytes.
Frame Size Max	The maximum frame size in bytes.
Curve	The number of one of four curves that are amalgamated into a single distribution.
Center	The frame size for the center of the distribution curve.
Width at Half Max	The width of the distribution curve at half of the curve weight, exclicked as the difference between the minimum and maximum frame size in bytes.
Weight	The priority to give the distribution curve. The four weights are normalized into a ratio.

Frame Size User-Defined Increment Step

The user-defined increment step for frame sizes is shown in *Figure:Frame Size User-Defined Increment Step*.

Figure:Frame Size User-Defined Increment Step



When this option is selected, the frame size increases by the selected step size, beginning with the minimum set size and ending with the maximum set frame size.

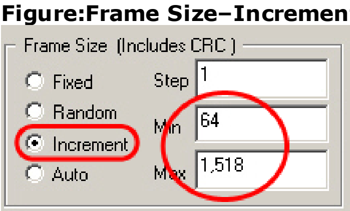
Using the Packet/Burst Setting in Incrementing Frame Size Mode

IxOS supports packets per burst setting in incrementing frame size mode for the following load modules in Packet Stream mode (and in Advanced Scheduler mode, where applicable):

- LM1000TX4, TXS4, STX4/24, STXS2/4/24, SFP4 and SFPS4
- LSM1000XMV family
- LSM10G1
- LSM10GXM2/4/8 family
- ASM1000XMV12X

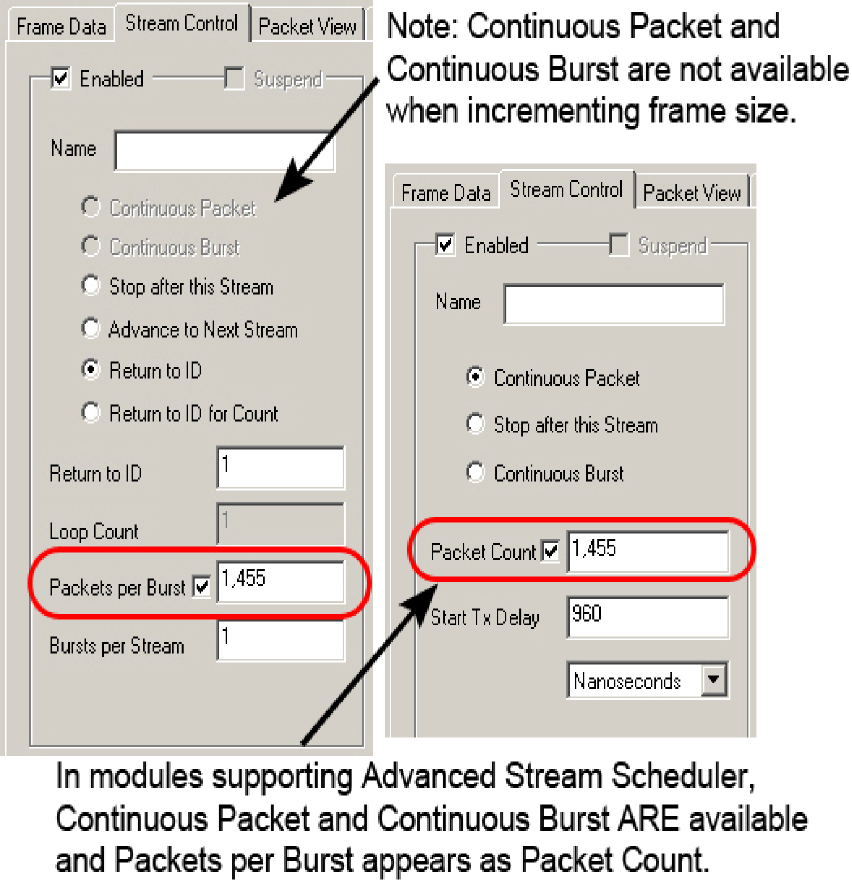
To configure this, in the *Stream Properties* screen, *Frame Data* tab, under *Frame Size*, select **Increment** and enter a **Min** and **Max** as shown in *Figure:Frame Size–Increment*.

Figure:Frame Size–Increment



Then on the *Stream Control* tab, at the *Packets per Burst* field, a check box appears. Select the check box and enter a *Packets per Burst* value.*Figure:Stream Control–Packets per Burst* shows this.

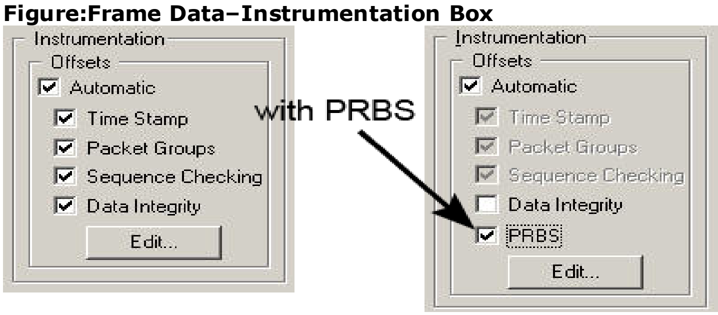
Figure:Stream Control–Packets per Burst



Instrumentation Box

The *Instrumentation* feature is used in defining specialized fields within the packet to be transmitted. The data within these fields can then be processed at the receiving end, to determine sequence of arrival, latency, and the condition (data integrity) of the packets. Packet groups, sequence signature, data integrity checking, and PRBS may not be available with all modules. The Instrumentation Box on the *Frame Data* tab is shown in *Figure:Frame Data–Instrumentation Box*.

Figure:Frame Data–Instrumentation Box



The fields of the Frame Data Instrumentation Offsets box are described in *Table:Instrumentation Offsets Box Contents*.

Table:Instrumentation Offsets Box Contents

Field	Usage
Automatic	If selected, sets the other offset options to the required configuration for auto-detect instrumentation streams.

Field	Usage
	You can clear any combination of the four options, or all of the four options, and the Automatic option can still be enabled. Click the *Edit* button to configure the parameters, as shown in *Edit Instrumentation Options—Signature Placement*. *Automatic Instrumentation Signature* for more information (for Auto Detect option of the Receive mode).
Time Stamp	(Not available for DCC Packet Flows.) If selected, indicates that the 6 bytes before the FCS should hold a 48-bit timestamp. This timestamp contains a 20ns resolution time value from the start of the data transmission.
Packet Groups	If selected, timestamp is also implied and the timestamp option is selected automatically. If selected, this indicates that transmitted packets includes a packet group signature and packet group ID. Press the *Edit* button to configure the parameters, as shown in *Edit Instrumentation Options—Packet Groups/Sequence Checking*.
Sequence Checking	If selected, sequence numbers are inserted in each outbound packet. Press the *Edit* button to configure the parameters, as shown in *Edit Instrumentation Options—Packet Groups/Sequence Checking*.
Data Integrity	If selected, Data Integrity values are inserted for each outbound packet. Click the *Edit* button to configure the parameters, as shown in *Edit Instrumentation Options—Data Integrity*. If PRBS is enabled, Data Integrity is disabled.
PRBS	Refer to *PRBS* for more information. If selected, PRBS is enabled at stream level. If PRBS is enabled at the stream level, then Automatic configuration is enabled by default. If PRBS is enabled, Data Integrity is disabled, and vice-versa.
Edit	Displays the *Edit Instrumentation Options* dialog. This dialog allows the position and values of the signatures and inserted data items to be defined. Refer to *Edit Instrumentation Options—Signature Placement*, *Edit Instrumentation Options—Packet Groups/Sequence Checking*, and *Edit Instrumentation Options—Data Integrity* for more information. NOTE The offsets of the options cannot be changed. The options are either enabled with their default offsets, or not enabled.

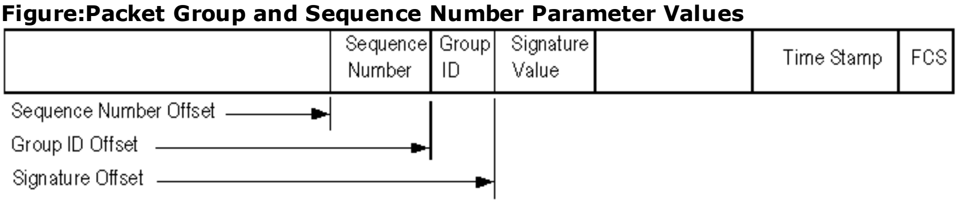
The Instrumentation Box also allows automatically to set the fields for auto-detect instrumentation transmission. *Automatic Offsets*.

The timestamp, packet group signature, and sequence signature fields are related. The position of these fields within a packet is shown in *Figure:Packet Group and Sequence Number Parameter Values*. A single signature offset and value is shared by the packet group ID and the sequence number. The group ID and sequence number each have individual offsets and values. The signature value must occur at a 4-byte boundary, and the packet group ID must occur at a 2-byte boundary.

NOTE The Instrumentation Box should not be used to insert a timestamp and group ID in the packet when the 'No CRC' option is selected in the force errors box. It overrides any CRC set by other means and almost always results in a packet with a faulty CRC value.

Refer to the Packet Group Operation and Sequence Checking Operation sections in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

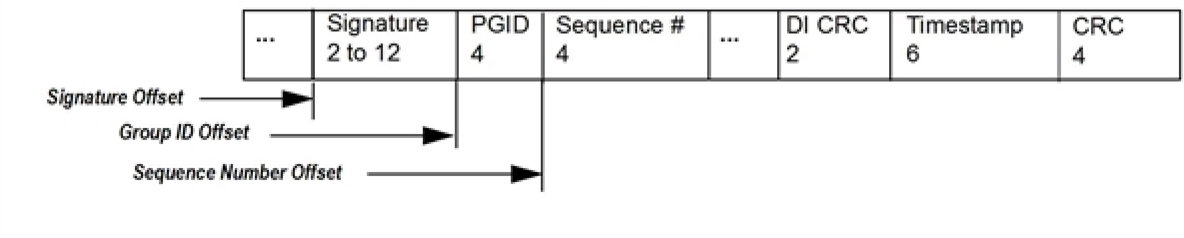
Figure:Packet Group and Sequence Number Parameter Values



Automatic Offsets

If Automatic Offsets is enabled in Frame Data tab, Packet View have the enabled options with their default offsets as specified in *Figure:Default Offsets and Field Sizes*. Either an option is there in that order/offset, or it is not there.

Figure:Default Offsets and Field Sizes



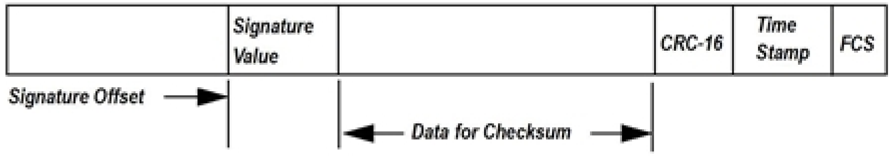
In the case of auto frame size packets, if both Packet Group and Sequence Checking are disabled, and if the frame size limit is so small that it causes DI CRC to immediately follow the Signature, then four bytes of background are padded. In this way, the payload for DI CRC calculation is not empty.

NOTE If Automatic offsets are enabled, the offsets of the options cannot be changed. The options are either enabled with their default offsets, or not enabled.

Data Integrity

A separate Signature value is used for Data Integrity, as shown in *Figure:Data Integrity Parameter Values*. Refer to the Data Integrity Checking Operation section of the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

Figure:Data Integrity Parameter Values



PRBS

If PRBS is enabled at the stream level, then Automatic configuration is enabled by default, as shown in *Figure:Frame Data–Instrumentation Box*. For detailed information, including a description of the packet format when PRBS is enabled,*PRBS Mode* (Packet Group Statistics View) and *PRBS Mode* (Receive Mode).

> **NOTE** In order for latency and sequence checking statistics to be active and accurate, it is necessary to create a latency/sequence checking view, as described in Chapter 16, *Packet Group Statistic View*.

Edit Instrumentation Options—Signature Placement

The Automatic Instrumentation Signature option allows the transmit port to place a signature at a variable offset from the start of frames. The instrumentation block supports Sequence Checking, Timestamp, Data Integrity functionality, with signature and Packet Group ID (when Automatic Offsets is enabled, these transmit port options are enabled as well).

For more information on Automatic Instrumentation Signature, *Automatic Instrumentation Signature* of Chapter 13, *Filter Properties*.

Figure:Signature Placement

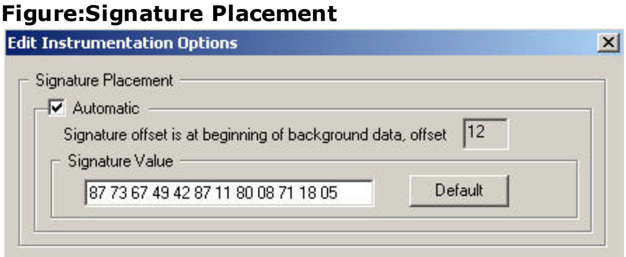


Table:Signature Placement Configuration describes the configuration options for Signature Placement.

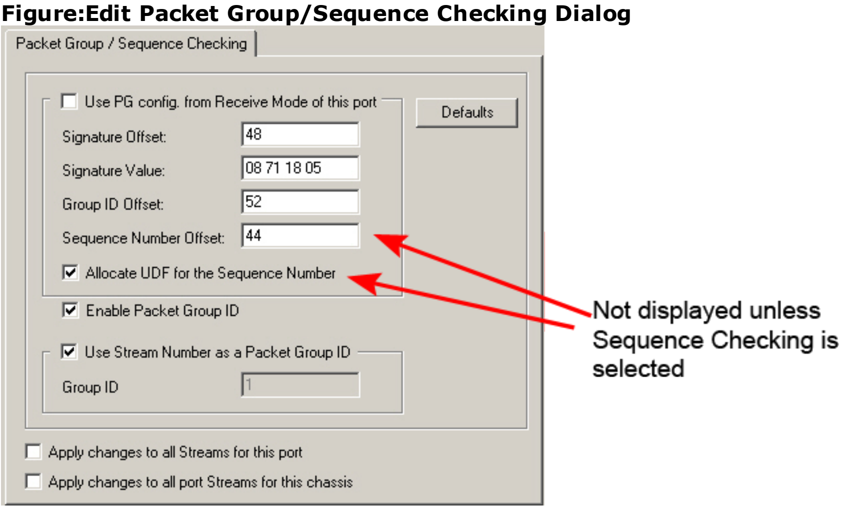
Table:Signature Placement Configuration

Control/Field	Description
Signature offset is at beginning of background data, offset	Where auto detect puts the signature in the packet for the instrumentation signature.
Signature Value	The data signature that is being matched. Editable field; minimum length 2 bytes, maximum length 12 bytes. When numbers are entered, zeroes (0) are padded to the left to make the number of bytes even, if needed.
Default	Resets the default signature block value.

Edit Instrumentation Options—Packet Groups/Sequence Checking

Since the packet group signature and sequence signature options use common values for signature offset, signature value, and group ID offset, one common dialog is displayed for editing both packet group and sequence signature options. The dialog with both options selected (but with Automatic deselected) is shown in *Figure:Edit Packet Group/Sequence Checking Dialog.* Minor differences are present when only one of the options is selected, and these differences are described in the figure.

Figure:Edit Packet Group/Sequence Checking Dialog



The fields in this dialog are described in *Table:Edit Packet Group/Sequence Checking Dialog*.

Table:Edit Packet Group/Sequence Checking Dialog

Field	Usage
Defaults	Click this button to restore the default settings for this dialog: • Use PG config from Receive Mode of this port is cleared (disabled), and default numerical values are displayed. • Use Stream Number as a Packet Group ID is selected (enabled).
Use PG Config from Receive Mode of this port	If selected, the signature offset, signature value, and (packet) group ID are copied from the values configured for Receive Mode.
Signature Offset	The offset from the beginning of the packet to the start of the signature value field.
Signature Value	The 4-byte value to use as a signature value. Any value may be chosen, but it should be something unlikely to appear in 'normal' data, so it can be easily recognized in the captured data.
Group ID Offset	The offset from the beginning of the packet to the start of the (packet) group ID field.
Sequence Number Offset	The offset from the beginning of the packet to the start of the embedded sequence number field.

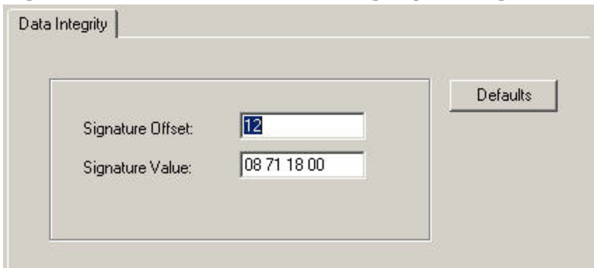
Field	Usage
Allocate UDF for the Sequence Number	Automatically assigns one of the user-defined fields to be used as the sequence number field. If Sequence Checking is enabled, this option is forced to be enabled, but greyed out. If Sequence Checking is disabled, the option is not displayed.
Use Stream Number as Packet Group ID	If selected, uses the ID number of the stream currently being configured as the packet group ID.
Group ID Value	If the check box above (for using stream number) is not selected, the value entered in this field is inserted into all transmitted packets for this stream, to be used as a packet group ID.
Apply changes to all Streams for this port	If selected, the values from this dialog are copied to all other streams for this port.
Apply changes to all port Streams for this chassis	If selected, the values from this dialog are copied to all streams for all ports on the current chassis.

NOTE In order for latency and sequence checking statistics to be active and accurate, it is necessary to create a latency/sequence checking view, as described in Chapter 16,*Packet Group Statistic View*.

Edit Instrumentation Options—Data Integrity

If Data Integrity Signature is selected in the Insert box, clicking **Edit** in the Insert box displays the **Data Integrity** dialog, as shown in *Figure:Edit Transmit Data Integrity Dialog*.

Figure:Edit Transmit Data Integrity Dialog



The fields in this dialog are described in *Table:Edit Transmit Data Integrity Dialog Fields*.

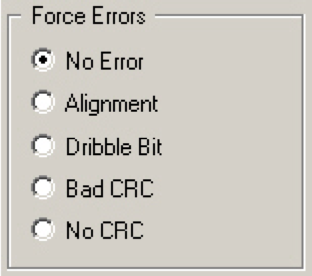
Table:Edit Transmit Data Integrity Dialog Fields

Field	Description
Defaults	Restores the default settings for this dialog.
Signature Offset	The offset from the beginning of the packet to the start of the data integrity signature value field.
Signature Value	The 4-byte value to use as a signature value. Any value may be chosen, but it should be something unlikely to appear in ‘normal’ data so it is easily recognized when viewing the captured data.

Force Errors Box

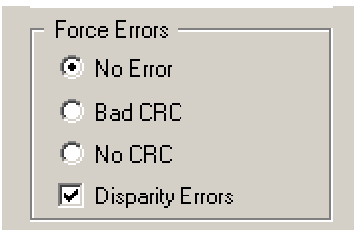
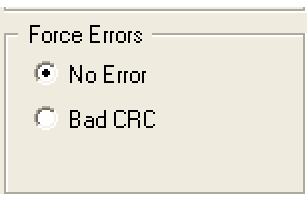
The Force Errors box is shown in *Figure:Frame Data—Force Errors/CRC Control*

Figure:Frame Data—Force Errors/CRC Control



The choices in this box control the inclusion and values of the 4-byte FCS (CRC) field located at the end of the packet's contents, as described in *Table:Force Error Choices*.

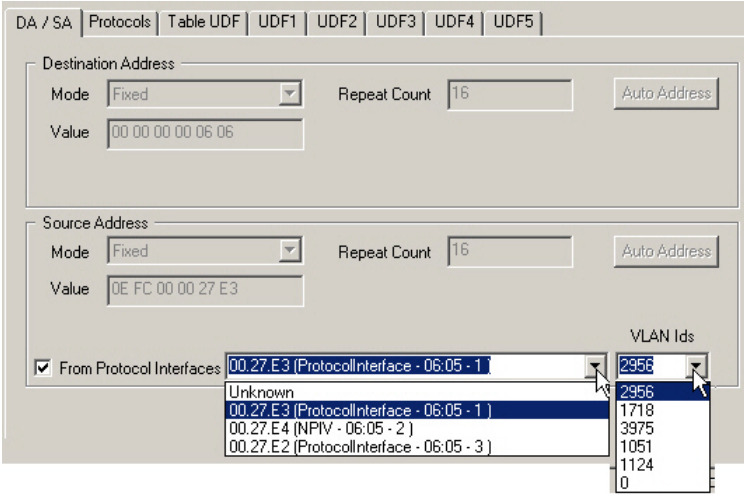
Table:Force Error Choices

Choice	Description
No Error	A correct CRC is placed at the end of the packet.
Alignment	For 10/100 and LM1000T5 cards and only. Four (4) bits are inserted after the end of the FCS. A bad CRC value is inserted.
Dribble Bit	For 10/100 and LM1000T5 cards only. Four extra bits are sent following the FCS. A correct CRC value is calculated and inserted.
Bad CRC	The value of the CRC is changed to force a bad CRC error.
No CRC	No CRC value is inserted. It is up to you to supply a CRC value through the use of the *Data Pattern Box or User Defined Fields, as described in Chapter 7,Frame Data–User Defined Fields (UDF).* NOTE *Instrumentation Box* The Instrumentation Box *should not be used to insert a Time Stamp and group ID in the packet when this option is selected; it overrides any CRC set by other means and almost always results in a packet with a faulty CRC value.*
Disparity Errors	For Fibre Channel Module only.  If selected, disparity errors are injected. Disparity error occurs when hardware wrongly selects 10B code for 8B hex value in the frame. It is 8B10B encoding error and is seen only in 10B encoded data.
Force Errors	For XDM10G32S load module only. 

DA/SA Property Sheet

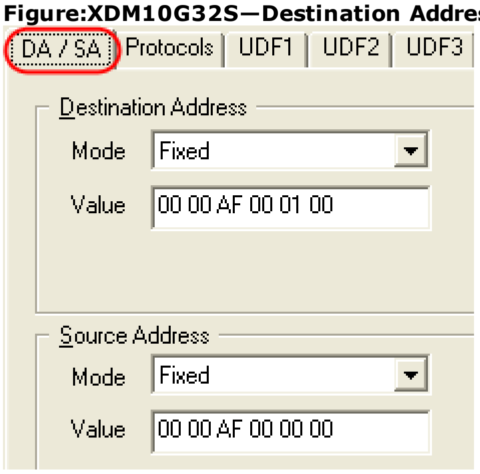
The DA/SA property sheet can be viewed by selecting the *DA/SA* sub-tab in the lower half of the *Frame Data* tab, for non-POS modules. The DA/SA property sheet is shown in the following figure:

Figure:Frame Data—Destination Address/Source Address (DA/SA)



The Fixed DA/SA mode tab supported by XDM10G32S load module is shown in the following figure:

Figure:XDM10G32S—Destination Address/Source Address (DA/SA)



The Destination Address and Source Address generation parameters are identical. A 6-byte MAC address is generated in each case. The Mode setting controls the values associated with the other fields, as described in *Table:DA/SA Mode Values*. The *Mask* field is not shown for the 10/100 TXS8, 10/100/1000 TXS4, or 1000 SFPS4 module, unless *Random* mode is selected.

Address Modes for incrementing or decrementing address values normally use a step size of '1.' For certain load modules, the step size may be specified by you. *DA/SA Address User-Defined Step* for additional information.

Table:DA/SA Mode Values

Mode	Description
Increment	The number of frames indicated by the *Repeat Count* field receive

Mode	Description
	incremented MAC address values, subject to the *Mask* field. The values start with the address indicated in the *Value* field. When the *Repeat Count* is exhausted, the value is reset to the contents of the *Value* field and continues again for the *Repeat Count*. Selecting this option also enables the *Do not reset value at stream load* check box. Selecting this check box means that the value of the increment continues after each new stream is sent.
Continuous Increment	Subsequent frames receive incremented MAC address values, subject to the forced '0' and '1' values set in the *Mask* field. The values start with the address indicated in the *Value* field. Selecting this option also enables the *Do not reset value at stream load* check box. Selecting this check box means that the value of the increment continues after each new stream is sent.
Decrement	The number of frames indicated by the *Repeat Count* field receive decremented MAC address values, subject to the forced '0' and '1' values set in the *Mask* field. The values start with the address indicated in the *Value* field. When the *Repeat Count* is exhausted, the value is reset to the contents of the *Value* field and continue again for the *Repeat Count*. Selecting this option also enables the *Do not reset value at stream load* check box. Selecting this check box means that the value of the decrement continues after each new stream is sent.
Continuous Decrement	Subsequent frames receive decremented MAC address values, subject to the forced '0' and '1' values set in the *Mask* field.The values start with the address indicated in the *Value* field. Selecting this option also enables the *Do not reset value at stream load* check box. Selecting this check box means that the value of the decrement continues after each new stream is sent.
Fixed	The address set in the *Value* field, as masked by the *Mask* field is used for all frames' MAC addresses. Note: XDM10G32S load module supports only Fixed DA/SA mode.
Random	All frames have random MAC addresses, subject to the *Mask* field.
ARP/Discovery	(Available only for Destination Address.) The first destination IP address described in the IP dialog (*Protocols—Network Layer) is ARP'd at the Default Gateway IP Address in the IxRouter dialog, for IPv4. The ARP response, if received, is used as the DA, otherwise, the first MAC address from the ARP table is used.*
CJPAT	The fixed Continuous Jitter Test Pattern (CJPAT), specified in IETF 802.3ae Annex 48A, is supplied. The data field may not be edited.
CRPAT	The fixed Continuous Random Test Pattern (CRPAT), specified in IETF 802.3ae Annex 48A, is supplied. The data field may not be edited.

The *Auto Address* button automatically sets the Mode value to *Fixed*, with a value constructed from the chassis, card, and port number in such a way that pairs of ports on the same card address each other.*Table:Auto Address Assignment* indicates the assigned addresses for an example using a 4-port Ethernet card.

Table:Auto Address Assignment

Port on Card	Destination MAC Address	Source MAC Address
1	00 00 00 00 C1 HH	00 00 00 00 C0 HH
2	00 00 00 00 C0 HH	00 00 00 00 C1 HH
3	00 00 00 00 C3 HH	00 00 00 00 C2 HH
4	00 00 00 00 C2 HH	00 00 00 00 C3 HH

In this table, 'HH' is the chassis number, and 'C' is the card number within the chassis.

The *Mask* field serves to control which address bits may vary and which should stay constant. (The *Mask* field is not present in the *DA/SA* dialog for the 10/100 TXS8 ports.) From the property sheet, individual nibbles (4-bit values) may be controlled. Individual bits of the Mask may be controlled from the *Bit Mask Dialog*. *Table:Mask Values describes the use of Mask values.*

Table:Mask Values

Mask Value	Description
0 through F	The corresponding four bits of the MAC address always contain this value.
X	The corresponding four bits of the MAC address varies according the Mode setting.
?	This indicates that the mask nibble value is a combination of 0's, 1's and X bit values. The *Bit Mask* dialog must be used to view/edit this value.

From Protocol Interfaces Option

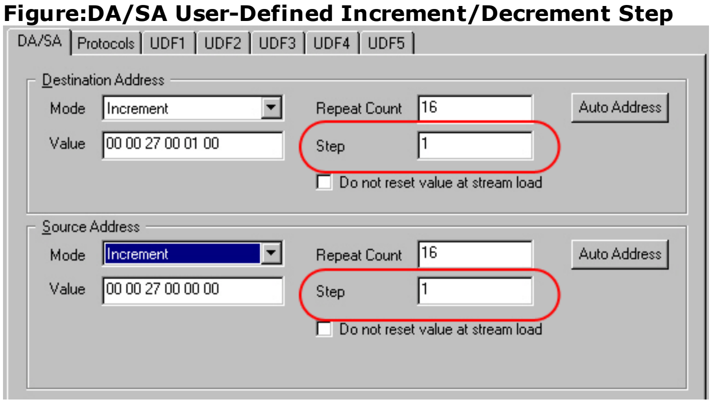
The *From Protocol Interfaces* check box, when selected, deactivates the other controls in the property sheet. A list is shown, listing all currently configured protocol interfaces. Another list, labelled VLAN Ids, allows the selection of all discovered and configured VLAN IDs for this interface if VLAN Discovery is enabled on FCoE Interface. For information on configuring interfaces,Chapter 10,*Protocol Interfaces*.

NOTE The *From Protocol Interfaces* check box only appears if an IP protocol is selected in the *Protocols* sub-tab of the *Frame Data* tab. See the topic in Chapter 6,Protocols—Network Layer for more information.

DA/SA Address User-Defined Step

DA and SA addresses are normally incremented or decremented by '1.' For certain modules, you may define the step size for the following Address Modes: Increment, Continuous Increment, Decrement, and Continuous Decrement. This option is shown for a 10/100 TXS8 module in *Figure:DA/SA User-Defined Increment/Decrement Step*.

Figure:DA/SA User-Defined Increment/Decrement Step



Note the *Do not reset value at stream load* control. When this option is selected, the values for the DA and SA do not get reset when the stream is reloaded.

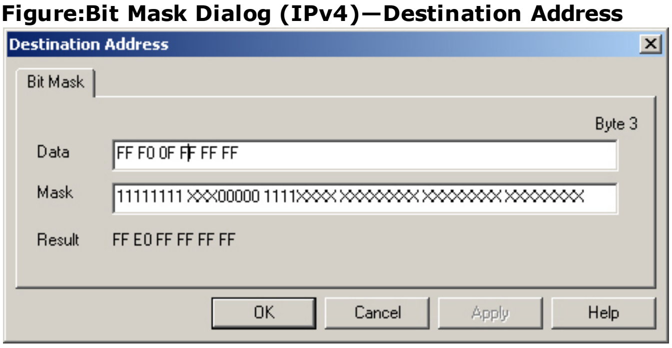
Bit Mask Dialog

The *Bit Mask* dialog (for IPv4) is used throughout the IxExplorer when masked data values are needed. This dialog box is accessed by setting the Destination Address or Source Address mode to *Random*. The *Bit Mask...* button is displayed. Select this button.

NOTE This description is for the IPv4 Bit Mask dialog only. The filter configuration Bit Mask dialog is described in *DA/SA Values*.

The *Bit Mask* dialog is shown in *Figure:Bit Mask Dialog (IPv4)—Destination Address*.

Figure:Bit Mask Dialog (IPv4)—Destination Address



The Data value that is being masked is shown in the upper field. Its value may be set using any hexadecimal character (0 through 9, a through f, and A through F); lowercase characters are displayed in uppercase. Each character corresponds to a 4-bit nibble, and spacing between bytes is automatically provided.

Each permitted byte of the mask consists of 8 symbols, with each symbol corresponding to one bit. Values of '0,' '1' or 'X' (or 'x') are permitted. Spacing between bytes of data is automatically provided. The first eight bits of mask operate on the first byte (2 nibbles) of the data value. Each '1'/'0' forces a value of '1'/'0' in the corresponding result, regardless of the data bit value. Each 'X' in the mask allows the data value to 'show through' to the result.

Data Pattern Box

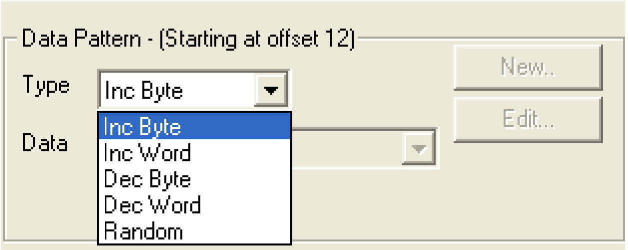
The *Data Pattern* feature generates data following the value that is used in the *Type* and *Data* fields.

The Data Pattern pane is shown in the following figure:

Figure:Frame Data: Data Pattern

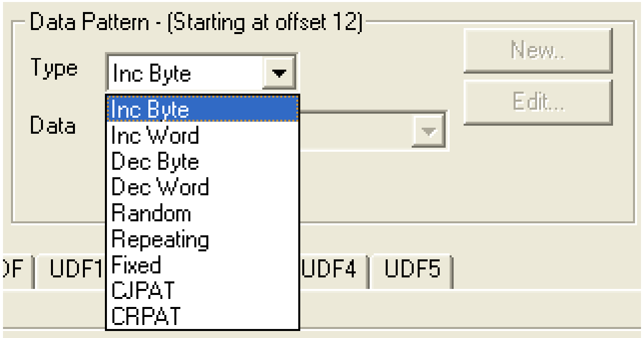
The Data Pattern pane for XDM10G32S is shown in the following figure:

Figure:XDM10G32S Data Pattern



The Data Pattern pane for Lava is shown in the following figure:

Figure:Lava Data Pattern



The *Type* fields available and the corresponding interpretation of the *Data* field is described in *Table:Data Pattern Type Values and Usage*. (See **Note** below for data patterns on OC-12c ports.)

Table:Data Pattern Type Values and Usage

Type	Description
Inc Byte	The data starts with a byte of 0x00, followed by 0x01, 0x02, ... , 0xFE, 0xFF, 0x00 to the end of the packet. New packets start again with a value of 0x00. The data field may not be edited.
Inc Word	The data starts with a word of 0x0000, followed by 0x0001, 0x0002, ... , 0xFFFE, 0xFFFF, 0x0000 to the end of the packet. Data is transmitted most significant byte first. The data field may not be edited.
Dec Byte	The data starts with a byte of 0xFF, followed by 0xFE, 0xFD, and so forth, to the end of the packet. New packets start again with a value of 0xFF. The data field may not be edited.
Dec Word	The data starts with a word of 0xFFFF, followed by 0xFFFE, 0xFFFD, and so forth, to the end of the packet. Data is transmitted with most significant byte first. The data field may not be edited.

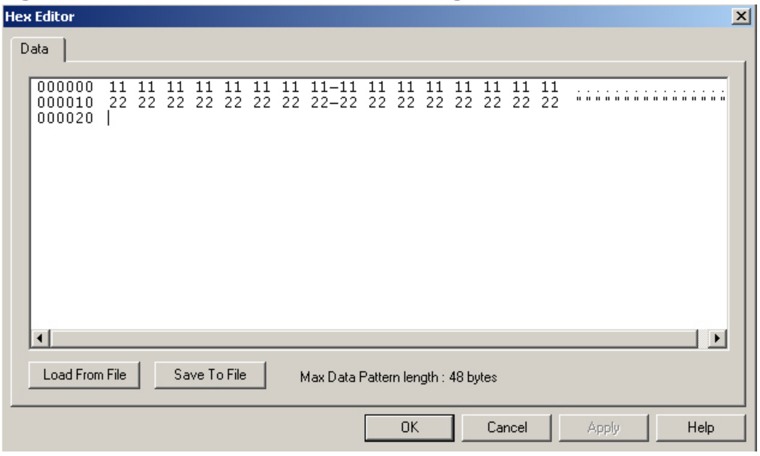
Type	Description
Random	Random data values are supplied. The data field may not be edited.
Repeating	Arbitrary data patterns may be supplied and repeated. These patterns may be created, edited, retrieved from disk, and/or stored to disk. Available patterns are shown in the *Data* field pull-down list.
Fixed	Fixed, arbitrary data patterns may be supplied and repeated. These patterns may be created, edited, and retrieved from disk and/or stored to disk. Available patterns are shown in the *Data* field pull-down list.
CJPAT	(For 10GE modules only.) The fixed Continuous Jitter Test Pattern (CJPAT), specified in IETF 802.3ae Annex 48A, is supplied. The data field may not be edited. *10GE Module Jitter Test Patterns—CJPAT & CRPAT* for additional information.
CRPAT	(For 10GE modules only.) The fixed Continuous Random Test Pattern (CRPAT), specified in IETF 802.3ae Annex 48A, is supplied. The data field may not be edited. *10GE Module Jitter Test Patterns—CJPAT & CRPAT* for additional information.
New	(Available only for the *Repeating* and *Fixed* options.) Click this button to open the *Hex Editor* dialog to create a new custom data pattern. *Data Pattern–Hex Editor Dialog* for additional information.
Edit	(Available only for the *Repeating* and *Fixed* choices.) Click this button to open the *Hex Editor* dialog to edit an existing custom data pattern. *Data Pattern–Hex Editor Dialog* for additional information.

NOTE For OC-12c POS ports, when any Data Pattern other than *Fixed* is selected, the maximum frame size is 15,257 bytes.

Data Pattern–Hex Editor Dialog

The Data Pattern *New* button opens an empty data window in the *Hex Editor* dialog. The Data Pattern *Edit* button opens a data window which contains the value to be edited, as shown in *Figure:Data Pattern—Hex Editor Dialog*. You may create and edit a custom-defined data pattern in this dialog.

Figure:Data Pattern—Hex Editor Dialog



The fields and controls in this dialog are described in *Table:Data Pattern—Hex Editor Dialog*.

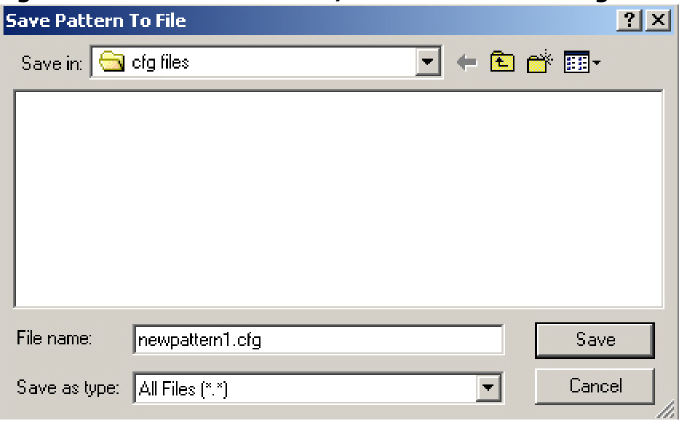
Table:Data Pattern—Hex Editor Dialog

Type	Description
(window)	The first column is for display purposes only; it indicates the hex offset of the information for that row. The second column shows the data pattern in hex. Information may be entered or edited using any hexadecimal characters (0 through 9, a through f, and A through F). (Lowercase alpha characters is automatically converted to upper-case.)
Load From File	Click to open the **Load Pattern From File** dialog, where a data pattern file, previously saved to disk, can be imported into the current data window. *Save To/Load From File Dialog* for additional information.
Save To File	Click to open the **Save Pattern To File** dialog, where the data pattern in the current data window can be saved to a file and stored on disk. *Save To/Load From File Dialog* for additional information.
Max Pattern Length (xx) Bytes	The maximum allowable pattern length is automatically calculated and displayed here. The number of bytes depends on the overall length of the packet and the number of bytes previously assigned for addressing and other uses.

Save To/Load From File Dialog

The *Save To File/Load From File* dialog is shown in *Figure:Data Pattern Save To/Load From File Dialog*.

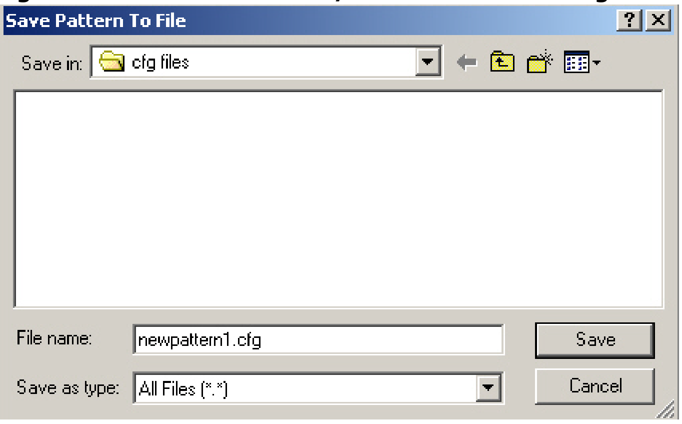
Figure:Data Pattern Save To/Load From File Dialog



Save To/Load From File Dialog

The *Save To File/Load From File* dialog is shown in *Figure:Data Pattern Save To/Load From File Dialog*.

Figure:Data Pattern Save To/Load From File Dialog



10GE Module Jitter Test Patterns—CJPAT & CRPAT

The 10GE module interfaces may be tested by using the CJPAT and CRPAT test patterns specified in IEEE 802.3ae Annex 48A.

The ports may be configured for these tests in the *Packet Streams Grid* window, or through the *Frame Data* tab. In the *Packet Streams Grid* window, the configuration process is greatly simplified. After a stream entry is created in the grid, the pop-up menu offers the options: 'Force CJPAT Stream' and 'Force CRPAT Stream.' When one of these options is selected for that stream, the stream configuration values are forced to match the values specified by the specs. If the configuration is performed **manually**, numerous values must be set, as follows:

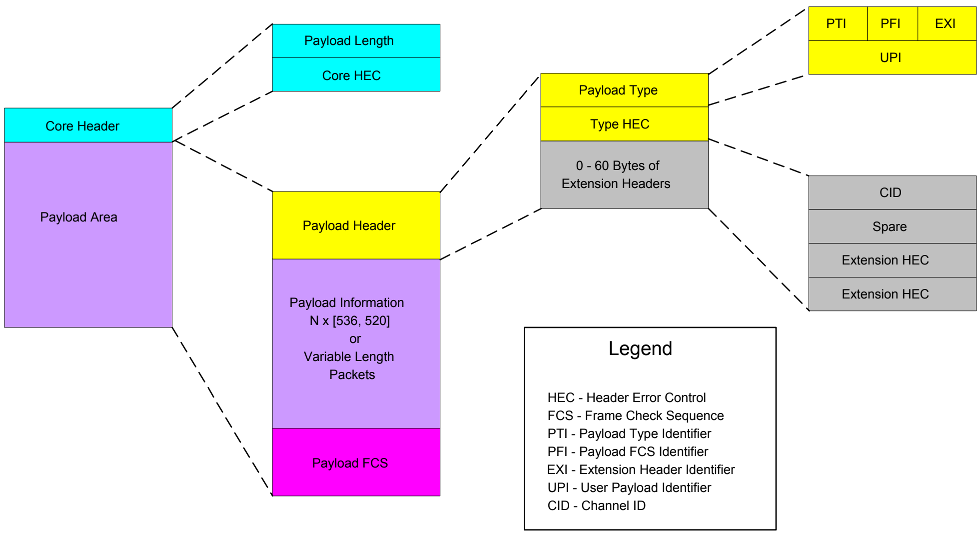
- Data Pattern - Select CJPAT or CRPAT
- Frame Size - Set to 1508 bytes for CJPAT, or 1492 for CRPAT
- Preamble = 8 bytes. Value = FB 55 55 55 55 55 55 D5
- Continuous Packet Stream mode
- IPG - 12 bytes (idle bytes) minimum
- No IP addresses - since these are MAC Layer tests

- No layer 2 or layer 3 protocol
- MAC DA:
  - Mode CJPAT - 0B 7E 7E 7E 7E 7E
  - Mode CRPAT - BE BE BE BE D7 D7
- MAC SA:
  - Mode CJPAT - 7E 7E 7E 7E 7E 7E
  - Mode CRPAT - D7 D7 23 23 23 23
- No UDFs configured
- No Timestamp
- CRC set to No Error—CRCs are specified exactly by the 802.3ae Annex 48 document, for each of the test modes.

Frame Data for GFP

Ixia's optional Generic Framing Procedure (GFP) feature is implemented on the OC-48c POS module, per ITU-T G.7041/Y.1303. A diagram of the format for a GFP frame, based on that specification, is shown in *Figure:GFP Frame Elements*.

Figure:GFP Frame Elements



The GFP frame data options are displayed by setting the port to GFP in the Port Properties dialog, as described in *Port Properties for GFP*.

The GFP section of the *Frame Data* tab for use in constructing GFP frames is shown in *Figure:GFP Frame Data Dialog*.

Figure:GFP Frame Data Dialog

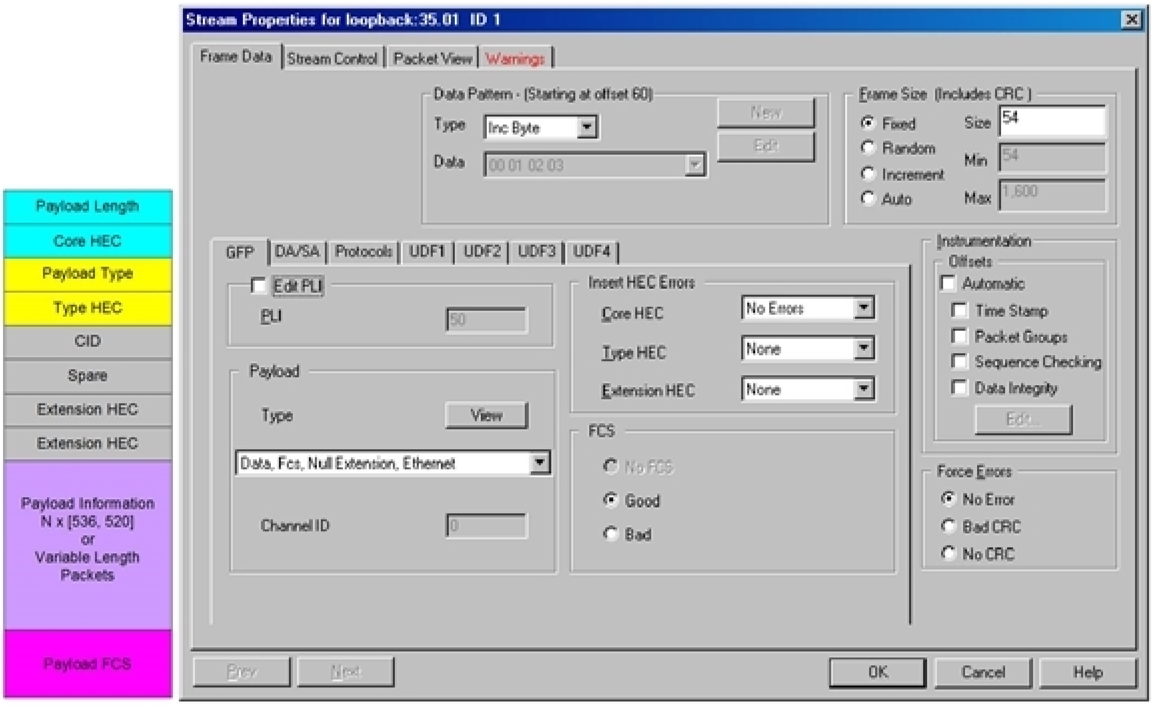


Table: GFP Configuration Fields describes the fields in the GFP tab.

Table: GFP Configuration Fields

Group	Field	Usage
Enable PLI		Selecting this check box enables the Payload Length Indicator in the GFP frame.
	PLI	Allows to set the Payload Length Indicator, in number of octets expected in the payload. The PLI is automatically adjusted to reflect what type of payload is set in the Payload Type pull-down menu.
Payload		This section allows to select a payload type for the GFP frame. Payload types are variants of Ethernet or PPP encapsulation, and either data or control frames.
	Type	Allows to select a payload type for the GFP frame from a pull-down list. Each payload type contains four elements: 1. Whether the payload is data or management information 2. Whether a Frame Check Sequence (FCS) is employed 3. Whether an eHEC is used 4. If the GFP is using Ethernet or PPP. The payload options are:

Group	Field	Usage
		• Data, FCS, Null Extension, Ethernet • Data, NoFCS, Null Extension, Ethernet • Data, FCS, Linear Extension, Ethernet • Data, NoFCS, Linear Extension, Ethernet • Management, FCS, Null Extension, Ethernet • Management, NoFCS, Null Extension, Ethernet • Management, FCS, Linear Extension, Ethernet • Management, NoFCS, Linear Extension, Ethernet • Data, FCS, Null Extension, PPP • Data, NoFCS, Null Extension, PPP • Data, FCS, Linear Extension, PPP • Data, NoFCS, Linear Extension, PPP • Management, FCS, Null Extension, PPP • Management, NoFCS, Null Extension, PPP • Management, FCS, Linear Extension, PPP • Management, NoFCS, Linear Extension, PPP When an Ethernet type payload is selected, the *DA/SA* sub-tab is displayed for MAC address manipulation. *DA/SA Property Sheet* for information on configuring MAC address usage.
	Channel ID	This field sets a Channel ID number for management GFP frames.
	View/Edit	This button opens the *Payload Header* dialog box, which displays what header types are included in the Payload Header. See *GFP Payload Header Dialog* for more information on Payload Headers.
Insert HEC Errors		Allows to insert errors into Header Error Correction (HEC) values, for Core, Type, and Extension HECs. NOTE Insert HEC Errors fields are not present for channelized mode POS boards.
	Core HEC	Core Header Error Correction Errors. The four octets of the GFP Core Header consist of a 16-bit PDU Length Indicator field and a 16-bit Core Header Error Check (cHEC) field. This header allows GFP frame delineation independent of the content of the higher layer PDUs.

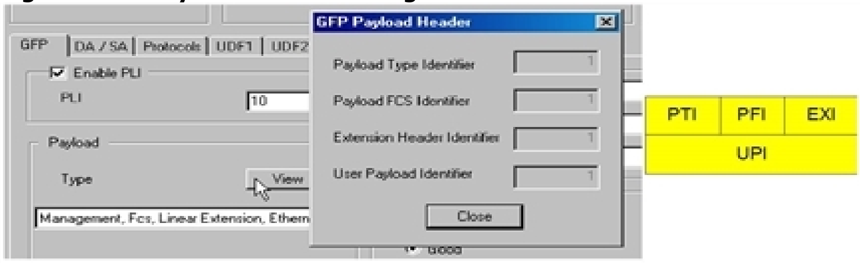
Group	Field	Usage
		Choose the number of bit errors to insert in the HEC byte: • None (errors not inserted) • 1 Bit • Multiple Bits
	Type HEC	The two-octet Type Header Error Control field contains a CRC-16 error control code that protects the integrity of the contents of the Type Field by enabling both single-bit error correction and multi-bit error detection. Choose the number of bit errors to insert in the HEC byte, from none to 16.
	Extension HEC	The two-octet Extension Header Error Control field contains a CRC-16 error control code that protects the integrity of the contents of the extension headers by enabling both single-bit error correction (optional) and multi-bit error detection. Choose the number of bit errors to insert in the HEC byte, from none to 16.
FCS		The Payload Frame Check Sequence (FCS) is generated using the CRC-32 generating polynomial (ISO/IEC 3309) G(x) = x32 + x26 + x23 + x22 + x16 + x12 + x11 + x10 + x8 + x7 + x5 + x4 + x2 + x1 + 1 where x32 corresponds to the Most Significant Bit and x0 corresponds to the Least Significant Bit. Depending on the Payload Type, the FCS becomes enabled. You can select whether to use a good (meaning valid) FCS number, or a bad (meaning invalid) number
	No FCS	This is selected when the payload type used includes an FCS that is part of the GFP frame. NOTE No FCS is unavailable for channelized mode POS boards.
	Good	When a payload type is selected for the GFP that includes an FCS, this option button sets the FCS number to be a valid number.
	Bad	When a payload type is selected for the GFP that includes an FCS, this option button sets the FCS number to be an invalid number. NOTE Bad FCS is unavailable for channelized mode POS boards.

GFP Payload Header Dialog

The *GFP Payload Header* dialog displays what identifiers are included in the Payload Header section of the GFP frame. It is accessed by selecting the *View/Edit* button as shown in *Figure:GFP Frame Data Dialog*.

Figure:GFP Payload Header Dialog shows the *GFP Payload Header* dialog and the section of the GFP frame being modified.

Figure: GFP Payload Header Dialog



The Identifier fields display either a 0 or a 1.*Table:GFP Payload Header Configuration* explains the significance of these settings.

Table:GFP Payload Header Configuration

Field	Usage
Payload Type Identifier	A 3-bit subfield of the Type field identifying the type of GFP client frame. Two kinds of client frames are currently defined, User Data frames (PTI = 000) and Client Management frames (PTI = 100).
Payload FCS Identifier	A one bit subfield of the Type field indicating the presence (PFI = 1) or absence (PFI = 0) of the Payload FCS field.
Extension Header Identifier	A 4-bit subfield of the Type field identifying the type of Extension Header GFP. Three kinds of Extension Headers are currently defined, a Null Extension Header, a Linear Extension Header, and a Ring Extension Header. Ixia supports the Null and Linear extensions, indicated by a 0 (Null extension) or a 1 (Linear extension).
User Payload Identifier	An 8-bit field identifying the type of payload conveyed in the GFP Payload Information field. Interpretation of the UPI field is relative to the type of GFP client frame as indicated by the PTI subfield.

These fields are automatically set when a payload type is selected, and cannot be changed.

Frame Data for ATM/POS 622

The following sections discuss the frame data for the ATM/POS 622 module. The different framing types are covered in:

- *ATM Frames*
- *POS 622 Frame Data*

ATM Frames

ATM Frame Data for information on the ATM *Frame Data* tab.

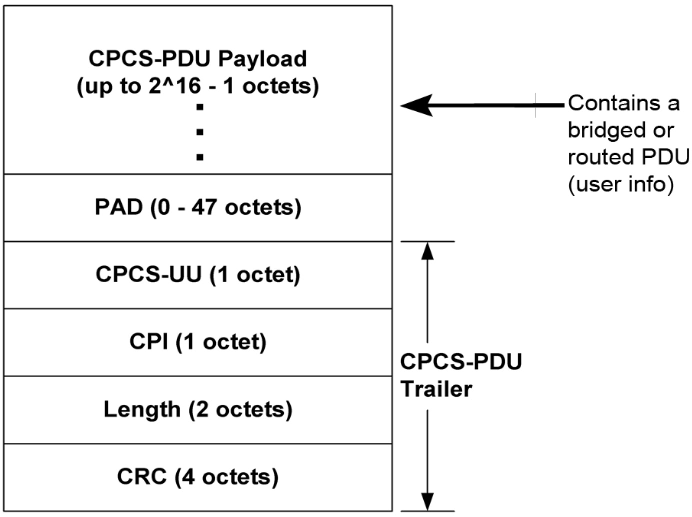
Connection-less routed and bridged PDUs, such as Ethernet frames, can be carried across a connection-oriented ATM link. Extensive fragmentation of a routed PDU such a as an IP packet is undesirable, so a method has been developed whereby they are first encapsulated as the payload of a CPCS PDU by the ATM AAL 5 layer defined in ITU-T I.363.5. The AAL5 CPCS PDUs (frames) are then fragmented into 48-byte sections which can be inserted into the payloads of ATM cells, ATM headers attached, and then transmitted across the ATM (over SONET) link. In cases where a CPCS PDU cannot be aligned, it is segmented into 48-byte sections and any remainder is aligned with added padding bytes. The IP packet is reassembled by the receiver.

When there is no Service Specific Convergence Sublayer (SSCS) present, routed and bridged PDUs traverse the AAL CPCS using one of the two following ATM multiplexing methods: LLC Encapsulation (multiplexing by protocol) or VC Multiplexing (multiplexing by virtual connection/VC). These methods are defined in RFC 2684.

- **LLC encapsulation** is used when one VC may carry more than one protocol, and requires that the protocol type be specified for routed PDUs. This information is carried in an IEEE 802.2 LLC header. Fewer VCs are required, since one VC can support multiple protocols.
- **VC Multiplexing** requires less payload overhead, such as PIDs, since it sets up the binding between the ATM VC and the network protocol on the VC. However, with one protocol per VC, more VCs are required for multiple protocols.

The bridged or routed PDU is then encapsulated within an AAL5 CPCS-PDU, as the payload, as shown in *Figure:ATM AAL5 CPCS-PDU Format*.

Figure:ATM AAL5 CPCS-PDU Format



The fields in this PDU are described in *Table:ATM AAL5 CPCS-PDU Format*.

Table:ATM AAL5 CPCS-PDU Format

Field	Description
CPCS-PDU Payload	The bridged or routed PDU of user information encap-

Field	Description
	sulated within the AAL5 CPCS-PDU.
PAD	Padding for alignment—so the end of the CPCS-PDU trailer is right-justified in the last 48-byte cell created by the SAR. Range is from 0 to 47 octets of padding.
CPCS-UU	CPCS User-to-User Indication. Not used in the RFC 2684 implementations described in this document.
CPI	Common Part Indicator. Used for 64-bit alignment of the CPCS-PDU trailer. Must be 0x00.
Length	Length of the payload field—up to 65,535 octets.
CRC	The CRC-32 used to detect CPCS-PDU bit errors.

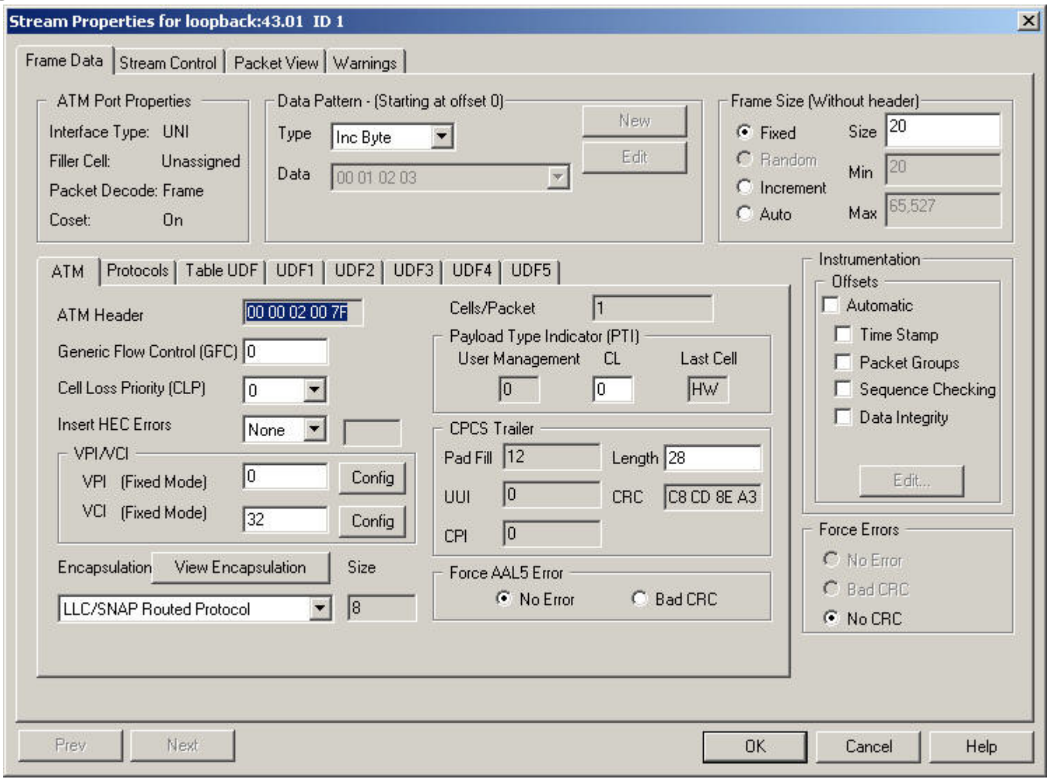
NOTE When using ATM ports, different types of ATM encapsulation result in different length headers. The data portion of the packet normally follows the header, except in the case of the two LLC Bridged Ethernet choices, where 12 octets of MAC address and 2 octets of Ethernet type follow the header. The offsets are with respect to the beginning of the AAL5 packet and must be adjusted by hand to account for the header.

ATM Frame Data

The Stream properties for the ATM 622 load module are set in the *Frame Data* and *Stream Control* tabs. The *Frame Data* tab with an ATM sub-tab is shown in *Figure:ATM Streams—Frame Data*. This sub-tab is only visible if the port is set to ATM mode. See *ATM/POS 622 Modules* for more information.

The contents of the ATM Frame and the encapsulation method are configured in the *ATM* sub-tab.See *Frame Data Structure* for information on the other parts of this dialog.

Figure: ATM Streams—Frame Data



The fields and controls in this dialog are described in *Table: ATM Stream—Frame Data (ATM Tab)*.

Table: ATM Stream—Frame Data (ATM Tab)

Section	Field/Control	Description
ATM Port Properties		(Read-only) Displays the values for parameters configured in the ATM Port Properties page. *ATM Tab* for additional information.
	Interface Type	(Read-only) One of: • **UNI** : The ATM Forum-defined User-to-Network- Interface. • **NNI**: The ATM Forum-defined Network-to-Node-Interface.
	Filler Cell	SONET frame transmission is continuous even when data or control messages are not being transmitted. The cell type to be transmitted during those intervals is one of the following: • Idle Cell (VPI/VCI = 0 and CLP = 1) • Unassigned Cell (VPI/VCI = 0 and CLP = 0)
	Packet Decode	Sets the mode for the display in Packet View. Choose one of: • Frame (AAL5) • Cell (53-byte ATM cells)

Section	Field/Control	Description
	Coset	(Read-only) The *Coset On* check box allows the user to add/enable the Coset algorithm to be used with the Header Error Control (HEC). The code used for HEC is a cyclic code with generating polynomial x^8 + x^2 + x + 1. If Coset is turned on, the result of this polynomial is XOR'd with 0x55 (Coset Leader). One of: • On (Enabled) • Off (Disabled)
ATM	ATM Header	The 5 bytes used as the header for the ATM cell.
	Generic Flow Control (GFC)	(4 bits) For use with UNI mode only. For device control signalling. Uncontrolled equipment uses a setting of 0000 (Null value).
	Cell Loss Priority (CLP)	(1 bit) Used for setting discard priority level. It indicates whether the cell should be discarded if it encounters extreme congestion as it moves through the network. A CLP value = 0 has higher priority than a CLP value = 1.
	Insert HEC Errors	Header Error Correction Errors. Choose the number of bit errors to insert in the HEC byte: • None (errors not inserted) • 1 Bit • 2 Bits • 3 Bits • 4 Bits • 5 Bits • 6 Bits • 8 Bits
	HEC Value	(Read-only) The decimal value corresponding to the HEC Error setting in the field to the left. It is the calculated HEC value with the HEC error setting applied. (It changes with the VPI/VCI.)
VPI/VCI	VPI (Fxed Mode)	Virtual Path Identifier (VPI) for this stream.
		Click to display the *VPI Configuration* dialog. *ATM VPI/VCI Configuration Dialogs* for additional information. The selected Mode is dis-

Section	Field/Control	Description
		played in parenthesis.
	VCI (Fxed Mode)	Virtual Connection/Circuit Identifier (VCI) for this stream.
		Press this button to display the *VCI Configuration* dialog. *ATM VPI/VCI Configuration Dialogs* for additional information. The selected Mode is displayed in parenthesis.
Encapsulation		The RFC 2684-defined ATM encapsulation mode groups are LLC Encapsulation and VC Multiplexing. The various types available for those modes are listed below.
	(encapsulation type) Choose one of:	LLC/SNAP Routed Protocol *ATM LLC/SNAP Routed Protocol Dialog* for additional information.
		LLC Bridged Ethernet/802.3 *ATM LLC Bridged Ethernet/802.3 Dialog* for additional information.
		LLC Bridged Ethernet/802.3 no FCS *ATM LLC Bridged Ethernet/802.3 no FCS Dialog* for additional information.
		LLC Encapsulated PPP *ATM LLC Encapsulated PPP Dialog*.
		VC Multiplexed PPP *ATM VC Multiplexed PPP Dialog*.
		VC MUX Routed Protocol (no configuration dialog). *ATM VC MUX Routed Protocol* for additional information.
		VC MUX Bridged Ethernet *ATM VC MUX Bridged Ethernet/802.3 Dialog* for additional information.
		VC MUX Bridged Ethernet with No FCS *ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog* for additional information.
	Edit/View Encapsulation (button)	Press this button to access the specific dialog for the selected type of encapsulation. This button changes from *Edit* to *View*, depending upon the encapsulation type. The specific

Section	Field/Control	Description
		options are discussed in the sections describing the encapsulation types.
	Size	(Read-only) Displays encapsulation header size.
Cells/Packet		(Read-only) Shows how many cells are occupied by a packet (once the packet has been defined).
Payload Type Indicator (PTI)		Overall, PTI field is 3 bits, and each bit has a different meaning.
	User Management	(Read-only) This bit indicates if the ATM cell is a control or data cell. 0 - ATM data cell 1 - ATM control cell
	CL	This bit indicates Congestion/No Congestion. Choose one of: 0 - Congestion Not Experienced 1 - Congestion Experienced
	Last Cell	(Read-only) This bit indicates if this is the last ATM cell of the frame. 'HW' means that Hardware inserts the appropriate values. [ATM User to ATM user indication = 0 for the first and intermediate ATM cells. AUU = 1 for the last ATM cell.]
CPCS Trailer		The fields that make up the CPCS Trailer at the end of a CPCS-PDU.
	Pad Fill	PAD Field of the CPCS Trailer. It is octet-aligned. The valid range is 0 to 47 bytes in length.
	UUI	CPCS-PDU User-to-User Indication.
	CPI	Common Part Indicator field of the CPCS Trailer, for aligning the trailer to 64 bits.
	Length	Encodes CPCS-PDU payload length, in number of octets.
	CRC	For transmission, the CRC is calculated over the CPCS-PDU, including PAD and the first 4 octets of the trailer.
Force AAL5 Error	No Error	If this option is selected, no AAL5 error is inserted.
	Bad CRC	If this option is selected, a Bad AAL5 CRC is inserted.

ATM VPI/VCI Configuration Dialogs

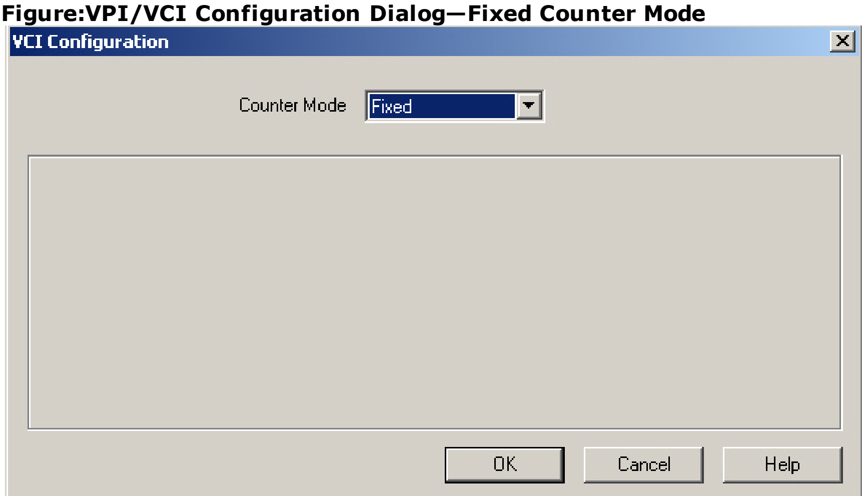
When the *VPI* or *VCI Config* button is clicked, the *VPI/VCI Configuration* dialog is displayed. The format for the dialog is the same for configuration of the VPIs and VCIs. There are four counter modes for this dialog, as described in the following sections:

- *VPI/VCI Configuration Dialog—Fixed Counter Mode*
- *VPI/VCI Configuration Dialog—Counter Counter Mode*
- *VPI/VCI Configuration Dialog—Random Counter Mode*
- *VPI/VCI Configuration Dialog—Table Counter Mode*

VPI/VCI Configuration Dialog—Fixed Counter Mode

The ATM *VPI/VCI Configuration* dialog in Fixed Counter Mode is shown in *Figure:VPI/VCI Configuration Dialog—Fixed Counter Mode*.

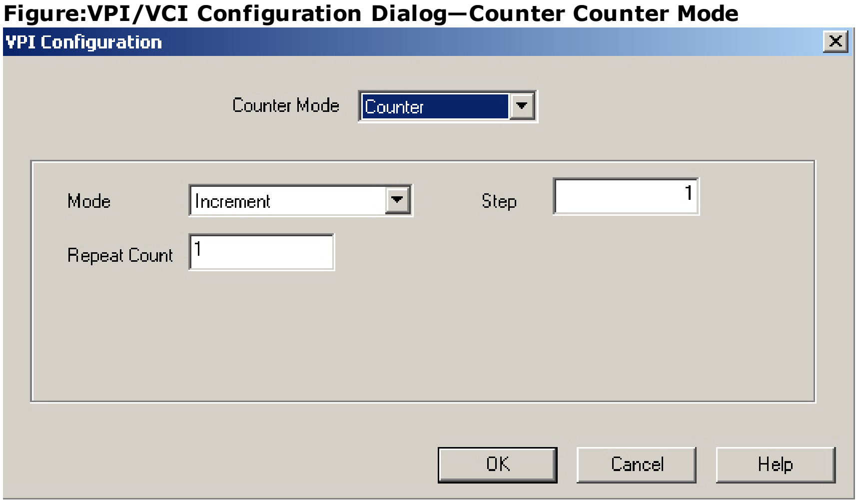
Figure:VPI/VCI Configuration Dialog—Fixed Counter Mode



VPI/VCI Configuration Dialog—Counter Counter Mode

The ATM *VPI/VCI Configuration* dialog in Counter Counter Mode is shown in *Figure:VPI/VCI Configuration Dialog—Counter Counter Mode*.

Figure:VPI/VCI Configuration Dialog—Counter Counter Mode



The fields in this dialog are described in *Table:VPI/VCI Configuration Dialog—Counter Counter Mode*.

Table:VPI/VCI Configuration Dialog—Counter Counter Mode

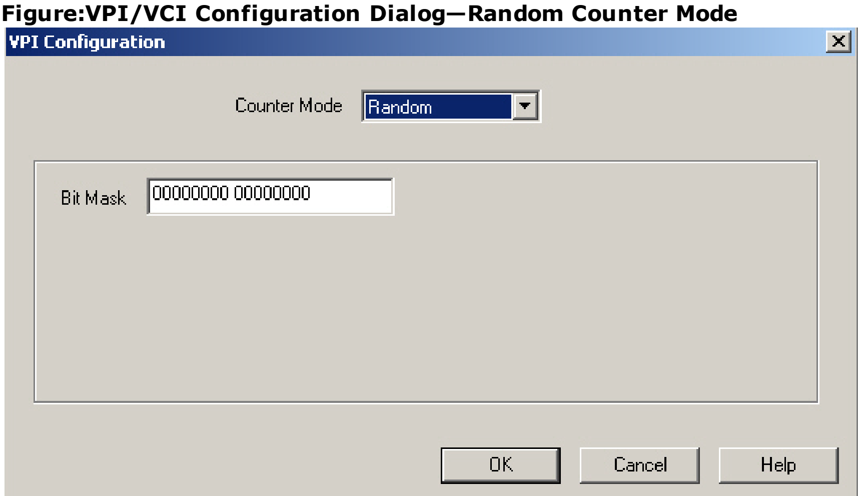
Field/Control	Description
Counter Mode	Counter
Mode	Choose the method for counting:

Field/Control	Description
	• Increment • Continuous Increment • Decrement • Continuous Decrement
Step	The amount by which the previous value is increased (incremented) or decreased (decremented).
Repeat Count	Available only for Increment or Decrement. The number of times that the counting process is implemented.

VPI/VCI Configuration Dialog—Random Counter Mode

The ATM *VPI/VCI Configuration* dialog in Random Counter Mode is shown in *Figure:VPI/VCI Configuration Dialog—Random Counter Mode*.

Figure:VPI/VCI Configuration Dialog—Random Counter Mode



The fields in this dialog are described in *Table:VPI/VCI Configuration Dialog—Random Counter Mode*.

Table:VPI/VCI Configuration Dialog—Random Counter Mode

Field/Control	Description
Counter Mode	Random
Bit Mask	When the Random counter mode is selected, a 16-bit *Bit Mask* field is displayed. Random values are used in conjunction with the bit mask. You may control which mask bit values is set to '0' or '1,' or allowed to change ('X').

VPI/VCI Configuration Dialog—Table Counter Mode

The fields in this dialog are described in *Table:VPI/VCI Configuration Dialog—Counter Counter Mode*.

Table:VPI/VCI Configuration Dialog—Counter Counter Mode

Field/Control	Description
Counter Mode	Table

Field/Control	Description
Data	2-byte user-defined values. Use the right-click menu, *New* option, to add entries to the list.

Frame Data—ATM Encapsulation

The types of ATM encapsulation supported in the ATM *Frame Data* tab are described in the following sections:

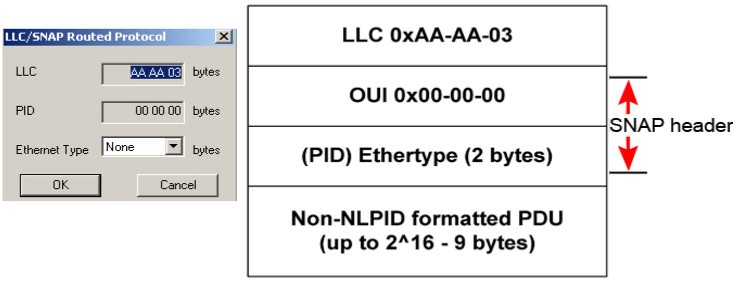
- LLC Encapsulation:
  - *ATM LLC/SNAP Routed Protocol Dialog*
  - *ATM LLC Bridged Ethernet/802.3 Dialog*
  - *ATM LLC Bridged Ethernet/802.3 no FCS Dialog*
  - *ATM LLC Encapsulated PPP Dialog*
- VC Multiplexing:
  - *ATM VC Multiplexed PPP Dialog*
  - *ATM VC MUX Routed Protocol*
  - *ATM VC MUX Bridged Ethernet/802.3 Dialog*
  - *ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog*

ATM LLC/SNAP Routed Protocol Dialog

The ATM *LLC/SNAP Routed Protocol* dialog is shown in *Figure:ATM LLC/SNAP Routed Protocol Dialog*. This dialog is accessed by selecting the *LLC/SNAP Routed Protocol* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

This format is used for routed PDUs, and is the default format for IP datagrams. In addition, the default size of the IP MTU used with ATM AAL5 is 9180 bytes, per RFC 2225.

Figure:ATM LLC/SNAP Routed Protocol Dialog



The fields and controls in this dialog are described in *Table:ATM LLC/SNAP Routed Protocol Dialog*.

Table:ATM LLC/SNAP Routed Protocol Dialog

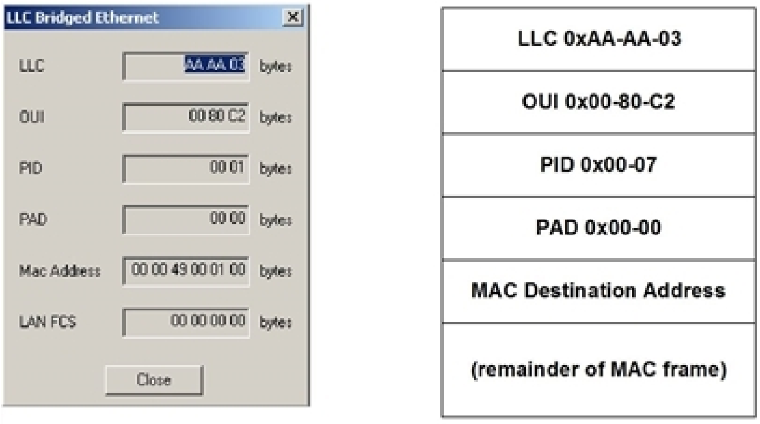
Field/Control	Description
LLC	(Read-only) Link Layer Control. An IEEE 802.2 LLC header is included in the PDU. The value 0xAA-AA-03 indicates that this is the payload format for a routed Formatted PDU.

Field/Control	Description
PID	(Read-only) Protocol Identifier for Ethertype. (The OUI would be 0x00-00-00, indicating that the PID is Ethertype.)
Ethernet Type	Choose one of: • None • IPv4 • IPv6 • MPLS

ATM LLC Bridged Ethernet/802.3 Dialog

The ATM *LLC Bridged Ethernet* dialog applies to Bridged Ethernet IEEE 802.3 PDUs, as shown in *Figure:ATM LLC Bridged Ethernet/802.3 Dialog*. This dialog is accessed by selecting the *LLC Bridged Ethernet/802.3* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

Figure:ATM LLC Bridged Ethernet/802.3 Dialog



NOTE

When using ATM ports, different types of ATM encapsulation result in different length headers. The data portion of the packet normally follows the header, except in the case of the two LLC Bridged Ethernet choices, where 12 octets of MAC address and 2 octets of Ethernet type follow the header. the offsets are with respect to the beginning of the AAL5 packet and must be adjusted by hand to account for the header.

The fields and controls in this dialog are described in *Table:ATM LLC Bridged Ethernet/802.3 Dialog*.

Table:ATM LLC Bridged Ethernet/802.3 Dialog

Field/Control	Description
LLC	(Read-only) Link Layer Control. An IEEE 802.2 LLC header is included in the PDU. The value 0xAA-AA-03 indicates that this is the payload format for a routed Formatted PDU.
OUI	(Read-only) Organizationally Unique Identifier: Part of the SNAP header.

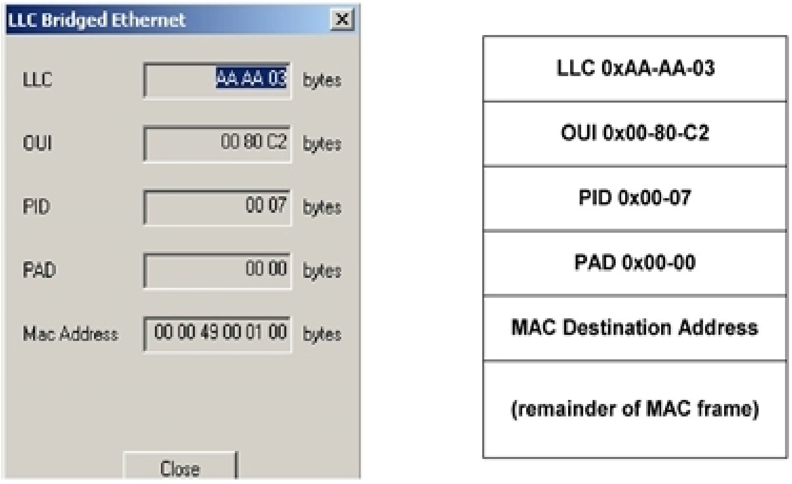
Field/Control	Description
PID	(Read-only) Protocol Identifier: Part of the SNAP header. The value 0x 00-01 indicates that the LAN FCS is present, which also means that padding must be included.
PAD	(Read-only) Indicates that padding is included.
MAC Address	(Read-only) The 6-byte MAC Address, in canonical form.
LAN FCS	(Read-only) The 4-byte LAN Frame Check Sequence. If present, the PID is 0x00-01.

NOTE When this encapsulation is selected, the option to use Cisco ISL also becomes available. If Cisco ISL is used, the IP statistics and checksum is not accurate.

ATM LLC Bridged Ethernet/802.3 no FCS Dialog

The ATM *LLC Bridged Ethernet* dialog (with no FCS) applies to Bridged Ethernet IEEE 802.3 PDUs, as shown in *Figure:ATM LLC Bridged Ethernet/802.3 no FCS Dialog*. This dialog is accessed by selecting the *LLC Bridged Ethernet/802.3* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

Figure:ATM LLC Bridged Ethernet/802.3 no FCS Dialog



NOTE When using ATM ports, different types of ATM encapsulation result in different length headers. The data portion of the packet normally follows the header, except in the case of the two LLC Bridged Ethernet choices, where 12 octets of MAC address and 2 octets of Ethernet type follow the header. the offsets are with respect to the beginning of the AAL5 packet and must be adjusted by hand to account for the header.

The fields and controls in this dialog are described in *Table:ATM LLC Bridged Ethernet/802.3 no FCS Dialog*.

Table:ATM LLC Bridged Ethernet/802.3 no FCS Dialog

Field/Control	Description
LLC	(Read-only) Link Layer Control. An IEEE 802.2 LLC header is included in the PDU. The value 0xAA-AA-03 indicates

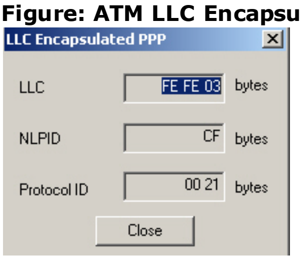
Field/Control	Description
	that this is the payload format for a routed Formatted PDU.
OUI	(Read-only) Organizationally Unique Identifier: Part of the SNAP header.
PID	(Read-only) Protocol Identifier: Part of the SNAP header. The value 0x 00-07 indicates that the LAN FCS is not present, which also means that padding is optional.
PAD	(Read-only) Indicates that padding is included. Since no LAN FCS is included, padding is optional.
Mac Address	(Read-only) The 6-byte MAC Address, in canonical form.

NOTE When this encapsulation is selected, the option to use Cisco ISL also becomes available. If Cisco ISL is used, the IP statistics and checksum is not accurate.

ATM LLC Encapsulated PPP Dialog

The ATM *LLC Encapsulated PPP* dialog is shown in *Figure:ATM LLC Encapsulated PPP Dialog*. This dialog is accessed by selecting the *LLC Encapsulated PPP* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

Figure: ATM LLC Encapsulated PPP Dialog



The fields in this dialog are described in *Table: ATM LLC Encapsulated PPP Dialog*.

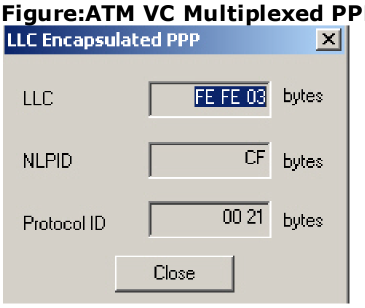
Table: ATM LLC Encapsulated PPP Dialog

Field/Control	Description
LLC	(Read-only) Link Layer Control. An IEEE 802.2 LLC header is included in the PDU.
NLPID	(Read-only) (in bytes) per ISO/IEC TR 9577, the Network Layer Protocol ID (NLPID) identifies the routing protocol. 0xCF = PPP
Protocol ID	(Read-only) The 2-byte Protocol Identifier.

ATM VC Multiplexed PPP Dialog

The ATM *VC Multiplexed PPP* dialog is shown in *Figure:ATM VC Multiplexed PPP Dialog*. This dialog contains only the read-only 2-byte Protocol Identifier (ID). This dialog is accessed by selecting the *VC Multiplexed PPP* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

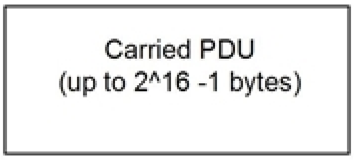
Figure:ATM VC Multiplexed PPP Dialog



ATM VC MUX Routed Protocol

For routed protocols, the only content of the AA5 CPCS-PDU must be the routed protocol PDU, which is shown in *Figure:ATM VC MUX Routed Protocol*. This dialog is accessed by selecting the *VC MUX Routed Protocol* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

Figure:ATM VC MUX Routed Protocol

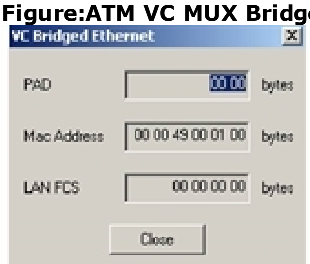


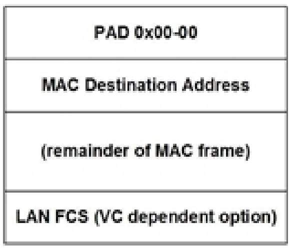
ATM VC MUX Bridged Ethernet/802.3 Dialog

NOTE The software cannot determine whether this type of ATM encapsulation has a CRC unless there is a proper entry in the VCI/VPI map. Use the VCI/VPI and Encapsulation fields (on both the transmit and receive ports) to set up a proper mapping. When the transmitting and receiving ports are using the same encapsulation and it has been placed in the map, the software is able to easily determine what type of packet has been transmitted, and then accurately identify the timestamp and other information.

The ATM *VC MUX Bridged Ethernet* dialog applies to IEEE 802.3 PDUs, and is shown in *Figure:ATM VC MUX Bridged Ethernet Dialog*. This dialog is accessed by selecting the *VC MUX Bridged Ethernet/802.3* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

Figure:ATM VC MUX Bridged Ethernet Dialog





The fields and controls in this dialog are described in *Table:ATM VC MUX Bridged Ethernet/802.3 Dialog*.

Table:ATM VC MUX Bridged Ethernet/802.3 Dialog

Field/Control	Description
PAD	(Read-only) Padding bytes.
Mac Address	(Read-only) The Destination MAC Address.
LAN FCS	(Read-only) The 4-byte LAN Frame Check Sequence.

NOTE When this encapsulation is selected, the option to use Cisco ISL also becomes available. If Cisco ISL is used, the IP statistics and checksum will not be accurate.

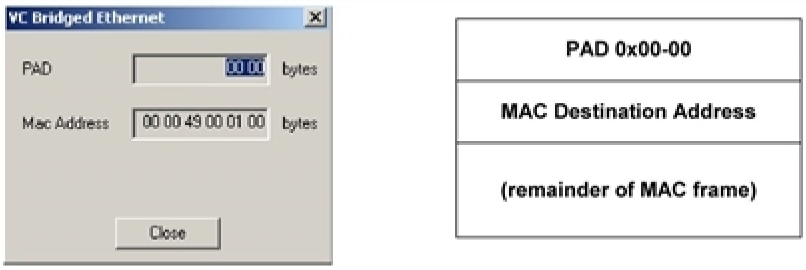
ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog

NOTE The software cannot determine whether this type of ATM encapsulation has a CRC unless there is a proper entry in the VCI/VPI map. Use the VCI/VPI and Encapsulation fields (on both the transmit and receive ports) to set up a proper mapping. When the transmitting and receiving ports are using the same encapsulation and it has been placed in the map, the software is able to easily determine what type of packet has been transmitted, and then accurately identify the timestamp and other information.

The ATM *VC MUX Bridged Ethernet* dialog (with no FCS) applies to IEEE 802.3 PDUs, and is shown in *Figure:ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog*. This dialog is accessed by selecting the *VC MUX Bridged Ethernet/802.3 no FCS* option from the Encapsulation list, and then selecting the *View Encapsulation* button.

In this case, the AAL5 CPCS-PDU Payload field carries a bridged PDU, without including the LAN FCS.

Figure:ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog



The fields and controls in this dialog are described in *Table:ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog*.

Table:ATM VC MUX Bridged Ethernet/802.3 no FCS Dialog

Field/Control	Description
PAD	(Read-only) Padding bytes.
Mac Address	(Read-only) The Destination MAC Address.

NOTE When this encapsulation is selected, the option to use Cisco ISL also becomes

NOTE available. If Cisco ISL is used, the IP statistics and checksum will not be accurate.

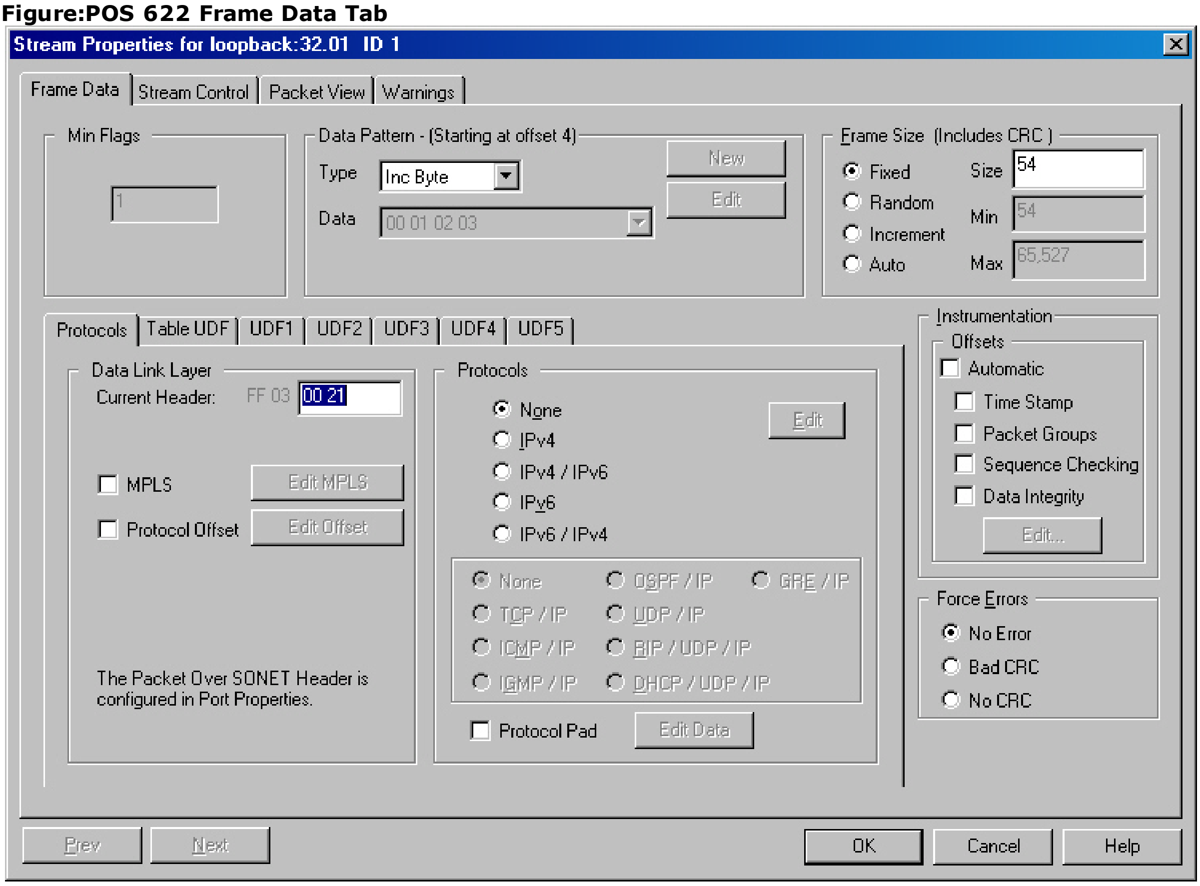
POS 622 Frame Data

The *Frame Data* tab for the ATM/POS 622 module in POS mode (OC-12c/OC-3c POS) combines aspects of the Frame Data configuration of both standard POS and TXS Ethernet modules.

This tab is only visible if the port is set to POS mode.ATM/POS 622 Modules for more information.

The *Frame Data* tab for the POS 622 (OC-12c/OC-3c POS) is shown in *Figure:POS 622 Frame Data Tab*.

Figure:POS 622 Frame Data Tab



The components of this tab are described in the following sections:

- *Min Flags Box*
- *Data Pattern Box*
- *Frame Size*
- *Instrumentation Box*
- *Force Errors*
- Protocols Section, as described in Chapter 6, Frame Data–Protocol Control
- User Defined Fields, as described in Chapter 7, Frame Data–User Defined Fields (UDF)

Frame Data for FCM

Fibre Channel (FC) is logically a bi-directional, point-to-point, serial data channel, structured for high performance capability.

The Stream Properties for the FC load module are set in the Frame Data and Stream Control tabs. The *Frame Data* tab with a *Fibre Channel Header* sub-tab is shown in *Figure:Frame Header tab*. This sub-tab is only visible if the port is set to FCM mode. The contents of the FC Frame and the encapsulation method are configured in the *Fibre Channel Header* sub-tab.

The fields in the FCM Frame Data tab in the *Stream Properties* window are described in *Table:The Frame Data tab*.

Table:The Frame Data tab

Section	Field/Control	Description
Delimiters	SOF	The Start-of-Frame (SOF) delimiter is an Ordered Set that immediately precedes the frame content. The multiple SOF delimiters defined for Sequence control are as follows: • SOFn1-Normal Class 1 or 6: The SOFn1 is used for all frames except the first frame of a Sequence for Class 1 service or Class 6 service. • SOFn2 - Normal Class 2: The SOFn2 is used for all frames except the first frame of a Sequence for Class 2 service. • SOFn3 - Normal Class 3 (default): The SOFn3 is used for all frames except the first frame of a Sequence for Class 3 service.
		• SOFn4 - Normal Class 4: The SOFn4 is used for all frames except the first frame of a Sequence for Class 4 service. • SOFi2 - Initiate Class 2: The SOFi2 is used on the first frame of a Sequence for Class 2 service. • SOFi3 - Initiate Class 3: The SOFi3 is used on the first frame of a Sequence for Class 3 service. • SOFi4 - Initiate Class 4: The SOFi4 is used on the first frame of a Sequence for Class 4 service. • SOFc4 - Connect Class 4: The SOFc4 is used on the first frame of a Connect for Class 4 service. • SOFf - Fabric: If an Nx_Port or Fx_Port receives a Class F frame, indicated by an SOFf delimiter, it is discarded by the Nx_Port

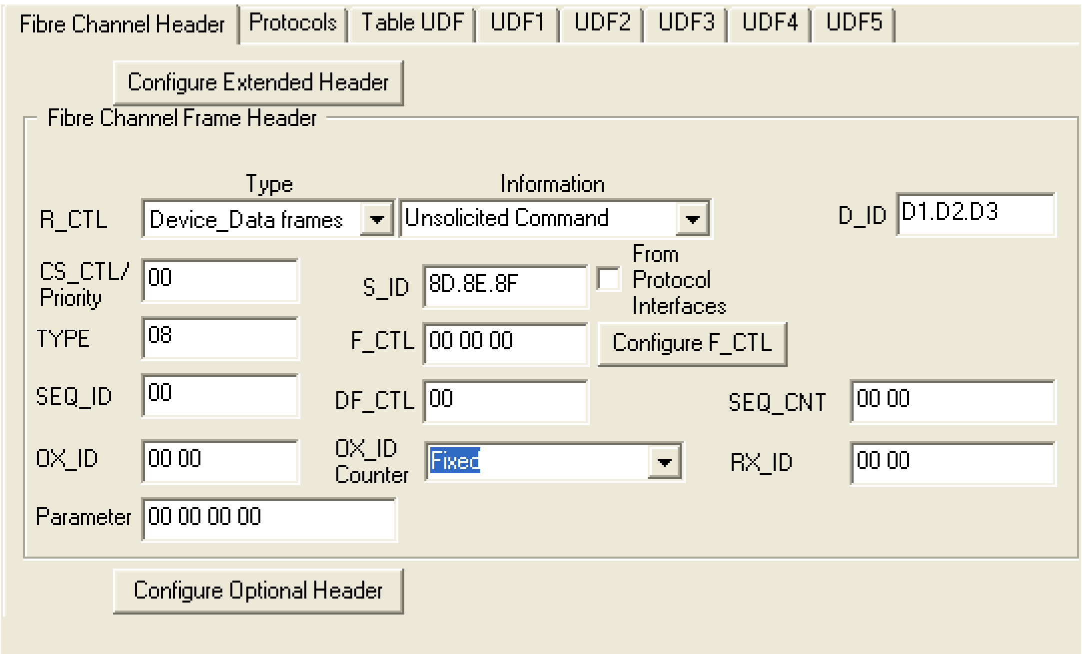
Section	Field/Control	Description
		or Fx_Port. The receiving Nx_Port or Fx_Port may send an R_RDY.
	EOF	The End-of-Frame (EOF) delimiter is an Ordered Set that immediately follows the CRC. The EOF delimiter designates the end of the frame content. All frames other than the last frame of a Sequence is terminated with an EOFn delimiter. The multiple EOF delimiters defined for Sequence control are as follows: • EOFn - Normal: The EOFn identifies the end of frame when one of the other EOF delimiters indicating valid frame content is not required. • EOFt - Terminate: The EOFt indicates that the Sequence associated with this SEQ_ID is complete. EOFt or EOFdt is used to properly close a Sequence without error. • EOFrt - Remove Terminate: The EOFrt removes a dedicated connection through a Fabric. The connection is removed and terminated. • EOFni - Normal Invalid: EOFni replaces an EOFn or EOFt, indicating that the frame content is invalid. • EOFrti - Remove Terminate Invalid: The EOFrti replaces a recognized EOFrt delimiter on a frame of invalid frame content. • EOFa - Abort: The EOFa terminates a partial frame due to a malfunction in a link facility during transmission.
Data Pattern		The Data Pattern feature generates data for the type of data selected. For FCM, the pattern starts at an offset value of 60. Refer *Data Pattern Box* for information.
Frame Size		Refer *Frame Size* for information.
Instrumentation		Refer *Instrumentation Box* for information.
Force Errors		Refer *Force Errors Box* for information.
Fibre Channel Header	Configure Extended Header	Click to open the *Extended Header* dialog. Refer *Extended Header* for more information.
	Fibre Channel Frame Header	Refer *Fibre Channel Header* for more information.
	Configure Optional Header	Click to open the *Optional Header* dialog. Refer *Optional Header* for more information.

Fibre Channel Header

The smallest unit of data transmission and routing in Fibre Channel (FC) is the frame. FC frames contain Start-of-Frame (SOF), End-of-Frame (EOF) and the contents of the Fibre Channel Frame.

The *Fibre Channel Header* tab in the FC *Frame Data* dialog is shown in *Figure:Frame Header tab*.

Figure:Frame Header tab



The fields and options present in the *Fibre Channel Header* tab are described in *Table:Frame Channel Header*.

Table:Frame Channel Header

Field/Control	Description
	Adds Extended Headers to a normal Frame Header in Fibre Channel. Click this button to open the *Extended Header* dialog. Refer to *Extended Header* for more information.
Fibre Channel Frame Header	Configures the frame header of Fibre Channel module.
R_CTL	The Routing Control (R_CTL) field is a one-byte field in Word 0 Bits 31-24. It contains routing bits and information bits to categorize the frame function. When the R_CTL field is used in combination with the TYPE field (Word 2, bits 31-24), it provides an FC_Port with assistance in frame routing, data routing, or addressing. The R_CTL field is further subdivided into the ROUTING field and the INFORMATION field.

Field/Control	Description
R_CTL Type	The R_CTL Frame Types are as follows: • Device_Data frames • Extended Link Services • FC-4 Link Data • Video_Data • Extender_Headers • Basic Link Services • Link_Control Frame • Extended Routing
R_CTL Information	The INFORMATION field is included in R_CTL to assist the receiver of a Data frame in directing the Data Field content to the appropriate buffer pool. Information categories for R_CTL Type = Device_Data or FC-4 Link_Data are as follows: • Uncategorized information • Solicited Data • Unsolicited Control • Solicited Control • Unsolicited Data • Data Descriptor • Unsolicited Command • Command Status • Reserved Information categories for R_CTL Type = Extended Link Services: • Solicited Data • Request • Reply • Reserved Information categories for R_CTL Type = Video_Data: • Unsolicited Data • Reserved Information categories for R_CTL Type = Extended Headers: • Virtual Fabric Tagging Head • Inter-Fabric Routing Header • Encapsulation Header

Field/Control	Description
	• Reserved Information categories for R_CTL Type = Basic Link Services: • No Operation • Abort Sequence • Remove Connection • Basic_Accept • Basic_Reject • Dedicated Connection Preempted • Reserved
R_CTL Information (continued)	Information categories for R_CTL Type = Link Control Frame: • Acknowledge_1 • Acknowledge_0 • Nx_Port Reject • Fabric Reject • Nx_Port Busy • Fabric Busy to Data Frame • Fabric Busy to Link_Control Frame • Link Credit Reset • Notify • End • Reserved Information categories for R_CTL Type = Extended Routing: • Vendor Unique • Reserved
D_ID	The Destination ID (D_ID) is a three-byte field (Word 0, Bits 23-0) that contains the address identifier of the destination Nx_Port.
CS_CTL/Priority	CS_CTL field is controlled by the CS_CTL/Priority Enable bit (F_CTL, bit 17). When the CS_CTL/Priority Enable bit is set to zero and word 1, bits 31-24 are interpreted to be CS_CTL information. When the CS_CTL/Priority Enable bit is set to one and word 1, bits 31-24 is interpreted to be Priority information. When bit 17 of F_CTL is set to zero and Word 1, bits 31-24 of the Frame_Header is defined as

Field/Control	Description
	the CS_CTL field. It contains management information for the class of service identified by the SOF. The meaning of the CS_CTL field is dependent on the class of service. The class of service are Class 1, Class 2, and Class 3 as shown in the following sections:

CS_CTL field-Class 1:

Bit	Abbr.	Meaning
31	Simplex - obsolete	Reserved
30	Stacked Connect-request	0 = Stacked Connect-request not requested 1 = Stacked Connect-request requested
29	COR - obsolete	Reserved
28	BCR - obsolete	Reserved
27-24		Reserved

CS_CTL field-Class 2:

Bits	Abbr.	Meaning
31	PREF	0 = Frame is delivered with no Preference 1 = Frame may be delivered with Preference
30		Reserved for additional Preference function
29-24	DSCP	Differentiated Services Code Point

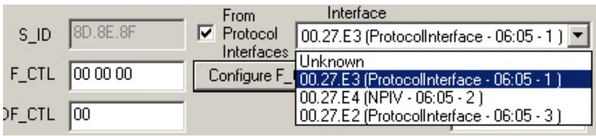
CS_CTL field-Class 3:

Bit	Abbr.	Meaning
31	PREF	0 = Frame is delivered with no Preference 1 = Frame may be delivered with Preference
30		Reserved for additional Preference function
29-24	DSCP	Differentiated Services Code Point

Field/Control	Description
TYPE	The data structure type is a one-byte field that identifies the protocol of the frame content for Data frames. When R_CTL = Basic or Extended Link_Data, the TYPE value is as follows: • 00 = Basic Link Service • 01 = Extended Link Service • 01 to CF = Reserved • D0 to FF = Vendor Specific When R_CTL = Video_Data, the TYPE value is as follows: • 02 to 5F = Reserved

Field/Control	Description
	• 60 = FC-AV Container • 61 = ARINC 818 • 62 to 63 = Reserved for FC-AV • 64 to CF = Reserved • D0 to FF = Vendor Specific When R_CTL = Device_Data and Link_Data, the TYPE value is as follows: • 00 to 03 = Reserved • 04 = Obsolete • 05 = IPv4, IPv6, and ARP over Fibre Channel • 06 to 07 = Reserved • 08 = Fibre Channel Protocol • 09 = Obsolete • 0A to 0F = Reserved - SCSI • 10 = Reserved • 11 to 13 = Obsolete • 14 = Fibre Channel SATA Tunnelling Protocol
SEQ_ID	The Sequence ID (SEQ_ID) is a one-byte field (Word 3, Bits 31-24) assigned by the Sequence Initiator. It is unique for a specific D_ID and S_ID pair while the Sequence is open. It is independent of X_ID. Both the Sequence Initiator and the Sequence Recipient track the status of frames within the Sequence using fields within the Sequence_Qualifier. If its X_ID is unassigned, it uses any other field or fields (for example, S_ID, D_ID, or the other Nx_Port's X_ID) for tracking.
OX_ID	The Originator Exchange_ID (OX_ID) is a two-byte field (Word 4, Bits 31-16) that identifies the Exchange_ID assigned by the Originator of the Exchange. Each Exchange is assigned an identifier unique to the Originator or Originator-Responder pair. If the Originator enforces uniqueness through the OX_ID mechanism, it sets a unique value for OX_ID other than FF FFh in the first Data frame of the first Sequence of an Exchange. An OX_ID of FF FFh indicates that the OX_ID is unassigned and that the Originator is not enforcing uniqueness through the OX_ID mechanism. If an Originator uses the unassigned value of FF FFh to identify the Exchange, it has only one

Field/Control	Description
	Exchange (OX_ID set to FF FFh) with a given Responder.
Parameter	The Parameter field has meanings based on frame type. For Link_Control frames, the Parameter field is used to carry information specific to the individual Link_Control frame. For data frames with the relative offset present bit set to 1, the Parameter field specifies relative offset. For data frames with the relative offset Present bit set to zero, the Parameter field is set and interpreted in a protocol specific manner that may depend on the type of Information Unit carried by the frame.
S_ID	Three-byte field that contains the address identifier of the source Nx_Port. You can select the *From Protocol Interfaces* check box and get the value of the corresponding interface from the *Interface* list.
F_CTL	The Frame Control (F_CTL) field (Word 2, Bits 23-0) is a three-byte field that contains control information relating to the frame content. If an error in bit usage is detected, a reject frame (P_RJT) is transmitted in response with an appropriate reason code for Class 1, Class 2, and Class 6.
	Click this button to open the *FCoE F_CTL Configuration* dialog. Refer *F_CTL Configuration* for more information on the format of the F_CTL bits.
DF_CTL	Data Field Control (DF_CTL) is a one-byte field that specifies the presence of optional headers at the beginning of the Data_Field. See DF_CTL Bit Definition given as follows:
DF_CTL Bit Definition:	

<table>
<tr><th>Field/Control</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Word 3, Bit(s)</th><th>Optional Header</th><th>Applicability</th></tr>
<tr><td>23</td><td>Reserved</td><td>all frames</td></tr>
<tr><td>22</td><td>0 = Neither ESP_Header nor ESP_Trailer
1 = Both ESP_Header and ESP_Trailer</td><td>all frames</td></tr>
<tr><td>21</td><td>0 = No Network_Header
1 = Network_Header</td><td>Device_Data and Video_Data frames</td></tr>
<tr><td>20</td><td>0 = No Association_Header
1 = Association_Header</td><td>Device_Data and Video_Data frames</td></tr>
<tr><td>19-18</td><td>Reserved</td><td>all frames</td></tr>
<tr><td>17-16</td><td>00b = No Device_Header
01b = 16 Byte Device_Header
10b = 32 Byte Device_Header
11b = 64 Byte Device_Header</td><td>Device_Data and Video_Data frames</td></tr>
</table>
</td></tr>
<tr><td>OX_ID Counter</td><td>The decrement/increment options enable changing the value for the Exchange IDs through UDFs instead of manually setting different values in the streams. Options are as follows:
Fixed
Increment
Decrement
Continuous Increment
Continuous Decrement
Random</td></tr>
<tr><td>From Protocol Interfaces (check box)</td><td>Selecting this check box synchronizes the S_ID with the values set in FCoE interfaces that have been created using the Protocol Interfaces wizards. Configured and Discovered VLAN IDs are also display. When selected, choose the desired FCoE interface from the listing.


Chapter 10, Protocol Interfaces for more information.

From Protocol Interfaces also shows up on the DA/SA page. See From Protocol Interfaces Option.</td></tr>
<tr><td>SEQ_CNT</td><td>The sequence count is a two-byte field that indicates the sequential order of Data frame</td></tr>
</table>

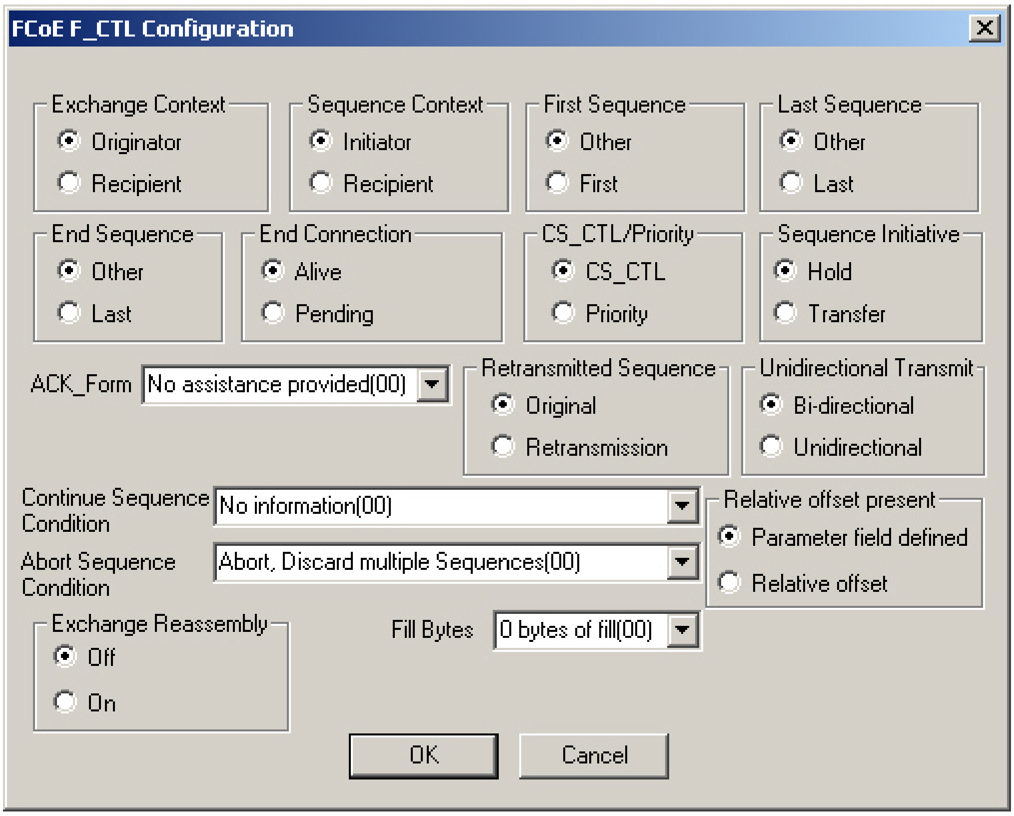
Field/Control	Description
	transmission within a single Sequence or multiple consecutive Sequences for the same Exchange. The SEQ_CNT of the first Data frame of the first Sequence of the Exchange transmitted by either the Originator or Responder is binary zero. The SEQ_CNT of each subsequent Data frame in the Sequence is incremented by one.
RX_ID	The Responder Exchange_ID is a two byte field assigned by the Responder that provides a unique, locally meaningful identifier at the Responder for an Exchange established by an Originator and identified by an OX_ID.
	Optional headers are provided for use of the FC-4 layer. Refer *Optional Header* for more information.

F_CTL Configuration

The *F_CTL Configuration* dialog consists of options to configure the format of the F_CTL bits. When a bit is designated as meaningful under a set of conditions, this bit is ignored if the corresponding set of conditions are not present. For example, bit 18 is meaningful only when bit 19 is set to one. Bit 18 is ignored unless bit 19 is set to one.

The *F_CTL Configuration* dialog is accessed by clicking  button. The dialog is shown in *Figure:F_CTL Configuration dialog*.

Figure:F_CTL Configuration dialog



Field definitions for the *F_CTL Configuration* dialog are described in *Table:F_CTL Configuration*.

Table:F_CTL Configuration

Field/Control	Description
Exchange Context	0 = Originator of exchange 1 = Recipient (responder) of exchange
Sequence Context	0 = Sequence Initiator 1 = Sequence Recipient
First Sequence	0 = Other–sequence other than first of exchange 1 = First sequence of exchange
Last Sequence	0 = Other–sequence other than last of exchange 1 = Last sequence of exchange
End Sequence	0 = Other–data frame other than last of sequence 1 = Last data frame of sequence
End Connection	0 = Alive–connection active 1 = Pending–end of connection pending
CS_CTL/Priority	0 = CS_CTL 1 = Priority
Sequence Initiative	0 = Hold sequence initiative

Field/Control	Description
	1 = Transfer sequence initiative
ACK_Form	00 = No assistance provided 01 = Ack_1 Required 10 = reserved 11 = Ack_0 Required
Retransmitted Sequence	0 = Original Sequence transmission 1 = Retransmission of sequence
Unidirectional Transmit	0 = Bi-directional transmission 1 = Unidirectional transmission
Continue Sequence Condition	Last Data frame–Sequence Initiator 00 = No information 01 = Sequence to follow-immediately 10 = Sequence to follow-soon 11 = Sequence to follow-delayed
Abort Sequence Condition	*ACK frame–(Sequence Context = Recipient)* 00 = Continue sequence 01 = Abort Sequence, Perform ABTS 10 = Stop Sequence 11 = Immediate Sequence retransmission requested *Data frame (1st of Exchange)–(Sequence Context = Initiator)* 00 = Abort, Discard multiple Sequences 01 = Abort, Discard a single Sequence 10 = Process policy with infinite buffers 11 = Discard multiple Sequences with immediate retransmission
Exchange Reassembly	Off On
Fill Bytes	End of Payload - bytes of fill (following Payload) 00 = 0 bytes of fill 01 = 1 byte of fill 10 = 2 bytes of fill 11 = 3 bytes of fill
Relative offset present	0 = Parameter field defined for some frames 1 = Relative offset

Extended Header

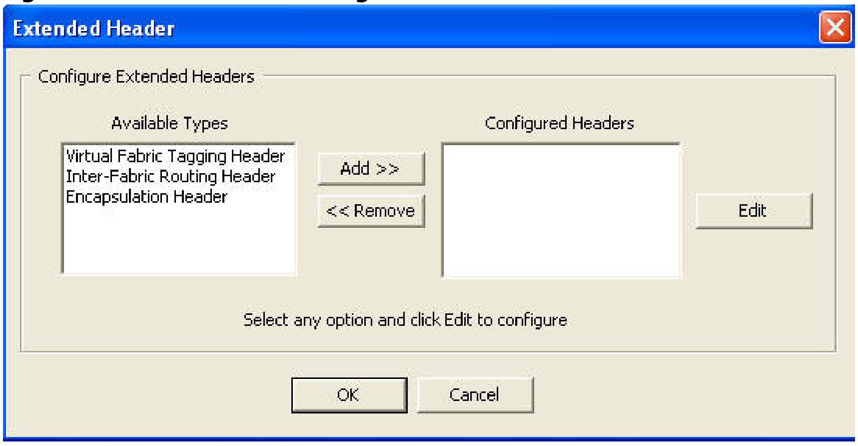
An Extended Header is a sequence of words that may be present in a frame between the SOF delimiter and the Frame_Header to support frame handling functions that are not enabled by the Frame_Header.

Extended Header, if present, immediately follows the SOF delimiter and precede the Frame Header. The presence or absence of Extended Headers in a frame does not affect the size of the Data_Field.

Extended Headers are used to extend the functionality provided by the Frame_Header. Each Extended Header, although of different length, is word aligned within the frame and has a length that is a multiple of four bytes.

Click the *Configure Extended Header* option button in the *Fibre Channel Header* tab to open the *Extended Header* dialog. The *Extended Header* dialog is shown in *Figure:Extended Header Dialog*.

Figure:Extended Header Dialog



To configure a extended header, do the following:

1. Select the type of header from *Available Types* box.
2. Click the *Add* button to shift the selected header type to *Configured Header* box.

   The selected header shifts to the *Configured Header* box.
3. Select the header type in the *Configured Header* box and click the *Edit* button.

The selected header opens in the edit mode in a separate dialog where additional packet details are available for the specific type of extender header.

The fields in the *Extended Header* dialog are described in *Table:Extended Header dialog*

Table:Extended Header dialog

Field/Control	Description
Available Types	The types of Extended Headers, one of the following: • Virtual Fabric Tagging Header (VFT_Header) • Inter-Fabric Routing Extended Header (IFR_ Header) • Encapsulation Header The specific values for each extended header in the R_

Field/Control	Description
	CTL field that determine the header length, are shown as follows:

Extended Header Types:

R_CTL	Description	Extended_Header Length
50h	VFT_Header (Virtual Fabric Tagging Header, see 10.2)	8 bytes
51h	IFR_Header (Inter-Fabric Routing Header, see 10.3)	8 bytes
52h	Enc_Header (Encapsulation Header, see 10.4)	24 bytes
53h .. 5Fh	Reserved	—

Field/Control	Description
Add >>	Click this button to add the selected type of extended header to the *Configured Headers* box.
<< Remove	Click this button to remove an already added extended header type from the *Configured Headers* box.
Configured Headers	Displays the types of extended header selected for configuration.
Edit	Opens the selected extended header in edit mode in a separate dialog where additional packet details are available for the specific type of extender header.
OK	Click *OK* after configuring the extended header to complete the process.
Cancel	Click *Cancel* to exit from the operation.

The types of extended headers are as follows:

- *Virtual Fabric Tagging Header (VFT Header)*
- *Inter Fabric Routing Header (IFR)*
- *Encapsulation Header (ENC)*

Virtual Fabric Tagging Header (VFT Header)

The Virtual Fabric Tagging Header (VFT Header) allows Fibre Channel frames to be tagged with the Virtual Fabric Identifier (VF_ID) of the Virtual Fabric to which they belong. Tagged frames, that is frames with a VFT_Header, belonging to different Virtual Fabrics may be transmitted over the same physical link.

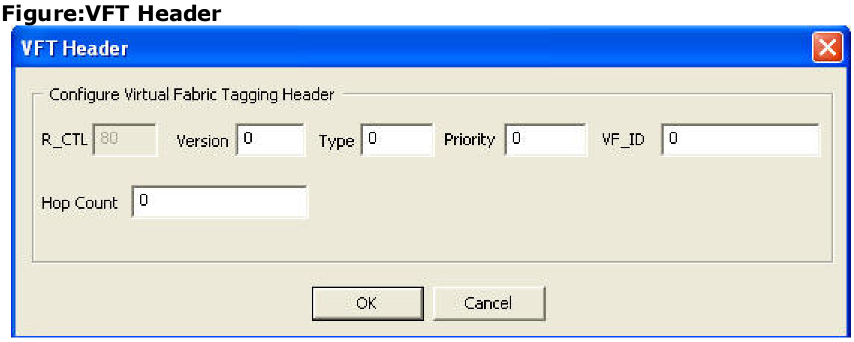
The VFT Header Format is shown in *Figure:VFT Header Format*.

Figure:VFT Header Format

Bits Word	31 .. 24	23	22	21 .. 18	17	16	15 .. 13	12 .. 01	0
0	R_CTL	Ver		Type	R	R	Priority	VF_ID	R
1	HopCt	Reserved							

The *VFT Header* dialog is shown in *Figure:VFT Header*.

Figure:VFT Header



The fields in this dialog are described in *Table:VFT Header Dialog*.

Table:VFT Header Dialog

Field/Control	Description
R_CTL	The R_CTL field is a one-byte field that contains routing bits and information bits to categorize the frame function. The R_CTL is set to the value 50h to identify the VFT Extended Header.
Version	Specifies the version of the VFT Header. Default is 0.
Type	Specifies the kind of tagged frame. To use with Fibre Channel, type is set to 0h. The use of other values is beyond the scope of this standard. No device sends a VFT tagged frame with a Type value in the VFT_Header other than 0h. A device receiving a VFT tagged frame with a Type value in the VFT_Header having a non-zero value discards the frame.
Priority	The Class Specific Priority of the VFT header. When set to zero, it is interpreted to contain management information for the class of service.
VF_ID	The ID of the VFT header. It specifies the Virtual Fabric Identifier of the Virtual Fabric to which the tagged frame belongs. The values are shown as follows:

VFT_ID Values:

Value	Description
000h	Shall not be used as Virtual Fabric Identifier
001h .. EFFh	Available as Virtual Fabric Identifiers
F00h .. FEEh	Reserved
FEFh	Control VF_ID (see FC-LS and FC-SW-4)
FF0h .. FFEh	Vendor Specific
FFFh	Shall not be used as Virtual Fabric Identifier

Field/Control	Description
Hop Count	The count by which the VFT header packet is forwarded in the stream. It specifies the number of

Field/Control	Description
	remaining hops that are traversed before the frame is discarded. A value of 00h indicates that the frame is not discarded due to number of hops traversed. A Switch receiving a VFT tagged frame with HopCt = 01h discards the frame. Each Switch, on forwarding a VFT tagged frame, decrements the HopCt by one. The default initial value for the HopCt field is 16 and it is configured for each tagging port. If a frame passes from a tagging link to a second tagging link through one or more non tagging links, the HopCt value is reset to the initial value configured for the egress FC_Port attached to the second tagging link upon egress onto the second tagging link.

Inter Fabric Routing Header (IFR)

The Inter-Fabric Routing Extended Header (IFR_Header) provides the necessary information to support fabric-to-fabric routing. The information includes the following:

- The fabric identifier of the destination fabric (DF_ID)
- The fabric identifier of the source fabric (SF_ID)
- Information appropriate to determine the expiration time or hop count

The IFR_Header is used at every Inter-Fabric Router to route the frame toward the destination fabric.

The IFR Header Format is shown in *Figure:IFR Header Format*.

Figure:IFR Header Format

Bits / Word	31 .. 30	29 .. 27	26	25	24	23 .. 20	19 .. 8	7 .. 4	3 .. 0
0	R_CTL = 51h					R	DF_ID	Exp_Time	
1	Ver	Pri	R	etv	hcv	R	SF_ID	R	Hop_Cnt

The **IFR Header** dialog box is shown in *Figure:IFR Header*.

Figure:IFR Header

Bits / Word	31 .. 30	29 .. 27	26	25	24	23 .. 20	19 .. 8	7 .. 4	3 .. 0
0	R_CTL = 51h					R	DF_ID	Exp_Time	
1	Ver	Pri	R	etv	hcv	R	SF_ID	R	Hop_Cnt

The fields in this dialog box are described in *Table:IFR Header dialog*.

Table:IFR Header dialog

Field/Control	Description
R_CTL	The R_CTL field is a one-byte field that contains routing bits and information bits to categorize the frame function. This field is set to the value 51h to identify the IFR_ Header.
DF_ID	The Destination Fabric Identifier (DF_ID) field is set as spe-

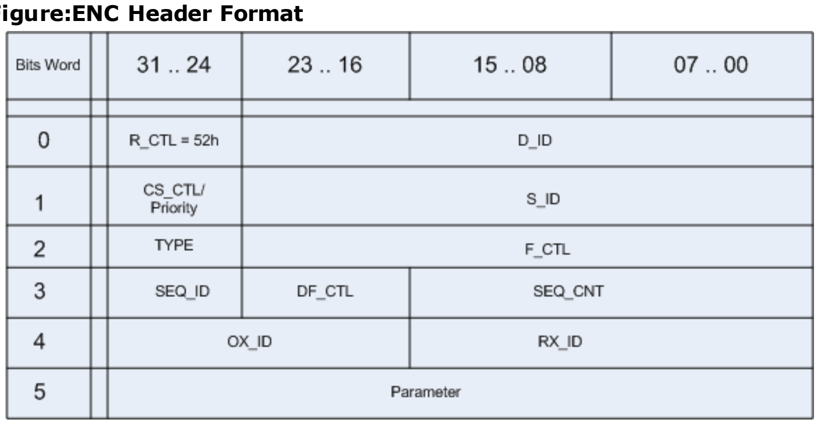
Field/Control	Description
	cified in FC-IFR.
Version	Specifies the version of the IFR_Header. This field is set to a default value of 00b.
Priority	Specifies the Quality of Service (QoS) value for the frame. When set to zero, is interpreted to contain management information for the class of service.
Expiration Time Valid	If EXP_Time field is valid, Expiry Time Valid bit is set to one. If EXP_Time field is invalid, Expiry Time Valid bit is set to zero.
Hop Count Valid	If Hop Count field is valid, Hop Count Valid bit is set to one. If Hop Count field is invalid, Hop Count Valid bit is set to zero.
SF_ID	The Source Fabric Identifier (SF_ID) field is set as specified in FC-IFR.
Hop Count	The count by which the VFT header packet is forwarded in the stream. If the Hop Count Valid (HCV) bit is set to one, the Hop Count (Hop_Cnt) field specifies the number of hops remaining before the frame is discarded.
EXP_Time	If the Expiration Time Valid (ETV) bit is set to one, the Expiration Time (Exp_Time) field is used by Inter-Fabric Routers to enforce frame lifetime requirements across the Inter-Fabric.

Encapsulation Header (ENC)

The Encapsulation Extended Header (ENC Header) is used to transmit frames between Inter-Fabric Routers when connected through an FC-SW-3 or FC-SW-4 compliant fabric. To preserve backward compatibility, the Inter-Fabric Routers appear as N_Ports to the FC-SW-3 or FC-SW-4 compliant Fabric.

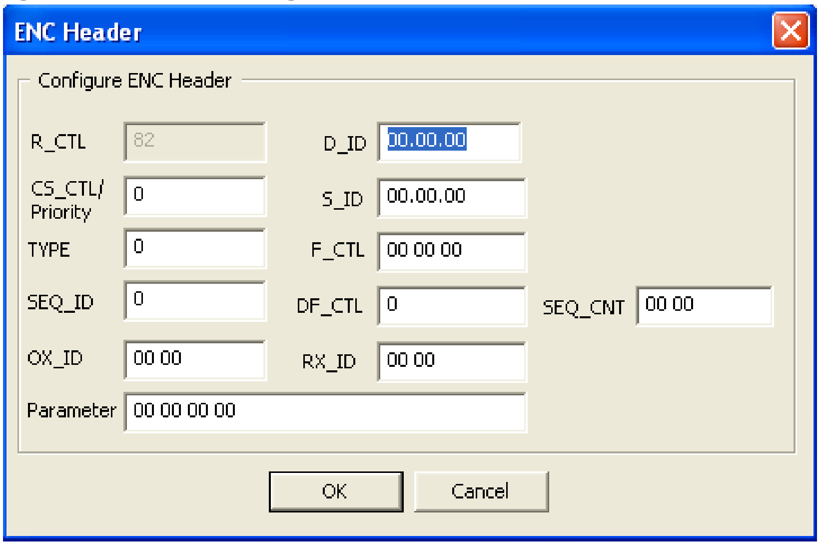
The ENC Header Format is shown in *Figure:ENC Header Format*.

Figure:ENC Header Format



The *ENC Header* dialog is shown in *Figure:ENC Header dialog*.

Figure:ENC Header dialog



The fields in this dialog are described in *Table:ENC Header dialog*.

Table:ENC Header dialog

Field/Control	Description
R_CTL	The R_CTL field is a one-byte field that contains routing bits and information bits to categorize the frame function. This field is set to the value 52h to identify the IFR_ Header.
CS_CTL/Priority	CS_CTL field is controlled by the CS_CTL/Priority Enable bit (F_CTL, bit 17).
TYPE	The data structure type is a one-byte field that identifies the protocol of the frame content for Data frames.
SEQ_ID	The Sequence ID (SEQ_ID) is a one-byte field (Word 3, Bits 31-24) assigned by the Sequence Initiator.
OX_ID	The Originator Exchange_ID (OX_ID) is a two-byte field (Word 4, Bits 31-16) that identifies the Exchange_ID assigned by the Originator of the Exchange.
Parameter	The Parameter field has meanings based on frame type. For Link_Control frames, the Parameter field is used to carry information specific to the individual Link_Control frame. For Data frames with the relative offset present bit set to 1, the Parameter field specifies relative offset. For Data frames with the relative offset Present bit set to zero, the Parameter field is set and interpreted in a protocol specific manner that may depend on the type of Information Unit carried by the frame.
D_ID	The Destination ID (D_ID) is a three-byte field (Word 0, Bits 23-0) that contains the address identifier of the destination Nx_Port.
S_ID	The Source ID (S_ID) is a three-byte field that contains

Field/Control	Description
	the address identifier of the source Nx_Port.
F_CTL	The Frame Control (F_CTL) field (Word 2, Bits 23-0) is a three-byte field that contains control information relating to the frame content. If an error in bit usage is detected, a reject frame (P_RJT) is transmitted in response with an appropriate reason code for Class 1, Class 2, and Class 6.
DF_CTL	Data Field Control (DF_CTL) is a one-byte field that specifies the presence of optional headers at the beginning of the Data_Field.
SEQ_CNT	The Sequence Count is a two-byte field that indicates the sequential order of Data frame transmission within a single Sequence or multiple consecutive Sequences for the same Exchange. The SEQ_CNT of the first Data frame of the first Sequence of the Exchange transmitted by either the Originator or Responder is binary zero. The SEQ_CNT of each subsequent Data frame in the Sequence is incremented by one.
RX_ID	The Responder Exchange_ID is a two byte field assigned by the Responder that provides a unique, locally meaningful identifier at the Responder for an Exchange established by an Originator and identified by an OX_ID.

Optional Header

Optional headers are provided for use of the FC-4 layer. The use of the optional headers is not defined by this standard.

Optional headers, defined within the Data Field of a frame, are of the following types:

- *Encapsulating Security Payload (ESP)*
- *Network Header*
- *Association Header*

Control bits in the DF_CTL field of the Frame_Header define the presence of optional headers. The sum of the length in bytes of the Payload, the number of fill bytes, and the lengths in bytes of all optional headers shall not exceed 2 112.

The sequential order of the optional headers, Payload, and their sizes are shown in *Figure:Frame Structure without ESP Header* and *Figure:Frame Structure with ESP Header*.*Figure:Frame Structure without ESP Header* shows the frame structure without adding the ESP header.

Figure:Frame Structure without ESP Header

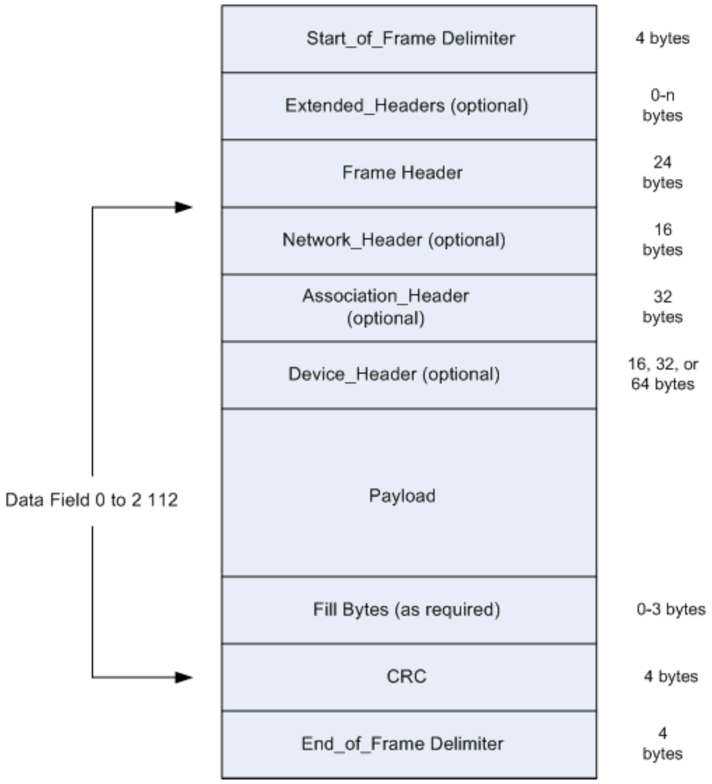
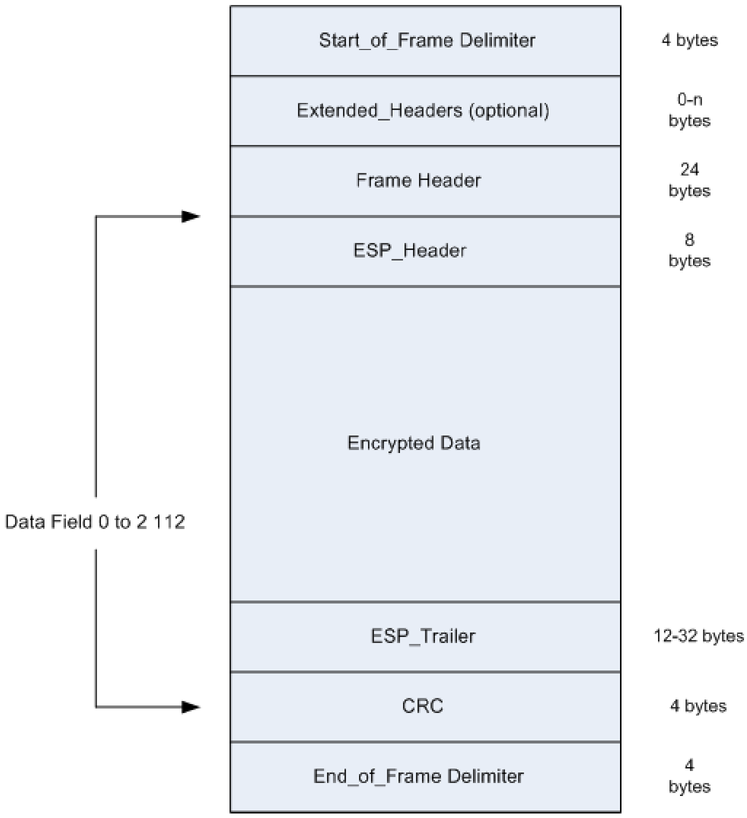


Figure:Frame Structure with ESP Header shows the frame structure with the ESP header.

Figure:Frame Structure with ESP Header

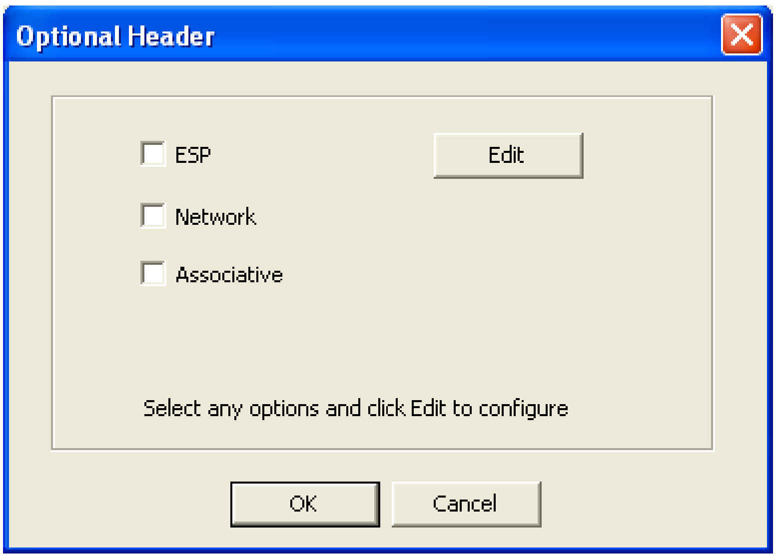


To open the *Optional Header* dialog, click Configure Optional Header button. The *Optional Header* dialog opens, allowing you to select between ESP, Network, and Associative headers. One or more headers can be selected.

NOTE Since more than one optional headers are allowed to select, the Edit menu has separate tabs for each of the optional headers.

The Optional Header dialog is shown in *Figure:Optional Header dialog*.

Figure:Optional Header dialog



The fields in this dialog are described in *Table:Optional Header dialog*.

Table:Optional Header dialog

Field/Control	Description
ESP (check box)	If selected, allows to configure Encapsulating Security Payload (ESP) in the Edit menu. Refer *Encapsulating Security Payload (ESP)* for more information.
Network (check box)	If selected, allows to configure Network header in the Edit menu. Refer *Network Header* for more information.
Associative (check box)	If selected, allows to configure Associative header in the Edit menu. Refer *Association Header* for more information.
	Click this button to open the selected optional header in the edit mode to configure the header.

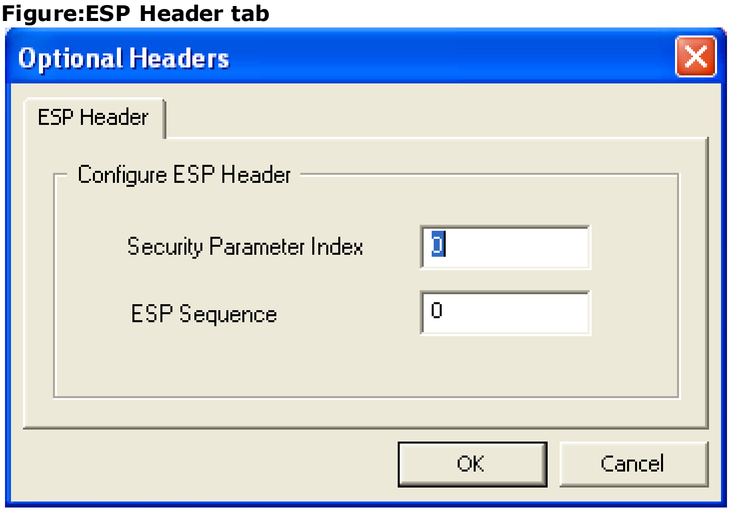
Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) is a generic mechanism to provide confidentiality, data origin authentication, and anti-replay protection to IP packets. ESP is applied to Fibre Channel frames in transport mode.

To open the *ESP Header* tab, select the *ESP* check box in the *Optional Header* dialog and then click the 

button. The *ESP Header* tab opens, as shown in *Figure:ESP Header tab*.

Figure:ESP Header tab



The fields in this tab are described in *Table:ESP Header tab*.

Table:ESP Header tab

Field/Control	Description
Security Parameter Index (SPI)	It is a 32-bit value that is used by a receiver to identify the source address to which an incoming packet is bound. The SPI field is mandatory in an ESP header.

Field/Control	Description
ESP Sequence	It is an unsigned 32-bit field that contains a counter value that increases by one for each packet sent, as per the source address packet sequence number.

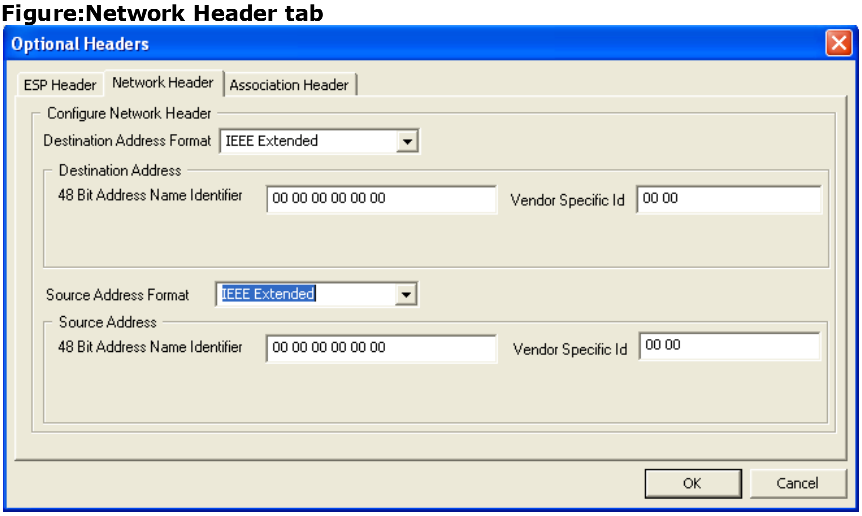
Network Header

The Network Header is an optional header within the Data_Field content. Its presence is indicated by bit 21 in the DF_CTL field being set to one. The Network Header may be used for routing between Fibre Channel networks of different Fabric address spaces, or Fibre Channel and non-Fibre Channel networks. The Network Header contains Name Identifiers for Network Destination Address and Network Source Address.

To open the *Network Header* tab, select the *Network* check box in the *Optional Header* dialog and then click the 

button. The *Network Header* tab opens, as shown in *Figure:Network Header tab*.

Figure:Network Header tab



The fields in this tab are described in *Table:Network Header tab*.

Table:Network Header tab

Field/Control	Description
Destination Address Format	It indicates the format of the Name Identifier used for the network destination address. The format options are as follows: • IEEE 48 Bit Address • IEEE Extended • Locally Assigned • IEEE Registered • IEEE Registered Extended • EU164 Mapped See *Name Identifier Formats* for a description of the Name Identifier formats.
Destination Address	Contains the Name Identifiers depending on the des-

Field/Control	Description
	tination address format selected.
48 Bit Address Name Identifier	The 48 bit address name identifier when the destination address format is IEEE 48 Bit Address.
Vendor Specific Id	The vendor specific identifier that is mapped with the address format. It is present only when destination address format is IEEE Extended.
Locally Administered Value	The locally administered value that is present only when destination address format is Locally Assigned.
IEEE Company Id	The IEEE Company Identifier that is present only when destination address format is IEEE Registered.
Vendor Specific Id Extension	The vendor specific identifier extension that is present only when destination address format is IEEE Registered Extended.
Source Address Format	It indicates the format of the Name Identifier used for the network source address. The format options are as follows: • IEEE 48 Bit Address • IEEE Extended • Locally Assigned • IEEE Registered • IEEE Registered Extended • EU164 Mapped See *Name Identifier Formats* for a description of the Name Identifier formats.
Source Address	Contains the Name Identifiers depending on the source address format selected.
48 Bit Address Name Identifier	The 48 bit address name identifier when the source address format is IEEE 48 Bit Address.
Vendor Specific Id	The vendor specific identifier that is mapped with the address format. It is present only when source address format is IEEE Extended.
Locally Administered Value	The locally administered value that is present only when source address format is Locally Assigned.
IEEE Company Id	The IEEE Company Identifier that is present only when source address format is IEEE Registered.
Vendor Specific Id Extension	The vendor specific identifier extension that is present only when source address format is IEEE Registered Extended.

Name Identifier Formats

Name Identifiers are used to identify entities in Fibre Channel such as N_Port, Node, F_Port, Fabric, or other Fibre Channel objects. The Name Identifier for an entity is unique within the Fibre Channel interaction space.

The list of supported Name Identifier formats in Fibre Channel are given in *Table:Name Identifiers*

Table:Name Identifiers

Words 0, bits 31–28	Name Identifier	Length
0h	Name not present	-
1h	*IEEE 48-bit Address*	64
2h	*IEEE Extended*	64
3h	*Locally Assigned*	64
4h	Obsolete	64
5h	*IEEE Registered*	64
6h	*IEEE Registered Extended*	128
7h to Bh	Reserved	-
Ch	*EUI64 Mapped*	64
Dh	EUI-64 Mapped	64
Eh	EUI-64 Mapped	64
Fh	EUI-64 Mapped	64

IEEE 48-bit Address

When the Name_Identifier format is IEEE 48-bit Address, the name value field contains a 48-bit IEEE Standard 802.1A Universal LAN MAC Address (ULA). The ULA is represented as an ordered string of six bytes numbered from 0 to 5. ULA Bytes 0, 1, and 2 are generated using the IEEE Company_ID.

Figure:IEEE 48-bit Address Name Identifier shows how the bytes of an ULA are mapped to two words in the IEEE 48-bit Address Name Identifier.

Figure:IEEE 48-bit Address Name Identifier

Bits Word	31 .. 28	27 .. 24	23 .. 16	15 .. 10	9	8	07 .. 00
0	1h	0 00h		ULA Byte 0	U/ L	I/ G	ULA Byte 1
1	ULA Byte 2		ULA Byte 3	ULA Byte 4			ULA Byte 5

IEEE Extended

When the Name_Identifier format is IEEE Extended, the name value field contains the 48-bit IEEE address preceded by a 12 bit value. The 12 bit value is an extension to the company assigned address portion of the 48-bit address that forms a unique 60-bit value. The 48-bit IEEE address is defined same as for the IEEE 48-bit Address Name_Identifier format.

Figure:IEEE Extended Name Identifier shows the IEEE Extended Name Identifier format.

Figure:IEEE Extended Name Identifier

Bits Word	31 .. 28	27 .. 24	23 .. 16	15 .. 10	9	8	07 .. 00
0	2h	Vendor Specific		ULA Byte 0	U/ L	I/ G	ULA Byte 1
1	ULA Byte 2		ULA Byte 3	ULA Byte 4			ULA Byte 5

Locally Assigned

When the Name_Identifier format is locally assigned, the name value field is assigned in a manner determined by the administration of the Fabric in which it is assigned. A locally assigned Name_Identifier is unique within the Fibre Channel interaction space wherein it is assigned.

Figure:Locally Assigned Name Identifier shows the Locally Assigned Name Identifier format.

Figure:Locally Assigned Name Identifier

Bits Word	31 .. 28	27 .. 24	23 .. 16	15 .. 08	07 .. 00
0	3h	Locally administered value			
1	Locally administered value				

IEEE Registered

When the Name_Identifier format is IEEE Registered, the name value field contains the 24-bit IEEE Company_ID in canonical form, as specified by IEEE, followed by a 36-bit unique Vendor Specified Identifier (VSID).

Figure:IEEE Registered Name Identifier shows the IEEE Registered Name Identifier format.

Figure:IEEE Registered Name Identifier

Bits Word	31 .. 28	27 .. 24	23 .. 16	15 .. 8	07 .. 04	03 .. 00
0	5h	IEEE Company_ID				VSID (35-32)
1	VSID (31-0)					

IEEE Registered Extended

When the Name_Identifier format is IEEE Registered Extended, the name value field contains the 24-bit IEEE Company_ID in canonical form, as specified by IEEE, followed by a 36-bit unique vendor specified id (VSID). Name_Identifiers that identify Fibre Channel Nodes or FC_Ports are limited to 64 bits and therefore shall not use the IEEE Registered Extended format.

Figure:IEEE Registered Extended Name Identifier shows the IEEE Registered Extended Name Identifier format.

Figure:IEEE Registered Extended Name Identifier

Bits Word	31 .. 28	27 .. 24	23 .. 16	15 .. 8	07 .. 04	03 .. 00
0	5h	IEEE Company_ID				VSID (35-32)
1	VSID (31-0)					

EUI64 Mapped

When the Name_Identifier format is EUI64 Mapped, The NAA field contains either 0Ch, 0Dh, 0Eh, or 0Fh. The name value field contains a modified 22-bit IEEE Company_ID, followed by a 40-bit unique VSID.

Figure:EUI64 Mapped Name Identifier shows the EUI64 Mapped Name Identifier format.

Figure:EUI64 Mapped Name Identifier

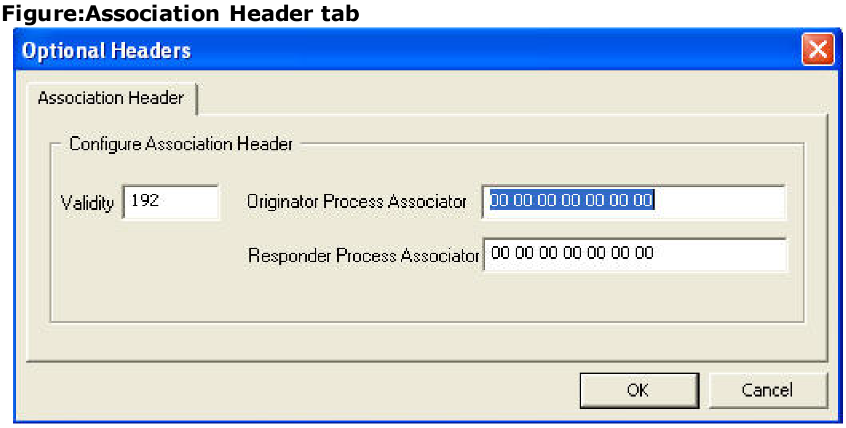
Bits / Word	31...30	29...24	23...16	15...8	7...0
0	11b	IEEE Company_ID (modified)			VSID (39-32)
1	VSID (31-0)				

Association Header

The Association Header is an optional header within the Data Field content. Its presence is indicated by bit 20 in the DF_CTL field, located in the Frame Header, being set to one. The Association Header is 32-bytes in size. The Association Header is used to identify a specific process or group of Processes within a node associated with an Exchange.

To open the *Association Header* tab, select the *Associative* check box in the *Optional Header* dialog and then click the Edit button. The *Association Header* tab opens, as shown in *Figure:Association Header tab*.

Figure:Association Header tab



The fields in this tab are described in *Table:Association Header tab*.

Table:Association Header tab

Field/Control	Description
Validity	Denotes the validity of the Association Header.
Originator Process Associator	It is a value used in the Association Header to identify an originator process or a group of processes within a node.
Responder Process Associator	It is a value used in the Association Header to identify a responder process or a group of processes within a node.

Frame Data for Flex

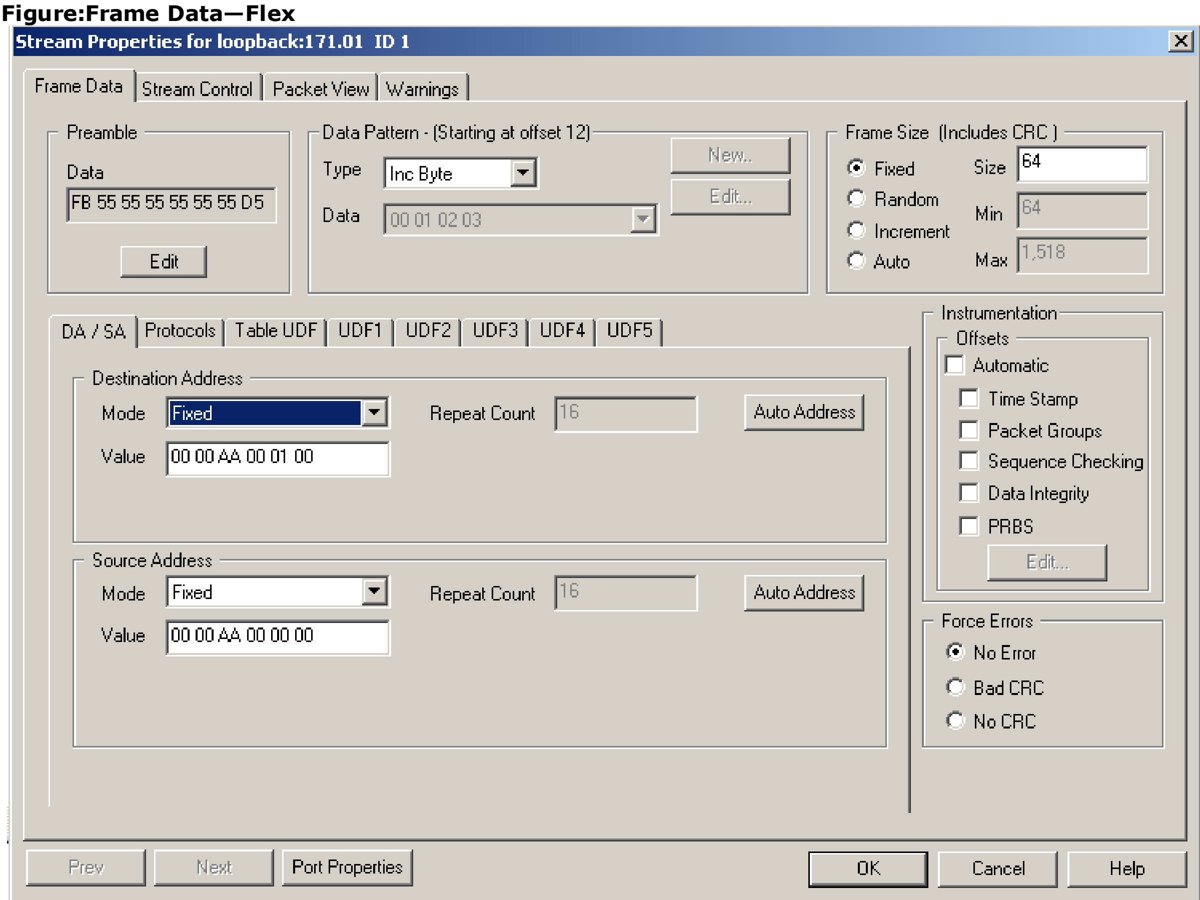
The Xcellon architecture features aggregation of multi-core CPUs and massive memory to meet testing needs for ultra-high scale and performance.

The Stream Properties for the Flex load module are set in the Frame Data and Stream Control tabs.

To access the Frame Data tab, double-click in a stream/flow entry in the Packet Streams/Packet Flows/Advanced Streams window, then select the Frame Data tab. Alternatively, right-click a port in the Resources window, and select Edit Streams from the displayed menu.

The Frame Data tab for Flex load modules is shown in *Figure:Frame Data—Flex*.

Figure:Frame Data—Flex



The options and controls in this tab are mentioned in *Table:Frame Data tab—Flex*.

Table:Frame Data tab—Flex

Field/Control	Description
Preamble	*The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see Ixia Platform Reference Manual. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count value displayed in the field includes the SFD.* for more information.
Data Pattern	See *Data Pattern Box* for more information.
Frame Size	See *Frame Size* for more information.
Instrumentation Offsets	See *Instrumentation Box* for more information.
Force Errors	See *Force Errors Box* for more information.
DA/SA	See *DA/SA Property Sheet* for more information.
Protocols	See Data Link Layer Protocols Control for more information.
Table UDF	See Chapter 7, Frame Data–User Defined Fields (UDF) for more information.

Frame Data for XDM10G32S

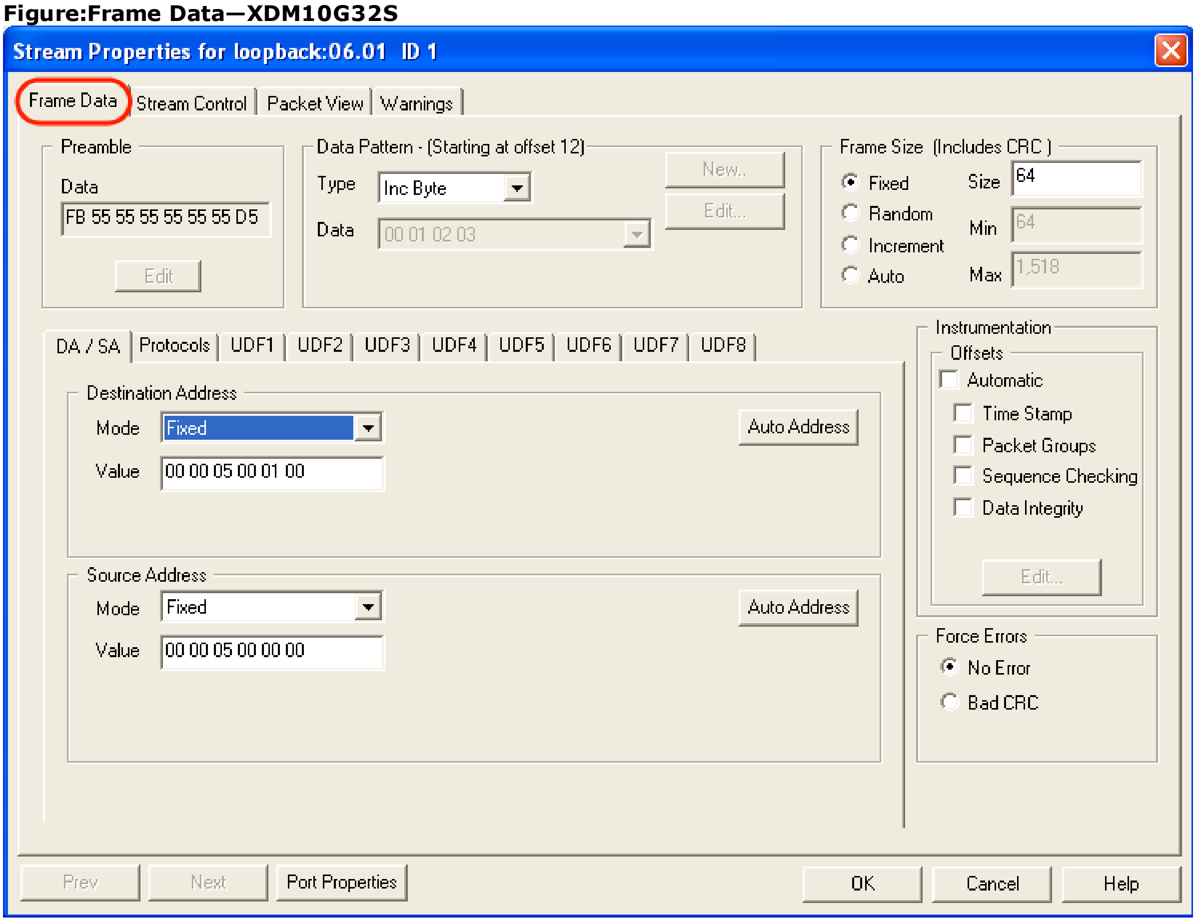
XDM10G32S is a 32 port load module with 10GE density per port. Each slot in this load module consists of 32 ports that can scale up to 384 ports in a single XM12 chassis. The high scalability feature of Xdensity load module provides test solutions for high density 10GE converged data center switches and routers.

The Stream Properties for the XDM10G32S load module are set in the Frame Data and Stream Control tabs.

To access the Frame Data tab, double-click in a stream/flow entry in the Advanced Streams window, then select the Frame Data tab. Alternatively, right-click a port in the Resources window, and select Edit Streams from the displayed menu.

The Frame Data tab for XDM10G32S load modules is shown in the following figure:

Figure:Frame Data—XDM10G32S



The options and controls in this tab are mentioned in the following table:

Table:Frame Data tab—XDM10G32S

Field/Control	Description
Preamble	*The Preamble is a variable number of bytes of data, where each byte has an identical value of 0xAA. The preamble size range varies between cards, see Ixia Platform Reference Manual. The preamble contents is always a string of 0xAA bytes and is terminated by a SFD (Start Frame Descriptor) with a value of 0xAD. The Preamble Size count*

Field/Control	Description
	value displayed in the field includes the SFD. for more information.
Data Pattern	XDM10G32S supports Increment (word/byte), Decrement (word/byte), and Random as Data Pattern types. See *Data Pattern Box* for more information.
Frame Size	XDM10G32S only supports Uniform Distribution of Weighted Random Frame Size. See *Frame Size* and *Weighted Random Frame Size—Uniform Distribution* for more information.
Instrumentation Offsets	The **Automatic** check box is immediately selected when any of the options in the Instrumentation Offsets pane is selected. This is because XDM10G32S supports only Floating Timestamp. See *Instrumentation Box* for more information.
Force Errors	See *Force Errors Box* for more information.
DA/SA	XDM10G32S only supports Fixed DA/SA mode. See *DA/SA Property Sheet* for more information.
Protocols	See Data Link Layer Protocols Control for more information.
UDF	XDM10G32S supports up to 8 UDFs. See Chapter 7,Frame Data–User Defined Fields (UDF) for more information.

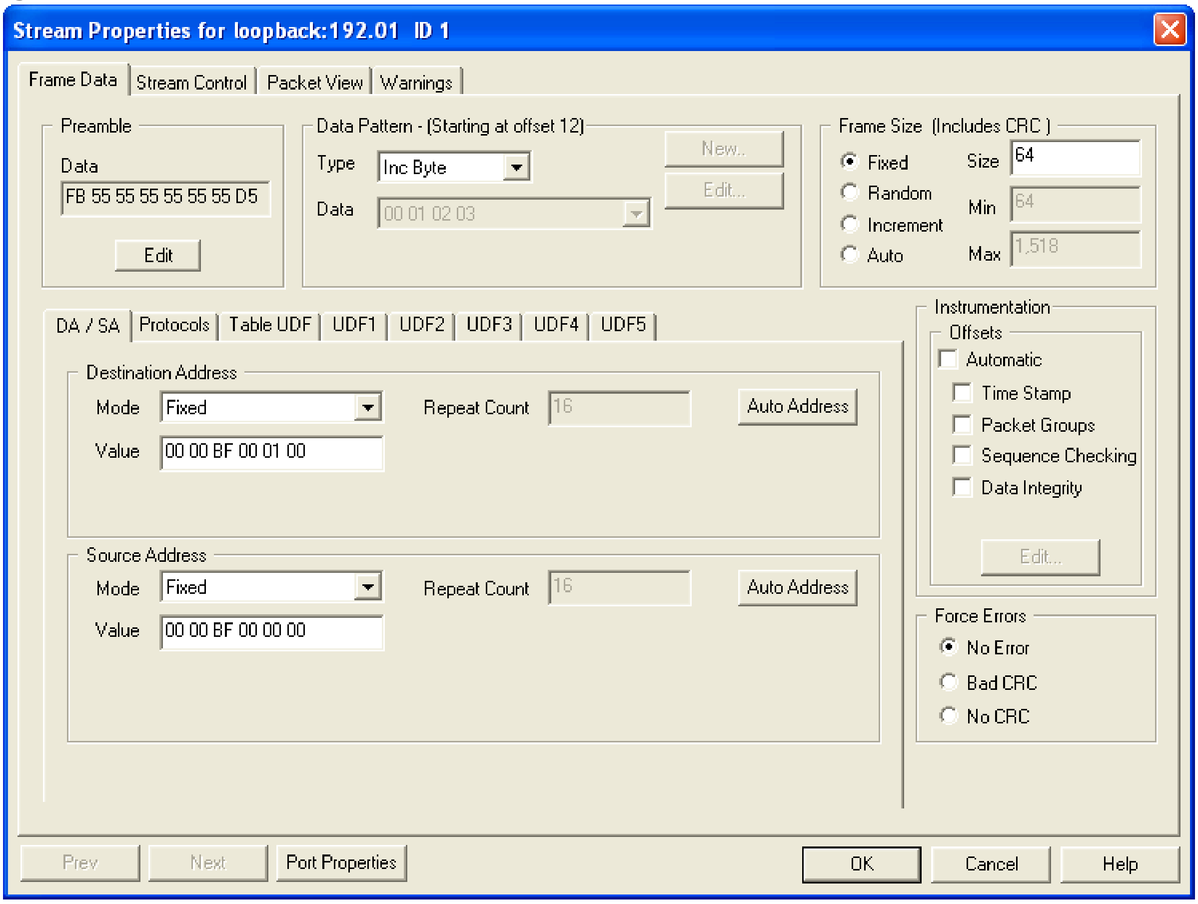
Frame Data for Lava 40GE/100GE

The Stream Properties for the Lava load module are set in the Frame Data and Stream Control tabs.

To access the Frame Data tab, double-click in a stream/flow entry in the Packet Streams/Packet Flows/Advanced Streams window, then select the Frame Data tab. Alternatively, right-click a port in the Resources window, and select Edit Streams from the displayed menu.

The Frame Data tab for Lava AP40/100GE is shown as follows:

Figure:Frame Data for Lava



The options and controls in this tab are mentioned in the following table:

Table:Frame Data tab—Lava

Field/Control	Description
Preamble	See *Lava AP40/100 GE— Preamble* for more information.
Data Pattern	Lava supports Increment (word/byte), Decrement (word/-byte), Random, Repeating, Fixed, CJPAT and CRPAT as Data Pattern types. See *Data Pattern Box* for more information.
Frame Size	Lava supports Fixed, Random, Increment and Auto Frame Size. Under Random it supports Uniform, Weight, Pre-defined and Quad Gaussian. See *Frame Size* and *Weighted Random Frame Size—Uni-form Distribution* for more information.
Instrumentation Offsets	Lava supports Time Stamp, Packet Groups, Sequence Checking and Data Integrity options of Automatic Instru-mentation Offsets. See *Instrumentation Box* for more information.
Force Errors	See *Force Errors Box* for more information.
DA/SA	Lava supports DA/SA mode. See *DA/SA Property Sheet* for more information.

Field/Control	Description
Protocols	See Data Link Layer Protocols Control for more information. (OAM is not supported in Lava).
Table UDF	See Table UDF for more information.
UDF	Lava supports up to 5 UDFs. See Chapter 7,Frame Data–User Defined Fields (UDF) for more information.

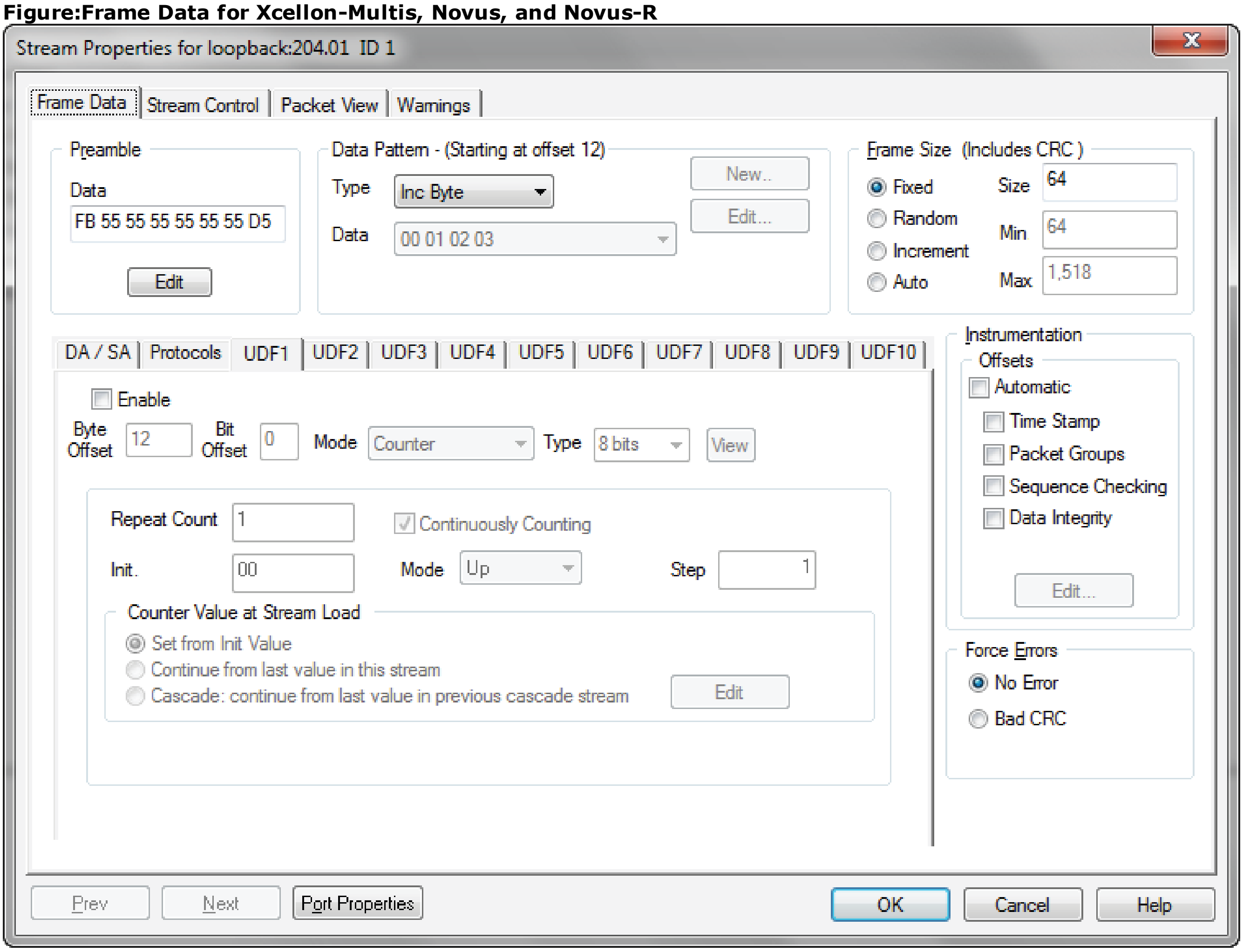
Frame Data for Xcellon-Multis, Novus, and Novus-R

The Stream Properties for the Xcellon-Multis load module are set in the Frame Data and Stream Control tabs.

To access the Frame Data tab, double-click in a stream/flow entry in the Packet Streams/Packet Flows/Advanced Streams window, then select the Frame Data tab. Alternatively, right-click a port in the Resources window, and select Edit Streams from the displayed menu.

The Frame Data tab for Xcellon-Multis is shown as follows:

Figure:Frame Data for Xcellon-Multis, Novus, and Novus-R



The options and controls in this tab are mentioned in the following table: Table 5-44. Frame Data tab—Xcellon-Multis

Field/Control	Description
Preamble	See *Xcellon-Multis— Preamble* for more information.
Data Pattern	Multis supports Increment (word/byte), Decrement (word/byte), Random, Repeating, Fixed, CJPAT and CRPAT as Data Pattern types. See *Data Pattern Box* for more information.
Frame Size	Multis supports Fixed, Random, Increment and Auto Frame Size. Under Random it supports Uniform, Weight, Predefined and Quad Gaussian. See *Frame Size* and *Weighted Random Frame Size—Uniform Distribution* for more information.
Instrumentation Offsets	Multis supports Time Stamp, Packet Groups, Sequence Checking and Data Integrity options of Automatic Instrumentation Offsets. See *Instrumentation Box* for more information.
Force Errors	See *Force Errors Box* for more information.
DA/SA	Multis supports DA/SA mode. See *DA/SA Property Sheet* for more information.
Protocols	See Data Link Layer Protocols Control for more information.
UDF	Multis supports up to 10 UDFs. See Chapter 7, Frame Data–User Defined Fields

[This page intentionally left blank]

Chapter 6 - Frame Data–Protocol Control

The *Frame Data* tab in the *Stream Properties* dialog provides control over all aspects of packets transmitted by the Ixia hardware. These frames are also referred to as datagrams or packets in some contexts. Many frames may be generated in the processing of a stream. Many of the controls available allow the specification of a series of values applied to subsequent frames.

This chapter discusses protocol frame data structure. For other parts of frame data construction, see:

- *Frame Data–Basic Frame Structure*
- *Frame Data–User Defined Fields (UDF)*

The Protocols section allows the header bytes of the packet to be formatted according to different conventions and protocols. This tab can be viewed by selecting the *Protocols* sub-tab in the lower area of the *Frame Data* tab. The different formats for this page are described in the following sections:

- *Data Link Layer Protocols Control*, which is covered in the following general sections:
  - *Protocol Control for Ethernet and 10 GE Modules*
  - *Protocol Control for 10GE LSM MACSec Modules* .
  - *Protocol Control for Standard POS and ATM/POS 622 Modules*
- *Protocols—Network Layer*
- *Frame Data for Fibre Channel Support*.

The *Protocols* page is accessed by:

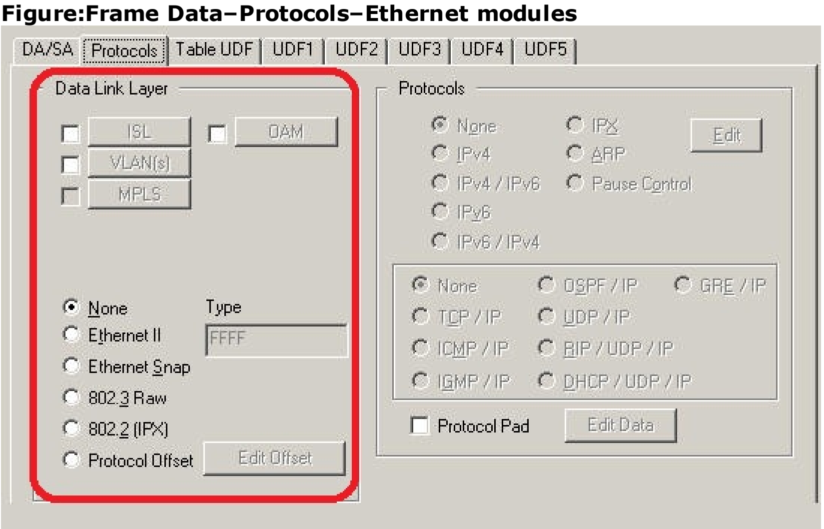
1. Selecting a port in the Resources window. This should cause several selections to appear in the right window of the main IxExplorer dialog.
2. Double-click the *Packet Streams* icon. This should cause the *Stream Grid* display to appear.
3. Double-click any stream in the view. This should open the *Stream Properties* dialog to appear.
4. Select the *Frame Data* tab.
5. Select the *Protocols* sub-tab.

Data Link Layer Protocols Control

Protocol Control for Ethernet and 10 GE Modules

The Protocols property page for Ethernet and 10 Gigabit Ethernet is shown in *Figure:Frame Data–Protocols–Ethernet modules*.

Figure:Frame Data–Protocols–Ethernet modules

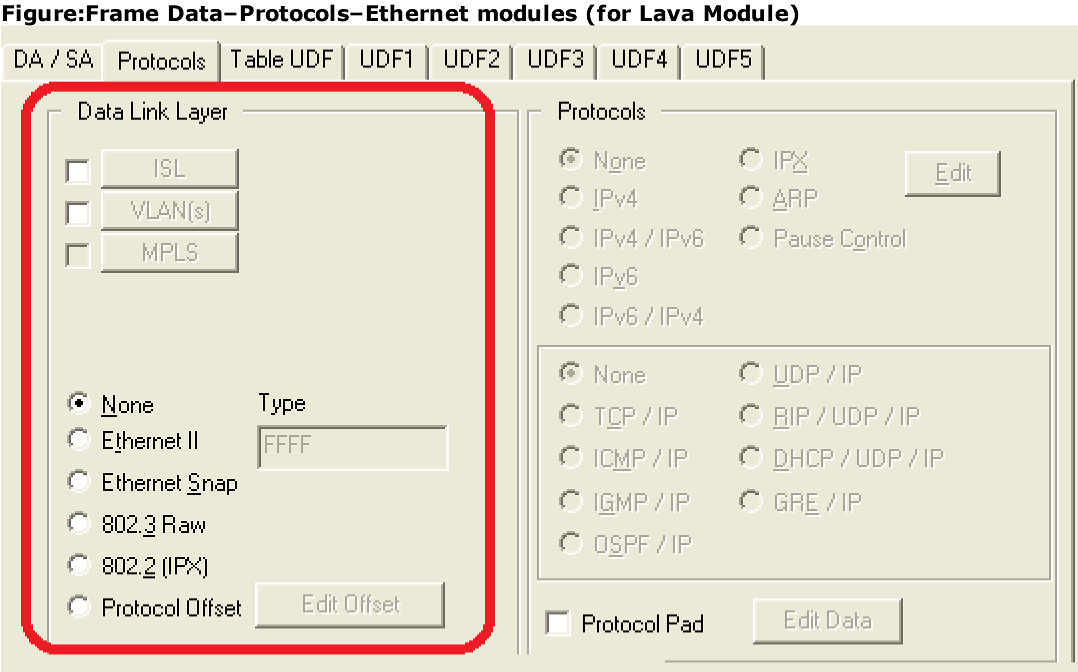


The two areas on this page relate to Data Link Layer (Layer 2 of the OSI Model) and Network Protocol (Layer 3) formatting. The *Edit* button in the Protocol section allows for the specification of header parameters specific to Transport and/or Network protocols.

Protocol Control for 40/100 GE Modules

The Protocols property page for 40/100 Gigabit Ethernet is shown in *Figure:Frame Data–Protocols–Ethernet modules (for Lava Module)*.

Figure:Frame Data–Protocols–Ethernet modules (for Lava Module)



For Ethernet-type modules, the choices available for Data Link Layer are described in *Table:Data Link Layer Protocols–Ethernet-Type Modules*.

Table:Data Link Layer Protocols–Ethernet-Type Modules

Data Link Layer Protocol	Description
ISL	Specifies that the packet is to be encapsulated according to Cisco

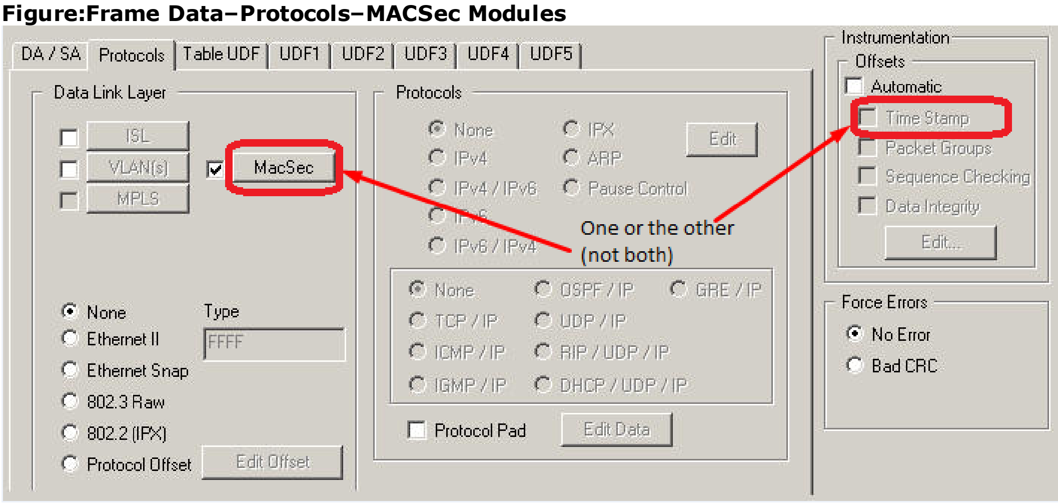
Data Link Layer Protocol	Description
	Inter-Switch Link (ISL) encapsulation. Refer to *Edit ISL*.
VLAN	Specifies that a VLAN tag is to be added to the header. The contents of the tag may be edited by pressing the **VLAN(s)** button.*Edit VLAN*.
MPLS	Specifies that an MPLS label stack is to be added between the data link layer and the network layer (for example, IP layer). The contents of the tag may be edited by clicking **Edit MPLS***Edit MPLS*.
OAM	The contents of the stream may be edited by pressing the **Edit OAM** button.*Edit OAM*. NOTE When OAM is selected, all other protocols are grayed-out. Instrumentation Offsets (automatic) is also grayed-out. The DA/SA tab is also changed when OAM is selected (the DA cannot be modified. DA is slow protocols multicast address).
None	No protocol-specific handling is performed.
Ethernet II	The packet is formatted according to the Ethernet II encapsulation. The format of an Ethernet II encapsulated packet is shown in the Ethernet II Packet Format.
Ethernet Snap	The packet is formatted according to the Ethernet SNAP protocol. The format of an Ethernet SNAP packet is shown in the *Ethernet SNAP Packet Format*.
802.3 Raw	The packet is a raw 802.3 packet. The format of a raw 802.3 is shown in *802.3 Raw Packet Format*.
802.2 (IPX)	The packet is formatted according to 802.2 encapsulation for use with IPX. The format of this type of packet is shown in the *802.2 (IPX) Packet Format*.
Protocol Offset	If selected, you may customize the configuration of the offset in the packet where the 2-byte *Protocol Type* field appears, as well as the data in the *Protocol Type* field. *Protocol Offset Dialog* for additional information.

Protocol Control for 10GE LSM MACSec Modules

Ixia incorporates MACsec in accord with *IEEE standard 802.1 AE-2006, Media Access Control (MAC) Security*. Refer to that specification for detailed explanations of MACsec functionality. When setting up MACsec, set up the port properties first, then the stream properties. To set up the MACSec Tx/Rx port properties,*10GE Port Properties–MACSec Tx/Rx Tabs*(Chapter 20: 10GE Port Properties).

The Protocols property page for 10GE LSM MACSec modules is shown in *Figure:Frame Data–Protocols–MACSec Modules*.

Figure:Frame Data–Protocols–MACSec Modules



For MACSec load modules, Auto Timestamp is the **only** way that Timestamp can be added to MACSec frames. Legacy Timestamp is always placed just before CRC. But MACSec frames place ICV at that location, so the only way to make a timestamp work is to allow it to ‘float’.

The following rules apply for MACSec.

- If MACSec protocol is **not** enabled:
  - Then legacy Timestamp and Auto Instrumentation with Timestamp are both available. (*Auto Instrumentation Tab for Ethernet Modules.*)
- If MACSec protocol is enabled, then legacy Timestamp is grayed out and not selectable.
  - If legacy Timestamp is enabled, and then MACSec is enabled, the application forces legacy Timestamp to become unavailable and grayed out.

For MACSec modules, the choices available for Data Link Layer include those described in *Table:Data Link Layer Protocols–Ethernet-Type Modules*, with the additional option shown in the table below,*Table:Data Link Layer Protocols–MACSec Modules*.

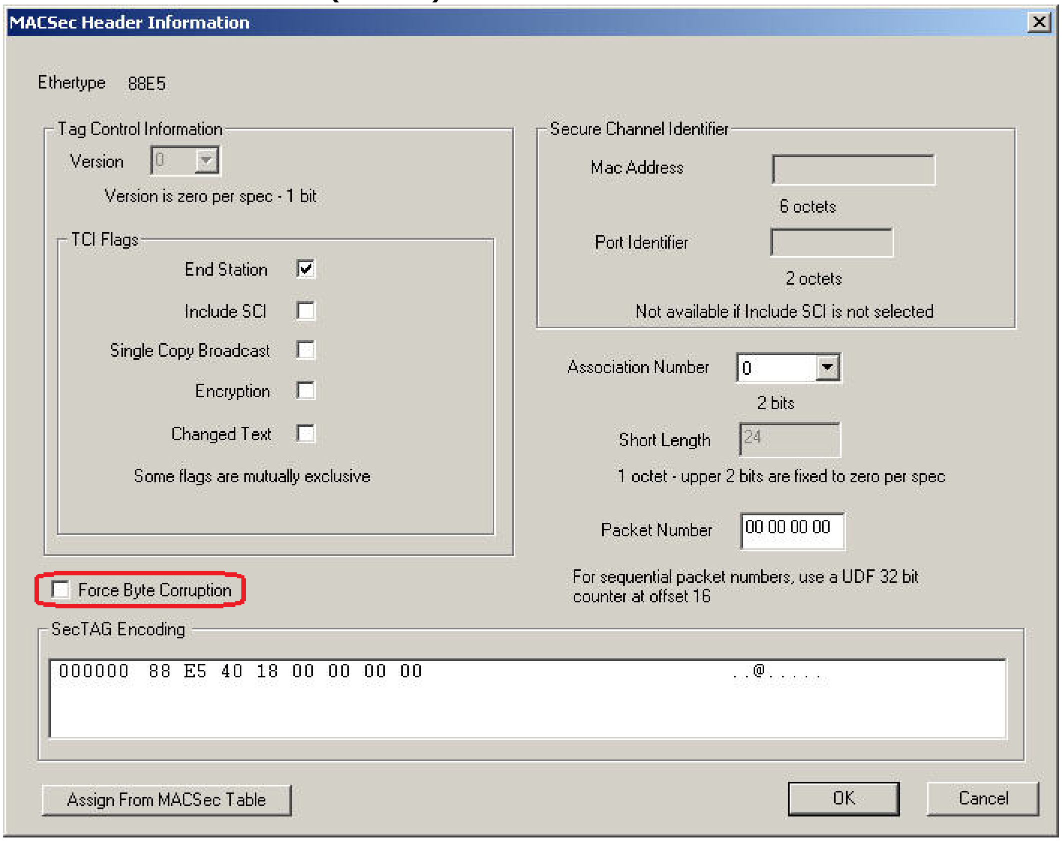
Table:Data Link Layer Protocols–MACSec Modules

Data Link Layer Protocol	Description
MacSec	If selected, MACSec button opens the MACSec Header Information window.

MACSec Header Information Editor

The MACSec Header Information editor is used to edit the Security TAG (SecTAG), and is shown in *Figure:MACSec Header Information (SecTAG) Editor*. These fields comprises the encoding of the SecTAG, which is shown in the lower pane of the screen.

Figure:MACSec Header Information (SecTAG) Editor



These fields of the MACSec Header Information window are defined in *Table:MACSec Header Information Editor*.

NOTE The IEEE Std. 802.1AE refers to TCI bits as bit 8 through 1, not 7 through 0. The information in the table below has been standardized to the 7-0 configuration used by Ixia.

Table:MACSec Header Information Editor

Heading	Field	Usage
Ethertype		Fixed value, set at 0x88E5.
Tag Control Information		Comprises bits 7 to 2 of octet 3 of the SecTAG.
	Version	The version is set to ‘0’ in bit 7, per the spec (802.1 AE-2006).
TCI Flags		Note: Some flags are mutually exclusive.
	End Station	(Default) If selected, sets bit 6 of the TCI.
	Include SCI	If selected, sets bit 5 of the TCI. Then the *Secure Channel Identifier* section of this screen becomes available.
	Single Copy Broadcast	If selected, sets bit 4 of the TCI.
	Encryption	If selected, sets bit 3 of the TCI.

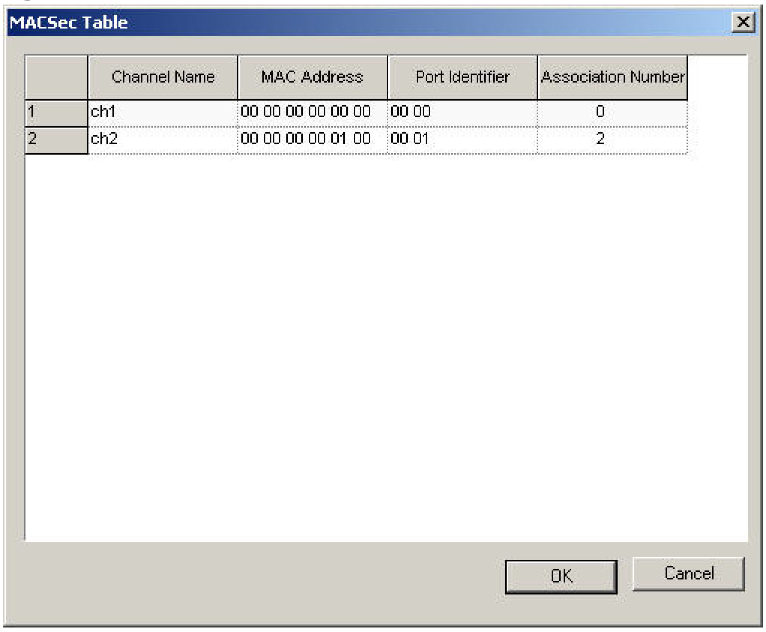
Heading	Field	Usage
	Changed Text	If selected, sets bit 2 of the TCI.
Secure Channel Identifier	MAC Address	Octets 9 through 14 of the SecTAG (six octets) encode a globally unique MAC address uniquely associated with the transmitting security entity. NOTE SCI is only available if **Include SCI** is selected. This corresponds to the MAC Address in Port Properties, MACSec Tx or Rx tab.
	Port Identifier	Octets 15 and 16 of the SecTAG encode the Port Identifier component of the SCI, as an integer. NOTE SCI is only available if **Include SCI** is selected. This corresponds to the Port Identifier in Port Properties, MACSec Tx or Rx tab.
Association Number		2 bits (bits 1 and 0 of the TCI) Choose 0, 1, 2, or 3. This corresponds to the Association Number AN 0 through AN 3 in Port Properties, MACSec Tx or Rx tab.
Short Length		The Short Length is the number of bytes between the last byte of the SecTAG and the first byte of the ICV, if that number is less than 48; otherwise, SL is set to 0. This number is hardware-generated, based on length of the frame, with the assumption that ICV immediately precedes FCS (the hardware does not currently support padding). NOTE 1 octet - upper 2 bits are fixed to '0' per spec
Packet Number		4 octets: Default is 00 00 00 00. NOTE For sequential packet numbers, use a UDF 32-bit counter at offset 16. If UDF is not used, this constant value goes out. If a UDF is used, the UDF overrides whatever value is entered in this field.
Force Byte Corruption		Enables byte corruption for Negative Testing.Negative Testing(Chapter 20: 10GE Port Properties).
SecTAG Encoding		The resulting header for this protocol. 8 bytes or (if Include SCI is enabled) 16 bytes.

Heading	Field	Usage
		This field displays the resulting code generated by the selections made above on this screen.
	Assign from MACSec Table	When clicked, this button opens the MACSec Table shown below.

MACSec Table

The MACSec Table is populated with values that must be set up using the MACSec Tx/Rx port properties pages.*10GE Port Properties–MACSec Tx/Rx Tabs* (Chapter 20: 10GE Port Properties).

Figure:MACSec Table



MACSec and VLAN

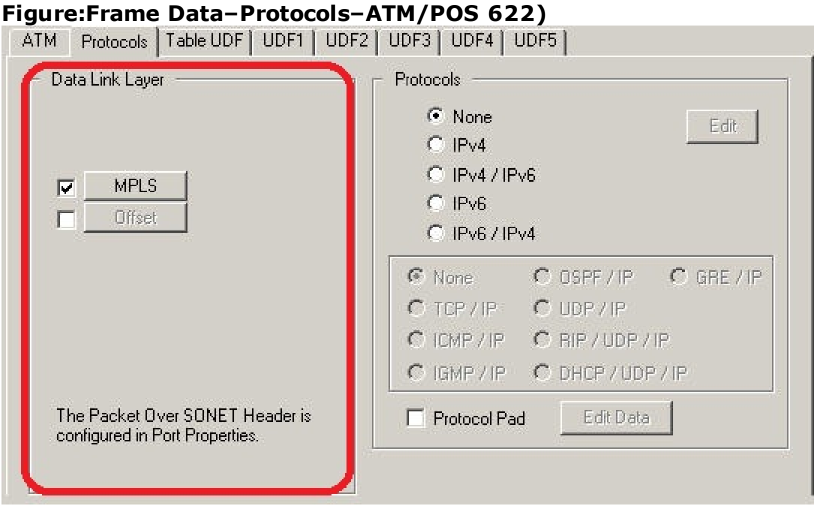
If both MACSec and VLAN protocols are enabled, the VLAN tag follows the MACSec header in the packet. *Figure:MACSec Frame Format Showing VLAN Tag* for an illustration.

Protocol Control for Standard POS and ATM/POS 622 Modules

The *Protocols* sub-tab for a POS and an ATM/POS 622 are the same.

The *Protocols* sub-tab for an ATM/POS 622 module with a PPP SONET header for IPv4 selected, is shown in *Figure:Frame Data–Protocols–ATM/POS 622)*.

Figure:Frame Data–Protocols–ATM/POS 622)



NOTE The options available in the left pane of these dialogs are affected by the settings in the POS SONET Header dialog. For more information on these settings,*SONET Properties*.

NOTE The figure above is for an ATM/POS 622 module in ATM mode. Standard POS modules do not have the *ATM* or *UDF 5* sub-tab options.

Protocols–Data Link Layer

The choices available for the Data Link Layer are based on the settings for the SONET header in the *Port Properties* dialog, as shown in *Table:Data Link Layer Protocol Choices–Packet over SONET*. Only the corresponding header type is displayed.

Table:Data Link Layer Protocol Choices–Packet over SONET

Data Link Layer	Type	Description
Current Header		The current Data Link Layer header format, as selected in the Port Properties/SONET page. The hexadecimal format for the specific header is displayed in the field. This field cannot be directly edited unless the SONET header selection in Port Properties is set to *Other*.
	PPP/IPv4 **or** PPP/IPv6	The currently selected SONET frame header format is *PPP*, and a version of the IP protocol has been selected in the Protocol section. The two versions are IPv4 and IPv6.
	CISCO HDLC/IPv4 **or** CISCO HDLC/IPv6	The currently selected SONET frame header format is *Cisco HDLC*, and a version of the IP protocol has been selected in the Protocol section. The two versions are IPv4 and IPv6.
	Frame Relay	The current SONET frame header format is Frame Relay per RFC 2427. When this is displayed, the FR header can be edited by pressing the *Edit FR* button. *Frame Relay Header (RFC 2427)*.

Data Link Layer	Type	Description
		The Frame Relay header is available for use with IPv4 only.
	Cisco Frame Relay	The current SONET frame header format is Cisco Frame Relay. When this is displayed, the FR header can be edited by pressing the *Edit FR* button. *Cisco Frame Relay Header*. The Cisco Frame Relay header is available for use with IPv4 only.
	Edit FR	This button is available for Frame Relay per RFC 2427 or Cisco Frame Relay header type. Press this button to display the corresponding *Frame Relay Configuration* dialog—for either Frame Relay (RFC 2427) or Cisco Frame Relay. This button only appears if the Frame Relay option is selected in the Port Properties dialog.Chapter 19,*Port Properties–POS and ATM Families* for more information.
	Blank (SRP)	For standard use, when Spatial Reuse Protocol (SRP) is selected for the SONET frame header format, no header type is displayed here, but the first two octets configured for the header in the SONET page are displayed here (for Address and Control). The SRP header is available for use with IPv4 only (not IPv6). NOTE FOR OPTIONAL SRP FEATURE: *Frame Data for SRP*for information on the SRP feature for OC-192c POS modules. When the optional SRP feature is being used on an OC-192c or OC-48c POS module, the SRP Header values are displayed in the Data Link Layer section (read-only), and an*Edit SRP* button is available.
	Edit SRP	*Frame Data for SRP* for information on the optional SRP feature on OC-192c and OC-48c POS modules. This button is available **only** for use with the optional SRP feature on an Ixia OC-192c or OC-48c POS module. Press this button to display the corresponding *SRP Header* dialog.
	Ring Control	(Read-only) The 2-byte RPR *Ring Control* field. The value depends on the settings in the *RPR Ring Control* dialog. *Frame Data for RPR* for information on the optional SRP feature on OC-192c and OC-48c POS modules.
	Edit Ring Control	This button is available **only** for use with the optional RPR feature on an Ixia OC-192c or OC-48c POS module. Press this button to display the corresponding *RPR Ring Control* dialog.

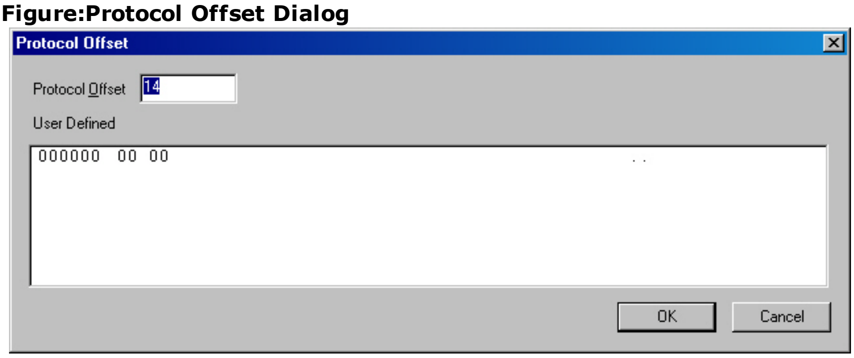
Data Link Layer	Type	Description
		Frame Data for RPR for information on the optional SRP feature on OC-192c and OC-48c POS modules.
	Other	The current SONET frame header format is one other than those listed above. It can be configured manually in hexadecimal format in this *Data Link Layer Header* field, for Address, Control, and Protocol. The first two octets of the 'Other' header may be edited manually in the SONET header section of the Port Properties for Address and Control. This header type may be used with IPv4 or IPv6.
	MPLS	If selected, specifies that an MPLS label stack is to be added between the data link layer (Layer 2) and the network layer (Layer 3) in the packet. The MPLS button is available for port types which support MPLS. The contents of the MPLS tag may be edited through the *Edit MPLS*.
	Offset	If selected, you may custom-configure the offset in the packet where the 2-byte *Protocol Type* field appears, as well as the data in the *Protocol Type* field. *Protocol Offset Dialog* for additional information.

Protocol Offset Dialog

The *Protocol Offset* dialog for certain modules is shown in *Figure:Protocol Offset Dialog*. It allows to create a user-defined field after the MAC addresses and before the start of the network layer (Layer 3) protocol header, and is intended for use with IPv4 and IPv6. This field can be from 2 to 48 bytes in length, and may contain information such a PPPoE header (for use with other Ixia applications). This dialog is accessed by selecting the Protocol Offset option button in the Protocols sub-tab. *Protocol Control for Ethernet and 10 GE Modules* for more information.

See an example of Protocol Offset configuration in *Protocol Offset—Example*.

Figure:Protocol Offset Dialog



The fields in this dialog are described in *Table:Protocol Offset Dialog*.

Table:Protocol Offset Dialog

Field	Description
Protocol Offset	(in bytes) The number of bytes from the start of the packet where the start of the protocol header is located. The default value is 14 bytes. Since the DA and SA MAC addresses occupy the first 12 bytes, this allows for a default of 2 bytes for the user-defined field. The valid range for the protocol offset is 14 bytes to the maximum stream frame size minus the size of the CRC (4 bytes). For older 10/100 and GBIC Modules, the maximum offset size is 40 bytes.
User Defined	Enter the desired user data in this field. This is the User Defined field/tag that is inserted into the packet between the end of the MAC addresses and the start of the Layer 3 protocol header. The valid range for the length of the *User Defined* field is from 2 to 48 bytes. If the data value entered here is smaller than the space between the old and new offsets, the remainder of the field is padded with zeroes. If the data value entered here is larger than the space between the old and new offsets, it is truncated.

Protocol Offset—Example

An example of a Protocol Offset configuration is shown in *Figure:Protocol Offset—Example*,*Figure:Protocol Offset—Example Diagram*, and *Figure:Protocol Offset Example Shown in Packet View*. In this example, the Protocol Offset is 20 bytes, so the User Defined tag/field is 8 bytes long. The selected network protocol is IPv4.

Figure:Protocol Offset—Example

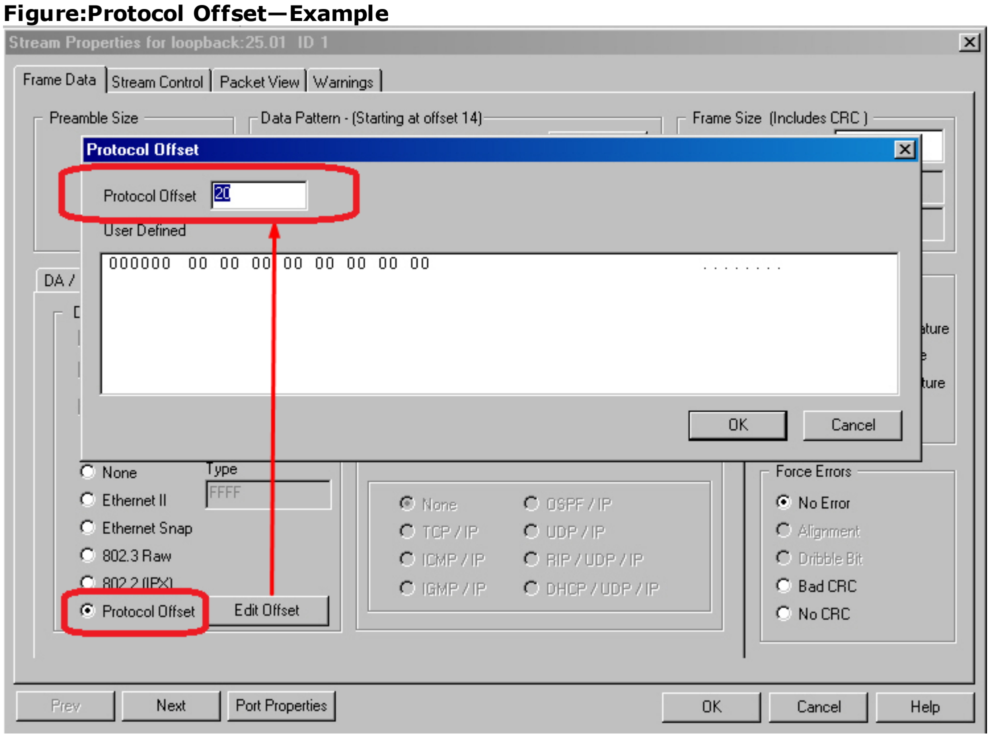


Figure:Protocol Offset—Example Diagram

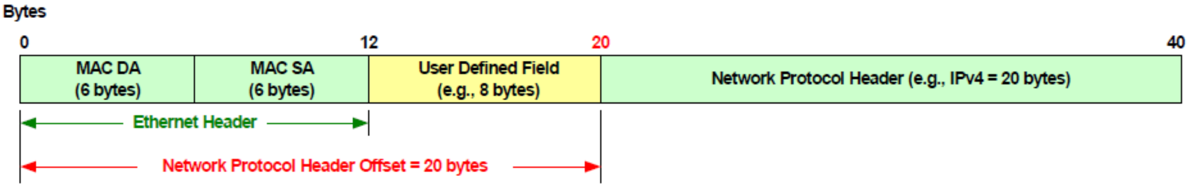
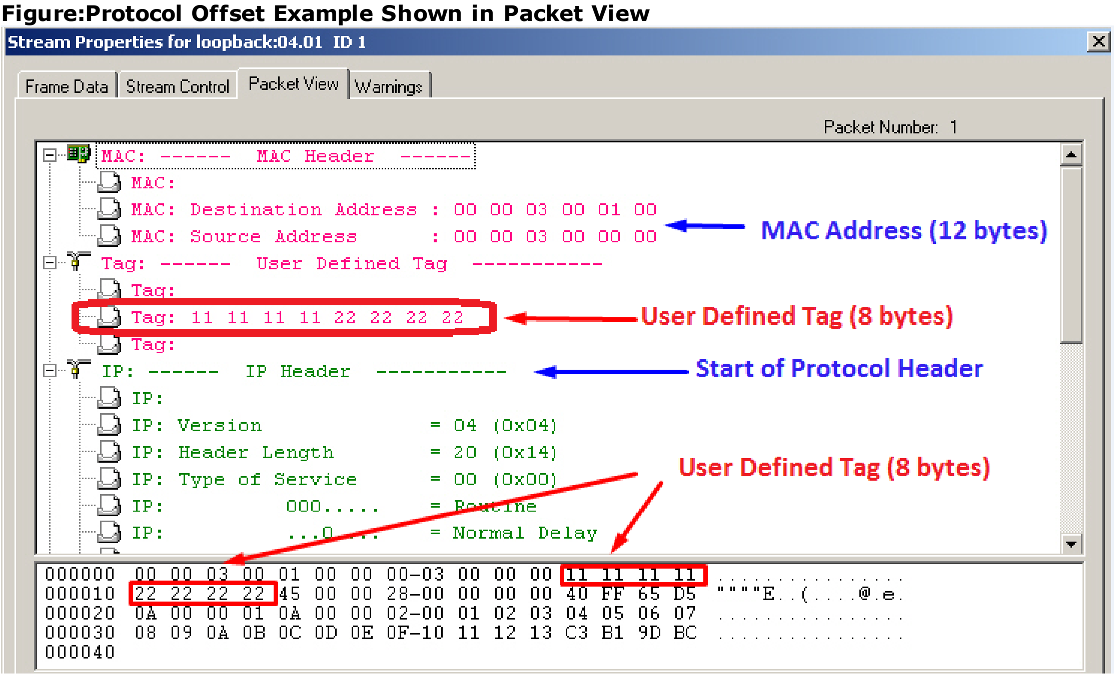


Figure:Protocol Offset Example Shown in Packet View

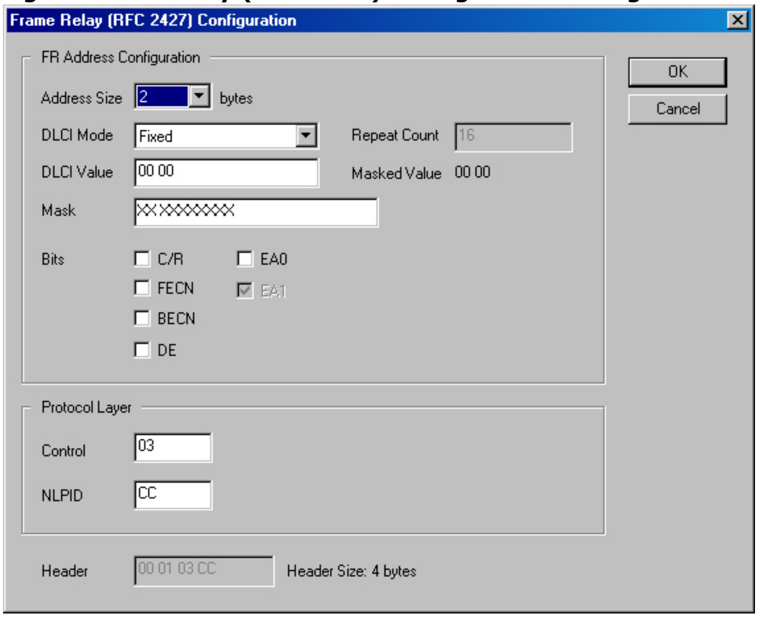


NOTE When employing the Protocol Offset feature, offset Layer 3 protocol information (in the Capture View) in received packets is not correctly decoded.

Frame Relay Header (RFC 2427)

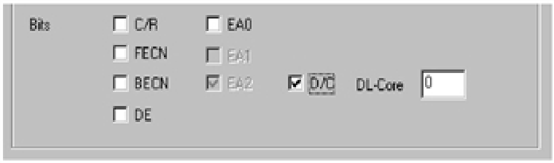
The *Frame Relay (RFC 2427) Configuration* dialog is shown in *Figure:Frame Relay (RFC 2427) Configuration Dialog* . This dialog is accessed by first selecting the *Frame Relay* option in the *Port Properties* dialog (Chapter 19,*Port Properties–POS and ATM Families* for more information), then selecting the *Edit FR* button in the Data Link Layer section of the *Protocols* sub-tab.

Figure:Frame Relay (RFC 2427) Configuration Dialog

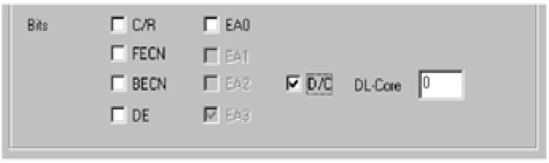


The bits check box options change depending on the selected number of bytes in the *Address Size* field.*Figure:Bits Options for Address Sizes shows the different options*.

Figure:Bits Options for Address Sizes



Address Size = 3 bytes



Address Size = 4 bytes

The fields and controls in the Frame Relay configuration dialog are described in *Table:Frame Relay (RFC 2427) Configuration Dialog* .

Table:Frame Relay (RFC 2427) Configuration Dialog

Section	Field/Control	Description
FR Address Configuration	Address size	The size of the Q.922 frame relay address in bytes. Choose one of: • 2 • 3 • 4
	DLCI Mode	For Multiple DLCIs (where supported). Data Link Connection Identifier (DLCI) incrementing

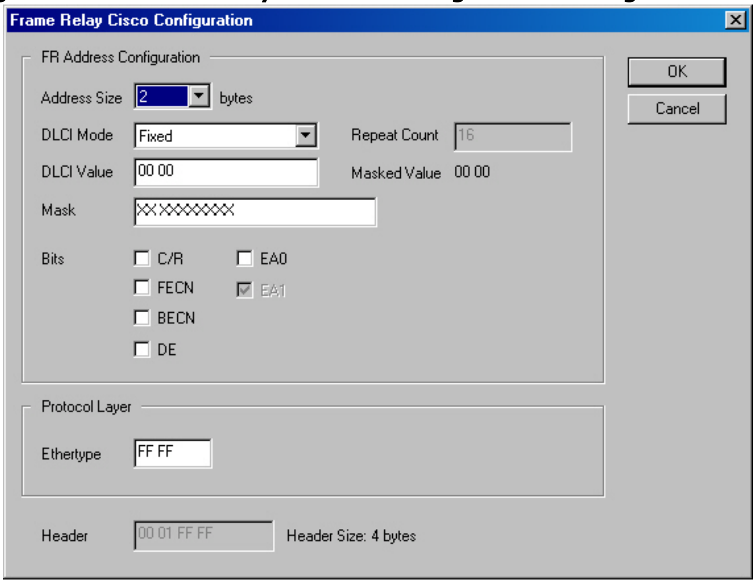
Section	Field/Control	Description
		mode. Choose one of: • Increment • Continuous Increment • Decrement • Continuous Decrement • Fixed • Random
	Repeat Count	For Multiple DLCIs (where supported). Enter an integer valuefor the number of times to repeat process (defined as DLCI mode) for creating DLCIs.
	DLCI Value	Data Link Connection Identifier value. Can be set to a maximum value of 00 7F FF FF
	Mask	For Multiple DLCIs (where supported). The mask is applied to the DLCI value (as exclicked in hexadecimal format). The mask length is defined by the number of bytes in the address—2, 3, or 4 bytes of 2 nibbles each. X's, 1's, and 0's may be entered. An 'X' allows the defined DLCI hex character to be visible, and active. A '1' or a '0' masks the DLCI character with that value, so only the entered '1' or '0' is visible and active. (The default is all X's.)
	Masked Value	The displayed masked value is the DLCI Value (exclicked in hexadecimal format), with the Mask applied. When Multiple DLCIs are not supported, the default value is applied—all X's—so the complete DCLI value is displayed in hex format.
	Bits	Sets the bits in the Frame Relay header for: • C/R: Command Response bit. • FECN: Forward Explicit Congestion Notification. • BECN: Backward Explicit Congestion Notification. • DE: Discard Eligibility. • EA0: Address Field Extension 0 - available for 2, 3, and 4-byte addresses. • EA1: Address Field Extension 1 - available for 2, 3, and 4-byte addresses. • EA2: Address Field Extension 2 - available for 3, and 4-byte addresses. • EA3: Address Field Extension 3 - available for 4-byte addresses.

Section	Field/Control	Description
		• D/C: Available for 3 and 4-byte addresses. • DL-Core: Available for 3 and 4-byte address, when D/C is selected. When the D/C bit is turned on, the high six bits of the lowest byte in the Address represent DL-Core value. They are not part of DLCI value. NOTE EAs occur as the last bit in an address byte. They allow the indication of 3 and 4-byte headers. NOTE Regular (non 622) POS modules only support fixed mode (listed in DLCI Modes above) when using the D/C bit.
Protocol Layer		To indicate the type of protocol being encapsulated by the frame relay header.
	Control	(For Frame Relay per RFC 2427 only) The Q.922 Control field. The default is 0x03.
	NLPID	(For Frame Relay per RFC 2427 only) The *Network Level Protocol ID* field indicates the type of encapsulation protocol which follows. When any of the IP protocols is selected for that port in the Protocol section of the *Frame Data* tab, the NLPID default value is 0xCC (as defined for IPv.4).
	Ethertype	(For Cisco Frame Relay only) The PID (Protocol Identifier) is the Ethertype (FF FF). There is no defined NLPID for this protocol, so by default, a SNAP header is being used for IP routing—indicated by the Ethertype of FF FF.
Header		Header Size: 4, 5, or 6 bytes. If the Address size is set to 2 bytes, the overall frame header size is 4 bytes, if set to 3 the header is 5, if set to 4 the header is 6. The contents of the header are displayed in the field (not editable).

Cisco Frame Relay Header

The *Frame Relay Cisco Configuration* dialog is shown in *Figure:Cisco Frame Relay—Header Configuration Dialog*. This dialog is accessed by first selecting the *Cisco Frame Relay* option in the *Port Properties* dialog (Chapter 19,*Port Properties–POS and ATM Families* for more information), then selecting the *Edit FR* button in the Data Link Layer section of the *Protocols* sub-tab.

Figure:Cisco Frame Relay—Header Configuration Dialog



Refer to *Table:Frame Relay (RFC 2427) Configuration Dialog* for information on the fields and controls in this dialog.

Ethernet II Packet Format

Figure:Ethernet II Packet Format

The Destination Address (Dest Addr) and Source Address (Source Addr) are MAC addresses programmed through the use of the *DA/SA Property Sheet. The Frame Check Sequence (FCS) is calculated according to the CRC-32 format. The Type field is automatically set to correspond to the Network/Transport protocol selected, as shown in Table:Type Field Values.*

Table:Type Field Values

Network/Transport Packet Type	Type Value
IP	0x0800
IPX	0x8137
Pause Control	0x8808
ARP	0x0806

802.2 (IPX) Packet Format

Figure:802.2 (IPX) Packet Format

The Destination Address (Dest Addr) and Source Address (Source Addr) are MAC addresses programmed through the use of the *DA/SA Property Sheet. The Frame Check*

Sequence (FCS) is calculated according to the CRC-32 format. The length field is automatically calculated.

Ethernet SNAP Packet Format

Figure:Ethernet SNAP Packet Format

Dest Addr	Source Addr	Length	DSAP 0xAA	SSAP 0xAA	cntl 0x03	org code 0x00 00 00	Type	Packet Data	FCS

The Destination Address (Dest Addr) and Source Address (Source Addr) are MAC addresses programmed through the use of the *DA/SA Property Sheet. The Frame Check Sequence (FCS) is calculated according to the CRC-32 format. The length field is automatically calculated. The type field is automatically set to correspond to the Network/Transport protocol selected, as shown in Table:Type Field Values.*

Table:Type Field Values

Network/Transport Packet Type	Type Value
IP	0x0800
IPX	0x8137
Pause Control	0x8808
ARP	0x0806

802.3 Raw Packet Format

802.3 raw packets are only useful for the IPX protocol.

Figure:802.3 Raw Packet Format

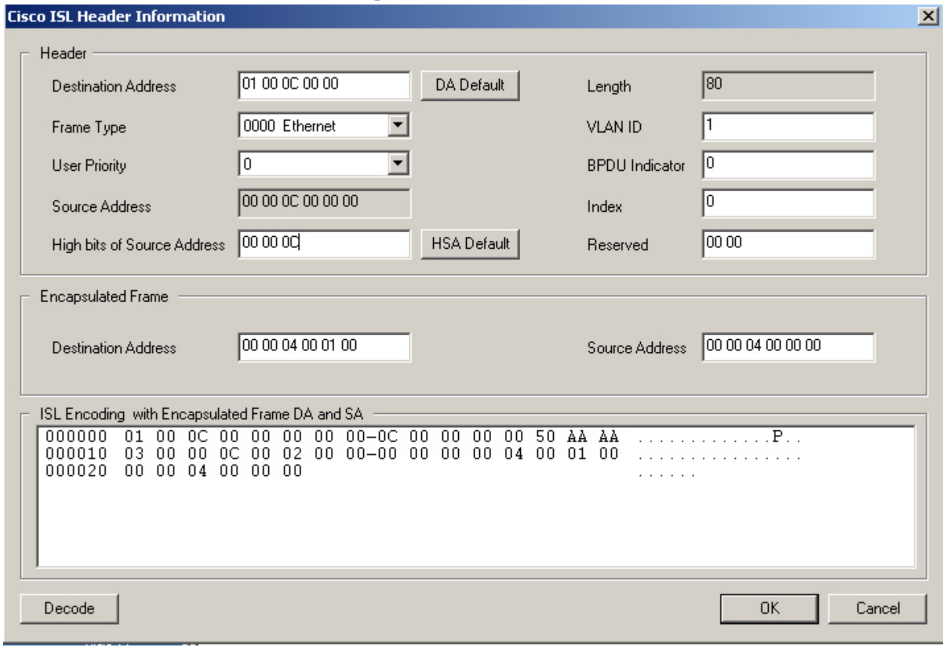
Dest Addr	Source Addr	length	Packet Data (First two bytes 0XFFFF)	FCS

The Destination Address (Dest Addr) and Source Address (Source Addr) are MAC addresses programmed through the use of the *DA/SA Property Sheet. The Frame Check Sequence (FCS) is calculated according to the CRC-32 format. The length field is automatically calculated. The first bytes of the packet data are 0xFFFF.*

Edit ISL

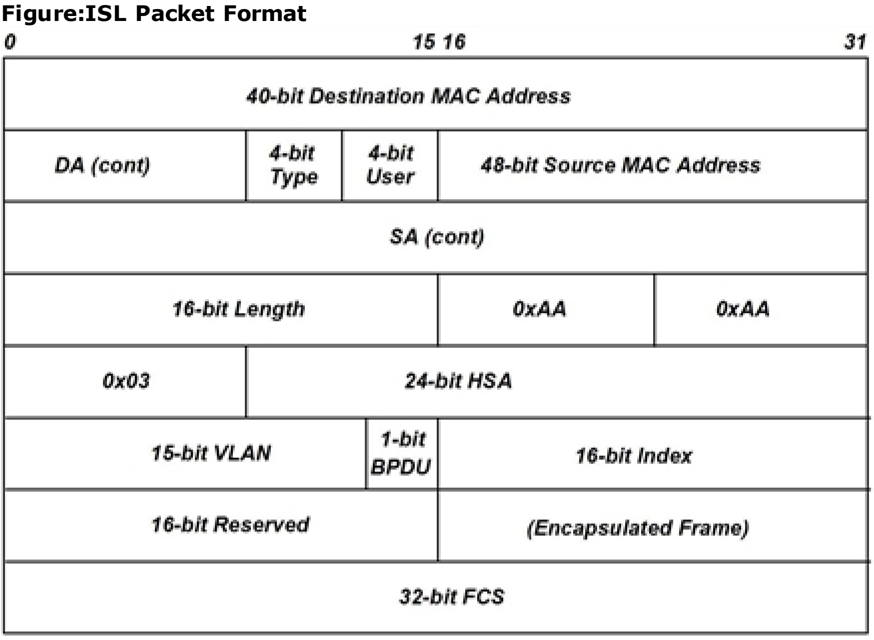
The *ISL* button opens the *Cisco ISL Header Information* dialog is used to edit the attributes of Cisco-proprietary InterSwitch Link (ISL) encapsulation data. The dialog is shown in *Figure:Cisco ISL Header Information Dialog*.

Figure:Cisco ISL Header Information Dialog



The format of an ISL encapsulation is shown in *Figure:ISL Packet Format*.

Figure:ISL Packet Format



The elements of the dialog and their correspondence to the contents of an ISL packet are described in *Table:Cisco ISL Header Information Dialog Elements*.

Table:Cisco ISL Header Information Dialog Elements

ISL Packet Field	Dialog Field	Description
Destination MAC Address	Destination Address	This address is a multicast address and is currently set to 0x01 00 0C 00 00. This value, as the first 40 bits of the DA, signals the receiver that the packet is in ISL format. The DA *Default* button sets this value.

ISL Packet Field	Dialog Field	Description
Type	Frame Type	The 4- bit type field indicates the type of frame that is encapsulated. The following options are available, with associated values: • 0000 - Ethernet • 0001 - Token-Ring • 0010 - FDDI • 0011 - ATM • 0100 through 1111 - Undefined
User	User Priority	For Ethernet frames, this 4-bit field indicates the priority of the packet as it passes through the switch. The valid range is 0 through 7.
Source MAC Address	Source Address	This is the MAC address of the packet source and is set from the *DA/SA Property Sheet. The upper 3 bytes of the SA are reflected in the HSA field, described below.*
HSA	High bits of Source Address	The HSA is the upper 3 bytes of the Source Address, which corresponds to the manufacturers ID. The HSA *Default* button sets this to the Cisco value: 0x00 00 0C.
Length	Length	The length of the original packet (minus the 18 bytes of the DA, Type, User, SA, Length, and FCS fields).
VLAN	VLAN ID	The Virtual LAN Identifier of the packet.
BPDU	BPDU Indicator	This bit is set for all Bridge Protocol Data Unit packets that are encapsulated by the ISL frame.
Index	Index	For diagnostic purposes when used with switches, this 16-bit value is the port index of the packet as it exits the switch. It is ignored upon receipt of the packet.
Reserved	Reserved	Used when Token Ring or FDDI packets are encap-sulated within an ISL packet. • For **Token Ring** packets, the AC and FC fields are placed here. • For **FDDI**, the FC field is placed in the least significant byte of this field. • For **Ethernet** packets, this field should be set to zeros.
Encapsulated Frame	Destination Address/Source Address	The *Encapsulated Frame* contains the original packet being sent. When the Ixia system sends ISL-encapsulated packets, the DA/SA fields are set from the ISL dialog, rather than in the *DA/SA Property Sheet*.
FCS		The 4-byte Frame Check Sequence (FCS) field

ISL Packet Field	Dialog Field	Description
		contains a 32-bit CRC that is automatically calculated and added to the end of the ISL frame.

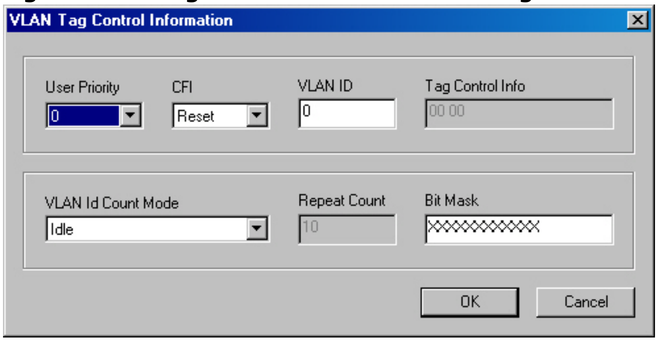
Edit VLAN

Depending on the module type, clicking the *VLAN* button opens the *VLAN Tag Control Information* dialog or the *VLAN(s)* dialog, allowing some of the contents of a VLAN tag header to be specified.

The TXS and LSM10G modules also allow for the creation of Q-in-Q VLANs (also known as stacked VLANs). The stacked VLAN configuration dialog is described in Stacked VLAN Configuration.

VLAN-tagged frames are used to direct data traffic for Virtual Local Area Networks (VLANs), per IEEE 802.1Q. This dialog is shown in *Figure:VLAN Tag Control Information Dialog*.

Figure:VLAN Tag Control Information Dialog



The format of a Tag Control Information (TCI) field for a VLAN tag header is shown in *Figure:VLAN Tag Control Information (TCI) Format*. The *VLAN Tag Control Information* dialog allows to specify the contents of this field. This field is included in the VLAN tag headers for Ethernet frames (as part of the Ethernet Tag Protocol Identifier/ETPID), and for SNAP protocol frames (as part of the SNAP Tag Protocol Identifier/STPID).

Figure:VLAN Tag Control Information (TCI) Format

The fields in this dialog are described in *Table:VLAN Tag Control Dialog*.

Table:VLAN Tag Control Dialog

Field	Description
User Priority	The user priority of the tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
CFI	The Canonical Format Indicator is a single bit flag. Choose one of: • Reset • Set
VLAN ID	A unique, 12-bit VLAN Identifier which specifies the VLAN with which this frame is associated.

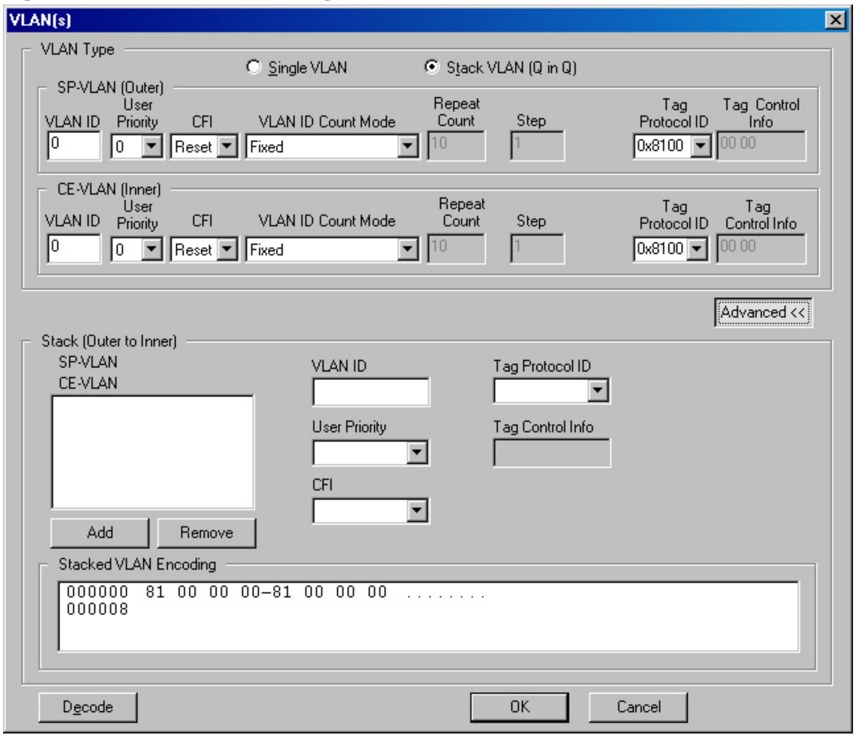
Field	Description
Tag Control Information	(TCI) A read-only field that indicates the two octets formed by the combination of other values in the upper part of this dialog.
VLAN ID Count Mode	Used to set the mode by which the VID varies. The choices are: • **Fixed**: The single ID specified in the VID field is used. • **Increment**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Decrement**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Continuous Increment**: The ID specified in the VID field is used as the start of an infinite sequence of VIDs, with the increment based on the value in the Step field. • **Continuous Decrement**: The ID specified in the VID field is used as the start of an infinite sequence of VIDs, with the decrement based on the value in the Step field. • **Random**: The VID is varied randomly as indicated by the Bit Mask field.
Repeat Count	(Integer) For use with the Increment and Decrement VLAN ID Mode choices, this indicates the length of the cycle of varied VIDs.
Bit Mask	For use with the Random VLAN ID Count Mode, the Bit Mask field indicates which bits of the VID counter may vary and which must remain constant. The Bit Mask field may contain the following characters: • 0: the corresponding VID bit is always '0.' • 1: the corresponding VID bit is always '1.' • X: the corresponding VID bit may vary according to the VLAN ID Count Mode and Repeat Count fields.

Stacked VLAN Configuration

VLAN Stacking (also known as Q in Q) refers to a mechanism where one VLAN (Virtual Local Area Network) may be encapsulated within another VLAN. This allows a carrier to partition the network among several national ISPs, while allowing each ISP to still utilize VLANs to their full extent. For more information on stacked VLANs, refer to the Stacked VLANs (Q in Q) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

The VLAN(s) dialog is used to configure stacked VLANs is shown in *Figure:Stacked VLAN Configuration*.

Figure:Stacked VLAN Configuration



The fields in this dialog are described in *Table:VLAN Tag Control Dialog*.

Figure:Stacked VLAN Header Information shows the stacked VLAN packet composition within a packet header.

Figure:Stacked VLAN Header Information

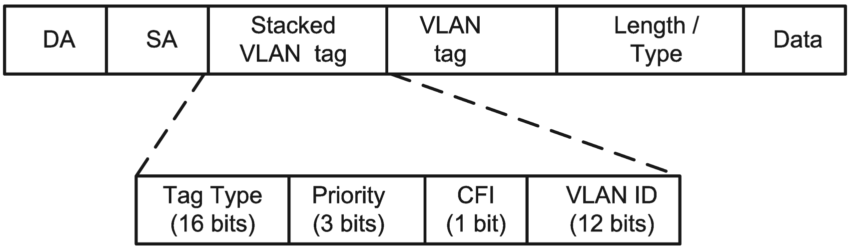


Figure:MACSec Frame Format Showing VLAN Tag shows the VLAN tag within a MACSec frame .

Figure:MACSec Frame Format Showing VLAN Tag

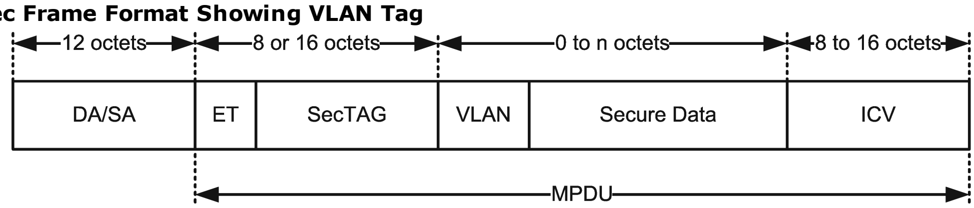


Table:VLAN Tag Control Dialog

Section	Field	Description
VLAN Type		Allows to select what type of VLAN is to be used.

Section	Field	Description
	Single VLAN	A simple, single VLAN is included with the packet.
	Stack VLAN (Q in Q)	A stacked VLAN configuration is included with the packet. Selecting this option expands the dialog so that both the outer and inner VLAN information can be configured.
SP-VLAN (Outer)		The Service Provider (SP) VLAN tag information.
	VLAN ID	A unique, 12-bit VLAN Identifier which specifies the VLAN with which this frame is associated.
	User Priority	The user priority of the tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
	CFI	The Canonical Format Indicator is a single bit flag. Choose one of the following: • Reset • Set
	VLAN ID Count Mode	Used to set the mode by which the VID varies. The choices are as follows: • **Fixed**: The single ID specified in the VID field is used. • **Increment**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Decrement**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Continuous Increment**: The ID specified in the VID field is used as the start of an infinite sequence of VIDs, with the increment based on the value in the Step field. • **Continuous Decrement**: The ID specified in the VID field is used as the start of an infinite sequence of VIDs, with the increment based on the value in the Step field. • **Random**: The VID is varied randomly as indicated by the Bit Mask field.
	Repeat Count	(Integer) For use with the Increment and Decrement VLAN ID Mode choices, this indicates the length of the cycle of varied VIDs.
	Step	(Not present for 10G LSM and MSM cards.) (Integer) For use with the Increment, Decrement, Continuous Increment, and Continuous Decrement fields. You can define the size the of the increment step.

Section	Field	Description
	Bit Mask	(Not present for 10G LSM and MSM cards.) For use with the Random VLAN ID Mode, the Bit Mask field indicates which bits of the VID counter may vary and which must remain constant. The Bit Mask field may contain the following characters: • 0: the corresponding VID bit is always '0.' • 1: the corresponding VID bit is always '1.' • X: the corresponding VID bit may vary according to the VLAN ID Mode and Repeat Count fields.
	Tag Protocol ID	EtherTypes identify the protocol that follows the VLAN header. Select from a list of hex options: • 0x8100 • 0x9100 • 0x9200 • 0x88A8 • 0x9300
	VLAN Tag Control Information	(TCI) A read-only field that indicates the two octets formed by the combination of other values in the upper part of this dialog.
CE-VLAN (Inner)		The Customer Edge (CE) VLAN tag information.
	VLAN ID	A unique,12-bit VLAN Identifier which specifies the VLAN with which this frame is associated.
	User Priority	The user priority of the tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
	CFI	The Canonical Format Indicator is a single bit flag. Choose one of: • Reset • Set
	VLAN ID Count Mode	Used to set the mode by which the VID varies. The choices are as follows: • **Fixed**: The single ID specified in the VID field is used. • **Increment**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Decrement**: The ID specified in the VID field is used as the start of a number of repeated sequence of VIDs as indicated by the Repeat Count field and the Step field. • **Continuous Increment**: The ID specified in the VID field is used as the start of an infinite

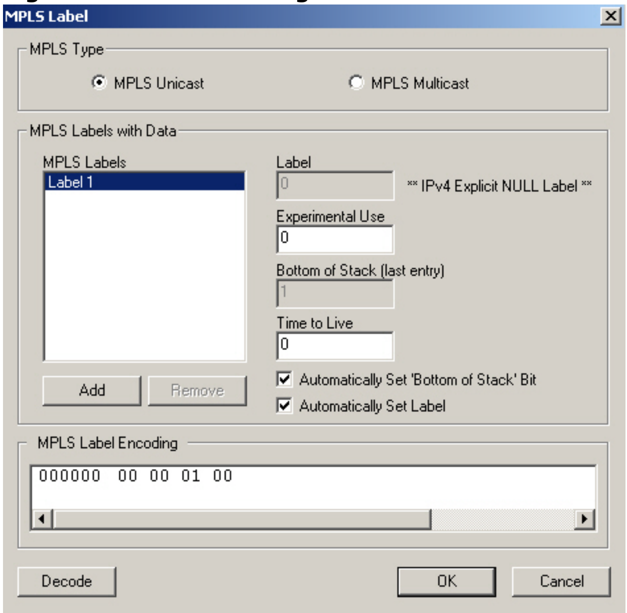
Section	Field	Description
		sequence of VIDs, with the increment based on the value in the Step field. • **Continuous Decrement**: The ID specified in the VID field is used as the start of an infinite sequence of VIDs, with the increment based on the value in the Step field. • **Random**: The VID is varied randomly as indicated by the Bit Mask field.
	Repeat Count	(Integer) For use with the Increment and Decrement VLAN ID Count Mode choices, this indicates the length of the cycle of varied VIDs.
	Step	(Not present for 10G LSM and MSM cards.) (Integer) For use with the Increment, Decrement, Continuous Increment, and Continuous Decrement fields. You can define the size the of the increment step.
	Bit Mask	(Not present for 10G LSM and MSM cards.) For use with the Random VLAN ID Count Mode, the Bit Mask field indicates which bits of the VID counter may vary and which must remain constant. The Bit Mask field may contain the following characters: • 0: the corresponding VID bit is always '0.' • 1: the corresponding VID bit is always '1.' • X: the corresponding VID bit may vary according to the VLAN ID Count Mode and Repeat Count fields.
	Tag Protocol ID	EtherTypes identify the protocol that follows the VLAN header. Select from a list of hex options: • 0x8100
	VLAN Tag Control Information	(TCI) A read-only field that indicates the two octets formed by the combination of other values in the upper part of this dialog.
	Advanced button	Selecting this button opens an expanded set of stacked VLAN options, specifically the ability to add more than one inner VLAN.
Stack (Outer to Inner)		Allows to create more than one inner VLAN and arrange them into a stack.
	VLAN ID	A unique, 12-bit VLAN Identifier which specifies the VLAN with which this frame is associated.
	User Priority	The user priority of the tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
	CFI	The Canonical Format Indicator is a single bit flag. Choose one of:

Section	Field	Description
		• Reset • Set
	Tag Protocol ID	EtherTypes identify the protocol that follows the VLAN header. Select from a list of hex options: • 0x8100
	VLAN Tag Control Information	(TCI) A read-only field that indicates the two octets formed by the combination of other values in the upper part of this dialog.

Edit MPLS

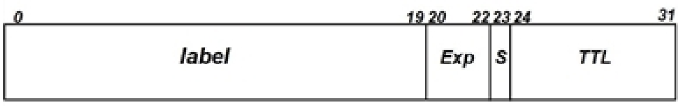
The *MPLS* button opens the *MPLS Label* dialog, which allows for the configuration of some MPLS label information. The dialog allows one or more MPLS labels to be inserted between the data link layer and network data layer of outgoing packets. The *MPLS Label* dialog is shown in *Figure:MPLS Label Dialog*.

Figure:MPLS Label Dialog



The format of an MPLS stack entry is shown in *Figure:MPLS Label Stack Entry*.

Figure:MPLS Label Stack Entry



The fields and controls in this dialog are described in *Table:MPLS Label Dialog*.

Table:MPLS Label Dialog

Section	Field/Control	Description
MPLS Type		Sets the overall packet type for the MPLS data.
	MPLS Unicast	Sets the overall packet type to unicast.
	MPLS Multicast	Sets the overall packet type to multicast.

Section	Field/Control	Description
MPLS Labels with Data		The data associated with all of the labels on the label stack.
	MPLS Labels	Representations of the labels on the label stack. Highlight an item in this list to edit its contents using the *Label* field. NOTE The *Label* field is available for use only if the *Automatically Set Label* check box is cleared.
	Label	The value of the label element of the entry. Several values have specific interpretations which are exclicked to the right of the label value: • 0: IPv4 Explicit NULL Label. Only valid as the one and only entry on the stack, indicating that the entry should be popped and forwarding of the packet should be done based on the IPv4 header. • 1: Router Alert Label. Valid anywhere in the stack except at the bottom. Used to signal an alert to the software associated with the router that finds this at the top of the stack. • 2: IPv6 Explicit NULL Label. As in '0', but with IPv6 header interpretation. • 3: Implicit NULL Label. A reserved value used within a router. • 4-15: Reserved.
	Experimental Use	A three-bit field that may be used for experimental purposes.
	Bottom of Stack (last entry)	A single bit that represents the last entry (bottom) of the stack.
	Time to Live	The TTL field. It is decremented by routers as they process label stack entries.
	Automatically Set 'Bottom of Stack' Bit	If selected, the *Bottom of Stack* field above is dimmed and made unavailable. The 'S' (bottom of stack) bit is automatically set for the bottom stack entry and reset for all other entries.
	Automatically Set Label	If selected, the *Label* field is dimmed (inactive). The label values are automatically assigned. If cleared, you can enter a custom value for the label that is highlighted in the *MPLS Labels* list.
	Add	Click this button to add a new label to the bottom of the label stack.
	Remove	Click this button to delete the highlighted label entry in the list.

Section	Field/Control	Description
		All entries below the deleted entry are renumbered up so that the stack always reads: *Label1, Label2, Label3, ...*
MPLS Label Encoding		The data display reflects the data associated with the entire stack. As changes are made in the *MPLS Labels with Data* field, they are reflected in this field. Changes can also be made in this field and then reflected back into the label stack through the *Decode* button.
	Decode	Used to move changes from the *MPLS Label Encoding* field back to the label stack.

Edit OAM

The *OAM* button opens the *OAM* dialog, which allows for the configuration of all stateless OAM PDUs, such as Information, Event Notification, Variable Request, Variable Response, Loopback, and Organization Specific. The *OAM* dialog differs depending on the Code field that is selected. It is shown (with Information code selected) in *Figure:OAM Dialog–Information Code*. It is shown with other code selections on the next page.

Figure:OAM Dialog–Information Code

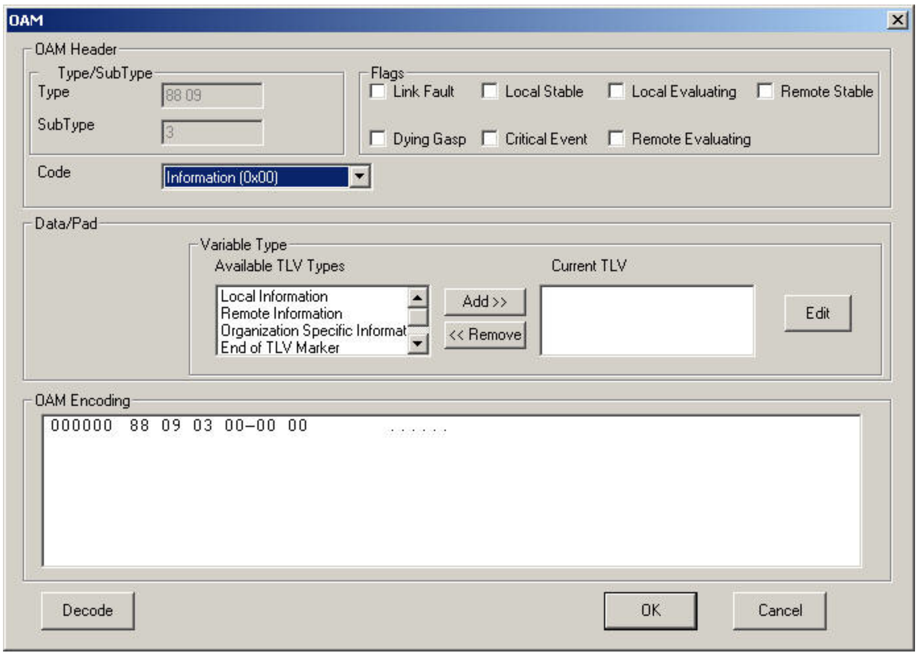


Figure:OAM Dialog–Event Notification Code

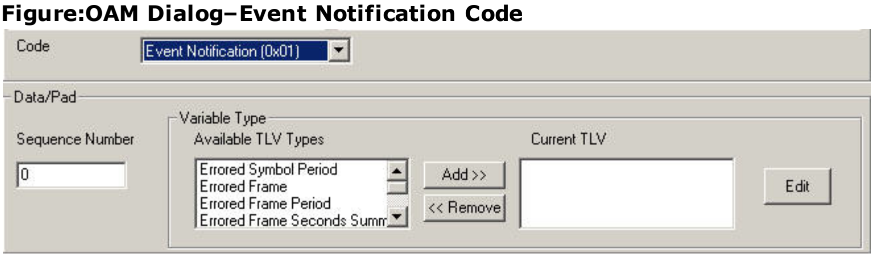


Figure:OAM Dialog–Variable Request Code

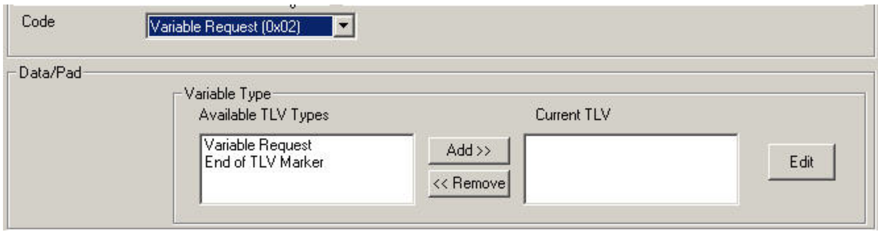


Figure:OAM Dialog–Variable Response Code

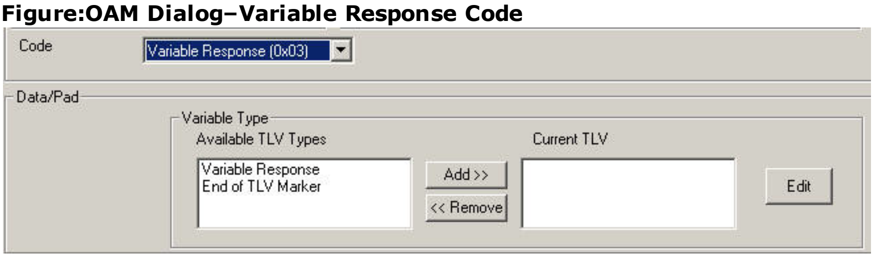


Figure:OAM Dialog–Loopback Control Code

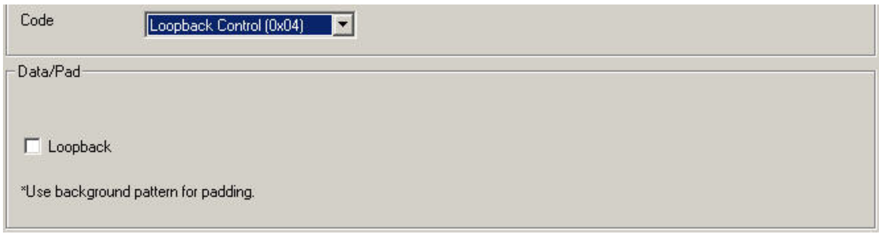
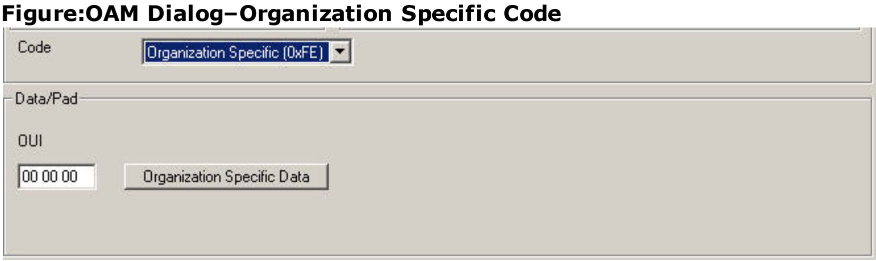


Figure:OAM Dialog–Organization Specific Code



The fields and controls in this dialog are described in *Table:OAM Dialog*.

Table:OAM Dialog

Section	Field/Control	Description
OAM Header	Type/Subtype	Type: 88 09 (Slow Protocols) Subtype: 3 (0x03 = OAM)
	Flags	check boxes to enable flags. A 2-byte flags field contains the discovery status of local and remote OAM entities, as well as fault indications. Link Fault Local Stable Local Evaluating Remote Stable Dying Gasp Critical Event

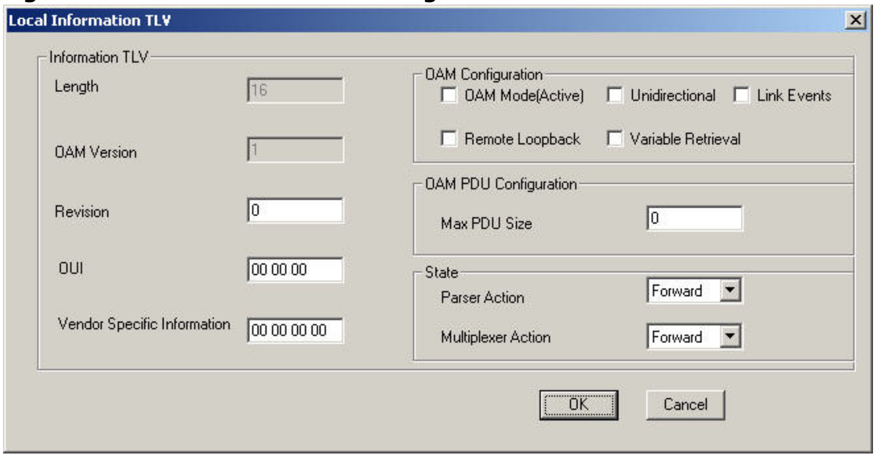
Section	Field/Control	Description
		Remote Evaluating
	Code	OAM PDU types: Information [0x00] Event Notification [0x01] Variable Request [0x02] Variable Response [0x03] Loopback Control [0x04] Organization Specific [0xFE]
Data/Pad	Sequence	Only present when Code = Event Notification (*Figure:OAM Dialog–Event Notification Code*) The OAM client increments the Sequence Number for each unique Event Notification OAMPDU formed by the OAM client. A particular Event Notification OAMPDU may be sent multiple times with the same sequence number. Upon receiving an Event Notification OAMPDU, the OAM client compares the Sequence Number with the last received Sequence Number. If equal, the current event is a duplicate and is ignored by the OAM client. Default = 0
	Loopback	Only present when Code = Loopback Control (*Figure:OAM Dialog–Loopback Control Code*) check box (to enable) NOTE Use background pattern for padding.
	OUI	Only present when Code = Organization Specific (*Figure:OAM Dialog–Organization Specific Code*) Organizationally Unique Identifier
	Organization Specific Data (button)	Click the **Organization Specific Data** button to open the editor to display and edit data. An example is shown below.
	Available TLV Types	List of TLV types depends on the Code selection For Code = Information [0x00] (*Figure:OAM Dialog–Information Code*) Local Information (*Local/Remote Information TLV Dialog*) Remote Information (*Local/Remote Information TLV Dialog*) Organization Specific Information (*Organization Specific Information/Event TLV Dialog*) End of TLV Marker For Code = Event Notification [0x01] (*Figure:OAM*

Section	Field/Control	Description
		Dialog–Event Notification Code) Errored Symbol Period (*Errored Symbol Period TLV Dialog*) Errored Frame (*Errored Frame / Period TLV Dialog*) Errored Frame Period (*Errored Frame / Period TLV Dialog*) Errored Frame Seconds Summary (*Errored Frame Seconds Summary TLV Dialog*) Organization Specific (*Organization Specific Information/Event TLV Dialog*) End of TLV Marker For Code = Variable Request [0x02] (*Figure:OAM Dialog–Variable Request Code*) Variable Request (*Variable Request TLV*) End of TLV Marker For Code = Variable Response [0x03] (*Figure:OAM Dialog–Variable Response Code*) Variable Response (*Variable Request TLV*) End of TLV Marker
	Current TLV	Click the **Edit** button to open the TLV editing dialog for the selected TLV.
OAM Encoding		Editable display of the OAM portion of packet view
	Decode button	After editing in the OAM Encoding pane, click **Decode** to load the revised values into the appropriate fields in the OAM configuration.

Local/Remote Information TLV Dialog

The Local and Remote Information TLV dialogs are identical in content. Local and remote information is used in the discovery process. The Local Information TLV dialog (identical to the Remote version) is shown in *Figure:Local Information TLV Dialog*.

Figure:Local Information TLV Dialog



The fields and controls are described in *Table:Local / Remote Information TLV Dialog*.

Table:Local / Remote Information TLV Dialog

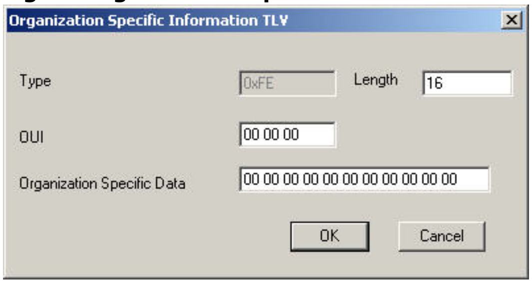
Section	Field/Control	Description
Information TLV	Length	*Read only.* Default = 0
	OAM Version	*Read only.* Value: 1 (0x01) The version supported by the DTE.
	Revision	Default = 0 The current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes.
	OUI	Default = 00 00 00 24-bit 3-octet field, Organizationally Unique Identifier.
	Vendor Specific Information	Default = 00 00 00 00 4-octet field, 32-bit identifier that may be used to differentiate a vendor's product models/versions.
OAM Configuration	OAM Mode (Active)	Active when selected, passive when cleared. DTE configured in active or passive mode.
	Unidirectional	OAM provides an OAM PDU-based mechanism to notify the remote DTE when one direction of a link is non-operational and therefore data transmission is disabled. The ability to operate a link in a unidirectional mode for diagnostic purposes supports failure detection and notification.
	Link Events	Selected = is capable of interpreting link events
	Remote Loopback	Selected = is capable of OAM remote loopback mode
	Variable Retrieval	Selected = is capable of variable retrieval (*Variable Request TLV*)
OAM PDU Con-	Max PDU Size	Default = 0

Section	Field/Control	Description
figuration		11-bit field which represents the largest OAM PDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.
State	Parser Action	Forward: Lower layer forwards request to upper layer. Loopback: Lower layer will send back request. Discard: Lower layer will discard request.
	Multiplexer Action	Forward: Sends on the request over the wire. Discard: Discards the request.

Organization Specific Information/Event TLV Dialog

The Organization Specific Information TLV is used for vendor extensions. The 32-bit vendor specific information is not defined and is used to encode the model or version of the platform. The Organization Specific Information TLV dialog is shown in *Figure:Organization Specific Information TLV Dialog*.

Figure:Organization Specific Information TLV Dialog



The fields and controls in this dialog are described in *Table:Organization Specific Information TLV Dialog*.

Table:Organization Specific Information TLV Dialog

Field	Description
Type	*Read only.* 0xFE = Organization Specific Information
Length	Editable. Default = 16
OUI	Default = 00 00 00 24-bit 3-octet field, Organizationally Unique Identifier.
Organization Specific Data	The value of the Organization Specific Information TLV. This field's length and contents are editable.

Event Notification TLVs

There are several types of Event Notification TLVs:

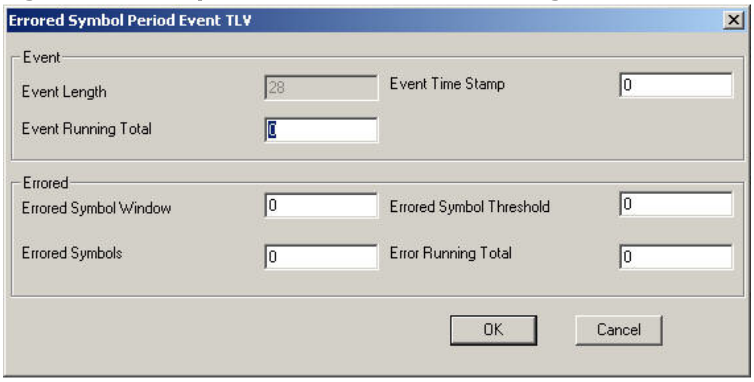
- Errored Symbol Period (*Errored Symbol Period TLV Dialog*)
- Errored Frame (*Errored Frame / Period TLV Dialog*)
- Errored Frame Period (*Errored Frame / Period TLV Dialog*)

- Errored Frame Seconds Summary (*Errored Frame Seconds Summary TLV Dialog*)
- Organization Specific (*Organization Specific Information/Event TLV Dialog*)

Errored Symbol Period TLV Dialog

The Errored Symbol Period Event TLV counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. The Errored Symbol Period Event TLV dialog is shown in *Figure:Errored Symbol Period Event TLV Dialog*.

Figure:Errored Symbol Period Event TLV Dialog



The fields and controls are described in *Table:Errored Symbol Period Event TLV Dialog*.

Table:Errored Symbol Period Event TLV Dialog

Section	Field/Control	Description
Event	Event Length	This one-octet field indicates the length (in octets) of this TLV_tuple. Errored Symbol Period Event uses a length value of 40 (0x28).
	Event Time Stamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
	Event Running Total	This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32-bit unsigned integer.
Errored	Errored Symbol Window	This eight-octet field indicates the number of symbols in the period, encoded as a 64-bit unsigned integer. Lower bound: the number of symbols in one second for the underlying physical layer. Upper bound: the number of symbols in one minute for the underlying physical layer.
	Errored Symbol Threshold	This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 64-bit unsigned

Section	Field/Control	Description
		integer. Lower bound: zero symbol errors. Upper bound: unspecified.
	Errored Symbols	This eight-octet field indicates the number of symbol errors in the period, encoded as a 64-bit unsigned integer.
	Error Running Total	This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

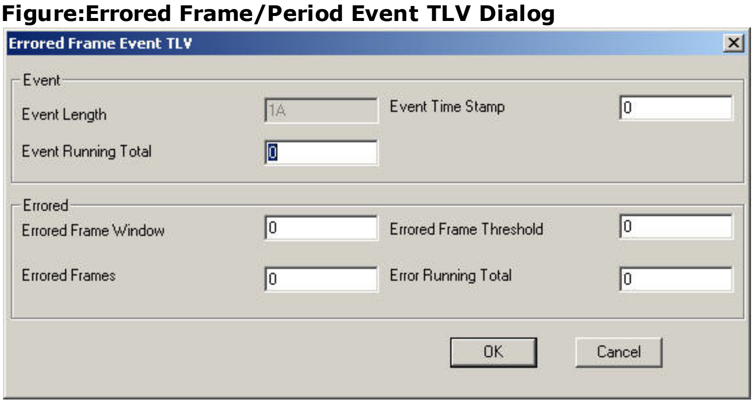
Errored Frame / Period TLV Dialog

The *Errored Frame Event TLV* counts the number of errored frames detected during the specified period. The period is specified by a time interval. This event is generated if the errored frame count is equal to or greater than the specified threshold for that period. This event is generated at the end of the event window rather than when the threshold is crossed.

The *Errored Frame Period Event TLV* counts the number of errored frames detected during the specified period. The period is specified by a number of received frames. This event is generated if the errored frame count is greater than or equal to the specified threshold for that period (for example, if the errored frame count is greater than or equal to 10 for the last 1,000,000 frames received). This event is generated at the end of the event window rather than when the threshold is crossed.

The *Errored Frame Event* and *Errored Frame Period Event* TLV dialogs are identical in content. The Errored Frame/Period Event TLV dialog is shown in *Figure:Errored Frame/Period Event TLV Dialog*.

Figure:Errored Frame/Period Event TLV Dialog



The fields and controls are described in *Table:Errored Frame/Period Event TLV Dialog*.

Table:Errored Frame/Period Event TLV Dialog

Section	Field/Control	Description
Event	Event Length	This one-octet field indicates the length (in octets) of this TLV_tuple. **Errored Frame Event**: uses a length value of 26 (0x1A).

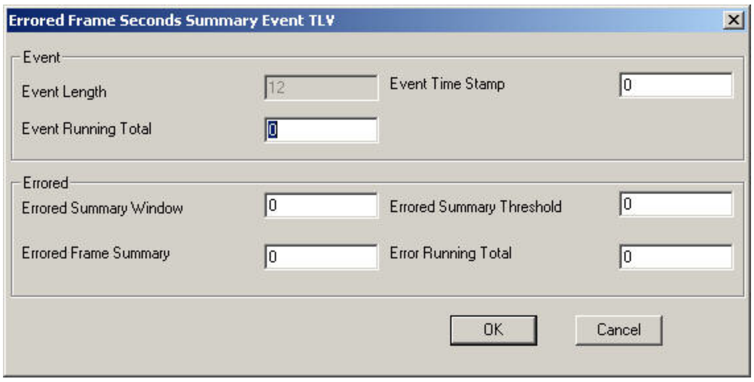
Section	Field/Control	Description
		Errored Frame Period Event: uses a length value of 28 (0 x 1C).
	Event Time Stamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
	Event Running Total	This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32-bit unsigned integer.
Errored	Errored Frame Window	**Frame Event**: this two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer. Lower bound - one second Upper bound - one minute **Frame Period Event**: this four-octet field indicates the duration of period in terms of frames, encoded as a 32-bit unsigned integer. Lower bound: the number of minFrameSize frames that can be received in 100 ms on the underlying physical layer. Upper bound: the number of minFrameSize frames that can be received in one minute on the underlying physical layer.
	Errored Frame Threshold	This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 32-bit unsigned integer. Lower bound: zero frame errors Upper bound: unspecified
	Errored Frames	This four-octet field indicates the number of detected errored frames in the period, encoded as a 32-bit unsigned integer.
	Error Running Total	This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Errored Frame Seconds Summary TLV Dialog

The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. The Errored Frame Seconds Summary TLV dialog is shown in *Figure:Errored Frame Seconds Sumary TLV Dialog*.

This event is generated at the end of the event window rather than when the threshold is crossed.

Figure:Errored Frame Seconds Sumary TLV Dialog



The fields and controls are described in *Table:Errored Frame Seconds Summary TLV Dialog*.

Table:Errored Frame Seconds Summary TLV Dialog

Section	Field/Control	Description
Event	Event Length	This one-octet field indicates the length (in octets) of this TLV_tuple. Errored Frame Seconds Summary Event uses a length value of 18 (0x12).
	Event Time Stamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
	Event Running Total	This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32-bit unsigned integer.
Errored	Errored Summary Window	This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer. Lower bound: 10 seconds Upper bound: 900 seconds
	Errored Summary Threshold	This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer. Lower bound: zero errored seconds Upper bound: unspecified
	Errored Frame Summary	This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.
	Error Running Total	This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Variable Request TLV

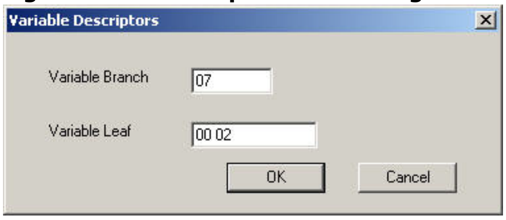
The process of variable retrieval involves transferring Ethernet counters and statistics through Variable Containers/Descriptors.

MIB variables are queried through the use of Variable Request OAMPDUs and returned through the use of Variable Response OAMPDUs. Variable Request OAMPDUs use data structures called Variable Descriptors. An OAM client may request one or more variables in each Variable Request OAMPDU.

Variable Response OAMPDUs use data structures called Variable Containers (*Variable Response TLV*). Each returned Variable Container resides within a single Variable Response OAMPDU. If a Variable Container does not fit within a Variable Response OAMPDU, an error code is returned. In returning requested variables, an OAM client generates at least one and perhaps additional Variable Response OAMPDUs per received Variable Request OAMPDU.

The Variable Request TLV dialog (Variable Descriptors) is shown in *Figure:Variable Request TLV Dialog*.

Figure:Variable Request TLV Dialog



The fields and controls in this dialog are described in *Table:Variable Request TLV Dialog*.

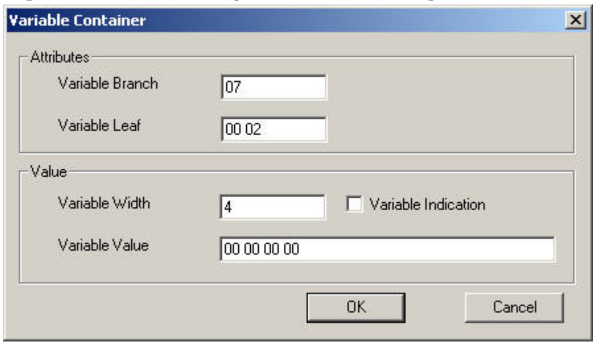
Table:Variable Request TLV Dialog

Field	Description
Variable Branch	One-byte hex number. *(default - 0x07)* Branch of data within the Management Information Base (MIB) Variable Branches may reference attributes, objects or packages. If an object or package is referenced, only the attributes within the object or package shall be found within the Variable Container.
Variable Leaf	Two-byte hex number. *(default - 00 02)* Sub-branch of data within the Management Information Base (MIB)

Variable Response TLV

The Variable Response TLV dialog (Variable Container) is shown in *Figure:Variable Response TLV Dialog*. Variable Containers are used to return MIB attributes, objects and packages. One or more Variable Containers may exist in the Data field of a Variable Response OAM PDU.

Figure:Variable Response TLV Dialog



The fields and controls are described in *Table:Variable Response TLV Dialog*.

Table:Variable Response TLV Dialog

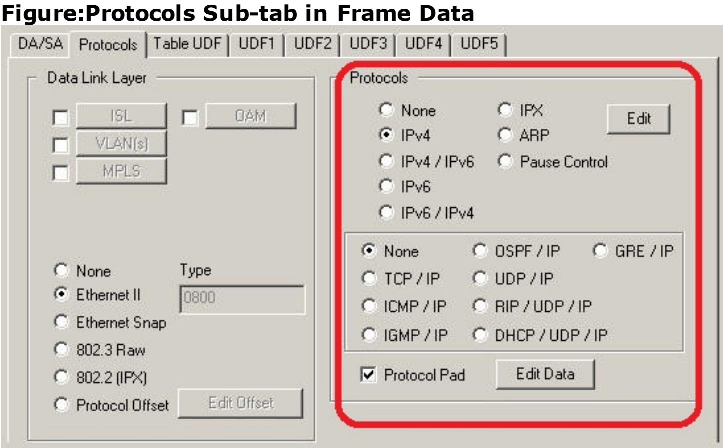
Section	Field/Control	Description
Attributes	Variable Branch	The one-octet Variable Branch field for the specific attribute, package or object being returned. NOTE At present, only attributes are supported (IxOS 5.10 SP2). Variable Branches may reference attributes, objects or packages. If an object or package is referenced, only the attributes within the object or package shall be found within the Variable Container.
	Variable Leaf	The two-octet Variable Leaf field for the specific attribute, package or object being returned.
Value	Variable Width	This field either contains the actual width of the attribute or a Variable Indication providing information as to the reason this particular attribute could not be returned. When bit 7 = 1, bits 6:0 represent a Variable Indication. There is no Variable Value field when bit 7 = 1. When bit 7 = 0, bits 6:0 represent the length of the Variable Value field in octets. An encoding of 0x00 equals 128 octets. All other encodings represent actual lengths.
	Variable Indication	See Variable Width, above. When selected, Variable Width changes to Indication Value.
	Variable Value	If the Variable Width field contains a width value, the fourth field is the Variable Value field, which contains the attribute. This field may be up to 128 octets in length. Octets of the attribute are ordered most significant first, followed by each successive octet.

Section	Field/Control	Description
		If the Variable Width field contains a Variable Indication, the Variable Value field does not exist.

Protocols—Network Layer

The network layer protocols are listed in *Table:Protocol Choices*. The *Edit* button in the Protocols section of the dialog allows the header parameters to be modified. The header parameters of the IP Version 4 and Version 6 protocols may be edited from the *Edit* button. The IP protocol section of the *Protocols* sub-tab is shown in *Figure:Protocols Sub-tab in Frame Data*.

Figure:Protocols Sub-tab in Frame Data



The header parameters of the IPv4 sub-protocols (UDP, TCP, ICMP, IGMP, RIP, DHCP, OSPF, and GRE) may be edited from the *Edit* button of the IPv4 protocol page. Headers for IPv6 sub-protocols (UDP, TCP, and ICMP) may be edited from the *Edit* button of the IPv6 protocol page.

Table: Protocol Choices

Protocol Type	Protocol Choice	Description
Main Protocol (Network Layer)	None	No protocol specific handling is performed.
	IPv4	Internet Protocol Version 4. Includes all others with an /IP designation for use with IPv4. *Configuring IPv4 Headers*.
	IPv4/IPv6	This selection is for use with IPv4 packets which are tunneled over IPv6. When the *Edit* button is clicked, the *IPv6 Header* dialog opens first. That dialog contains a button labeled *IPv4*, which opens the *IPv4 Header* dialog. *Configuring IPv4 Headers and Configuring IPv6 Headers.*
	IPv6	Internet Protocol Version 6. Includes all others with an /IP designation for use with IPv6 (TCP/IP, UDP/IP, and ICMP/IP). *Configuring IPv6 Headers*.
	IPv6/IPv4	This selection is for use with IPv6 packets which are tunneled over IPv4. When the *Edit* button is clicked, the *IPv4 Header* dialog opens first. That dialog contains a button labeled *IPv4*, which opens the *IPv6*

Protocol Type	Protocol Choice	Description
		Header dialog. *Configuring IPv4 Headers* and *Configuring IPv6 Headers*
	IPX	(Not available for POS modules.) Internetwork Packet Exchange. Used in Novell networking. *IPX Protocol*.
	ARP	(Not available for POS modules.) Address Resolution Protocol. An IP sub-protocol used to resolve IP addresses into MAC addresses.*ARP Header Dialog*.
	Pause Control	(Not available for POS modules.) A MAC/Layer 2 flow control mechanism used by switches and other network infrastructure elements. *Pause Control*.
Sub-protocol	None	No sub-protocol specific handling is performed.
	TCP/IP	Transmission Control Program. A connection-oriented, reliable IP sub-protocol. *TCP Header Dialog*. Available for use with IPv4 and IPv6.
	ICMP/IP	Internet Control Management Protocol. Used to control assorted IP parameters. *ICMP Header Dialog*. Available for use with IPv4 and IPv6.
	IGMP/IP	Internet Group Management Protocol. Used for multicast group management. *IGMP Header Dialog*. Available for use with IPv4.
	OSPF/IP	Open Shortest Path First Protocol. An internal routing protocol. *OSPF Header Dialog*. Available for use with IPv4.
	UDP/IP	User Datagram Protocol. A connection-less, unreliable IP sub-protocol.*UDP Header Dialog* and *RIP Header Dialog.* Available for use with IPv4 and IPv6.
	RIP/UDP/IP	Router Information Protocol. Used to communicate routing entries within a LAN.*RIP Header Dialog*. Available for use with IPv4.
	DHCP/UDP/IP	Dynamic Host Control Protocol and BOOTP. Used to set IP address and other parameters of hosts at host start time. *DHCP Header Dialog*. Available for use with IPv4.
	GRE/IP	Generic Routing Encapsulation.*GRE Header Dialog*. Available for use with IPv4.
Protocol Pad		Allows to add data padding between the Protocol Header and the Payload Data patterns.
Edit Data		Allows to edit the Protocol Pad data. This button is only active when the Protocol Pad check box is selec-

Protocol Type	Protocol Choice	Description
		ted.*Protocol Padding* for information on the *Protocol Padding* dialog.

Internet Protocol (IP) headers for Ethernet and POS frames can be configured for both IPv4 and IPv6 in the Protocol section of the Frame Data page. The Transport protocol-specific headers associated with the Internet Protocol frames may also be configured in this section.

Configuration dialogs for the IP and Transport protocols can be accessed by selecting the desired IP protocol version, the transport protocol, if any, and then pressing the *Edit* button. A dialog is displayed for selected version of the IP protocol. *Edit* buttons in the main dialog provide access to the dialogs for the transport protocol header configuration.

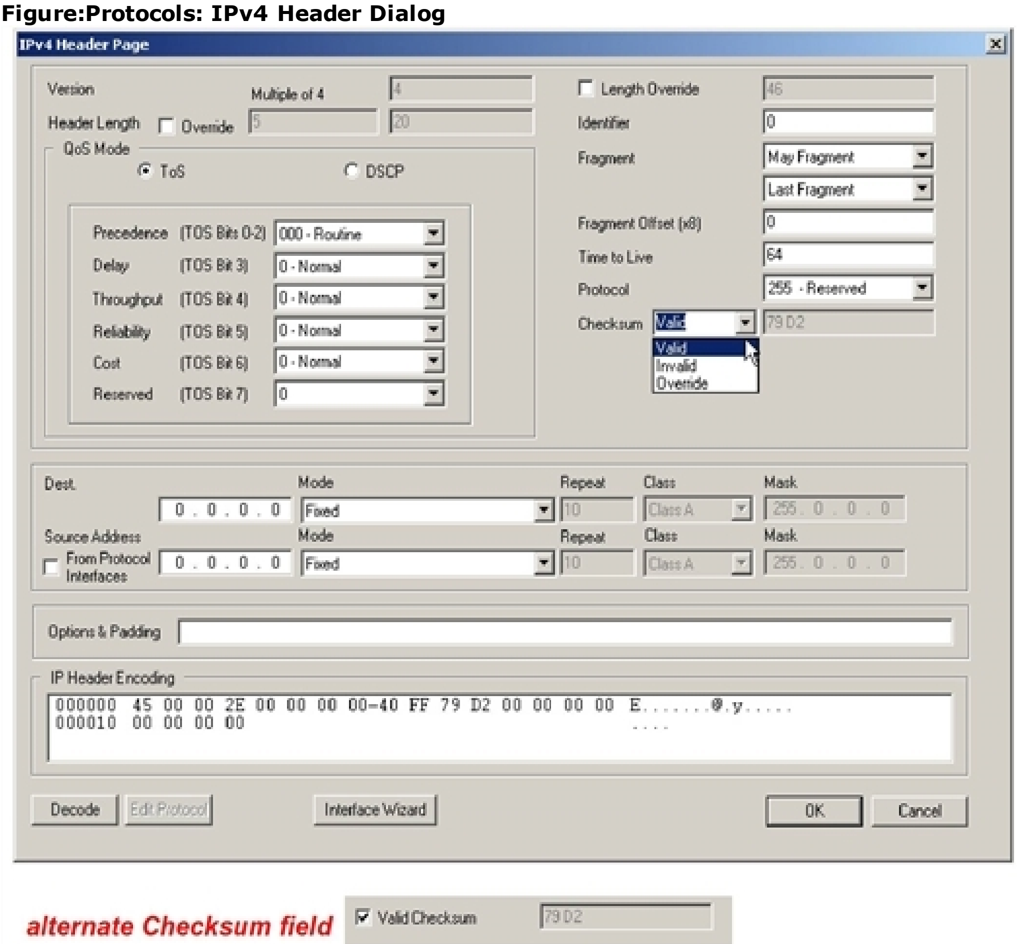
For information on configuring Internet Protocol frame headers, go to the appropriate section below.

- *Configuring IPv4 Headers*.
- *Configuring IPv6 Headers*.

Configuring IPv4 Headers

The *IPv4 Header* dialog is shown in *Figure:Protocols: IPv4 Header Dialog*. This dialog is accessed by selecting the *IPv4* option button in the Protocols section, then selecting the *Edit* button.

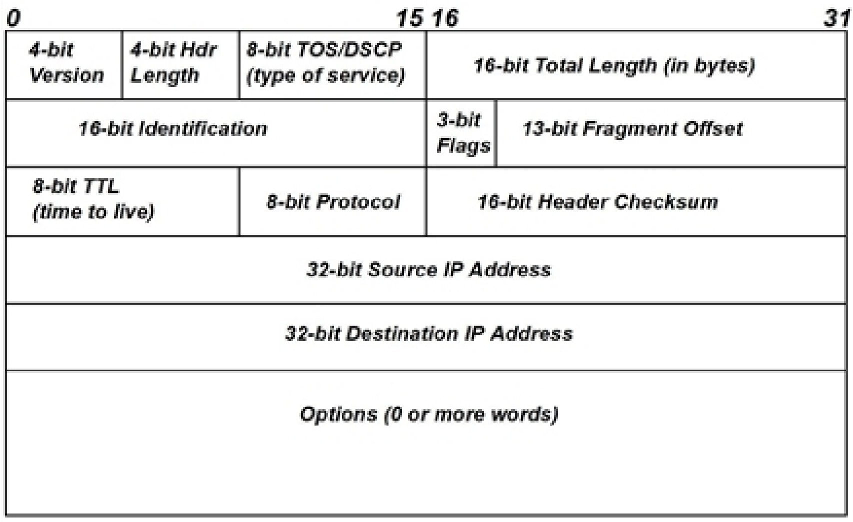
Figure:Protocols: IPv4 Header Dialog



When the protocols choice is set to *IPv4* before the *Edit* button is clicked, the dialog is as shown with the Protocol set to *255 - reserved*. When protocols including *UDP* are selected before the *Edit* button is clicked, the *Protocol* field is set to *17 - UDP*. For other protocols ending with /IP, the corresponding protocol is shown in the *Protocol* field, and *Edit* buttons for those protocols are displayed.

The fields in this dialog allow all parts of an IPv4 header to be specified. The format of an IPv4 header is shown in *Figure:Protocols: IPv4 Header Format*.

Figure:Protocols: IPv4 Header Format



The correspondence between the fields of an IPv4 header and the elements of the *IPv4 Header* dialog which set those fields are described in *Table:IPv4 Header Fields Set by the IPv4 Header Dialog*.

Table:IPv4 Header Fields Set by the IPv4 Header Dialog

IP Header Field	Dialog Fields	Description
Version	Version	Not editable. It is always set to 4.
Header Length	Header Length	Automatically calculated to include the minimum of five 32-bit words plus optional data and padding. Internet Header Length is the length of the internet header represented in 32- bit words or in multiples of 4 bytes. So max header length can be = 4*15 = 60 bytes. Minimum valid header length = 4*5 = 20 bytes.
	Overide	If selected, enables header length override.
	Multiple of 4	(default = 5) Enter a number that is multiplied by 4, resulting in the new header length.
QoS Mode		Select a option button for the QoS mode type, either TOS or DSCP.
TOS	Precedence (TOS Bits 0-2)	The precedence is set in the 3 most significant bits of the TOS. Eight choices are offered: • 000 - Routine

IP Header Field	Dialog Fields	Description
		• 001 - Priority • 010 - Immediate • 011 - Flash • 100 - Flash Override • 101 - CRITIC/ECP • 110 - Internet Control • 111 - Network Control.
	Delay (TOS Bit 3)	The next bit in the TOS signifies Delay, with choices of Normal and Low.
	Throughput (TOS Bit 4)	The next bit in the TOS signifies Throughput, with choices of Normal and High.
	Reliability (TOS Bit 5)	The next bit in the TOS signifies Reliability, with choices of Normal and High.
	Cost (TOS Bit 6)	The next bit is the TOS signifies Cost, with choices of Normal and Low.
	Reserved (TOS Bit 7)	The last bit in the TOS byte is reserved but may be set to 0 or 1.
DSCP	DSCP Mode	Allows you to select a DSCP mode from a list in the pull-down menu. Options are: • Default • Class Selector • Assured Forwarding • Expedited Forwarding • Custom The available configurable fields change depending on the DSCP mode choice. For more information regarding the options, *DSCP QoS Options*.
Total Length	Length Override	If the box is not selected, then the length field is automatically set, based on the Frame Size set in the *Frame Control* tab. If the box is selected, then the value may be overridden.
Identification	Identifier	Set according to the value in the dialog.
Flags	Fragment	Two choice dialogs are available to set the two most significant bits: May Fragment/Don’t Fragment; and Last Fragment/More Fragments.
Fragment Offset	Fragment Offset	Set according to the value in the dialog.
TTL	Time to Live	Set according to the value in the dialog.
Protocol	Protocol	Set according to the choice in the dialog. NOTE A new protocol type is added to this list. The new type is PIM denoted by the numeric value of 103. This type defines the next protocol after the IPv4

IP Header Field	Dialog Fields	Description
		NOTE header. If PIM filter is selected, the next protocol is PIM.
Header Checksum		NOTE Refer to the *Ixia Platform Reference Manual*, Table 1-7, for list of load modules supporting checksum override. Depending on the load module, there are 2 different ways in which Checksum is handled:
	Valid Invalid Override (list)	For load modules supporting Checksum Override, choose one of the following checksum options from the list: • Valid: The calculated header checksum is automatically calculated. • Invalid: The calculated header checksum is automatically calculated (with error). • Override: The header checksum can be set to a user-defined, 2-octet value in the box to the right.
	Valid Checksum (check box)	If selected, this causes a valid header checksum to be generated. If cleared, an invalid checksum is generated.
Source IP Address	Source Address	May be set to a constant value, or incremented/decremented across a range of addresses.*Source and Destination IPv4 Addresses for additional information.*
	From Protocol Interfaces	Selecting this check box synchronizes the Source or Destination Address with the values set in the Protocol Interfaces wizards. *Protocol Interfaces* for more information. Note that this check box only appears on certain modules.
Destination IP Address	Destination Address	May be set to a constant value, or incremented/decremented across a range of addresses.*Source and Destination IPv4 Addresses for additional information.*
	Sync from PPP (Source and Destination Address	Selecting this check box synchronizes the Source or Destination Address with the values set in the PPP negotiation window.*PPP Negotiation*. Note that these check boxes only appear on modules with PPP options enabled.
Options	Options & Padding	Additional IP options which may be added to the end of the IP headers. The header must be a multiple of words and therefore may require padding. Just type hex data into this field. When finished,

IP Header Field	Dialog Fields	Description
		select another field or press the *Decode* button.
Edit button		This button allows to edit the transport protocol selected on the Protocol sub-tab of the Frame Data tab (as discussed in *Protocols—Network Layer*). The button title changes depending on the selected protocol, and opens a different dialog depending on the selected protocol. There may also be more than one edit button if more than one protocol is selected. The protocol options are: • *UDP Header Dialog* • *RIP Header Dialog* • *TCP Header Dialog* • *IGMP Header Dialog* • *OSPF Header Dialog* • *ICMP Header Dialog* • *ARP Header Dialog* • *DHCP Header Dialog* • *GRE Header Dialog*
Interface Wizard		Selecting this button opens a wizard that allows to create or edit protocol interfaces for use with DHCP. For more information on creating protocol interfaces,Chapter 10,*Protocol Interfaces.* This option is not available on all load modules.

DSCP QoS Options

Differentiated Services Code Point is a way of prioritizing traffic, like ToS. For more information on DSCP, refer to the DSCP—Differentiated Services Code Point—section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

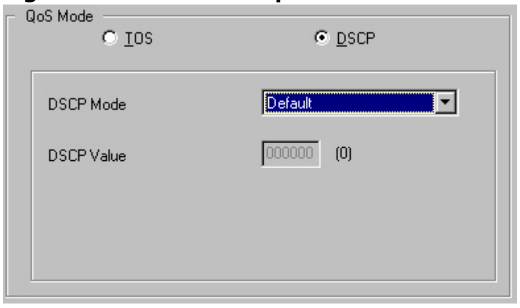
Depending on your selection, the list of configurable options changes. The following sections detail the DSCP options:

- *Default*
- *Class Selector*
- *Assured Forwarding*
- *Expedited Forwarding*
- *Custom*

Default

Selecting the *Default* DSCP options sets DSCP fields to the default setting of all zeros (0). This option is shown in *Figure:Default DSCP Option*.

Figure:Default DSCP Option

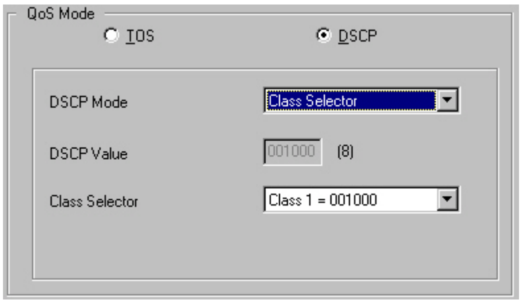


Note that the default mode sets the DSCP to 'best effort.' The DSCP value in bits is shown in the *DSCP Value* field.

Class Selector

The Class Selector option allows to specify the DSCP traffic class.*Figure:DSCP Class Selector* shows the dialog for the Class Selector option.

Figure:DSCP Class Selector



Use the Class Selector pull-down menu to choose the class. The options are:

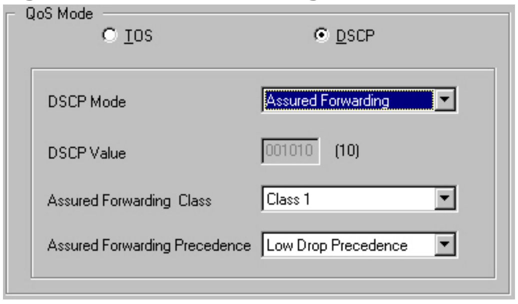
- Class 1 - 001000
- Class 2 - 010000
- Class 3 - 011000
- Class 4 - 100000
- Class 5 - 101000
- Class 6 - 101000
- Class 7 - 111000

The DSCP value in bits is shown in the *DSCP Value* field.

Assured Forwarding

The *Assured Forwarding* option allows to set both the Class and Precedence DSCP bits. *Figure:Assured Forwarding* shows the *Assured Forwarding* display.

Figure:Assured Forwarding



Use the Class Selector pull-down menu to choose the class. The options are:

- Class 1 - 001000
- Class 2 - 010000
- Class 3 - 011000
- Class 4 - 100000
- Class 5 - 101000
- Class 6 - 101000
- Class 7 - 111000

Use the Assured Forwarding Precedence pull-down menu to select the drop. The options are:

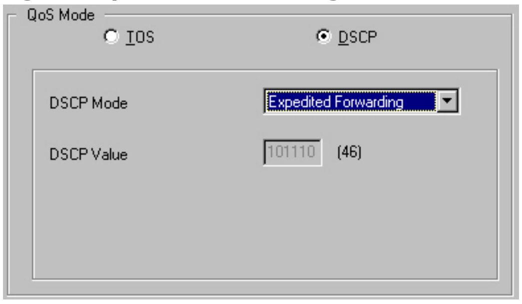
- Low
- Medium
- High

The DSCP value in bits is shown in the *DSCP Value* field.

Expedited Forwarding

The EF PHB can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (Diffserv) domains. Such a service appears to the end-points like a point-to- point connection or a virtual leased line. This service has also been described as Premium service. *Figure:Expedited Forwarding* shows the Expedited Forwarding option.

Figure:Expedited Forwarding

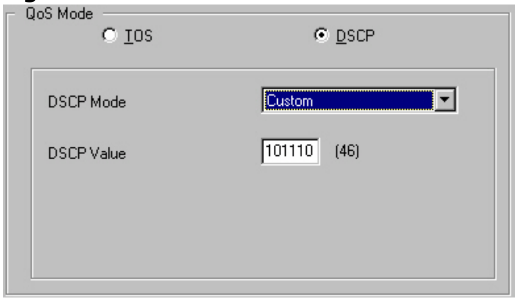


The DSCP value in bits is shown in the *DSCP Value* field. Expedited Forwarding sets the bit values to 101110.

Custom

This setting allows to set the DSCP bits to any combination.*Figure:Custom* shows the *Custom* option.

Figure:Custom



The DSCP value in bits is shown in the *DSCP Value* field. In Custom mode, it is possible to modify these bits directly.

Source and Destination IPv4 Addresses

The source and destination IPv4 addresses may be independently controlled and allowed to vary across a wide range of addresses. The Mode setting controls the interpretation of the other fields for each address, as described in *Table:IPv4 Address Mode Controls*.

Table:IPv4 Address Mode Controls

Mode	Fields Used	Usage
Fixed	Address	Indicates the single value that is used for all frames.
Increment Host/ Decrement Host	Address Repeat Mask	The Increment Host and Decrement Host modes modify the host part of the IP address. The Address field indicates the starting value. The Repeat field controls the number of increments/decrements that occurs. When the repetition is completed, the address is reset to the starting value and incrementing/decrementing continues. The Mask field indicates which parts of the IP address range are network versus hosts. The '1's indicate network and the '0's indicate hosts.
Continuous Increment Host/ Continuous Decrement Host	Address Mask	The Continuous Increment Host and Continuous Decrement Host modes modify the host part of the IP address. The Address field indicates the starting value. The Mask field indicates which parts of the IP address range are network versus hosts. The '1's indicate network and the '0's indicate hosts.
Increment Network/ Decrement Network	Address Repeat Mask	The Increment Network and Decrement Network modes modify the network part of the IP address.

Mode	Fields Used	Usage
		The Address field indicates the starting value. The Repeat field controls the number of increments/decrements that occurs. When the repetition is completed, the address is reset to the starting value and incrementing/decrementing continues. The Class field indicates what range of networks to iterate over. See the table below for a description of class choices.
Continuous Increment Network/Continuous Decrement Network	Address Mask	The Continuous Increment Network and Continuous Decrement Network modes modify the host part of the IP address. The *Address* field indicates the starting value. The *Class* field indicates what range of networks to iterate over. See the table below for a description of class choices.
Random	Address Mask	The *Random* mode causes the IP address to vary randomly.
Custom Mask Increment	BitMask	You can custom-define the entire 32-bit mask to be used with the address—by entering 1's and 0's to replace the X's. The Address field indicates the starting value.
Custom Mask Decrement	BitMask	You can custom-define the entire 32-bit mask to be used with the address—by entering 1's and 0's to replace the X's. The Address field indicates the starting value.
Custom Mask Continuous Increment	BitMask	You can custom-define the entire 32-bit mask to be used with the address—by entering 1's and 0's to replace the X's. The Address field indicates the starting value.
Custom Mask Continuous Decrement	BitMask	You can custom-define the entire 32-bit mask to be used with the address—by entering 1's and 0's to replace the X's. The Address field indicates the starting value.
Custom Mask Random	BitMask	You can custom-define the entire 32-bit mask to be used with the address—by entering 1's and 0's to replace the X's. The Address field indicates the starting value.

The Class field is used for incrementing/decrementing the network bits of an IPv4 address. The class of the network determines which bits may change. In *Table:Class to Bit Mask Conversion Table*, an 'A' stands for a bit that is set from the *Address* field and 'X' are bits that will be allowed to change according to the counting mode and values.

Table:Class to Bit Mask Conversion Table

Class	Bit Mask
Class A	AAAAAAAA.XXXXXXXX.XXXXXXXX.XXXXXXXX
Class B	AAAAAAAA.AAAAAAAA.XXXXXXXX.XXXXXXXX
Class C	AAAAAAAA.AAAAAAAA.AAAAAAAA.XXXXXXXX
No mask	XXXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

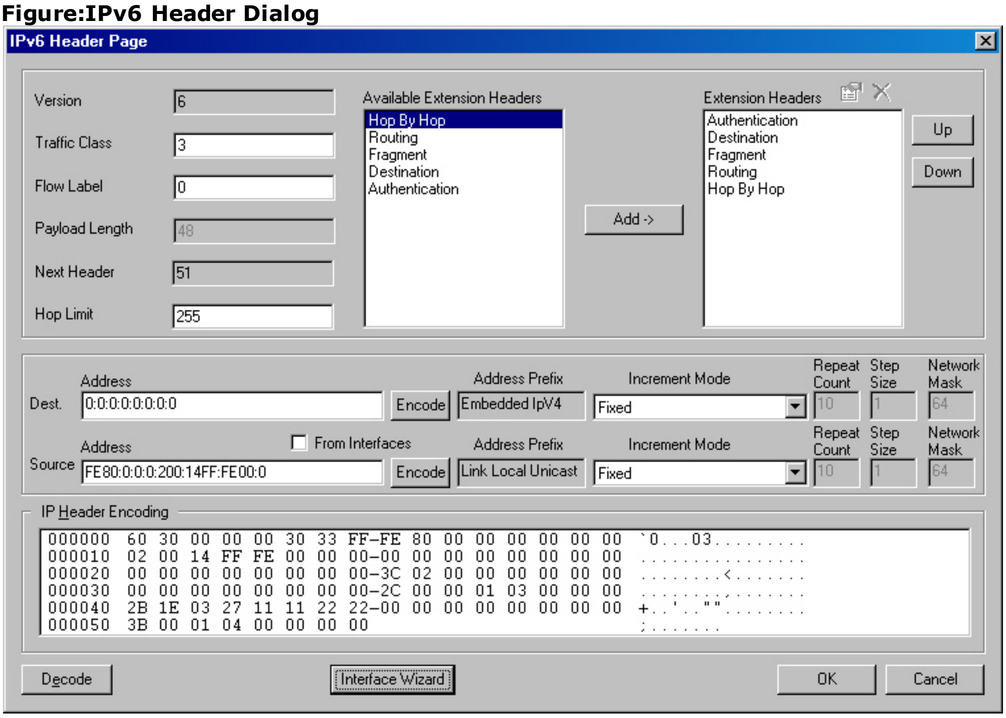
IPv4 Header Encoding

Values which are set in the dialog are reflected in the hexadecimal display of the IP Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from this display; all editing occurs in type-over mode. After any change, the *Decode* button should be clicked to reflect these changes back into the dialog fields.

Configuring IPv6 Headers

The *IPv6 Header* dialog can be accessed when the IPv6 protocol is selected, by pressing the *Edit* button. The *IPv6 Header* dialog is shown in *Figure:IPv6 Header Dialog*.

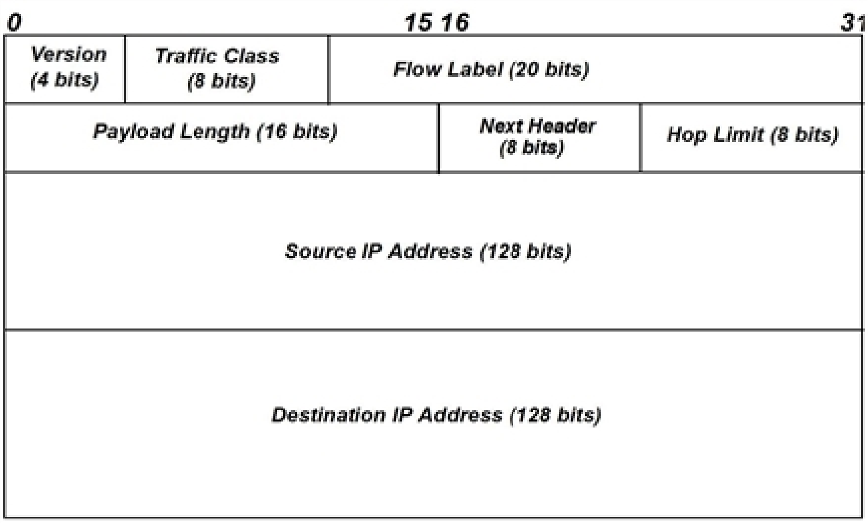
Figure:IPv6 Header Dialog



The fields in this dialog allow the parts of an IPv6 header to be specified. Note that when no IPv6 Extension headers are set up for the IPv6 header, the *Next Header* field value in the dialog is '59.' The format of an IPv6 header is shown in *Figure:Protocols: IPv6 Header Format*.

IPv6 Header Format

Figure:Protocols: IPv6 Header Format



The correspondence between the fields of an IPv6 header and the elements of the *IPv6 Header* dialog which set those fields are described in *Table:IPv6 Header Fields Set by the IPv6 Header Dialog*.

Table:IPv6 Header Fields Set by the IPv6 Header Dialog

IP Header Field	Dialog Field	Description
Version	Version	(Read-only). Always set to 6 to indicate IP version 6 header.
	Traffic Class	Identifies the class or priority of the IPv6 packet.
Flow Label	Flow Label	Labels a sequence of packets for which it requests special handling by IPv6-capable routers. Routers that do not support this function must set this field to zero when creating, forwarding, or receiving the packet.
Payload Length	Payload Length	Length of the IPv6 payload, which is the length of the entire packet which follows the IPv6 header (in octets). The payload includes any extension headers.
Next Header	Next Header	(Read-only) Identifies the type of the next extension header. When value = 59, means 'No Next Header.'
Hop Limit	Hop Length	The Hop limit is decremented by 1 by each node that forwards the packet. When the value reaches 0, the packet is discarded.
	Extension Headers	A list of IPv6 extension headers, which contain optional internet-layer information.
	Available Extension Headers	The extension headers currently available are: • Hop By Hop. *IPv6 Hop-by-Hop Extension Header* for additional information. • Routing. *IPv6 Routing Extension Header* for additional information. • Fragment. *IPv6 Fragment Extension Header* for

IP Header Field	Dialog Field	Description
		additional information. • Destination. *IPv6 Destination Extension Header* for additional information. • Authentication. *IPv6 Authentication Extension Header* for additional information.
	Add ->	Select/highlight an available Extension Header, and then press the *Add ->* button to add that header to the list of Extension Headers in the right pane.
	 Edit Icon	To edit an Extension header in the Extension Headers window. Highlight the Extension, then press the *Edit* icon. A corresponding dialog appears.
	 Delete Icon	To delete an Extension header in the Extension Headers window. Highlight the Extension, then press the *Delete* icon.
Destination Address	Destination Address	The 128-bit IPv6 destination address. May be set to a constant value, or incremented/decremented across a range of addresses. *Source and Destination IPv6 Addresses* for additional information.
Source Address	Source Address	The 128-bit IPv6 source address. May be set to a constant value, or incremented/decremented across a range of addresses. *Source and Destination IPv6 Addresses* for additional information.
	Sync from PPP (Source and Destination Address	Selecting this check box synchronizes the Source or Destination Address with the values set in the PPP negotiation window.See *PPP Negotiation*. Note that these check boxes only appear on modules with PPP options enabled.
	From Interfaces	Selecting this check box synchronizes the Source or Destination Address with the values set in the Protocol Interfaces wizards. *Protocol Interfaces* for more information. Note that this check box only appears on certain modules.
	Encode	Press the *Encode* button to display the *IPv6 Address* dialog, where specific types of IPv6 addresses can be configured. *IPv6 Address Dialog* for additional information.
	Address Prefix	Displays the selected IPv6 address prefix as set in the *IPv6 Address* dialog. *IPv6 Address Dialog* for additional information. Note when using the *User Defined* prefix, this field will not display *User Defined*. Instead, a prefix from the list of other prefixes is displayed, based on what the user defined prefix most closely resembles.

IP Header Field	Dialog Field	Description
	Mode Repeat Count Step Size Network Mask	*Source and Destination IPv6 Addresses* for additional information.
	IP Header Encoding	Values that are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display. All editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these the directly edited changes back into the dialog fields.

Source and Destination IPv6 Addresses

The Source and Destination IPv6 addresses may be independently controlled and allowed to vary across a wide range of addresses. The Mode setting controls the interpretation of the other fields for each address, as described in *Table:IPv6 Address Mode Controls*.

Table:IPv6 Address Mode Controls

Mode	Fields Used	Usage
Fixed	Address	Indicates the single address value that will be used for all frames.
Increment Host/ Decrement Host	Address Repeat Count Step Size Network Mask	The Increment Host and Decrement Host modes modify the host part of the IPv6 address. The **Address** field indicates the starting value. The **Repeat Count** field controls the number of increments/decrements that will occur. When the repetition is completed, the address is reset to the starting value and incrementing/decrementing continues. (Read-only and set to '1'.)The **Step Size** indicates the size of the increment/decrement. The **Network Mask** field indicates which parts of the IP address range are network versus hosts. It specifies the number of bits (counting from the left) in the network part of the 128-bit IPv6 address. The remainder of the bits specify the host part of the address (of which, only the last 32 bits may currently be configured). The default is 64 bits.
Increment Network/ Decrement Network	Address Repeat Count Step Size Network Mask	The Increment Network and Decrement Network modes modify the network part of the IPv6 address. The **Address** field indicates the starting value.

Mode	Fields Used	Usage
		The **Repeat Count** field controls the number of increments/decrements that will occur. When the repetition is completed, the address is reset to the starting value and incre-menting/decrementing continues. (Currently Read-only and set to '1'.)The **Step Size** indicates the size of the incre-ment/decrement. The **Network Mask** field indicates which parts of the IP address range are network versus hosts. It specifies the number of bits (counting from the left) in the network part of the 128-bit IPv6 address. The remainder of the bits specify the host part of the address (of which, only the last 32 bits may currently be configured). The default is 64 bits.

In addition, the options available for Mode differ depending on the IPv6 prefix con-figuration, as set in the *IPv6 Address* dialog (IPv6 Address Dialog for more information).*Table:Mode Options for Prefix Settings* shows the options available for each prefix setting.

Table:Mode Options for Prefix Settings.

IPv6 Address Prefix	Mode Options	Description
Reserved NSAP Allocation IPX Allocation User Defined Address	• Fixed • Incr/Decr Host • Incr/Dect Net-work	Fixed address, or increment/decrement the Host/Network addresses.
Global Unicast Address	• Fixed • Incr/Decr Inter-face ID • Incr/Decr Gbl Uni Top Lvl ID • Incr/Decr Gbl Next Lvl ID • Incr/Decr Gbl Site Lvl ID	Fixed address, or increment/decrement the Interface ID, Top Level ID, Next Level ID, or Site Level ID.
Link Local Unicast	• Fixed • Incr/Decr Inter-face ID	Fixed address, or increment/decrement the Interface ID.
Site Local Unicast	• Fixed • Incr/Decr Inter-face ID • Incr/Decr Site Local Uni Sub-	Fixed address, or increment/decrement the Interface ID or the Subnet ID.

IPv6 Address Prefix	Mode Options	Description
	net ID	
Multicast Address	• Fixed • Incr/Decr Multicast Group ID	Fixed address, or increment/decrement the Multicast Group ID.

IPv6 Address Dialog

When the *Encode* button is clicked for the IPv6 Source Address or Destination Address, the *IPv6 Address* dialog set is displayed. The IPv6 address prefix comprises the leftmost contiguous bits (leading bits) of the address, and is of variable length, depending on the address type. This set of dialogs allows configuration for 8 prefix types, one for each of the 7 main types of IPv6 addresses, plus a user-defined dialog for custom configuration.

- *IPv6 Reserved Address.*
- *IPv6 NSAP Allocation Address*.
- *IPv6 IPX Allocation Address*.
- *IPv6 Global Unicast Address*.
- *IPv6 Link-Local Unicast*.
- *IPv6 Site-Local Unicast Address*.
- *IPv6 Multicast Address*.
- *IPv6 User-Defined Address*.

IPv6 addressing provides 128-bit identifiers for individual interfaces and sets of interfaces. It is important to note that the IPv6 addresses apply **only** to interfaces, and not to nodes. The three types of IPv6 addresses are:

- **Unicast:** A unicast address identifies a single interface. A packet with this type of destination address is sent to that specific unicast interface.
- **Anycast:** An anycast address identifies a set of interfaces, usually for different nodes. A packet destined for an anycast address will be delivered to the 'nearest' single node in the set of interfaces, where the term 'nearest' refers to the node with the lowest routing metric cost.
- **Multicast:** A multicast address identifies a set of interfaces, usually for different nodes. A packet destined for a multicast address will be delivered to all of the nodes in the set of interfaces.

NOTE The IPv6 design does not support broadcast addresses. This function is replaced by the multicast addressing scheme.

IPv6 Address Shortcuts

Since the 128-bit IPv6 addresses are so long, RFC 2373 provides methods for creating comclicked versions of these addresses, in cases where there are long strings of consecutive zero bits.

- The standard form of an IPv6 address is written as:

  x : x : x : x : x : x : x : x

  where each 'x' represents 16 bits of data in hexadecimal format.

- If x = 16 zero bits (0000000000000000), x may be represented by a single '0', as in:

  x : x : x : x : 0 : x : x : x

- If several 16-bit groups in the middle of the address consist of all zero bits, they may be represented as shown in the example below:

  x : x : 0 : 0 : 0 : 0 : x : x

  or, using another shortcut:

  x : x **: :** x : x

- For environments where both IPv6 and IPv6 addresses are used, a convenient combination may be used, as shown in RFC 2373. This method uses the form:

  x : x : x : x : x : x : d.d.d.d

  where the x's in the six high order groups are combined with 32 low order bits exclicked as a decimal value, in the standard IPv4 address format. An example is:

  0 : 0 : 0 : 0 : 0 : 0 : 10.1.1.3

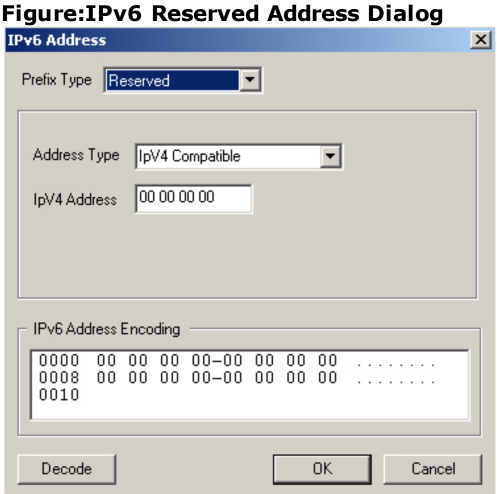
  which can be comclicked to the following form:

  : : 10.1.1.3

IPv6 Reserved Address

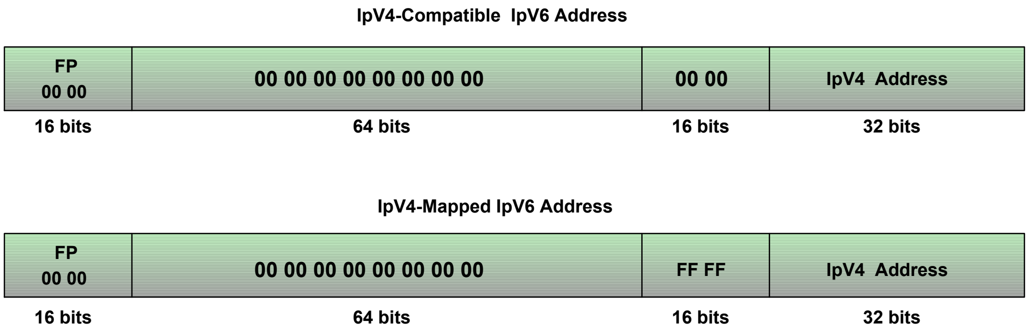
The dialog for the IPv6 Reserved address is shown in *Figure:IPv6 Reserved Address Dialog*. Its controls are displayed by selecting *Reserved* from the list in the *Prefix Type* field.

Figure:IPv6 Reserved Address Dialog



The dialog for the IPv6 Reserved address contains options which allow IPv6 traffic to be transmitted in IPv4 networks.

Figure:Format of IPv6 Addresses in Reserved Dialog



The fields in this address format and the corresponding implementation in the IxExplorer IPv6 address dialog is described in *Table:IPv6 Reserved Address Fields*.

Table:IPv6 Reserved Address Fields

Header Field	Dialog Element	Description
Format Prefix	Prefix Type: Reserved	The defined address prefix value = 0000 0000 (binary).
	Address Type	Choose one type of address: • **IpV4 Compatible**: With this method, IPv6 packets can be tunneled over IPv4 networks. • **IpV4 Mapped**: With this method, IPv6 nodes can communicate with IPv4 devices. However, a host or router must have an IPv4/IPv6 dual-stack for header translations.
	IpV4 Address	(4 octets) The IPv4 address of the interface (hex value).
	Ipv6 Address Encoding	Values which are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

IPv6 NSAP Allocation Address

The dialog for the IPv6 NSAP Allocation address is shown in *Figure:IPv6 NSAP Allocation Address Dialog*. Its controls are displayed by selecting *NSAP Allocation* from the list in the *Prefix Type* field.

Figure:IPv6 NSAP Allocation Address Dialog

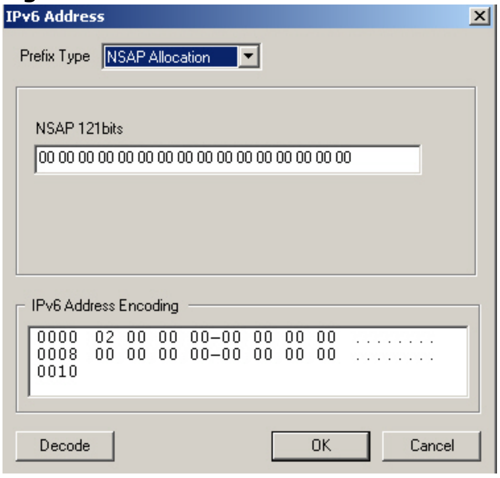
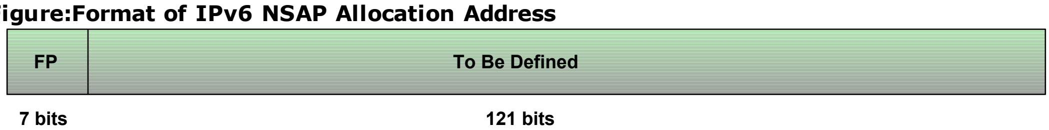


Figure:Format of IPv6 NSAP Allocation Address



The fields in this address format and the corresponding implementation in the dialog for the IPv6 NSAP Allocation address is described in *Table:IPv6 NSAP Allocation Address Fields*.

Table:IPv6 NSAP Allocation Address Fields

Header Field	Dialog Element	Description
Format Prefix	Prefix Type: NSAP Allocation	The defined address prefix value = 0000 001 (binary).
	NSAP 121 bits	These bits are to be entered by you.
	Ipv6 Address Encoding	Values which are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

IPv6 IPX Allocation Address

The dialog for the IPv6 IPX Allocation address is shown in *Figure:IPv6 IPX Allocation Address Dialog*. Its controls are displayed by selecting *IPX Allocation* from the list in the *Prefix Type* field.

Figure:IPv6 IPX Allocation Address Dialog

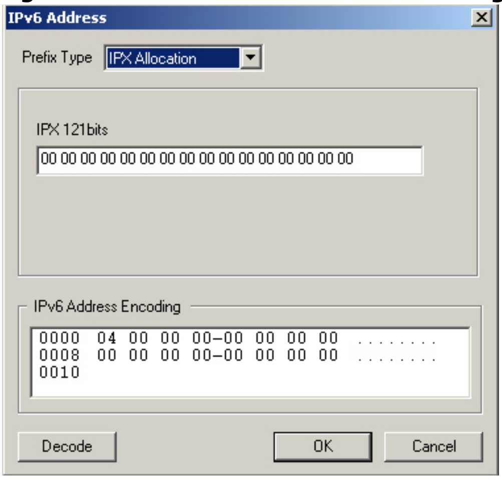
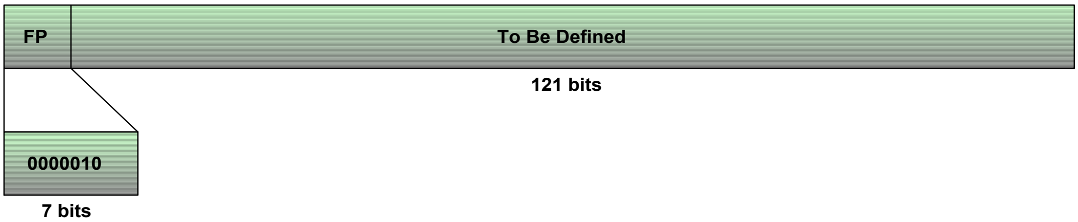


Figure:Format of IPv6 IPX Allocation Address



The fields in this address format and the corresponding implementation in the dialog for the IPv6 IPX Allocation address are described in *Table:IPv6 IPX Allocation Address Fields*.

Table:IPv6 IPX Allocation Address Fields

Header Field	Dialog Element	Description
Format Prefix	Prefix Type: IPX Alloc-ation	The defined address prefix value = 0000 010 (binary).
To Be Defined	IPX 121 bits	These bits are to be entered by you.
	Ipv6 Address Encoding	Values which are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encod-ing box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

IPv6 Global Unicast Address

The dialog for an IPv6 Global Unicast address is shown in *Figure:IPv6 Global Unicast Address Dialog*. Its controls are displayed by selecting *Global Unicast* from the list in the *Prefix Type* field.

Figure:IPv6 Global Unicast Address Dialog

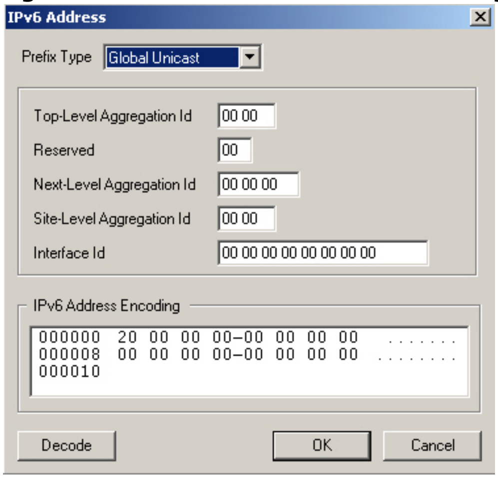
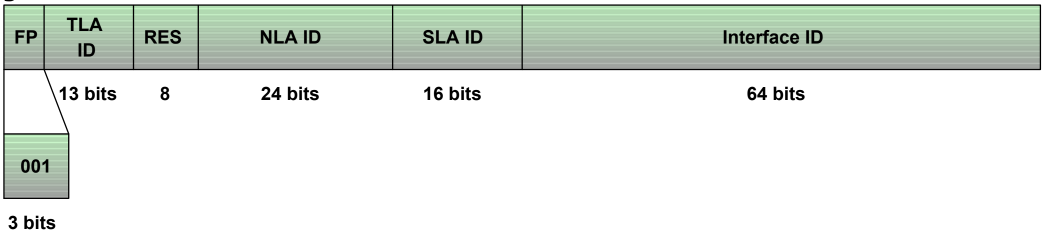


Figure:Format of IPv6 Global Unicast Address



The format of the IPv6 aggregratable Global Unicast address is shown in this diagram. The fields in this address format and the corresponding implementation in the dialog for an IPv6 Global Unicast address are described in *Table:IPv6 Global Unicast Address Fields*.

Table:IPv6 Global Unicast Address Fields

Header Field	Dialog Element	Description
Format Prefix (FP)	Format Prefix	The defined address prefix value = 001 (binary).
Top Level Aggregation ID (TLA ID)	Top Level Aggregation ID	Describes the highest level in the routing hierarchy. Values in Hex format.
Reserved (RSVD)	Reserved	Reserved for future use. Values in Hex format.
Next-Level Aggregator ID (NLA)	Next-Level Aggregator ID	To describe the next level down in the routing hierarchy. Values in Hex format.
Site-Level Aggregator ID (SLA)	Site-Level Aggregator ID	Local level in the hierarchy. Can be used to describe subnets at the site level. Local significance. Values in Hex format.
Interface ID	Interface ID	Describes the interface on the link, which must be unique on that link.

Header Field	Dialog Element	Description
	IPv6 Address Encoding	Values that are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

IPv6 Global Unicast 3587 Address

The dialog for an IPv6 Global Unicast address is shown in *Figure:IPv6 Global Unicast 3587 Address Dialog*. Its controls are displayed by selecting *Global Unicast 3587* from the list in the *Address Prefix* field.

Figure:IPv6 Global Unicast 3587 Address Dialog

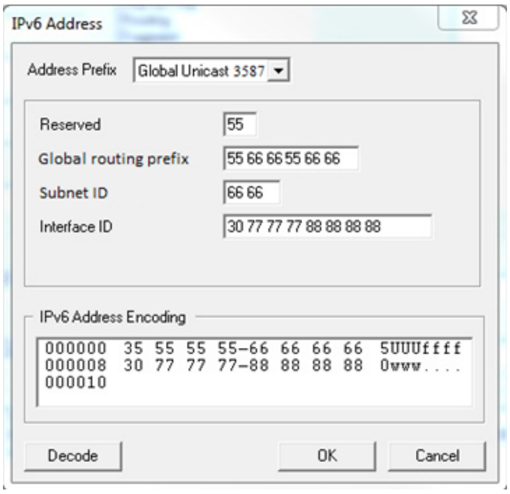


Figure:Format of IPv6 Global Unicast 3587 Address

```
| 3 |      45 bits         |  16 bits  |        64 bits             |
+---+----------------------+-----------+----------------------------+
|001|global routing prefix| subnet ID |        interface ID        |
+---+----------------------+-----------+----------------------------+
```

The format of the IPv6 Global Unicast 3587 address is shown in this diagram.

IPv6 Link-Local Unicast

Every IPv6 interface must have at least one Link-Local Unicast address. The dialog for the Link-Local Unicast address is shown in *Figure:IPv6 Link-Local Unicast Address Dialog*. Its controls are displayed by selecting *Link-Local Unicast* from the list in the *Prefix Type* field.

Figure:IPv6 Link-Local Unicast Address Dialog

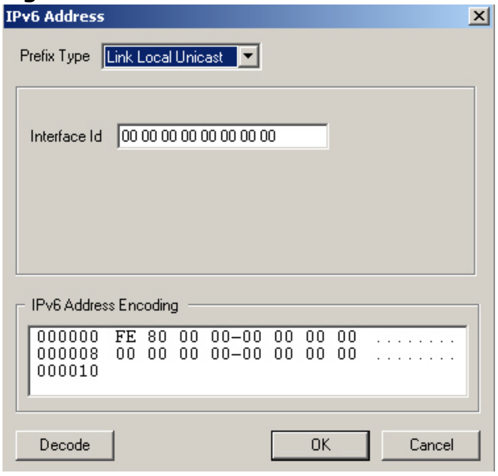
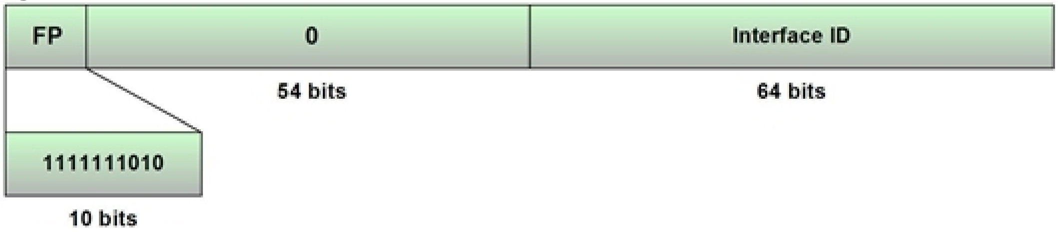


Figure:Format of IPv6 Link-Local Address



Link-local addresses are one of the two local-use unicast addresses: link-local and site-local. Link-local addresses are used on a single link, for purposes such as neighbor discovery, or when there are no routers present. IPv6 packets which include this type of address may not be forwarded to other links by a router.

The fields in this address format and the corresponding implementation in the dialog for the Link-Local Unicast address are described in *Table:IPv6 Link-Local Address Fields*.

Table:IPv6 Link-Local Address Fields

Header Field	Dialog Element	Description
Format Prefix	Prefix Type: Link-Local Unicast	The defined address prefix value = 1111 1110 10 (binary).
Interface ID	Interface ID	The interface of a node on this link.
	Ipv6 Address Encoding	Values that are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

IPv6 Site-Local Unicast Address

The dialog for the IPv6 Site-Local Unicast address is shown in *Figure:Site-Local Unicast Address Dialog*. Its controls are displayed by selecting *Site-Local Unicast* from the list in the *Prefix Type* field.

Figure:Site-Local Unicast Address Dialog

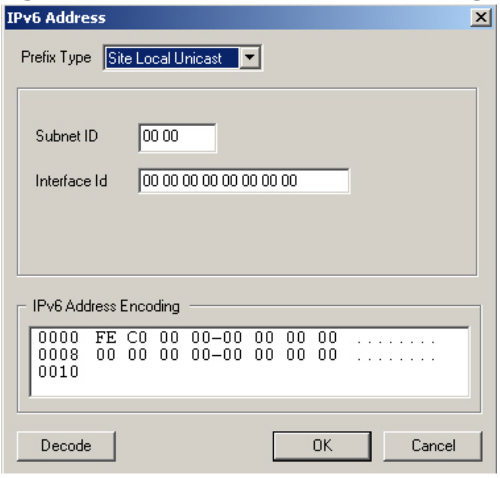
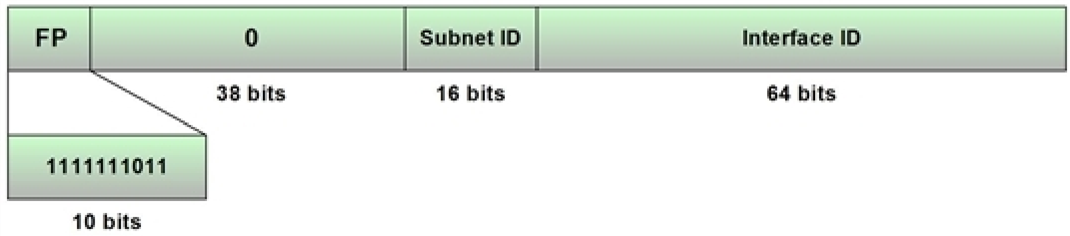


Figure:Format of IPv6 Site-Local Address



Site-local addresses are one of the two local-use unicast addresses: site-local and link-local. Site-local addresses are used inside a single site, on one subnet, and no global prefix is required. IPv6 packets which include this type of address may not be forwarded outside of the site by a router.

The fields in this address format and the corresponding implementation in the dialog for the IPv6 Site-Local Unicast address are described in *Table:IPv6 Site-local Unicast Address Fields*.

Table:IPv6 Site-local Unicast Address Fields

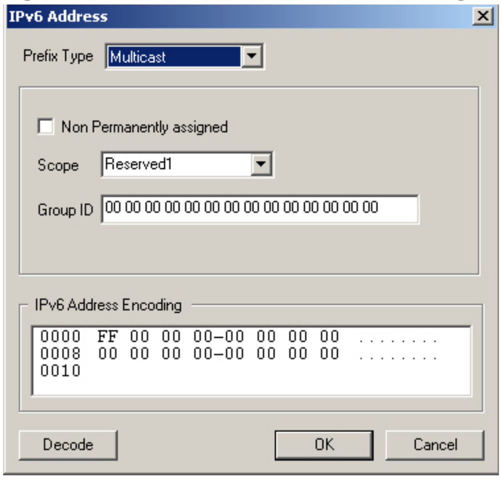
Header Field	Dialog Element	Description
Format Prefix	Prefix Type: Site-local Unicast	The defined address prefix value = 1111 1110 11 (binary).
Subnet ID	Subnet ID	The identifier for the subnet at this site.
Interface ID	Interface ID	The interface ID for a node at this site (on this defined subnet).
	Ipv6 Address Encoding	Values that are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited

Header Field	Dialog Element	Description
		changes back into the dialog fields.

IPv6 Multicast Address

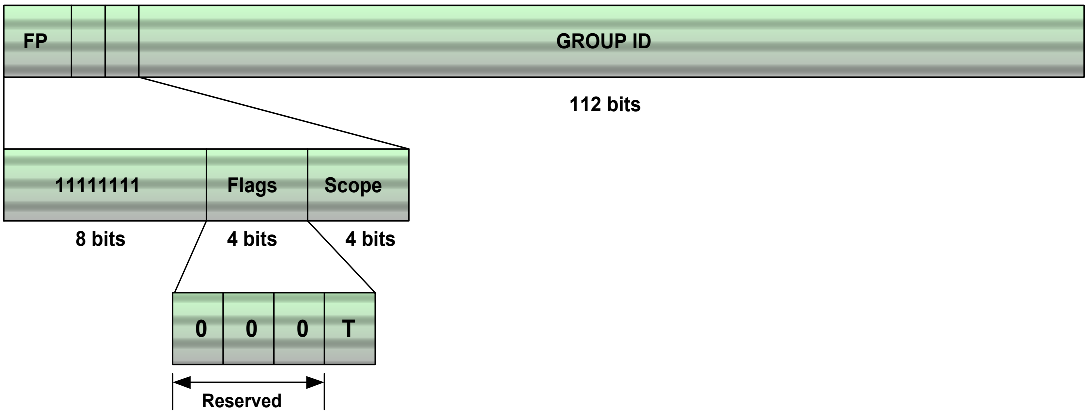
The dialog for the IPv6 Multicast addresses is shown in *Figure:IPv6 Multicast Addresses Dialog*. Its controls are displayed by selecting *Multicast* from the list in the *Prefix Type* field.

Figure:IPv6 Multicast Addresses Dialog



The IPv6 Multicast addresses are used as identifiers for groups of nodes. They must not be used as source address in any IPv6 protocol routing packet header or in IPv6 packets.

Figure:IPv6 Multicast Address Fields



The fields in this address format and the corresponding implementation in the dialog for the IPv6 Multicast addresses are described in *Table:IPv6 Multicast Address Fields*.

Table:IPv6 Multicast Address Fields

Header Field	Dialog Element	Description
Format Prefix	Prefix Type: Multicast	The defined address prefix value = 1111 1111 (binary).
Flags	Non Permanently assigned	Checking this box indicates that the multicast address is 'transient' - not permanently-assigned. (The Flags field is set to 000**1**.)

Header Field	Dialog Element	Description
		If box is left clear, indicates that this is a permanently-assigned ('well-known') multicast address, per the IANA. (The Flags field is set to 000**0**, which is the default.)
Scope	Scope	Limits the scope of a multicast group. The scope value identifies the type of scope.
		Unassigned: (Values = 3 & 4, 6 & 7, 9 through D)
		Reserved1: (Value = 0)
		Node-local scope: (Value = 1) This mutlicast address identifies the group of all IPv6 nodes within the Node-local scope. Also identifies the group of all IPv6 routers within the Node-local scope.
		Link-local scope: (Value = 2) This multicast address Identifies the group of all IPv6 nodes within the Link-local scope. Also identifies the group of all IPv6 routers within the Link-local scope.
		Site-local scope: (Value = 5) This multicast address Identifies the group of all IPv6 routers within the Site-local scope.
		Organization-local scope: (Value = 8) This multicast address Identifies the group of all IPv6 routers within the Organizational-local scope.
		Global scope: (Value = E) This multicast address Identifies the group of all IPv6 routers within the Global local scope.
		Reserved2: (Value = F)

Header Field	Dialog Element	Description
Group ID	Group ID	This value is an identifier for a multicast group (permanent or transient), within the given 'scope.'
	IPv6 Address Encoding	Values which are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect these directly edited changes back into the dialog fields.

The default values for the pre-defined Well-Known Multicast Addresses are shown in *Table:IPv6 Default Well-Known Multicast Addresses*. These addresses can never be assigned to any multicast group

Table:IPv6 Default Well-Known Multicast Addresses

Multicast Address Type (as listed in dialog)	Permanent Address
Reserved1	FF 00 00 00 00 00 00 00
Node-local	FF 01 00 00 00 00 00 00
Link-local	FF 02 00 00 00 00 00 00
Site-local	FF 05 00 00 00 00 00 00
Organization-local	FF 08 00 00 00 00 00 00
Global	FF 0E 00 00 00 00 00 00
Reserved2	FF 0F 00 00 00 00 00 00
*Unassigned	FF 03 00 00 00 00 00 00

NOTE

Per RFC 2373, Multicast Addresses with a Scope value of 3, 4, 6, 7, 9, A, B, and C are all 'Unassigned.'

IPv6 User-Defined Address

The dialog for a IPv6 User-Defined address is shown in *Figure:IPv6 User-Defined Address Dialog*. Its controls are displayed by selecting *User Defined* from the list in the *Prefix Type* field.

Figure:IPv6 User-Defined Address Dialog

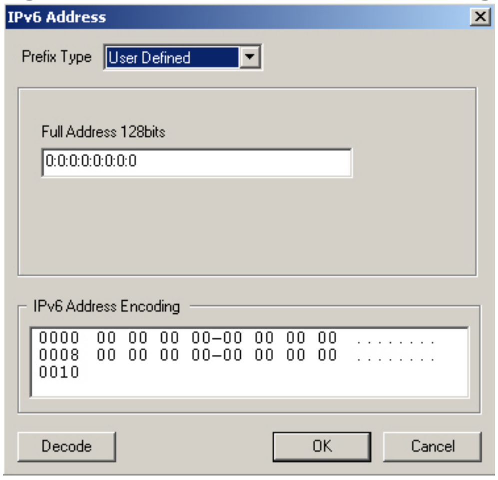
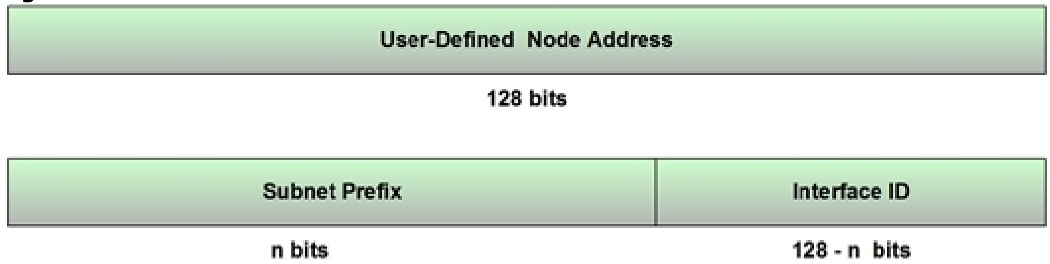


Figure:Possible Formats for IPv6 User-Defined Address



The fields in this address format and the corresponding implementation in the dialog for a IPv6 User-Defined address are described in *Table:IIPv6 User-Defined Address Fields*.

Table:IIPv6 User-Defined Address Fields

Header Field	Dialog Element	Description
N/A	Full Address (128 bits)	The 128-bit address can be set by you. However, the following rules apply: • 0:0:0:0:0:0:0:0, the 'unspecified address' must never be assigned to a node, and must not be used as a destination address in IPv6 packets or IPv6 routing protocol packet headers. • 0:0:0:0:0:0:0:1, the unicast 'loopback address' may never be assigned to any physical interface. It may be used when a node sends a packet to itself. It must not be the source address in IPv6 packets which are destined for another node or forwarded by a router.
	Ipv6 Address Encoding	Values which are set in the dialog are reflected in the hexadecimal display of the IPv6 Header Encoding at the bottom of the dialog. It is also possible to edit the IP Header directly from the display; all editing occurs in type-over mode.
	Decode	After any change in the IP Header Encoding box, the *Decode* button, should be clicked to reflect

Header Field	Dialog Element	Description
		these directly edited changes back into the dialog fields.

NOTE When using the *User Defined* prefix, the Address Prefix field (shown in *Figure: IPv6 Header Dialog* and described in *Figure:IPv6 Header Fields Set by the IPv6 Header*) does not display *User Defined*. Instead, a prefix from the list of other prefixes is displayed, based on what the user defined prefix most closely resembles.

IPv6 Extension Headers

Each of the IPv6 Header Extensions can be edited in dialogs which are accessed through the IPv6 Header dialog. When multiple header extensions are used, the extensions are included in the IPv6 header in the following order:

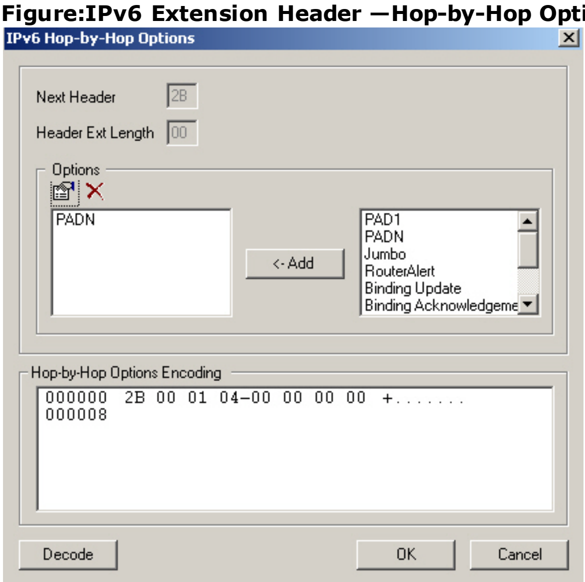
- *IPv6 Hop-by-Hop Extension Header*.
- *IPv6 Routing Extension Header*.
- *IPv6 Fragment Extension Header*.
- *IPv6 Destination Extension Header*.
- *IPv6 Authentication Extension Header*.

Header extensions are added by selecting a header in the *Available Extension Headers* field, and clicking the *Add* button. Alternatively, header extensions can be added by double-clicking a header in the *Available Extension Headers* field.

IPv6 Hop-by-Hop Extension Header

The *IPv6 Hop-by-Hop Options* dialog is shown in *Figure:IPv6 Extension Header —Hop-by-Hop Options*. It is accessed by selecting *Hop-by-Hop* in the *Header Extensions* field of the *IPv6 Header* dialog, then pressing the *Edit Extension Header* icon ( ). Alternatively, this dialog can be opened by double-clicking *Hop-by-Hop*.

Figure:IPv6 Extension Header —Hop-by-Hop Options



The fields and controls for the *IPv6 Hop-by-Hop Options* dialog are described in *Table:IPv6 Hop-by-Hop Options Dialog*.

Table:IPv6 Hop-by-Hop Options Dialog

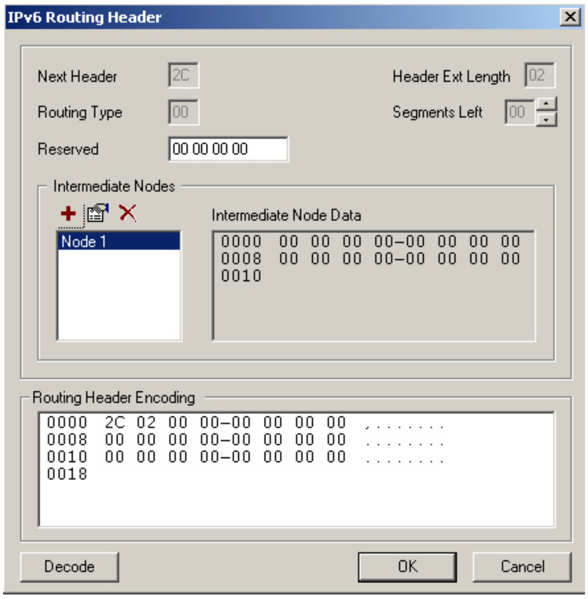
Header Field	Dialog Element	Usage
Next Header	Next Header	(Read-only) 8 bits. The type of header which follows this header.
Hdr Ext Len	Header Ext Length	(Read-only) 8 bits. The length of this header in bytes.
Options	Selected Options List (left window)	A list of the selected options, shown in the left pane. These options will be added to the IPv6 Hop-by-Hop Extension header. Double-click a selected option to display the associated configuration dialog.
	Available Options List	A list of different types of options which may be added to the IPv6 Hop-by-Hop Extension header. • PAD1 • PADN • Jumbo • RouterAlert • Binding Update • Binding Acknowledgment • Binding Request • MIpV6 Unique ID Sub • MIpV6AlternativeCoaSub
	<- Add	Select/highlight an available Extension Header, and then press the *<-Add* button to add that header to the list of selected options in the left pane.
	 Edit Option	When an option in the left window is high-lighted, clicking this icon displays the *IPv6 Option* dialog so that option can be modified.
	 Remove Option	When this icon is clicked, deletes the high-lighted option in the left pane.
	Hop-by-Hop Options Encoding	You may manually enter coding in this field.
Decode		After any change in the Hop-by-Hop Options Encoding box, the *Decode* button, should be clicked to reflect these the directly edited changes back into the dialog fields.

IPv6 Routing Extension Header

This dialog is accessed by selecting *Routing* in the *Header Extensions* field of the *IPv6 Header* dialog, then pressing the *Edit Extension Header* icon ( ). Alternatively, this dialog can be opened by double-clicking *Routing*.

The *IPv6 Routing Header* dialog is shown in *Figure:IPv6 Routing Extension Header*.

Figure:IPv6 Routing Extension Header



The fields and controls for the *IPv6 Routing Header* dialog are described in *Table:IPv6 Routing Header Dialog*.

Table:IPv6 Routing Header Dialog

Header Field	Dialog Element	Usage
Next Header	Next Header	(Read-only) 8 bits. The type of header which follows this header.
Hdr Ext Len	Header Ext Length	(Read-only) 8 bits. Length of this header in bytes.
Routing Type	Routing Type	(Read-only) Identifies the routing type. Default is 0.
Segments Left	Segments Left	(Read-only) Used if Routing Type is not recognized by this node. If segments left =0, this node ignores this header and goes on to the next header. If value = non-0, packet is discarded.
Reserved	Reserved	This value is set to zero when packet is transmitted, and ignored by the destination node.
type-specific data	Intermediate Nodes	Variable Length field. Lists the nodes to be traversed by the packet. Node 1, Node 2, and so on.
	Add Node	When clicked, adds a node to the list: Node

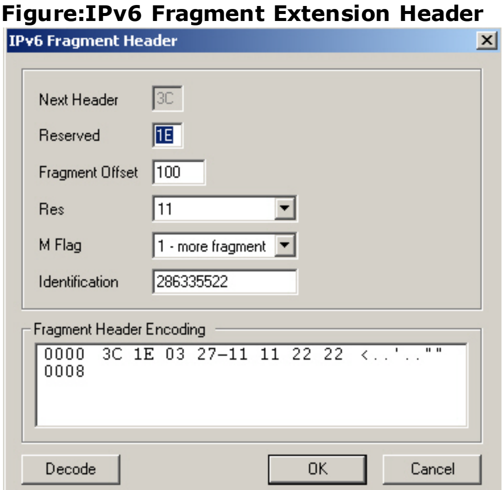
Header Field	Dialog Element	Usage
		1, Node 2, and so on.
	 Edit Node	When clicked, displays the *IPv6 Address* dialog.
	 Remove Node	When clicked, deletes the highlighted node in the list.
	Intermediate Node Data	(Read-only) Displays the 16-byte IPv6 addresses of the intermediate nodes. Shown as hex values.
	Routing Header Encoding	A display of the components of the Routing Header, shown as hex values.
Decode		After any change in the Routing Header Encoding box, the *Decode* button, should be clicked to reflect these the directly edited changes back into the dialog fields.

IPv6 Fragment Extension Header

Fragmentation of an IPv6 packet is done by the source node, and is done if the packet is larger than the Maximum Transmission Unit (MTU) for the path. The Next Header value for a Fragment extension header is 44. This dialog is accessed by selecting *Fragment* in the *Header Extensions* field of the *IPv6 Header* dialog, then pressing the *Edit Extension Header* icon (). Alternatively, this dialog can be opened by double-clicking *Fragment*.

The *IPv6 Fragment Header* dialog is shown in *Figure:IPv6 Fragment Extension Header*.

Figure:IPv6 Fragment Extension Header



The fields and controls for the *IPv6 Fragment Header* dialog are described in *Table:IPv6 Fragment Header dialog*.

Table:IPv6 Fragment Header dialog

Header Field	Dialog Element	Description
Next Header	Next Header	(Read-only) 8 bits. The type of header which

Header Field	Dialog Element	Description
		follows this header.
Reserved	Reserved	This value is set to zero when the packet is transmitted, and ignored by the destination node.
Fragment Offset	Fragment Offset	13-bits. The value of the offset for the data contained in this packet, relative to the start of the fragmentable part of the original packet. In 8-octet units. It is used in reassembling the data at the destination end of the link. If this is the first fragment, the offset value = 0. The fragmentable part of a packet contains extension headers which are processed ONLY at the final destination node, and the upper-layer header and data.
Res	Res	Reserved. This value is set to zero when packet is transmitted, and ignored by the destination node.
M flag	M Flag	Indicates type of fragment packet. • If '1,' there are more fragments of the original, large packet to be received. • If '0,' it contains the last fragment of the original packet.
Identification	Identification	A 32-bit value that identifies the original packet which is to be fragmented. This value must not have been assigned to another fragmented packet with the same source and destination addresses which has been sent 'recently'—within the lifetime of this previous packet, including transmission and reassembly.
	Fragment Header Encoding	A display of the components of the Routing Header, shown as hex values.
Decode		After any change in the Fragment Encoding box, the *Decode* button, should be clicked to reflect these the directly edited changes back into the dialog fields.

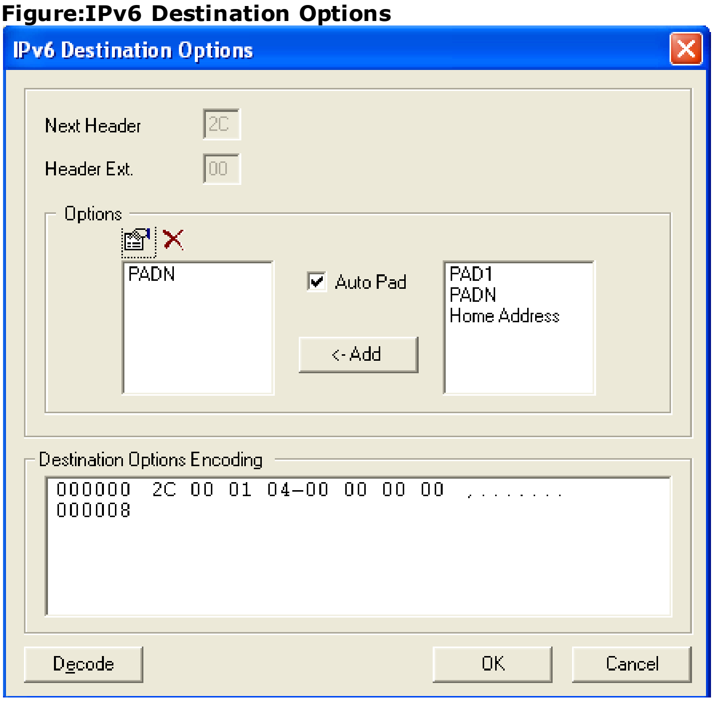
IPv6 Destination Extension Header

The Destination Options header is used to carry optional information that need to be examined only by a packet's destination node or nodes.

This dialog is accessed by selecting *Destination* in the *Extension Headers* field of the *IPv6 Header Page* dialog, then clicking the *Edit Extension Header* icon (). Alternatively, this dialog can be opened by double-clicking *Destination*.

The *IPv6 Destination Options* dialog is shown in *Figure:IPv6 Destination Options*.

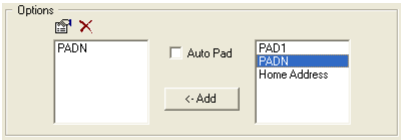
Figure:IPv6 Destination Options



The fields and controls for the *IPv6 Destination Options* dialog are described in *Table:IPv6 Destination Options dialog*.

Table:IPv6 Destination Options dialog

Header Field	Dialog Element	Description
Next Header	Next Header	(Read-only) 8 bits. The type of header which follows this header.
Header Ext.	Header Ext Length	(Read-only) 8 bits. Length of this header in bytes.
Options	Selected IPv6 Destination Options List (left window, as shown in *Figure:IPv6 Destination Options*	A list of the IPv6 Destination header options, shown in the left pane. These options are added to the IPv6 Destination Extension header. The options in the list are as follows: • PAD1: The PAD1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PADN option is used, rather than multiple Pad1 options. • PADN: The PadN option is used to insert two or more octets of padding into the Options area of a header. • Home Address: It is the 16 byte in length IPv6 Destination Header option. NOTE The sequence of options within the header is processed in the order they appear in the header.

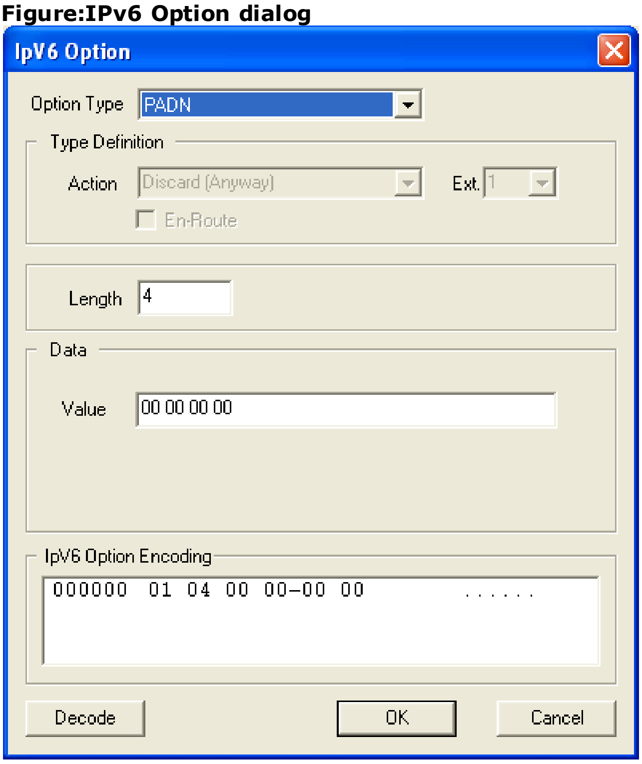
Header Field	Dialog Element	Description
		Double-click a selected option to display the associated configuration dialog.
		When an option in the left window is highlighted, clicking this icon displays the *IPv6 Option* dialog where that option can be modified. Refer *IPv6 Option* for more information.
		Click this icon to delete the highlighted option in the left pane.
	Auto Pad (check box)	If selected, adds a 'Pad N' option, if necessary, to make the option header extension length a multiple of 8 octets.
		Select or highlight an available Destination Extension Header in the right pane, and then click the <-Add button to add that header to the list of selected options in the left pane. The result is shown here: 
	Destination Options Encoding	You can manually enter coding in this field.
Decode		After any change in the *Destination Encoding* box, the *Decode* button is clicked to reflect the directly edited changes back into the dialog fields.

IPv6 Option

The *IPv6 Option* dialog contains the editable parameters of IPv6 Destination Extension Header. This dialog is accessed by selecting an available Destination Extension Header in the *IPv6 Destination Options* dialog, then clicking the *Edit Option* icon (). Alternatively, this dialog can be opened by double-clicking the selected or highlighted header option.

The IPv6 Option dialog is shown in *Figure:IPv6 Option dialog*.

Figure:IPv6 Option dialog



The fields and controls for the *IPv6 Options* dialog are described in *Table:IPv6 Options dialog*.

Table:IPv6 Options dialog

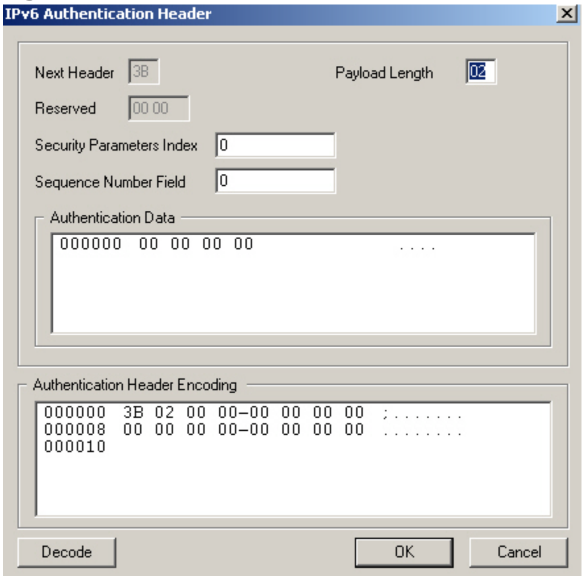
Section	Field	Description
Option Type		The list contains the IPv6 Destination header options. The options in the list are as follows.
Type Definition	Action	This field is disabled for IPv6 Destination Extension header options.
	Ext.	This field is disabled for IPv6 Destination Extension header options.
	En-Route	This field is disabled for IPv6 Destination Extension header options.
Length		Length of the header. NOTE The length value depends on the type of header selected.
Data	Value	Data value of the header. NOTE The data value depends on the type of header selected.
IPv6 Option Encoding		You can manually enter coding in this field.
Decode		After any change in the *IPv6 Option Encoding* box, the *Decode* button is clicked to reflect the directly edited changes back into the dialog fields.

IPv6 Authentication Extension Header

This dialog is accessed by selecting *Authentication* in the *Header Extensions* field of the *IPv6 Header* dialog, then pressing the *Edit Extension Header* icon ( ). Alternatively, this dialog can be opened by double-clicking *Authentication*.

The *IPv6 Authentication Header* dialog is shown in *Figure:IPv6 Authentication Header Extension*.

Figure:IPv6 Authentication Header Extension



The fields and controls for the *IPv6 Authentication Header* dialog are described in *Table:IPv6 Authentication Header Dialog*.

Table:IPv6 Authentication Header Dialog

Header Field	Dialog Element	Description
Next Header	Next Header	(Read-only) 8 bits. The type of payload which follows this header.
Payload Length	Payload Length	8 bits. Length of the Authentication Header in 32-bit words minus 2 (32-bit words).
Reserved	Reserved	(Read-only) Reserved for future use. Must be set to 0.
Security Parameters Index (SPI)	Security Parameters Index	Arbitrary 32-bit value which is added to the destination IP address and security protocol, to identify the Security Association. Values 1-255 are reserved by the IANA. Value 0 cannot be used for external purposes.
Sequence Number Field	Sequence Number Field	Counter - Mandatory.
Authentication Data	Authentication Data	Variable length Contains the packet's Integrity Check Value (ICV).
	Authentication Header Encoding	Reflects the values in the extension header fields in this dialog, and the authentication data.

Header Field	Dialog Element	Description
Decode		After any change in the Hop-by-Hop Options Encoding box, the *Decode* button, should be clicked to reflect these the directly edited changes back into the dialog fields.

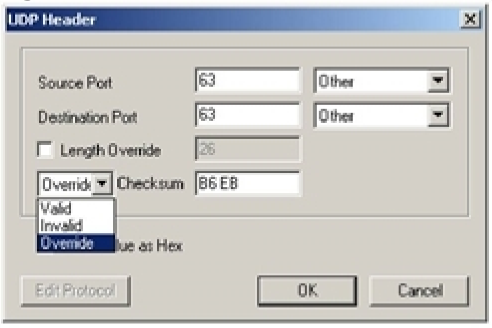
UDP Header Dialog

This dialog is accessed by selecting the *UDP/IP* option button in the Protocols section of the *Frame Data* tab. Then, from the *IPv4* or *IPv6 Header* dialog, select the *Edit UDP* button.

When the Protocol types are set to IPv4/6 and UDP (for UDP/IP, RIP/UDP/IP and DHCP/UDP/IP protocols), the *Edit UDP* button may be used to bring up a dialog which allows editing of the IPv4/6 UDP header. The UDP header follows the IP header in the packet.

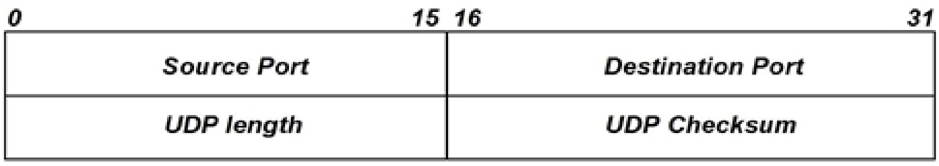
The *UDP Header* dialog is shown in *Figure:Protocols: IPv4 UDP Header Dialog*.

Figure:Protocols: IPv4 UDP Header Dialog



The format of an IPv4 UDP header is shown in *Figure:Protocols: IPv4 UDP Header Format*.

Figure:Protocols: IPv4 UDP Header Format



The correspondence between the fields of an UDP header and the elements of the *UDP Header* dialog which set those fields are described in *Table:UDP Header Fields Set by the IPv4 UDP Dialog*.

Table:UDP Header Fields Set by the IPv4 UDP Dialog

Header Field	Dialog Field	Description
Source Port	Source Port	Protocol source port number. One of: • RIP (Port 520) • DHCP Server (Port 67) • DHCP Client (Port 68) • PTP Event (Port 319) (*Figure:UDP Header for PTP*.) • PTP General (Port 320)*Figure:UDP Header for PTP* .)

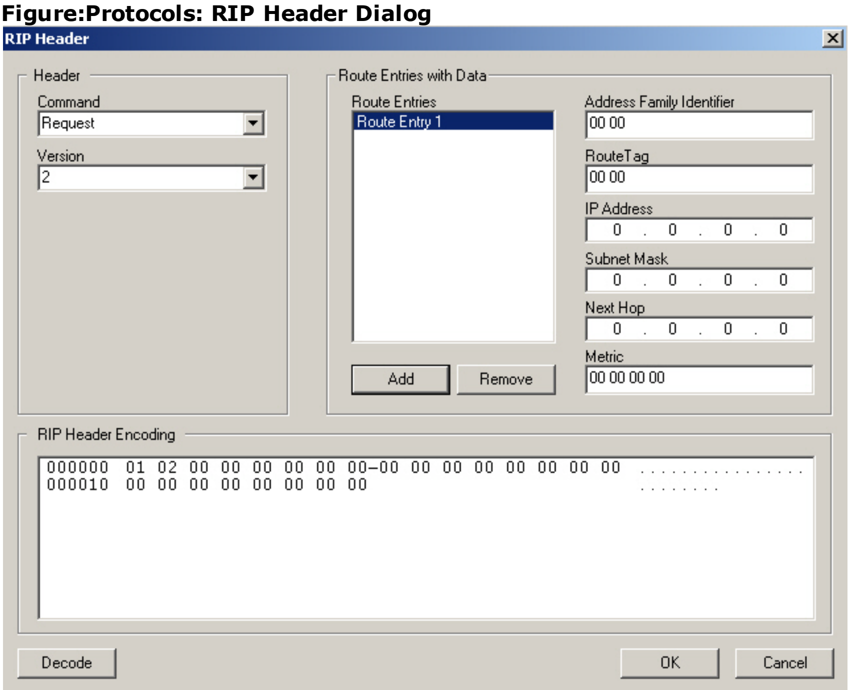
Header Field	Dialog Field	Description
		• Other (Port 63): If Other is selected, the *Edit Protocol* button is disabled (dimmed).
Destination Port	Destination Port	Protocol destination port number. One of: • RIP (Port 520) • DHCP Server (Port 67) • DHCP Client (Port 68) • PTP Event (Port 319)*Figure:UDP Header for PTP* .) • PTP General (Port 320)*Figure:UDP Header for PTP*.) • Other (Port 63)
UDP Length (Override)	Length	Length of the UDP header and data. This is set automatically by the Ixia hardware. By selecting the Length Override check box, the you can manually set the UDP length.
UDP Checksum	Checksum	Choose one of the following checksum options from the list: • **Valid**: The calculated checksum over the UDP header and UDP length is automatically calculated. • **Invalid**: The calculated checksum over the UDP header and UDP length is automatically calculated (with error). • **Override**: The UDP Checksum can be set to a user-defined, 2-octet value in the box to the right.
	Show value as Hex	If enabled through the check box, the values for Source Port, Destination Port, and Length are displayed as hexadecimal values.
	Edit Protocol	Enabled only if the protocol selected for the Source port is not set to 'Other.'

If either source or destination port address is set to the RIP port number (520), then the *Edit RIP* button is enabled. Clicking that button displays the RIP Header Dialog*. If both ports are set to DHCP (client or server), the Edit Protocol button is enabled, and changes to Edit DHCP.*

RIP Header Dialog

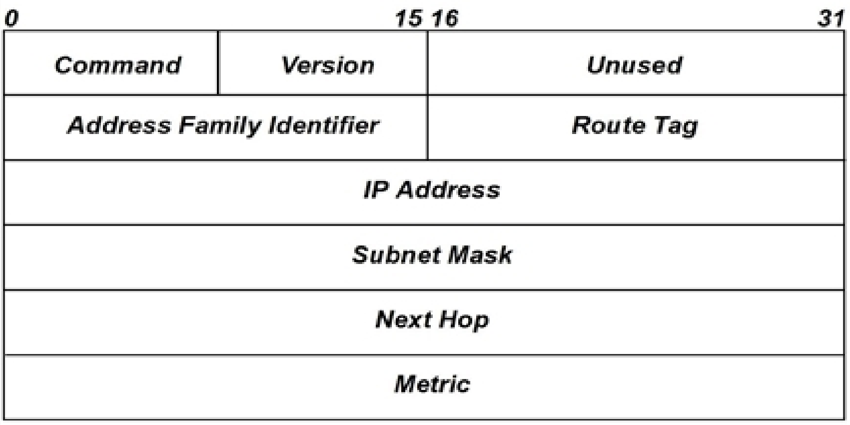
If either source or destination port address of the UDP Header Dialog *is set to the RIP port number (520), then the Edit RIP button is enabled. Selecting the button presents the dialog below. Either RIP version 1 or version 2 packets may be built. The RIP dialog may also be accessed from the IP Header dialog shown in Figure:Protocols: IPv4 Header Dialog.*

Figure:Protocols: RIP Header Dialog



This dialog allows the RIP specific header elements to be set. The format of a RIP packet is shown in *Figure:Protocols: RIP Entry Format*.

Figure:Protocols: RIP Entry Format



The first four bytes contain the RIP header. The remainder of the message may contain from 1 to 25 route entries.

The *Route Entries with Data* box allows multiple entries to be created and edited. To edit an existing entry, select it from the *Route Entries* list and modify the entries on the right. To save the work, press the *OK* button or select a different entry from the list. To create a new entry press the *Add* button; an empty entry will be added to the end of the list. The correspondence between the fields of an RIP header and the elements of the *RIP Header* dialog which set those fields are described in *Table:RIP Header Fields Set by the RIP Dialog*.

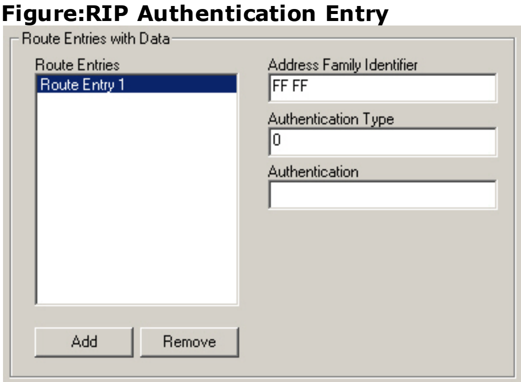
Table:RIP Header Fields Set by the RIP Dialog

Header Field	Dialog Field	Description
Command	Command	One of the RIP commands: • Unknown.

Header Field	Dialog Field	Description
		• Request: A request for the responding system to send all or part of its routing table. • Response: Response or update information from a sender. • Trace On: An obsolete message. • Trace Off: An obsolete message. • Reserved: Reserved for use by Sun Microsystems.
Version	Version	RIP Version Number, values of 1 (RIP version 1) or 2 (RIP version 2) are valid.
Address Family Identifier	Address Family Identifier	Valid values are 2 (IP protocol), 0xFFFF (authentication entry, see below for a further description) and 0 (if Metric=16, indicates request for entire routing table).
Route Tag	Route Tag	A number used to distinguish the source of routing information.
IP Address	IP Address	The IP address of the routing table entry.
Subnet Mask	Subnet Mask	For Version 2 records, the subnet mask that applies to the IP address.
Next Hop	Next Hop	For Version 2 records, the IP address of the next routing hop for IP address and subnet mask.
Metric	Metric	The routing cost metric, from 1 to 16, with 16 interpreted as unreachable.

For Version 2 authentication records, when the *Address Family Identifier* is set to '0xFFFF,' the route entry elements change in the dialog, as shown in *Figure:RIP Authentication Entry*.

Figure:RIP Authentication Entry



The format of the authentication entry, which may only exist once as the first routing table entry, is shown in *Figure:RIP Authentication Entry Format*.

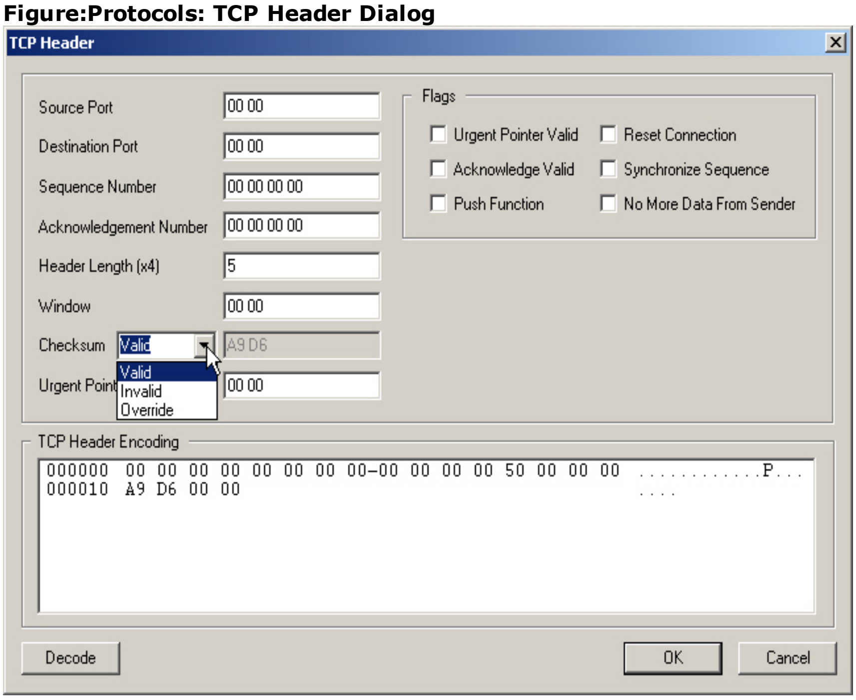
Figure:RIP Authentication Entry Format

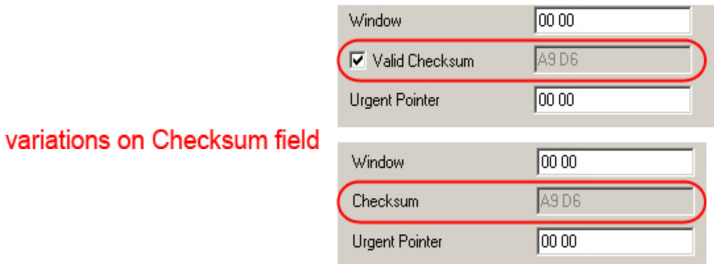
0 15	16 31
Address Family Identifier = 0xFFFF	*Authentication Type = 2*
16-byte Authentication Data	

TCP Header Dialog

When the Protocol type is set to *TCP/IP* on the IP Header dialog the *Edit TCP* button may be used to bring up a dialog which allows editing of the TCP header. The TCP header follows the IP header. The *TCP Header* dialog is shown in *Figure:Protocols: TCP Header Dialog*.

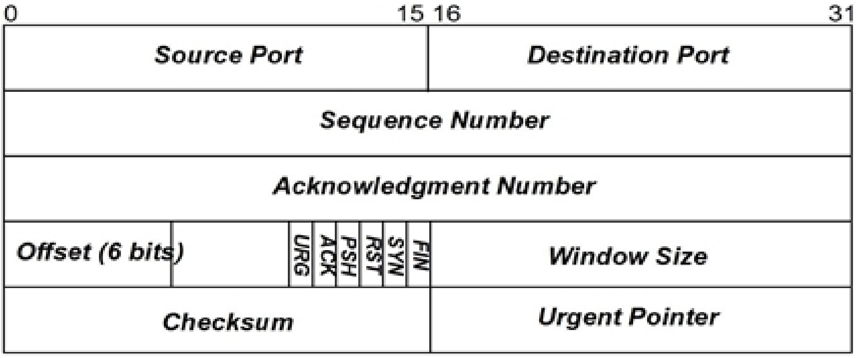
Figure:Protocols: TCP Header Dialog





The format of a TCP header is shown in *Figure:Protocols: TCP Header Format*.

Figure:Protocols: TCP Header Format



The correlation between the fields of an TCP header and the elements of the *TCP Header* dialog which set those fields are described in *Table:TCP Header Fields Set by the TCP Dialog*.

Table:TCP Header Fields Set by the TCP Dialog

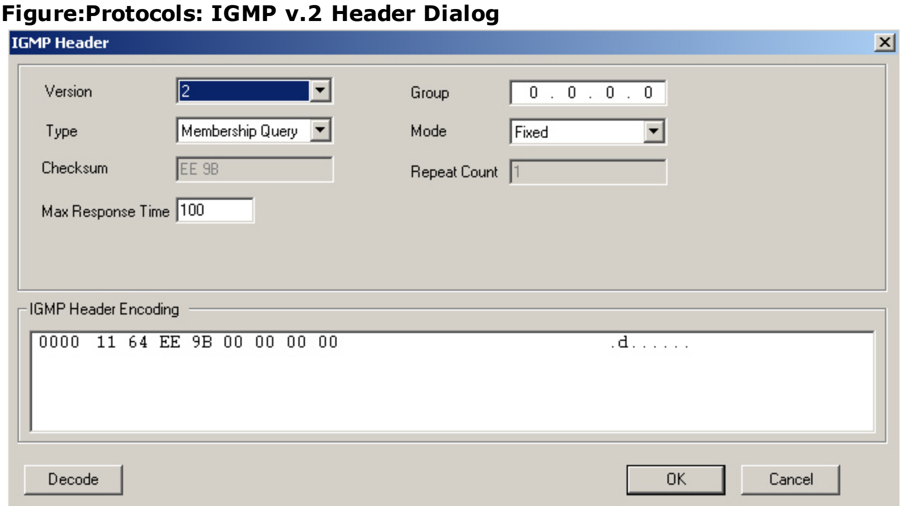
Header Field	Dialog Field	Description
Source Port	Source Port	Protocol source port number.
Destination Port	Destination Port	Protocol destination port number.
Sequence Number	Sequence Num-ber	The packet sequence number for the connection.
Acknowledge-ment Number	Acknowledg-ment Number	The next byte number that the sender expects for the connection.
Offset	Header Length [x4]	Offset from the beginning of the TCP header to the data.
Flag–FIN	No More Data From Sender	The sender indicates that this is the last packet it will transmit for the connection.
Flag–SYN	Synchronize Sequence	Indicates either a connection request (ACK = 0) or a connection accepted (ACK = 1) condition.
Flag–RST	Reset Connection	Reset the connection signal.
Flag–PSH	Push Function	Request that receiver deliver the packet to the application without buffering.
Flag–ACK	Acknowledge Valid	The acknowledgment number field is valid. Also used in establishing connections (see SYN above).
Flag -- URG	Urgent Pointer Valid	The urgent pointer field is valid.
Window Size	Window	The number of bytes that the recipient may send to the sender, starting at the acknowledge byte.
Checksum		Depending on the load module, there are 3 dif-ferent ways in which Checksum is handled:
	Valid Invalid Override (list)	NOTE Refer to the *Ixia Platform Reference Manual*, Table 1-7, for list of load mod-ules supporting checksum override. For load modules supporting Checksum Override, choose one of the following checksum options from the list:

Header Field	Dialog Field	Description
		• Valid: The calculated checksum over the TCP header and TCP length is automatically calculated. • Invalid: The calculated checksum over the TCP header and TCP length is automatically calculated (with error). • Override: The TCP Checksum can be set to a user-defined, 2-octet value in the box to the right.
	Checksum	(Read-only) The correct checksum will be automatically generated and transmitted.
	Valid Checksum (check box)	(Read-only) If selected, a valid checksum will be generated. If cleared, an invalid checksum will be generated.
Urgent Pointer	Urgent Pointer	Byte offset of the urgent data in the packet.

IGMP Header Dialog

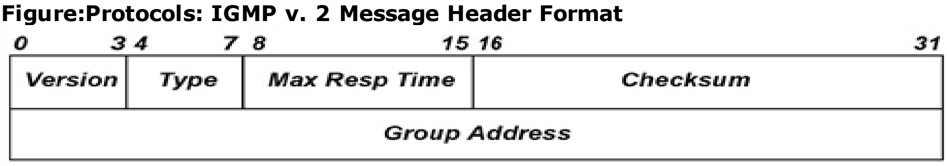
When the Protocol type is set to *IGMP/IP* on the IP Header dialog the *Edit IGMP* button may be used to bring up dialog which allows editing of the IGMP message header. The IGMP header follows the IP header. The *IGMP Header* dialog is shown in *Figure:Protocols: IGMP v.2 Header Dialog*.

Figure:Protocols: IGMP v.2 Header Dialog



The format for an IGMP v.2 message header (the default setting) is shown in *Figure:Protocols: IGMP v. 2 Message Header Format*.

Figure:Protocols: IGMP v. 2 Message Header Format



The correspondence between the fields of an IGMP header and the elements of the IGMP v. 2 message header dialog which sets those fields are described in *Table:IGMP v.2 Message Header Fields Set by the IGMP Dialog*.

Table:IGMP v.2 Message Header Fields Set by the IGMP Dialog

Header Field	Dialog Field	Description
Version	Version	IGMP Version Number. Choose one of: • Unknown • 1 • 2 - the version described in this table. • 3 - changes the composition of this dialog (*Figure:Protocols: IGMP v.3 Membership Query Message Dialog* for a description of this dialog) (The default is Version 2)
Type	Type	The IGMP message. Choose one of: • Membership Query • Membership Report • Leave Group (for Version 2 only)
Checksum	Checksum	The 16-bit ones complement of the ones complement sum of the 8-octet IGMP message.
Max Response Time	Max Response Time	
Group Address	Group	The IP address of the group associated with the message.
	Mode	Choose one of: • Fixed • Increment • Decrement • Continuous increment • Continuous decrement
	IGMP Header Encoding	After changes are made in the header dialog, press the *Decode* button to update the corresponding data in the IGMP Encoding display.

The dialog for an IGMP v.3 Membership Query header is shown in *Figure:Protocols: IGMP v.3 Membership Query Message Dialog*.

Figure:Protocols: IGMP v.3 Membership Query Message Dialog

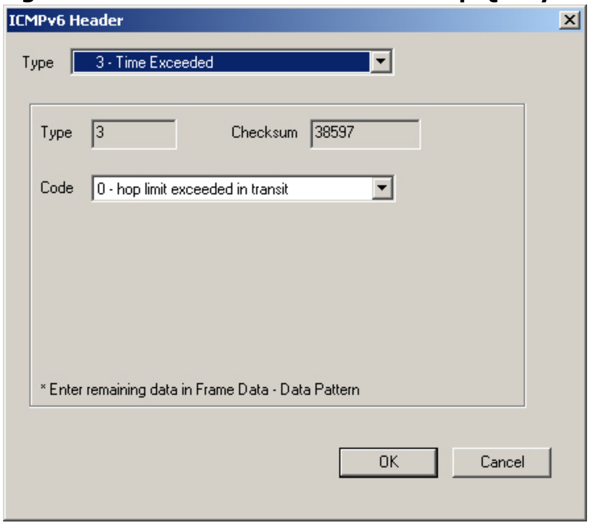
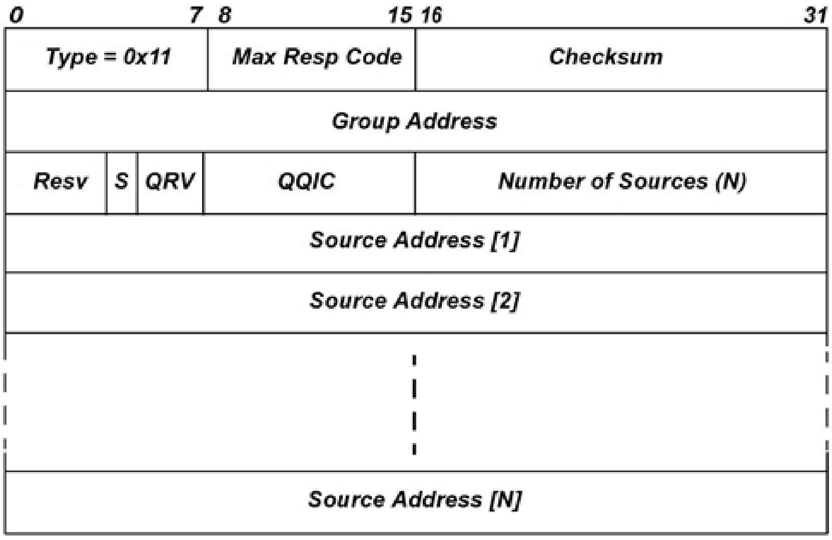


Figure:Protocols: IGMP v.3 Membership Query Message Format



The correspondence between the fields of an IGMP v.3 Membership Query message and the elements of the IGMP v. 3 dialog which sets those fields is described in *Table:IGMP v.3 Membership Query Message*.

Table:IGMP v.3 Membership Query Message

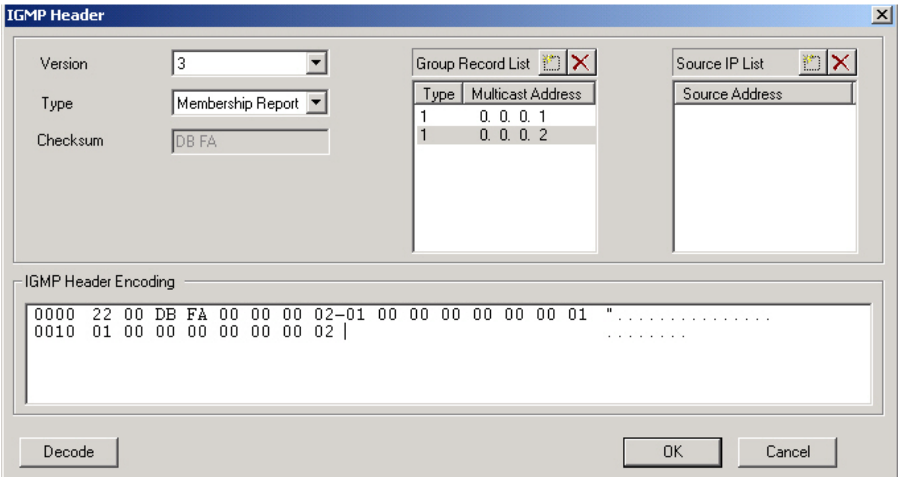
Header Field	Dialog Field	Description
Version	Version	IGMP Version Number. Select from: • Unknown • 1 • 2: this option changes the dialog (*Figure:Protocols: IGMP v. 2 Message Header Format* for a description) • 3: the version described in this table. (The default is Version 2.)
Type	Type	The IGMP message, one of: • Membership Query

Header Field	Dialog Field	Description
		• Membership Report • Leave Group (for Version 2 only)
Checksum	Checksum	The 16-bit ones complement of the ones complement sum of the entire IGMP message.
Max Response Code	Max Response Time	Specifies the maximum time allowed before sending a responding report. The actual time allowed is represented in units of 1/10 second and is configured in the following manner: • If Max Response Time is less than 128 (that is, less than 12.8 seconds), use the *Raw* option button and enter the number of 1/10 second units required. The maximum number allowed is 127 • If Max Response Time is greater than or equal to 128, it is represented by a floating-point value. Use the Float option button and enter a value between 12.8 to 16 (representing seconds). Note that because this is a floating point value, times entered will not necessarily be accurate to a tenth of a second. Small values of Max Response Time allow IGMPv3 routers to tune the ‘leave latency’ (the time between the moment the last host leaves a group and the moment the routing protocol is notified that there are no more members). Larger values, especially in the exponential range, allow tuning of the burstiness of IGMP traffic on a network.
Group Address	Group	The IP address of the group associated with the message.
	Mode	Choose one of: • Fixed • Increment • Decrement • Continuous increment • Continuous decrement
	Repeat Count	The number of times to modify the group address for increment or decrement modes.
Resv		Reserved for future use.
QQIC	QQIC	The Querier's Query Interval Code field specifies the Query Interval used by the querier. The actual time allowed is represented in units of 1/10 second and is configured in the following manner: • If the interval less than 128 (that is, less than 12.8 seconds), use the *Raw* option button and enter the number of 1/10 second units required. The maximum number allowed is 127

Header Field	Dialog Field	Description
		• If interval is greater than or equal to 128, it is represented by a floating-point value. Use the Float option button and enter a value between 12.8 to 16 (representing seconds). Note that because this is a floating point value, times entered will not necessarily be accurate to a tenth of a second.
QRV	QRV	(Querier's Robustness Variable). If QRV is not equal to zero, it is the robustness variable for the querier. If the variable is >7, QRV = 0.
S	S	(Suppress Router-Side Processing) When the 'S' flag is set by selecting the check box, receiving multicast routers will not send timer updates in the normal manner when a query is received.
	Source IP	Enter an IP unicast address in the field above the list box, then click the *Add* icon () to add the address to the Source IP list. Click the *Delete* icon () to delete a highlighted address from the Source IP list.
	IGMP Header Encoding	After changes are made in the header dialog, press the *Decode* button to update the corresponding data in the IGMP Encoding display.

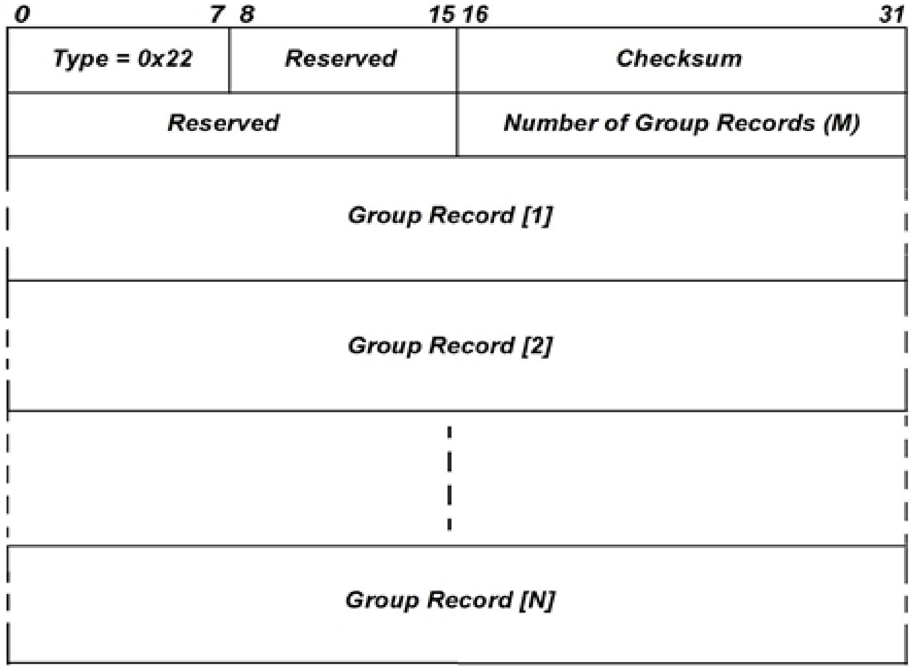
The dialog for the IGMPv.3 Membership Report is shown in *Figure:Protocols: IGMP v.3 Membership Report Message Dialog*.

Figure:Protocols: IGMP v.3 Membership Report Message Dialog



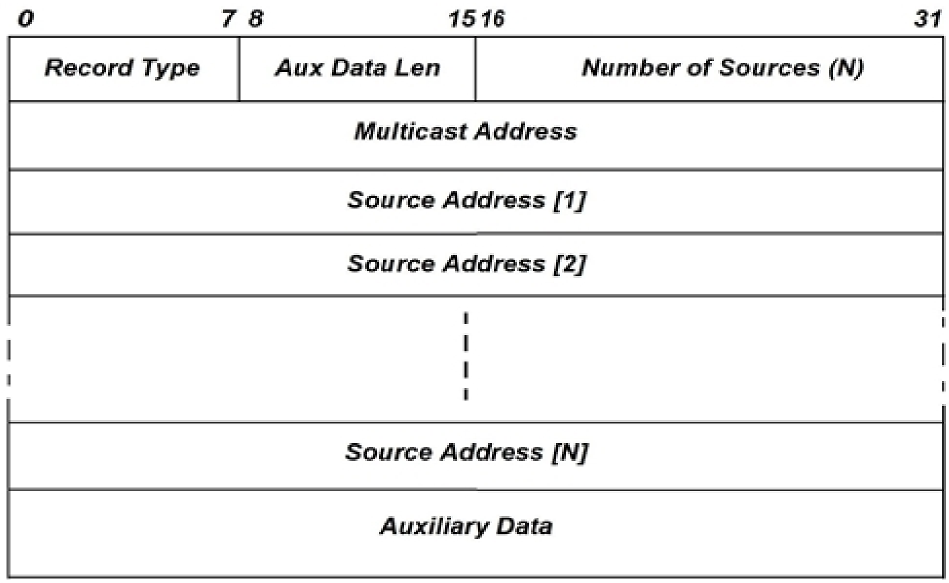
The format of an IGMP v.3 Membership Report Message is shown in *Figure:Protocols: IGMP v.3 Membership Report Format*.

Figure:Protocols: IGMP v.3 Membership Report Format



This IGMP message contains a number of Group Records. The format of an IGMP v.3 Group Record is shown in *Figure:Protocols: IGMP v.3 Group Record Format*.

Figure:Protocols: IGMP v.3 Group Record Format



The correspondence between the fields of an IGMP Membership Report, including references to the Group Records, and the elements of the dialog for IGMP Membership Report which set those fields is described in *Table:IGMP v.3 Membership Report Fields Set by the IGMP Dialog*.

Table:IGMP v.3 Membership Report Fields Set by the IGMP Dialog

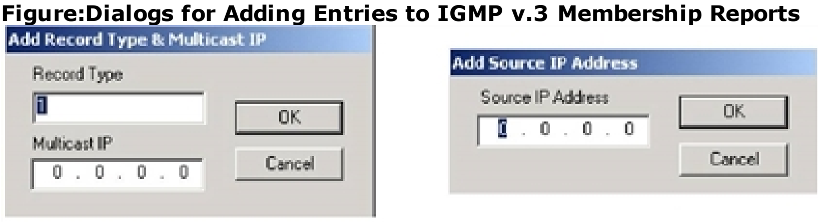
Header Field	Dialog Field	Description
	Version	IGMP Version Number. Choose one of:

Header Field	Dialog Field	Description
		• Unknown • 1 • 2 • 3: The version described in this table.
Type	Type	The IGMP message. Choose one of: • Membership Query • Membership Report • Leave Group (for Version 2 only)
Reserved		Reserved for future use.
Checksum	Checksum	The 16-bit ones complement of the ones complement sum of the entire IGMP message.
Reserved		Reserved for future use.
Number of Group Records	Group Record List	The number of entries in this list defines the number of group records. Click the *Add* button to add a new Group Record to the list. The *Add Record Type & Multicast IP* dialog will appear. *Figure:Dialogs for Adding Entries to IGMP v.3 Membership Reports*.
Group Record - Components		
Type	Type	Selects the group record type, from 1 through 6. The values are grouped into three categories. Current-State Records • Type 1 - MODE_IS_INCLUDE: Indicates that the interface has a filter mode of INCLUDE for the specified multicast address. The Source Address fields in this Group Record contain the interface's source list for the specified multicast address, if it is non-empty. • Type 2 - MODE_IS_EXCLUDE: Indicates that the interface has a filter mode of EXCLUDE for the specified multicast address. The Source Address fields in this Group Record contain the interface's source list for the specified multicast address, if it is non-empty. Filter-Mode-Change Records • Type 3 - CHANGE_TO_INCLUDE_MODE: Indicates that the interface has changed to INCLUDE filter mode for the specified multicast address. The Source Address fields in this Group Record contain the interface's new source list for the specified multicast address, if it is non-empty. • Type 4 - CHANGE_TO_EXCLUDE_MODE: Indicates that the interface has changed to EXCLUDE filter mode for the specified multicast address. The Source Address fields in this Group Record contain the interface's new

Header Field	Dialog Field	Description
		source list for the specified multicast address, if it is non-empty. (continued next page)
Type	Type	(continued) Source-List-Change Record • Type 5 - ALLOW_NEW_SOURCES: Indicates that the Source Address fields in this Group Record contain a list of the additional sources that the system wishes to hear from, for packets sent to the specified multicast address. If the change was to an INCLUDE source list, these are the addresses that were added to the list; if the change was to an EXCLUDE source list, these are the addresses that were deleted from the list. • Type 6 - BLOCK_OLD_SOURCES: Indicates that the Source Address fields in this Group Record contain a list of the sources that the system no longer wishes to hear from, for packets sent to the specified multicast address. If the change was to an INCLUDE source list, these are the addresses that were deleted from the list; if the change was to an EXCLUDE source list, these are the addresses that were added to the list.
Multicast Address	Multicast Address	A Multicast Address for a multicast group that this sender interface belongs to.
Number of Sources	Source IP List	The number of entries in this list defines the number of IP Source Addresses contained in this Group Record.
Source Address	Source Address	IP unicast addresses. Click the *Add* icon ( ) to add a new address to the Source IP list. The *Add Source IP Address* dialog will appear. *Figure:Dialogs for Adding Entries to IGMP v.3 Membership Reports*. Click the *Delete* icon ( ) to delete a highlighted address from the Source IP list.

The dialogs for adding entries to the lists in the IGMP v.3 Membership Report Messages are shown in *Figure:Dialogs for Adding Entries to IGMP v.3 Membership Reports*.

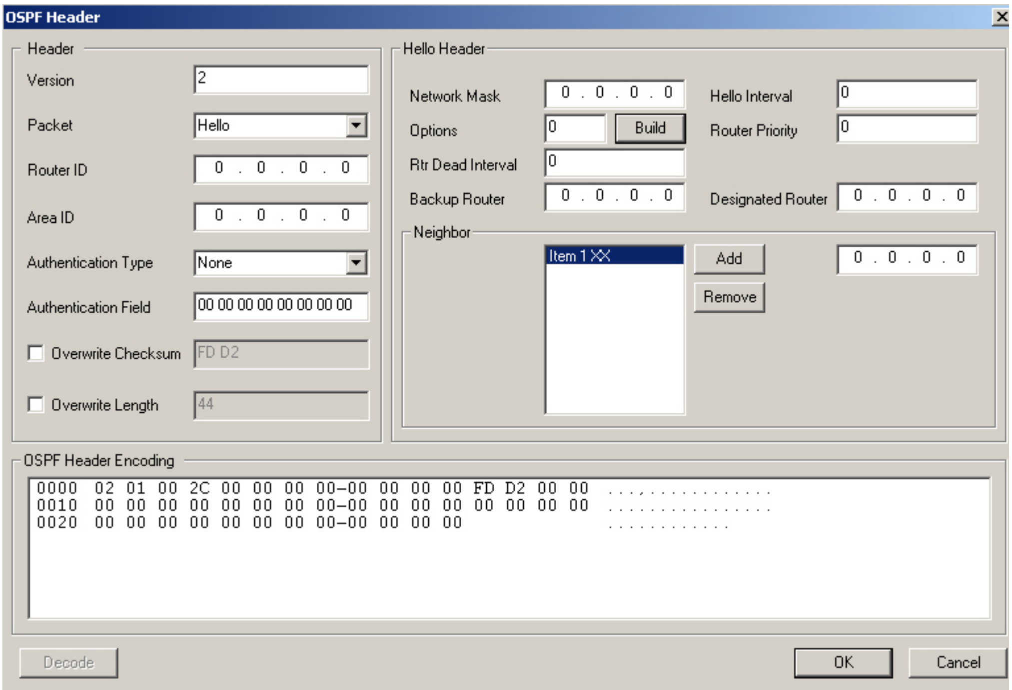
Figure:Dialogs for Adding Entries to IGMP v.3 Membership Reports



OSPF Header Dialog

When the Protocol type is set to *OSPF/IP* in the *IP Header* dialog, the *Edit OSPF* button may be used to bring up the dialog which allows editing of the OSPF header. The OSPF header follows the IP header. The *OSPF Header* dialog is shown in *Figure:Protocols—OSPF Header Dialog*. Refer to the OSPF section in Theory of Operation: Protocols in the Protocols Manual for an overview of the OSPF protocol.

Figure:Protocols—OSPF Header Dialog



The fields and controls in this dialog are described in *Table:OSPF Header Fields Set by the OSPF Header Dialog*.

Table:OSPF Header Fields Set by the OSPF Header Dialog

IP Header Field	Dialog Element	Description
Version	Version	Set to 2. The current version of the OSPF protocol, per RFC 2328.
	Packet	The type of packet. Choose one of: • Unknown. • Hello—used to discover/maintain neighbors. • Database Description—a summary of the database contents. • Link State Request—request for database download. • Link State Update—the database update. • Link State Ack—flooding acknowledgment.
TOS	Precedence (TOS Bits 0-2)	The precedence is set in the 3 most significant bits of the TOS. Choose one of: • 000 - Routine

IP Header Field	Dialog Element	Description
		• 001 - Priority • 010 - Immediate • 011 - Flash • 100 - Flash Override • 101 - CRITIC/ECP • 110 - Internet Control • 111 - Network Control
	Router ID	The 32-bit Router ID for the simulated router. It can be a value such as the lowest or highest IP interface address for this router.
	Area ID	The ID of the area to which the attached network belongs.
	Authentication Type	Choose one of: • None • Simple • Cryptographic
	Authentication Field	The authentication data (key) associated with the Authentication Type. If Type is Simple, this is a 64-bit clear password in the OSPF header. If Type is Cryptographic, the data is a shared ‘secret’ between sender and receiver.
	Overwrite Checksum	check box. Disabled by default.
	Overwrite Length	check box. Disabled by default.
	Network Mask	The IP Interface mask. A subnet mask associated with the IP interface address, which Identifies the attached network.
	Options	The *Options* field value, exclicked in hex. Results from the settings of the options bits in the *Options* dialog box. The Options field is present in: • Hello packets • Database Description packets • All LSAs
	Build	Opens the *Options* dialog box. This dialog allows the user to specify the OSPF options. Chose from a list of: • (7) Unused • (6) Opaque LSA’s Forwarded • (5) Demand Circuit • (4) External Attributes • (3) NSSA Capabilities • (2) Multicast Capability

IP Header Field	Dialog Element	Description
		• (1) External Routing • (0) Type of Service Routing
	Router Dead Interval	The number of seconds before declaring a silent router down.
	Backup Router	The IP address of the Backup Designated Router (BDR), based on 'election' by the Hello messages. It takes over the role of DR, in the case of failure of the DR.
	Hello Interval	The number of seconds between Hello packets sent from a router. The Ixia hardware sends Hello packets at this interval.
	Router Priority	The router's priority. Used in Designated Router and Backup Router negotiation. A 0 indicates that the router is ineligible to become either.
	Designated Router	The ID address of the Designated Router (DR), based on router priorities in the Hello messages. The Designated Router is the router which has the highest Router Priority in the network. It originates the Network LSAs for that network.
	Neighbor	Multiple OSPF neighbors which are attached to this network can be added by pressing the *Add* button: 'Item I XX', and so forth. The four-octet field to the right displays the IP address of the neighbor entry which is currently highlighted.
	OSPF Header Encoding/Encode	Values that are set in the dialog are reflected in the hexadecimal display. It is also possible to edit the OSPF header directly from the display. All editing occurs in type-over mode. After any change, the *Decode* button should be clicked to reflect these changes back into the dialog fields.

ICMP Header Dialog

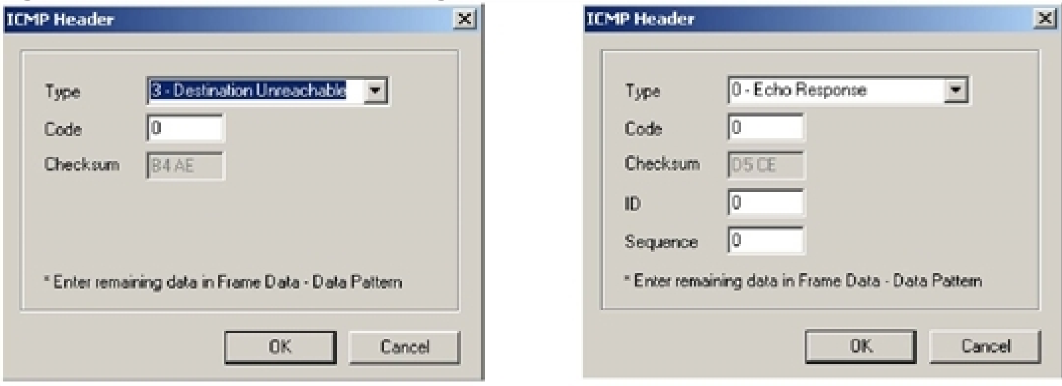
When the Protocol type is set to *ICMP/IP* in the *IP Header* dialog, the *Edit ICMP* button may be used to bring up a dialog which allows editing of the ICMP header. The ICMP header follows the IP header. There are two versions of ICMP:

- *ICMP for IPv4*.
- ICMP for IPv6.

ICMP for IPv4

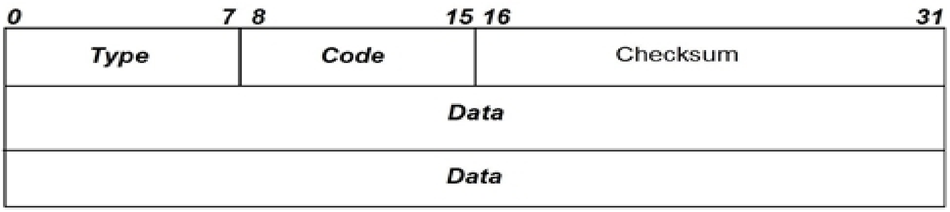
For configuring ICMP headers for IPv4, two dialog formats are shown in *Figure:Protocols: ICMP Header Dialogs*. The dialog format on the left applies to most ICMP messages, and the one on the right is specific to Echo Request/Reply.

Figure:Protocols: ICMP Header Dialogs



The format of an ICMPv4 header is shown in *Figure:Protocols: ICMPv4 Header Dialog*.

Figure:Protocols: ICMPv4 Header Dialog



The correlation between the fields of an ICMPv4 header and the elements of the *ICMPv4 Header* dialog which set those fields are described in *Table:ICMPv4 Header Fields Set by the ICMPv4 Dialog*.

Table:ICMPv4 Header Fields Set by the ICMPv4 Dialog

Header Field	Dialog Field	Description
Type	Type	The type of ICMPv4 message. Choose one of: • 0 =Echo Response • 1 & 2 = Reserved • 3 =Destination Unreachable • 4 =Source Quench • 5 = Redirect • 6 & 7 = (No specified use) • 8 =Echo Request • 9 = Router Advertisement • 10 = Router Solicitation • 11 =Time Exceeded • 12 =Parameter Fault • 13 =TimeStamp Request • 14 = TimeStamp Response • 15 = Information Request • 16 = Information Reply • 17 = Subnet Mask Request • 18 =Subnet Mask Reply • 19 = Reserved (for security)

Header Field	Dialog Field	Description
		• 20 - 29 = Reserved (for robustness) • 30 = Traceroute • 31 = Conversion Error • 32 = Mobile Host Redirect • 35 = Mobile Registration Request • 36 = Mobile Registration Reply • 37 = Domain Name Request • 38 = Domain Name Reply • 39 = SKIP Algorithm Discovery • 40 = Photuris Security Failures
Checksum	Checksum	The 16-bit ones complement of the ones complement sum of the 8-octet ICMPv4 message.
Data	ID and Sequence	For Echo Request and Echo Reply messages only. It sets the first data 32 bits: the first 16 bits are the ID, and the second 16 bits are the Sequence.

In general, the ICMP header dialog will not fill in the majority of the data bytes. These can be entered in the Data Pattern box of the Frame Data tab per RFCs 972 and 950.

ICMP for IPv6

There are two main groups of ICMPv6 messages—error messages (Types 0 to 127), and informational messages (Types 128 to 255). The ICMPv6 message headers are preceded by an IPv6 header, and may be preceded by IPv6 extension headers, and the Next Header value in the IPv6 part of the header with be '58.' The ICMP message header types for IPv6 are listed below.

- 1 - *Destination Unreachable Message*.
- 2 - *Packet Too Big Message*`.
- 3 - *Time Exceeded Message*.
- 4 - *Parameter Problem Message*.
- 128 - *Echo Request Message*.
- 129 - *Echo Reply Message*.
- 130 - *Multicast Listener Query*.
- 131 - *Multicast Listener Report*.
- 132 - *Multicast Listener Done*.
- 133 - *Router Solicitation Message Format*.
- 134 - *Router Advertisement Message Format*.
- 135 - *Neighbor Solicitation Message Format*.
- 136 - *Neighbor Advertisement Message Dialog*.
- 137 - Redirect Message Format.

An additional dialog is provided so that you can define custom IPv6 headers:

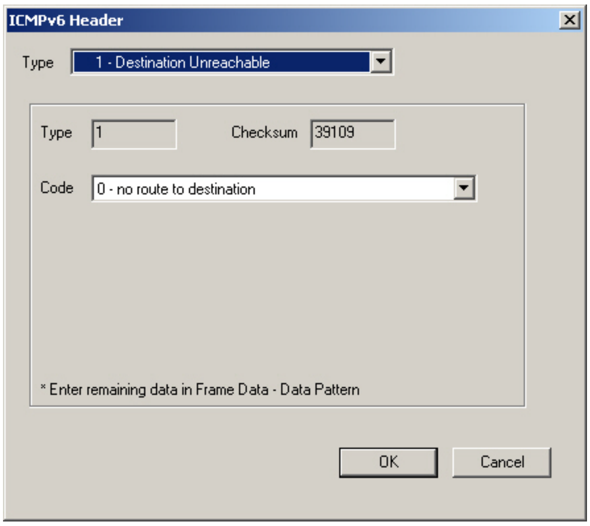
User Defined Message Dialog.

NOTE The **ICMPv6** dialog is reached by selecting the **IPv6** and **ICMP/IP** option buttons in the *Protocols* section of the *Frame Data* tab, selecting the **Edit** button, and then selecting the **Edit ICMP** button from the *IPv6 Header* dialog.

Destination Unreachable Message

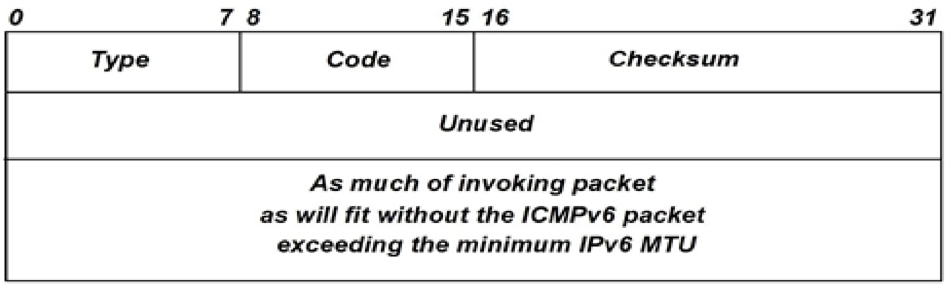
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Destination Unreachable* option in the *Type* pull-down list. The *Destination Unreachable* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Destination Unreachable Message*.

Figure:ICMPv6 Destination Unreachable Message



The format of an ICMPv6 Destination Unreachable Message header is shown in *Figure:ICMPv6 Destination Unreachable Message Format*.

Figure:ICMPv6 Destination Unreachable Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Destination Unreachable Message Header Fields*.

Table:ICMPv6 Destination Unreachable Message Header Fields

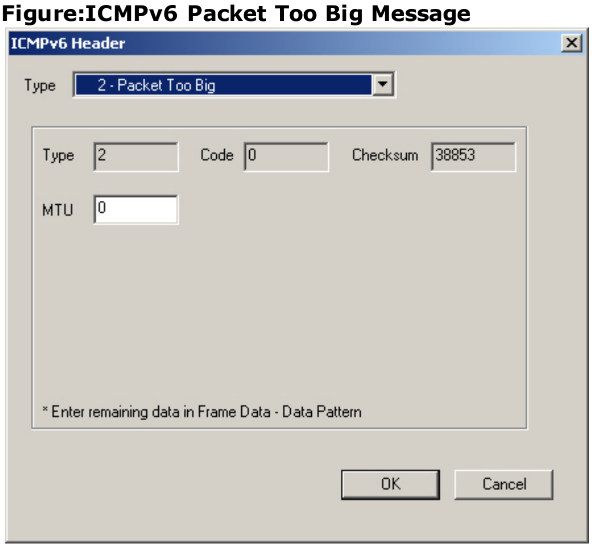
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 1 - Destination Unreachable
Type	Type	(Read-only) The Type is defined as '1'.
Code	Code	Choose one of: • 0 - no route to destination • 1 - communication with destination administratively

Header Field	Dialog Field	Description
		prohibited • 2 - (not assigned) • 3 - address unreachable • 4 - port unreachable
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
		NOTE Enter the remaining data in the Frame Data Dialog - Data Pattern box.

Packet Too Big Message

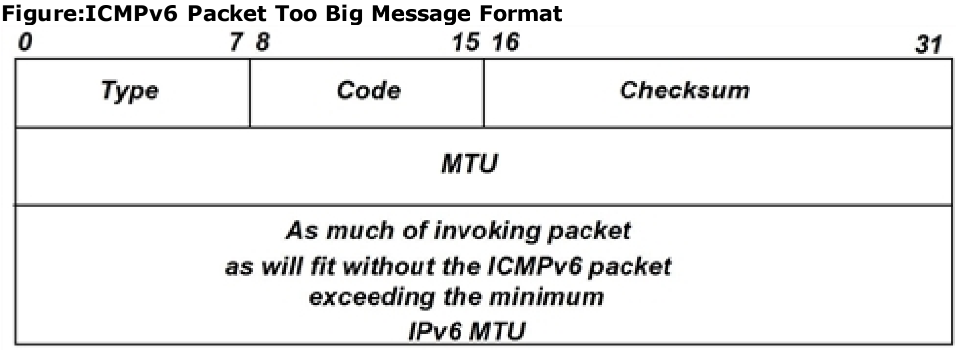
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Packet Too Big* option in the *Type* pull-down list. The *Packet Too Big* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Packet Too Big Message*.

Figure:ICMPv6 Packet Too Big Message



The format of an ICMPv6 Packet Too Big Message is shown in *Figure:ICMPv6 Packet Too Big Message Format*.

Figure:ICMPv6 Packet Too Big Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Packet Too Big Message Header Fields*.

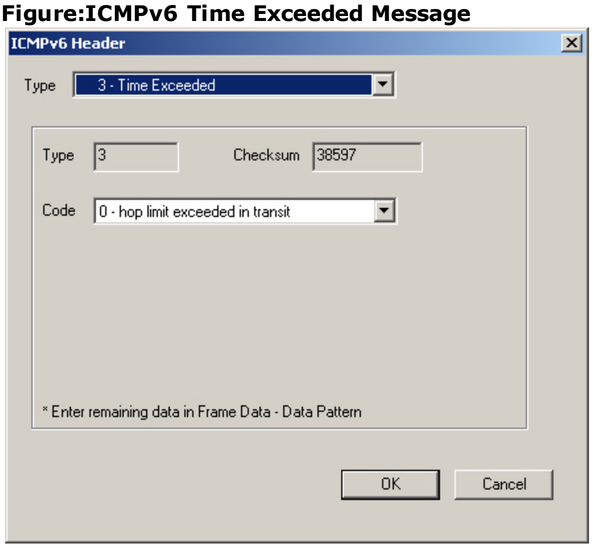
Table:ICMPv6 Packet Too Big Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 2–Packet Too Big
Type	Type	(Read-only) The Type is defined as '2'.
Code	Code	(Read-only) Sender sets this to '0'.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
MTU	MTU	Max Transmission Unit: The maximum size of the message that can be sent on this link to the next hop.
		NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Time Exceeded Message

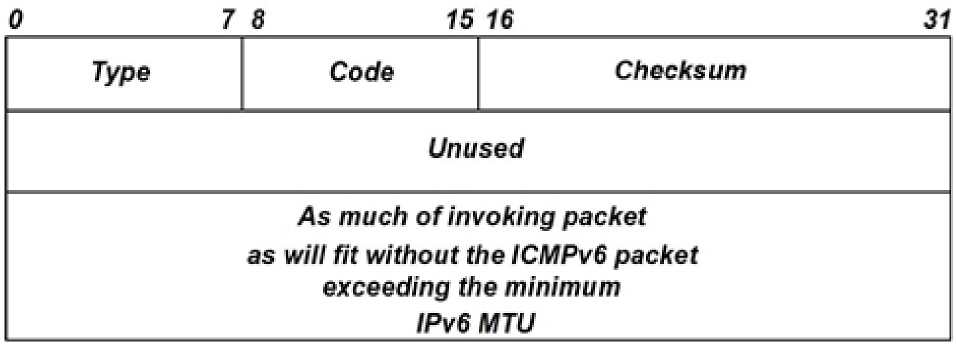
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Time Exceeded* option in the *Type* pull-down list. The *Time Exceeded* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Time Exceeded Message*.

Figure:ICMPv6 Time Exceeded Message



The format of an ICMPv6 Time Exceeded Message is shown in *Figure:ICMPv6 Time Exceeded Message Format*.

Figure:ICMPv6 Time Exceeded Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Time Exceeded Message Header Fields*.

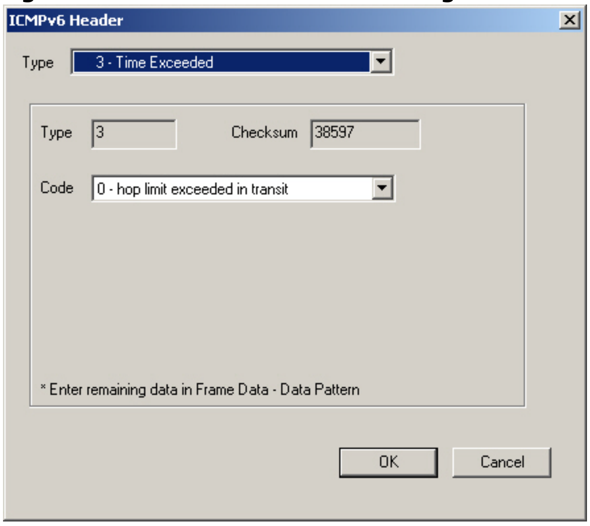
Table:ICMPv6 Time Exceeded Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 3 - Time Exceeded
Type	Type	(Read-only) The Type is defined as '3.'
Code	Code	Choose one of: • 0: hop limit exceeded in transit • 1: fragment reassembly time exceeded
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
		NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Time Exceeded Message

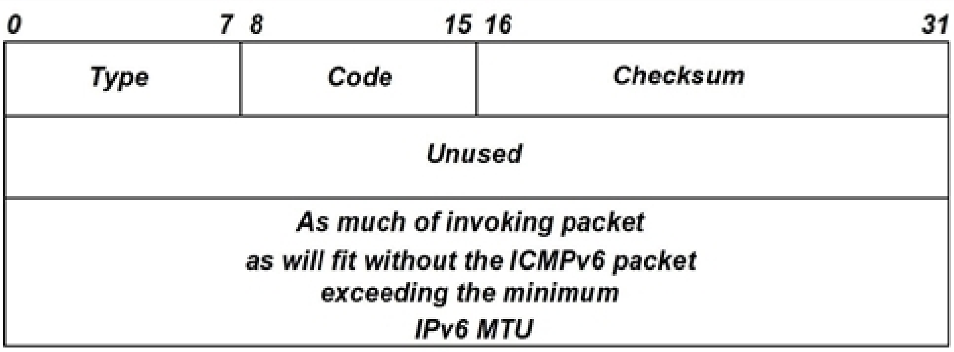
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Time Exceeded* option in the *Type* pull-down list. The *Time Exceeded* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Time Exceeded Message*.

Figure:ICMPv6 Time Exceeded Message



The format of an ICMPv6 Time Exceeded Message is shown in *Figure:ICMPv6 Time Exceeded Message Format*.

Figure:ICMPv6 Time Exceeded Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Time Exceeded Message Header Fields*.

Table:ICMPv6 Time Exceeded Message Header Fields

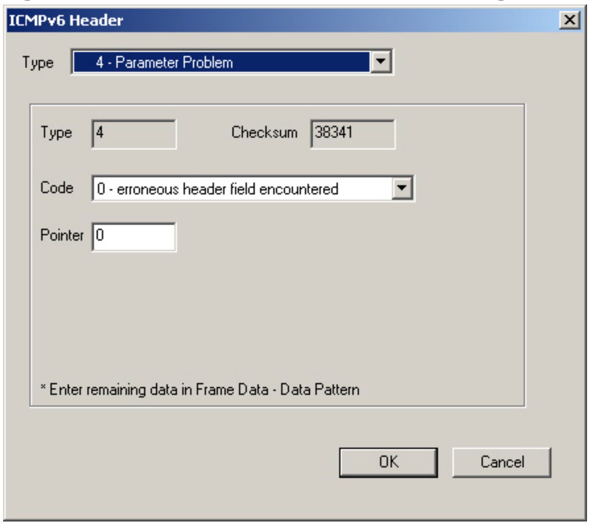
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 3 - Time Exceeded
Type	Type	(Read-only) The Type is defined as '3.'
Code	Code	Choose one of: • 0: hop limit exceeded in transit • 1: fragment reassembly time exceeded
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.

Header Field	Dialog Field	Description
		NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Parameter Problem Message

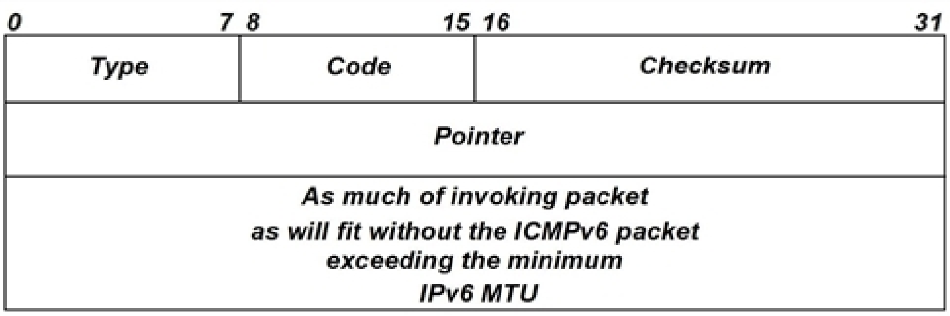
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Parameter Problem* option in the *Type* pull-down list. The *Parameter Problem* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Parameter Problem Message*.

Figure:ICMPv6 Parameter Problem Message



The format of an ICMPv6 Parameter Problem Message is shown in *Figure:ICMPv6 Parameter Problem Message Format*.

Figure:ICMPv6 Parameter Problem Message Format.



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Parameter Problem Message Header Fields*.

Table:ICMPv6 Parameter Problem Message Header Fields

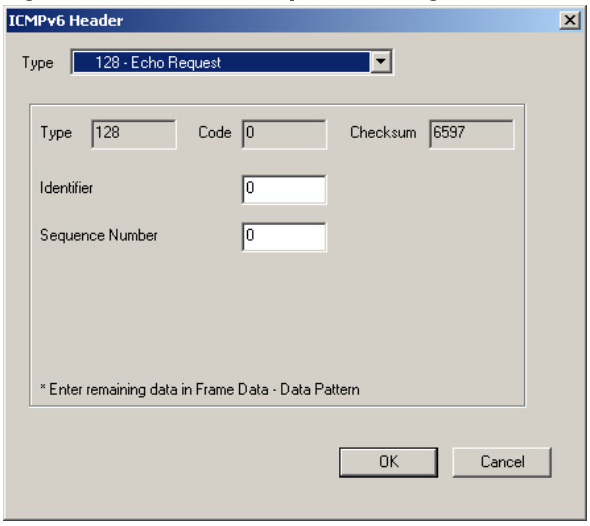
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 4 - Parameter Problem Message
Type	Type	(Read-only) The Type is defined as ‘4’.
Code	Code	Choose one of: • 0: erroneous header field encountered

Header Field	Dialog Field	Description
		• 1: unrecognized Next Header type encountered • 2: unrecognized IPv6 option encountered.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Pointer	Pointer	To identify the offset (octet) where the error was detected in the packet.
		NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Echo Request Message

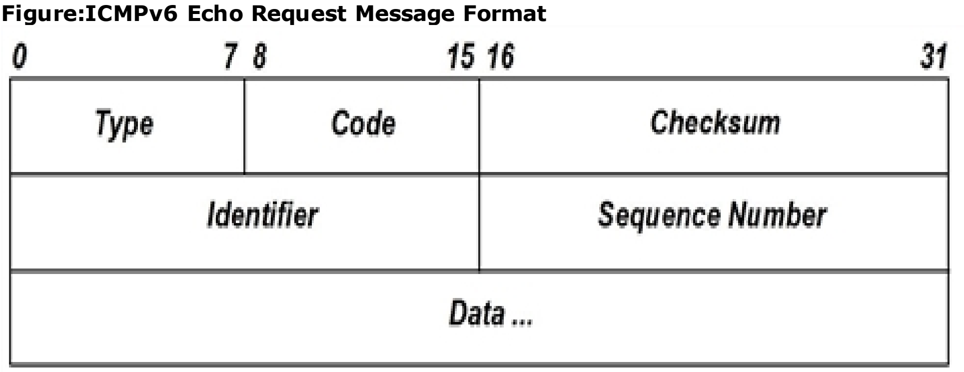
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Echo Request* option in the *Type* pull-down list. The *Echo Request* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Echo Request Message.*

Figure:ICMPv6 Echo Request Message



The format of an ICMPv6 Echo Request Message is shown in *Figure:ICMPv6 Echo Request Message Format*.

Figure:ICMPv6 Echo Request Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Echo Request Message Header Fields*.

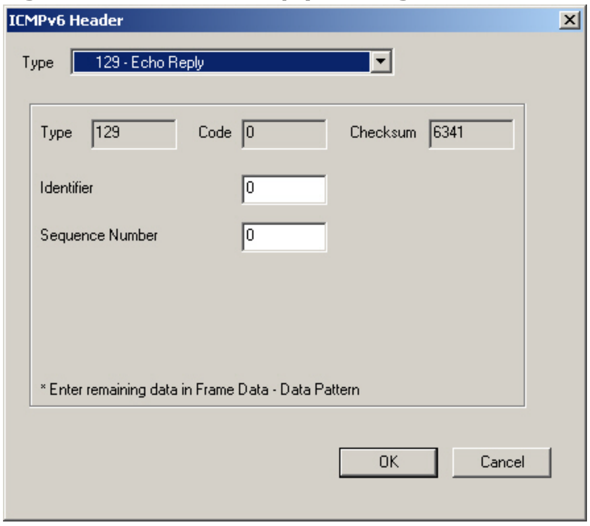
Table:ICMPv6 Echo Request Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 128 - Echo Request Message
Type	Type	(Read-only) The Type is defined as '128'.
Code	Code	(Read-only) '0'
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Identifier	Identifier	(May be '0'.) Identifier for matching Echo Replies and the Echo Request.
Sequence Number	Sequence Number	(May be '0'.) Sequence number for matching Echo Replies and the Echo Request.
Data ...		(Arbitrary data) NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Echo Reply Message

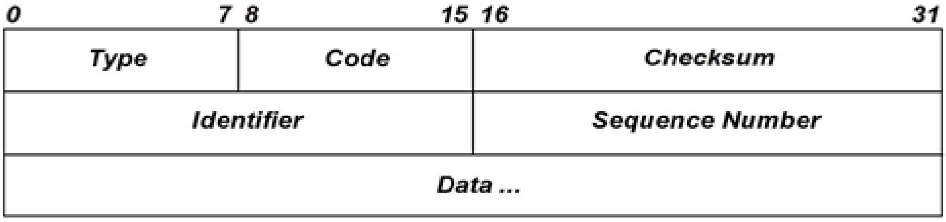
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Echo Reply* option in the *Type* pull-down list. The *Echo Reply* option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Echo Reply Message*.

Figure:ICMPv6 Echo Reply Message



The format of an ICMPv6 Echo Reply Message is shown in *Figure:ICMPv6 Echo Reply Message Format*.

Figure:ICMPv6 Echo Reply Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Echo Reply Message Header Fields*.

Table:ICMPv6 Echo Reply Message Header Fields

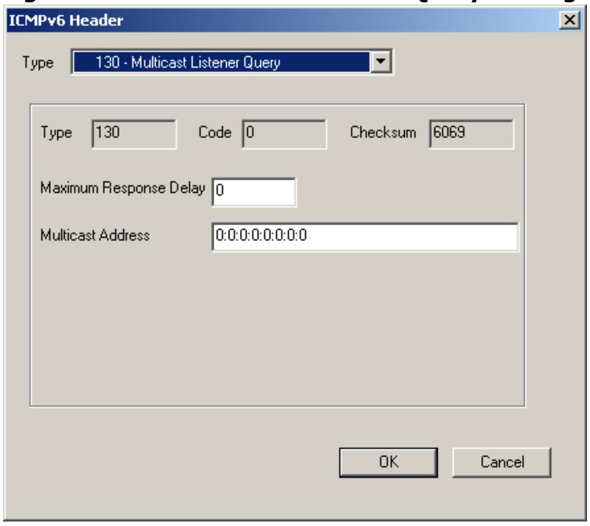
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 129 - Echo Reply Message
Type	Type	(Read-only) The Type is defined as '129'.
Code	Code	(Read-only) '0'.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Identifier	Identifier	The identifier used in the Echo Request message. (used for matching)
Sequence Number	Sequence Number	The sequence number used in the Echo Request message. (used for matching)
Data ...		(The arbitrary data sent in the Echo Request message.) NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

Multicast Listener Query

The Multicast Listener Query option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Multicast Listener Query Message*. It is part of the Multicast Listener Discovery (MLD) which is defined in RFC 2710, and the sender uses this message to learn about multicast listeners on directly connected links.

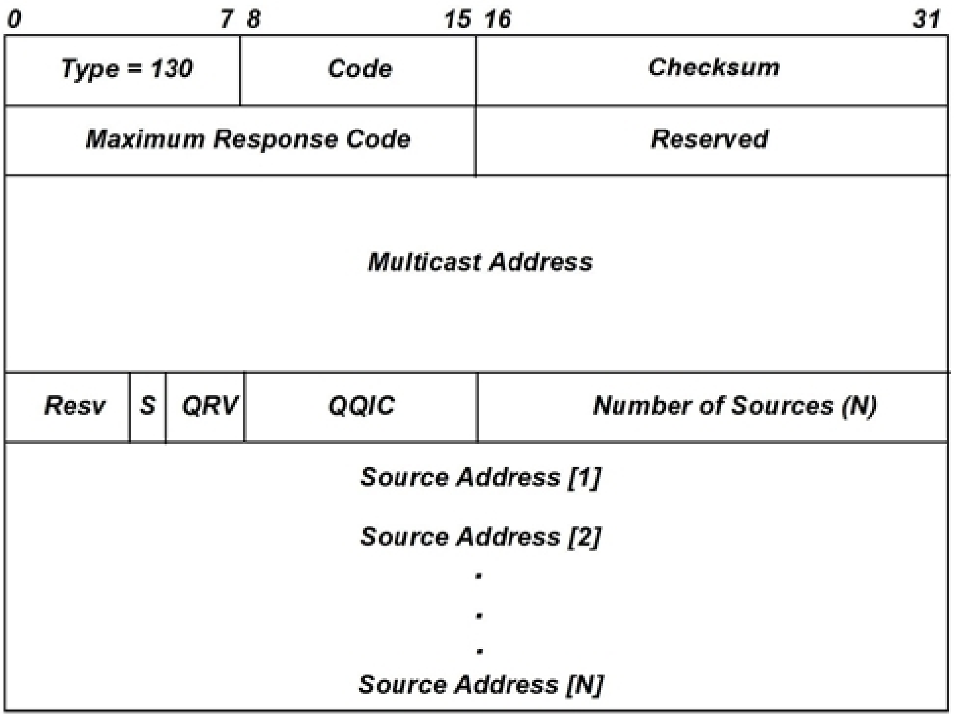
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Multicast Listener Query* option in the *Type* pull-down list.

Figure:ICMPv6 Multicast Listener Query Message



The format of an ICMPv6 Multicast Listener Query message is shown in *Figure:ICMPv6 Multicast Listener Query Message Format*.

Figure:ICMPv6 Multicast Listener Q uery Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Multicast Listener Query Message Header Fields*.

Table:ICMPv6 Multicast Listener Query Message Header Fields

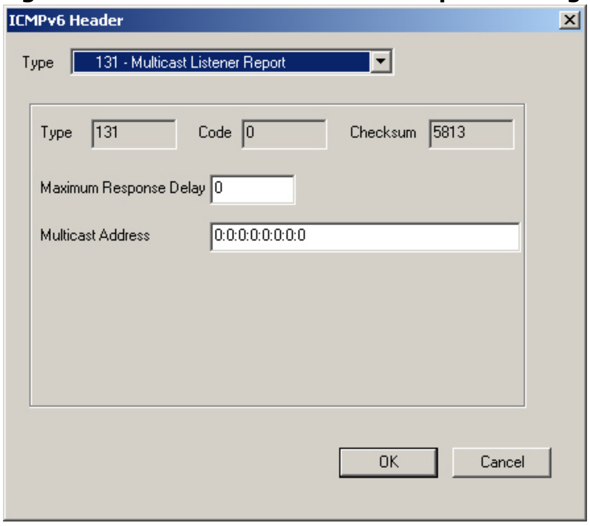
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 130 - Multicast Listener Query
Type	Type	(Read-only) The Type is defined as '130.'

Header Field	Dialog Field	Description
Code	Code	(Read-only) Set to '0' by the sender.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Maximum Response Code	Maximum Response Delay	(In milliseconds) The maximum delay allowed before a responding Multicast Listener Report message must be sent.
Multicast Address	Multicast Address	For general query type, set to '0.' For Multicast-Address-Specific Query specify an IPv6 multicast address.

Multicast Listener Report

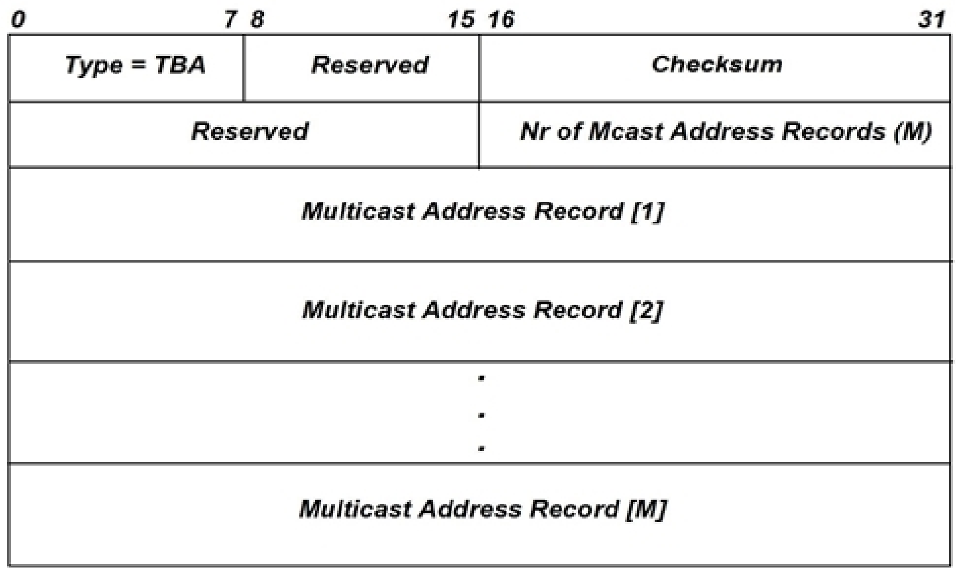
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Multicast Listener Report* option in the *Type* pull-down list. The dialog is shown in *Figure:ICMPv6 Multicast Listener Report Message*.

Figure:ICMPv6 Multicast Listener Report Message



The format of an ICMPv6 Multicast Listener Report message is shown in *Figure:ICMPv6 Multicast Listener Report Message Format*.

Figure:ICMPv6 Multicast Listener Report Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Multicast Listener Report Message Header Fields*.

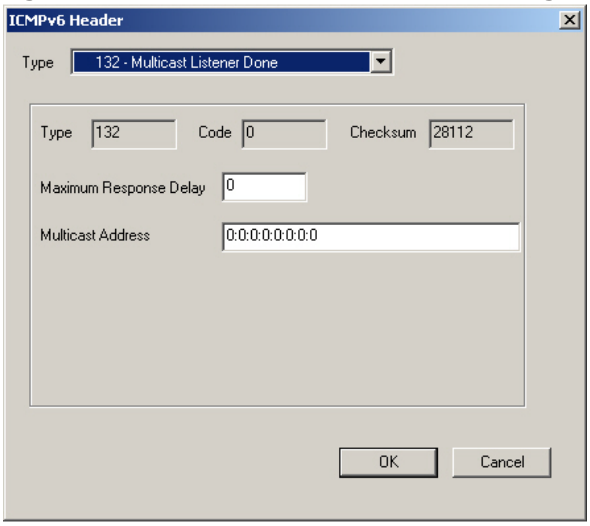
Table:ICMPv6 Multicast Listener Report Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 131- Multicast Listener Report
Type	Type	(Read-only) The Type is defined as '131'.
Code	Code	(Read-only) Set to '0' by the sender.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	Maximum Response Delay	(Used in Queries.) Set to '0' by sender; ignored by receiver.
	Multicast Address	The IPv6 multicast address specified by the sender's query.

Multicast Listener Done

The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Multicast Listener Done* option in the *Type* pull-down list. The Multicast Listener Done option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Multicast Listener Done Dialog*.

Figure:ICMPv6 Multicast Listener Done Dialog



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Multicast Listener Done Message Header Fields*.

Table:ICMPv6 Multicast Listener Done Message Header Fields

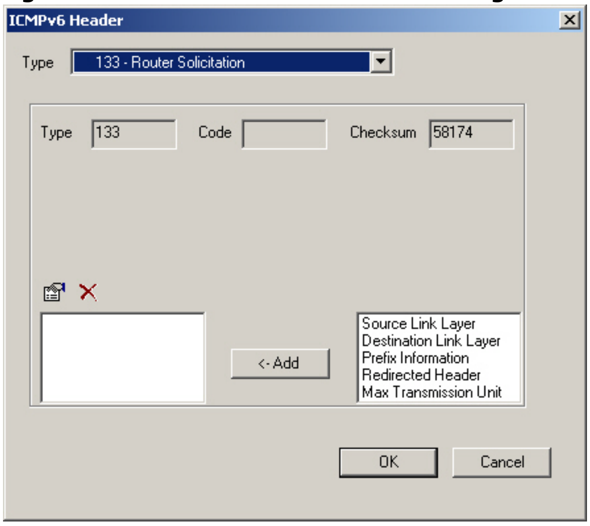
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 132 - Multicast Listener Done
Type	Type	(Read-only) The Type is defined as '132'.
Code	Code	(Read-only) Set to '0' by the sender.
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	Maximum Response Delay	(Used in Queries.) Set to '0' by sender; ignored by receiver.
	Multicast Address	The IPv6 multicast address specified by the sender's query.

Router Solicitation Message Format

The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Router Solicitation* option in the *Type* pull-down list. The Router Solicitation message format option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Router Solicitation Message Format Dialog*.

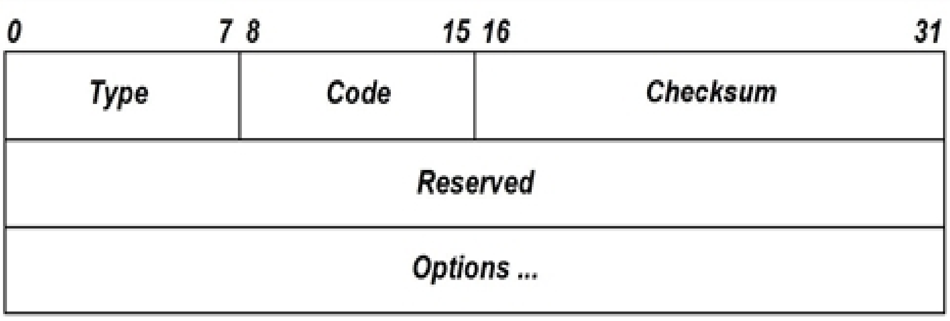
Message types 133 through 137 are defined in RFC 2463, 'Neighbor Discovery for IP Version 6 (IPv6).'

Figure:ICMPv6 Router Solicitation Message Format Dialog



The format of an ICMPv6 Router Solicitation message is shown in *Figure:ICMPv6 Router Solicitation Message Format*.

Figure:ICMPv6 Router Solicitation Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Router Solicitation Message Header Fields*.

Table:ICMPv6 Router Solicitation Message Header Fields

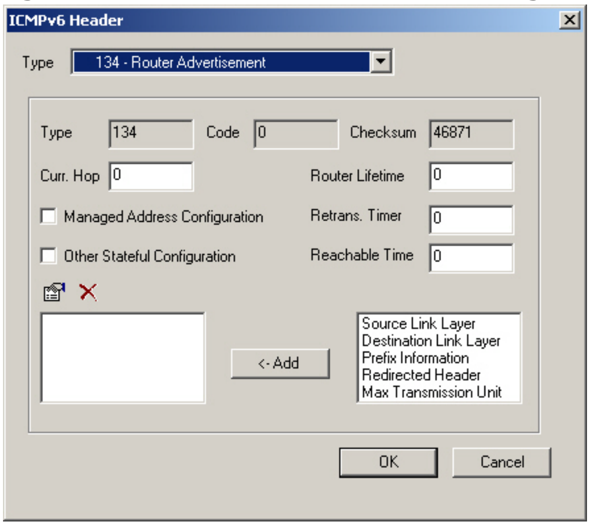
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 133 - Router Solicitation
Type	Type	(Read-only) The Type is defined as '133'.
Code	Code	(Read-only)
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Options	(Options Box)	Options: • Source Link Layer—Sender's link-layer address. • Destination Link Layer

Header Field	Dialog Field	Description
		• Prefix Information • Redirected Header • Max Transmission Unit NOTE *ICMPv6 Option Dialogs for additional information.*

Router Advertisement Message Format

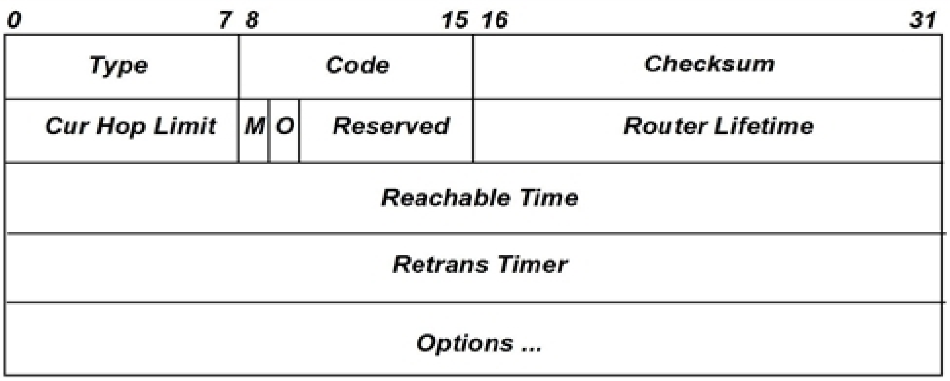
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Router Advertisement* option in the *Type* pull-down list. The Router Advertisement message format option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Router Advertisement Message Format Dialog*.

Figure:ICMPv6 Router Advertisement Message Format Dialog



The format of an ICMPv6 Router Advertisement message is shown in *Figure:ICMPv6 Router Advertisement Message Format*.

Figure:ICMPv6 Router Advertisement Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Router Advertisement Message Header Fields*.

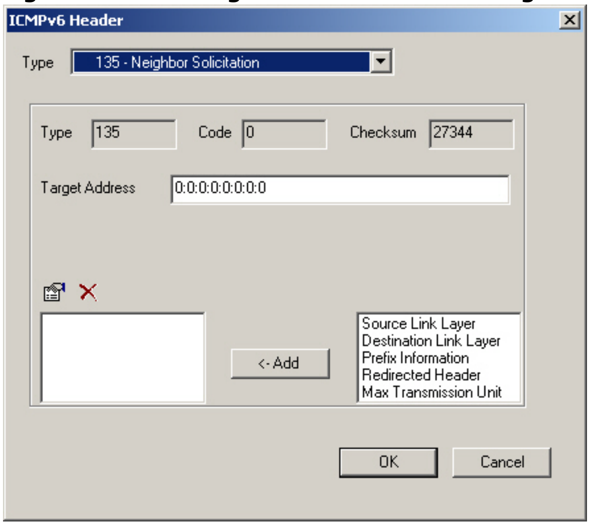
Table:ICMPv6 Router Advertisement Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 134 - Router Advertisement
Type	Type	(Read-only) The Type is defined as '134.'
Code	Code	(Read-only) '0'
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
Cur Hop Limit	Cur Hop Limit	Default value for the IP Header Hop Count field for outbound IP packets.
M	Managed Address Configuration	(1-bit flag) If selected, hosts use the stateful (administered) protocol for auto-configuration of addresses.
O	Other Stateful Configuration	(1-bit flag) If selected, hosts use the stateful (administered) protocol for auto-configuration of non-addressing (other) information.
Router Lifetime	Router Lifetime	Default router lifetime, in seconds. If Router Lifetime = 0, this is NOT a default router.
	Retrans Timer	(In milliseconds) Time interval between Neighbor Solicitation messages.
	Reachable Time	(In milliseconds) Amount of time that a neighbor is assumed to be reachable, following a confirmation of reachable.
	Options Box:	Options: • Source Link Layer • Destination Link Layer • Prefix Information • Redirected Header • Max Transmission Unit NOTE *ICMPv6 Option Dialogs* for additional information.

Neighbor Solicitation Message Format

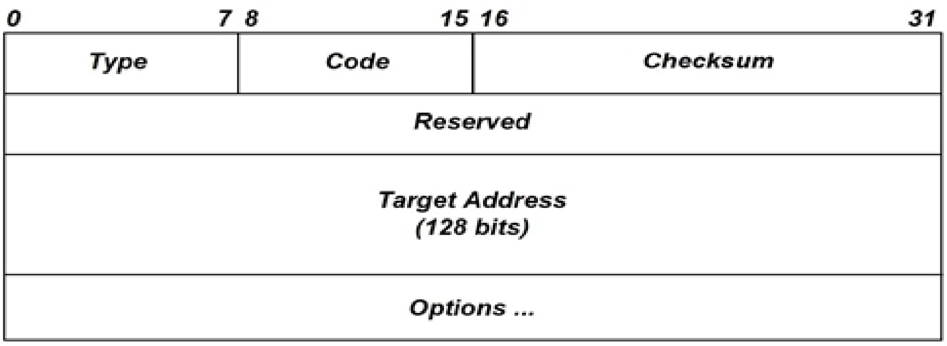
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Neighbor Solicitation* option in the *Type* pull-down list. The Neighbor Solicitation Message Format option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Neighbor Solicitation Message Dialog*.

Figure:ICMPv6 Neighbor Solicitation Message Dialog



The format of an ICMPv6 Neighbor Solicitation Message is shown in *Figure:ICMPv6 Neighbor Solicitation Message Format*.

Figure:ICMPv6 Neighbor Solicitation Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Neighbor Solicitation Message Header Fields*.

Table:ICMPv6 Neighbor Solicitation Message Header Fields

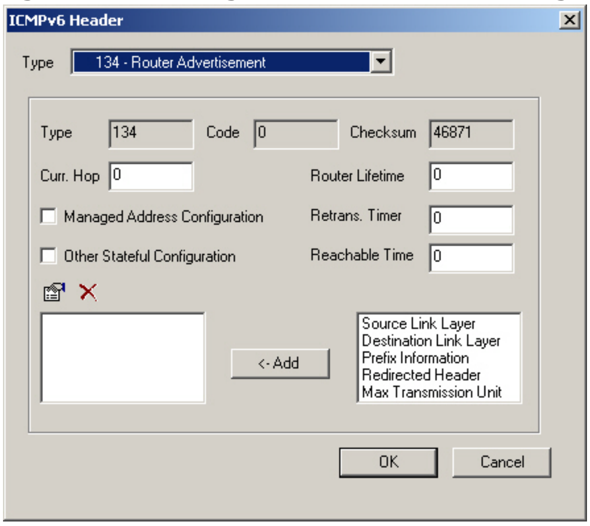
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 135 - Neighbor Solicitation Message Format
Type	Type	(Read-only) The Type is defined as '135'.
Code	Code	(Read-only) '0'
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	Target Address	The IPv6 address of the neighbor (target) to which the solicitation was sent. (MUST NOT be multicast IPv6 address.)

Header Field	Dialog Field	Description
Options	(Options Box)	Options: • Source Link Layer • Destination Link Layer • Prefix Information • Redirected Header • Max Transmission Unit NOTE *ICMPv6 Option Dialogs* for additional information.

Neighbor Advertisement Message Dialog

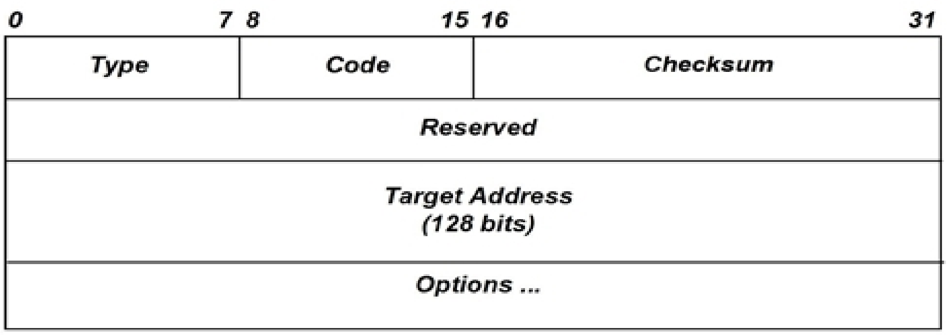
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Neighbor Advertisement Message Dialog* option in the *Type* pull-down list. The Neighbor Advertisement Message Format option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Neighbor Advertisement Message Dialog*.

Figure:ICMPv6 Neighbor Advertisement Message Format



The format of an ICMPv6 Neighbor Advertisement Message is shown in *Figure:ICMPv6 Neighbor Advertisement Message Format*.

Figure:ICMPv6 Neighbor Advertisement Message Format



The message header fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Neighbor Advertisement Message Header Fields*.

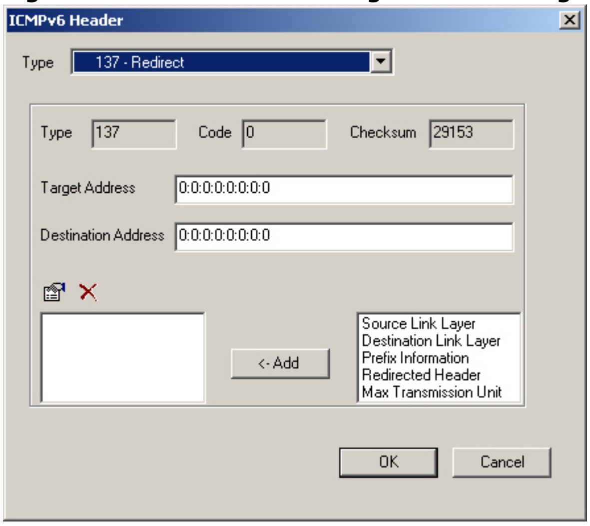
Table:ICMPv6 Neighbor Advertisement Message Header Fields

Header Field	Dialog Field	Description
Type	Type	The type for this message is: 136 - Neighbor Advertisement
Type	Type	(Read-only) The Type is defined as '136.'
Code	Code	(Read-only) '0.'
Checksum	Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	Router	(1-bit flag) If selected, this sender is a router (not a host).
	Solicited	(1-bit flag) If selected, this neighbor advertisement is sent in response to a neighbor solicitation message.
	Override	(1-bit flag) If selected, the information in this advertisement should override the existing entry and update the link layer address. Not for use with anycast addresses.
	Target Address	128-bit IPv6 address. (MUST NOT be multicast IPv6 address.): • For solicited advertisements: It is the target address in the Neighbor Solicitation Message. • For unsolicited advertisements: It is the address with a link-layer address which has changed.
	Options Box:	Options: • Source Link Layer • Destination Link Layer • Prefix Information • Redirected Header • Max Transmission Unit NOTE *ICMPv6 Option Dialogs* for additional information.

Redirect Message Format

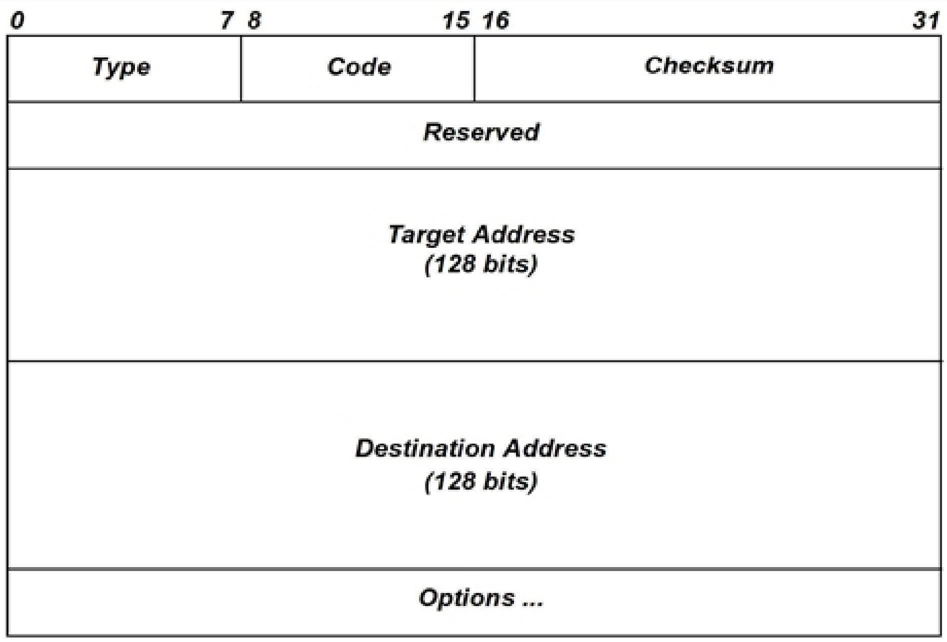
The controls in this version of the *ICMPv6* dialog are displayed by selecting the *Redirect* option in the *Type* pull-down list. The Redirect message format option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 Redirect Message Format Dialog*.

Figure:ICMPv6 Redirect Message Format Dialog



The format of an ICMPv6 Redirect Message is shown in *Figure:ICMPv6 Redirect Message Format*.

Figure:ICMPv6 Redirect Message Format



The message header fields and the corresponding fields in the dialog are described in *Table:ICMPv6 Redirect Message Header Fields*.

Table:ICMPv6 Redirect Message Header Fields

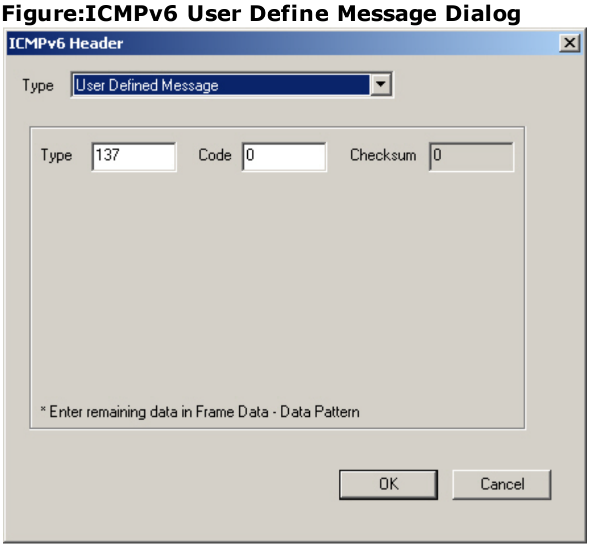
Header Field	Dialog Field	Description
Type	Type	The type for this message is: 137 - Redirect Message Format
Type	Type	(Read-only) The Type is defined as '137'.
Code	Code	(Read-only) '0'.
Checksum	Checksum	(Read-only)

Header Field	Dialog Field	Description
		The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	Target Address	128-bit IPv6 address. This is the **same address** as the Destination address if the destination is a neighbor. If the target is **not** a neighbor, this is the address of a router which is a better first-hop node.
	Destination Address	128-bit IPv6 address. This is the IP address of the destination. If the destination is a neighbor, this address will be used as the Target address, also.
	Options Box:	Options: • Source Link Layer • Destination Link Layer • Prefix Information • Redirected Header • Max Transmission Unit NOTE *ICMPv6 Option Dialogs* for additional information.

User Defined Message Dialog

The controls in this version of the *ICMPv6* dialog are displayed by selecting the *User Defined Message* option in the *Type* pull-down list. The User Defined Message option of the *ICMPv6 Header* dialog is shown in *Figure:ICMPv6 User Define Message Dialog.*

Figure:ICMPv6 User Define Message Dialog



The message fields in the dialog are described in *Table:ICMPv6 User Define Message Header Fields*.

Table:ICMPv6 User Define Message Header Fields

Dialog Field	Description
Type	The type for this message is: User Defined Message
Type	The user-definable Type value.
Code	The user-definable Code value.
Checksum	(Read-only) The 16-bit ICMPv6 checksum. This is the ones complement of the ones complement sum of the whole ICMPv6 message, which starts at the message type field. The 'whole' message includes the IPv6 header and extension header fields.
	NOTE Enter the remaining data in the *Frame Data* tab - Data Pattern box.

ICMPv6 Option Dialogs

For the IPv6 Neighbor Discovery message types 133 through 137, there are multiple options which can be included. Applicability of these options varies by the type of message, and when they do not apply the options are 'silently ignored' by the nodes.

These options can be configured through the dialogs in the following sections:

- *Source Link Layer Option Dialog*.
- *Destination Link Layer Option Dialog*.
- *Prefix Information Option Dialog*.
- *Redirected Header Option Dialog*.
- *Max Transmission Unit Option Dialog*.

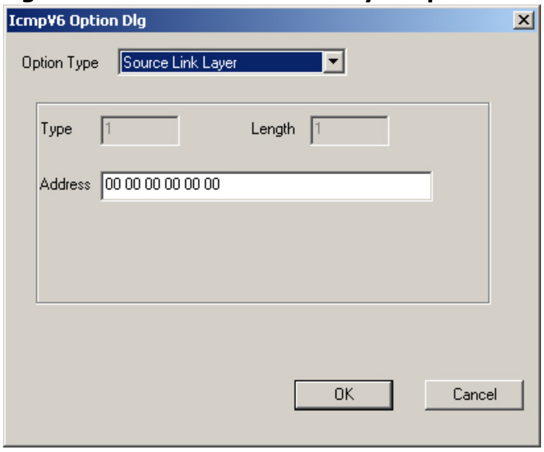
An additional option dialog is available so you can define custom ICMPv6 options:

- *User Define Option Dialog*.

Source Link Layer Option Dialog

The Source Link Layer selection in the *ICMPv6 Option* dialog is shown in *Figure:ICMPv6 Source Link Layer Option Dialog*.

Figure:ICMPv6 Source Link Layer Option Dialog



This option can be used in Neighbor Solicitation, Router Solicitation, and Router Advertisement messages. The option fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Source Link Layer Option Fields*.

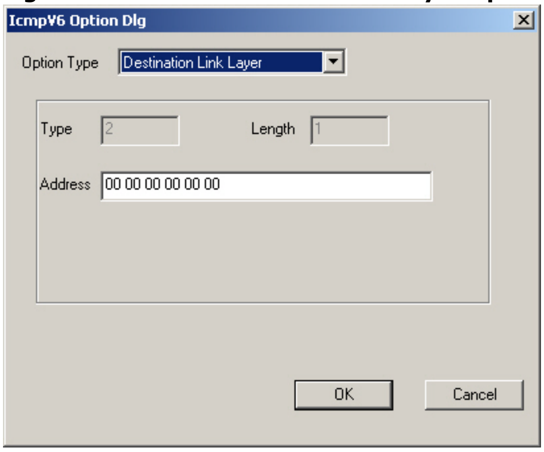
Table:ICMPv6 Source Link Layer Option Fields

Header Field	Dialog Field	Description
Type	Type	The type for this option is: Source Link Layer
Type	Type	(Read-only) The type value for this option = 1.
	Length	(Read-only) (8-bit integer) It is the length of the option, and includes type, length, and address fields. One unit of length = 8 octets. The default value = 2. A length value = 0 is invalid, and the node MUST silently discard a Neighbor Discovery packet where length = 0.
Link Layer Address	Address	(variable length) The link layer address of the node which sent the packet.

Destination Link Layer Option Dialog

The Destination Link Layer selection in the *ICMPv6 Option* dialog is shown *Figure:ICMPv6 Destination Link Layer Option Dialog*.

Figure:ICMPv6 Destination Link Layer Option Dialog



This option can be used in Neighbor Advertisement and Redirect messages. The option fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Destination Link Layer Option Fields*.

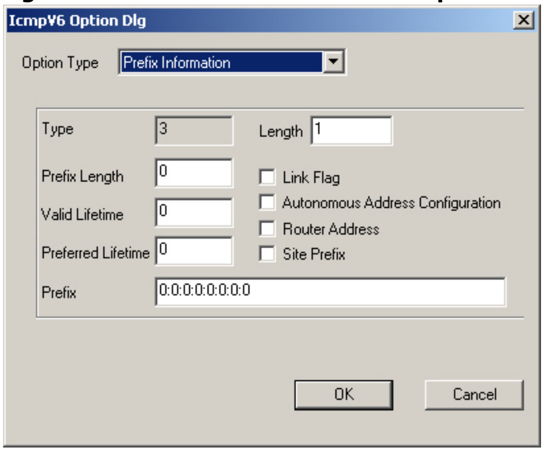
Table:ICMPv6 Destination Link Layer Option Fields

Option Field	Dialog Field	Description
Option Type	Type	The type for this message option is: Destination Link Layer
Type	Type	(Read-only) The type value for this option = 2.
Length	Length	(Read-only) (8-bit integer) The length of the option, and includes type, length, and address fields. One unit of length = 8 octets. The default value = 1. A length value = 0 is invalid, and the node MUST silently discard a Neighbor Discovery packet where length = 0.
Link-Layer Address	Address	(variable length) The target/destination link-layer address.

Prefix Information Option Dialog

The Prefix Information selection in the *ICMPv6 Option* dialog is shown in *Figure:ICMPv6 Prefix Information Option Dialog*.

Figure:ICMPv6 Prefix Information Option Dialog



This option may be used in Router Advertisement messages. The option fields, and the corresponding fields in the dialog, are described in *Table:ICMPv6 Prefix Information Option Fields*.

Table:ICMPv6 Prefix Information Option Fields

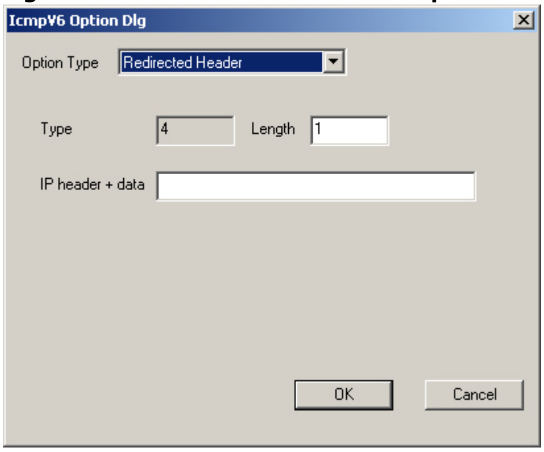
Option Field	Dialog Field	Description
Option Type	Type	The type for this message option is: Prefix Information.
Type	Type	(Read-only) The type value for this option = 3.
Length	Length	(8-bit integer) Length = 4. One unit of length = 8 octets. A length value = 0 is invalid, and the node MUST silently discard a Neighbor Discovery packet where length = 0.
Prefix Length	PrefixLength	(8-bit integer) The number of valid bits in the prefix.
Valid Lifetime	Valid Lifetime	(32-bit integer) The time, starting from packet transmission, that the prefix is valid in seconds. (0xffffffff = infinity.)
Preferred Lifetime	Preferred Lifetime	(32-bit integer) The time, starting from packet transmission, that the addresses generated from the prefix are 'preferred' in seconds. (0xffffffff = infinity.)
L	Link Flag	(1-bit flag) If selected, this prefix can be used for determining if the prefix is on-link.
A	Autonomous Address Configuration	(1-bit flag) If selected, this prefix can be used for autonomous address configuration.
	Router Address	If selected, indicates a router. The prefix option should not be sent by a router for a link-local prefix.
	Site Prefix	If selected, indicates a host/site. The prefix option should be ignored by a host, for a link-local prefix.
Prefix	Prefix	Can be an IPv6 address or an IPv6 address prefix. The valid leading bits are specified by the setting in the 'PrefixLength' field. All following bits MUST be set to

Option Field	Dialog Field	Description
		zero by the sending node and are ignored upon receipt.

Redirected Header Option Dialog

The Redirected Header selection in the *ICMPv6 Option* dialog is shown in *Figure:ICMPv6 Redirected Header Option Dialog*.

Figure:ICMPv6 Redirected Header Option Dialog



The option fields and the corresponding fields in the dialog are described in *Table:MPv6 Redirected Header Option Fields*.

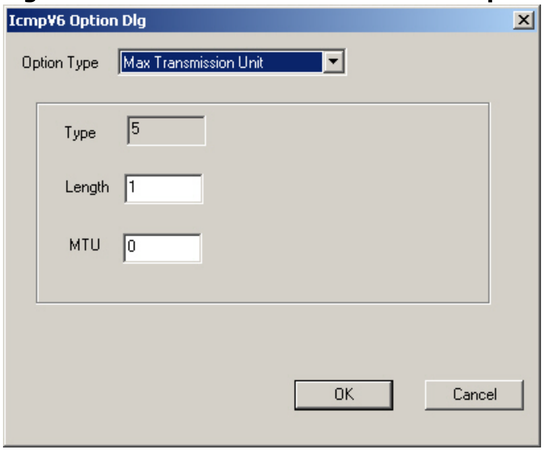
Table:MPv6 Redirected Header Option Fields

Option Field	Dialog Field	Description
Option Type	Type	The type for this message option is: Restricted Header
Type	Type	(Read-only) The type value for this option = 4.
Length	Length	(8-bit integer) The length of the option. One unit of length = 8 octets. A length value = 0 is invalid, and the node MUST silently discard a Neighbor Discovery packet where length = 0.
IP header + data	IP header + Data	Some of all of the contents of the original IP packet. It consists of as much of the original packet as can be carried in the Redirect message without going over the maximum allowed 1280 octets (bytes).

Max Transmission Unit Option Dialog

The Max Transmission Unit selection in the *ICMPv6 Option* dialog is shown in *Figure:ICMPv6 Max Transmission Unit Option Dialog*.

Figure:ICMPv6 Max Transmission Unit Option Dialog



The option fields and the corresponding fields in the dialog are described in *Table:ICMPv6 Max Transmission Unit Option Fields*.

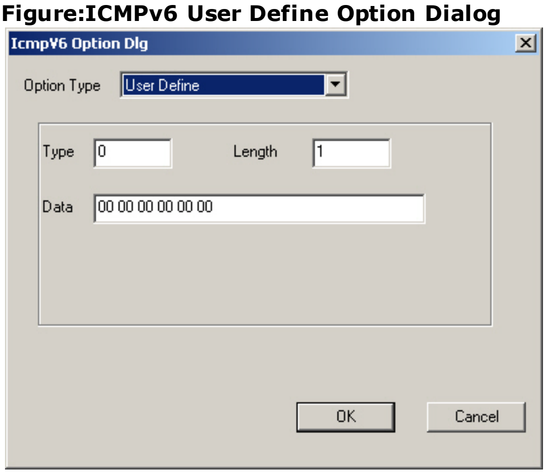
Table:ICMPv6 Max Transmission Unit Option Fields

Option Field	Dialog Field	Description
Option Type	Type	The type for this message option is: Max Transmission Unit
Type	Type	(Read-only) The type value for this option = 5.
Length	Length	(8-bit integer) Length = 1. A length value = 0 is invalid, and the node MUST silently discard a Neighbor Discovery packet where length = 0.
MTU	MTU	(32-bit integer) The recommended value of the Maximum Transmission Unit (MTU) on this link.

User Define Option Dialog

The User Define selection in the *ICMPv6 Option* dialog is shown in *Figure:ICMPv6 User Define Option Dialog*.

Figure:ICMPv6 User Define Option Dialog



The option fields in the dialog are described in *Table:ICMPv6 User Define Option Fields*.

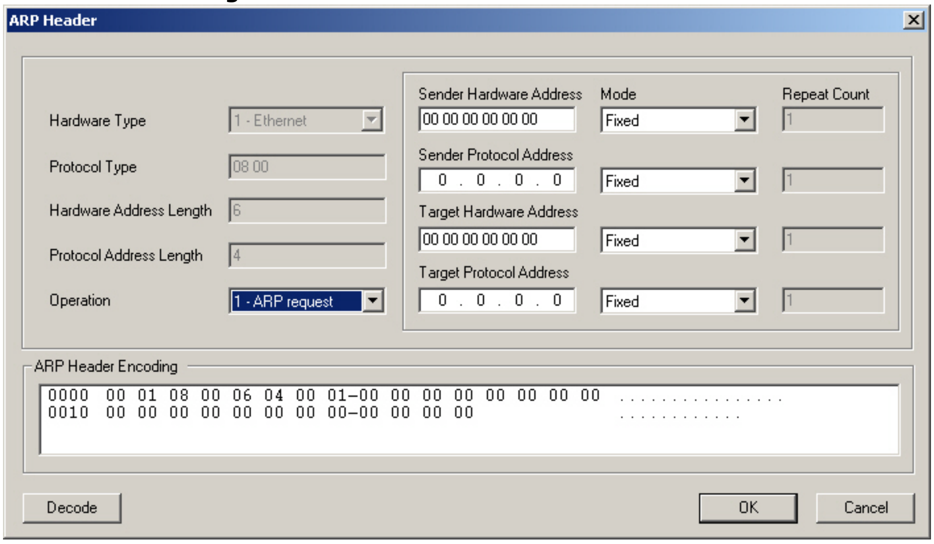
Table:ICMPv6 User Define Option Fields

Dialog Field	Description
Type	The type for this option is: User Define
Type	The user-definable Type value.
Length	The user-definable Length value, where one unit = one octet.
Data	The user-definable data field.

ARP Header Dialog

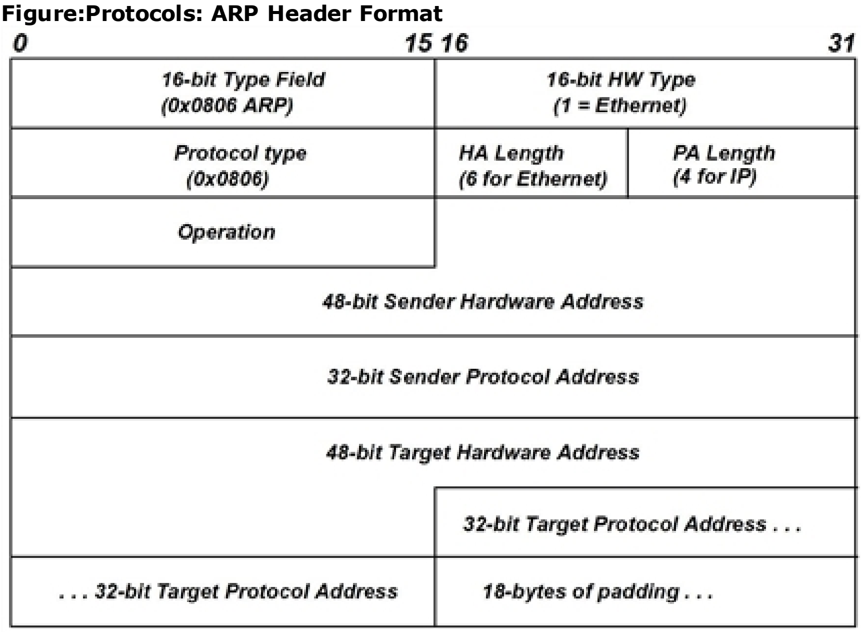
When the ARP option is selected in the Protocols section of the *Frame Data* tab, the *Edit* button opens the *ARP Header* dialog. This dialog allows for configuring various aspects of the ARP header information. The *ARP Header* dialog is shown in *Figure:Protocols: ARP Header Dialog*.

Figure:Protocols: ARP Header Dialog



The format of an ARP packet is shown in *Figure:Protocols: ARP Header Format.*

Figure:Protocols: ARP Header Format



The correspondence between the fields of an ARP packet and the elements of the *ARP Header* dialog which set those fields are described in *Table:ARP Header Fields Set by the ARP Header Dialog*.

Table:ARP Header Fields Set by the ARP Header Dialog

ARP Header Field	Dialog Element	Description
Type		Always 0x0806.
HW Type	Hardware Type	Always 1 for Ethernet.
Protocol Type	Protocol Type	Always 0x0806 for ARP.
HA Length	Hardware Address Length	Always 6 for Ethernet (in octets).
PA Length	Protocol Address Length	Always 4 for IP.
Operation	Operation	One of the ARP-related operations: • 0 - Unknown • 1 - ARP request • 2 - ARP reply • 3 - RARP request • 4 - RARP reply.
Sender Hardware Address	Sender Hard-ware Address	The MAC (Layer 2) address of the ARP packet sender. (See also Mode and Repeat Count.)
Sender Protocol Address	Sender Protocol Address	The IP (Layer 3) address of the ARP packet sender. (See also Mode and Repeat Count.)
Target Hardware Address	Target Hard-ware Address	The MAC (Layer 2) address of the target of the ARP packet. (See also Mode and Repeat Count.)
Target Protocol Address	Target Protocol Address	The IP (Layer 3) address of the target of the ARP packet. (See also Mode and Repeat Count.)
Pad		Extra padding to make a minimum-sized IP packet.
	Mode	The mode of modifying the IP address. Choose one of: • Fixed • Increment • Decrement • Continuous Increment • Continuous Decrement
	Repeat Count	The number of times to modify the IP address, using the selected mode for increment or decre-ment.

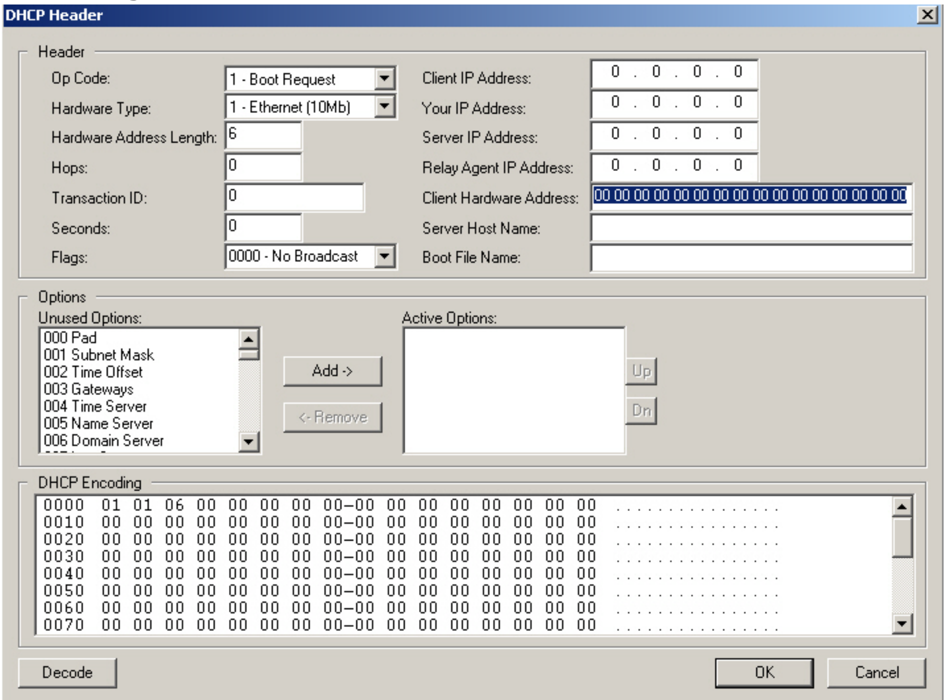
DHCP Header Dialog

The *DHCP Header* dialog is viewed from the *Frame Data* tab Protocols section, using the fol-lowing steps:

1. Select either the Ethernet II or the 802.2 SNAP choices from the Data Link Layer box.
2. Select DHCP/IP from the Protocols box, followed by the *Edit* button in the Protocols box.
3. In the resulting IP Header dialog, select the *Edit DHCP* button.

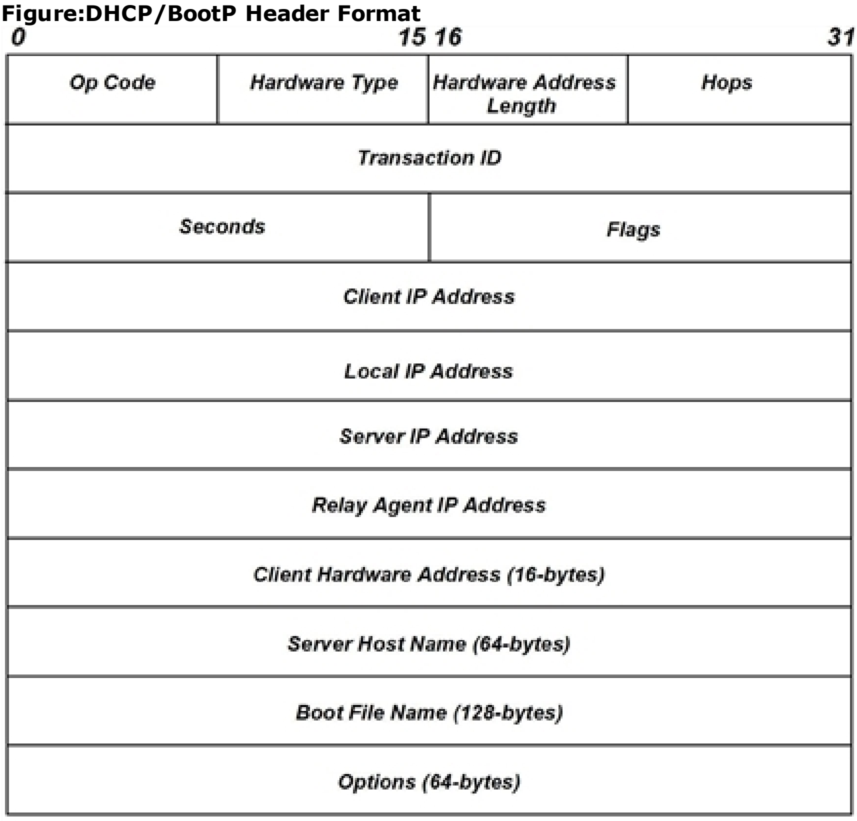
The *DHCP Header* dialog is shown in *Figure:DHCP Header Dialog*, followed by the format of a DHCP/BOOTP packet:

Figure:DHCP Header Dialog



The elements of the DHCP header are shown in *Figure:DHCP/BootP Header Format*.

Figure:DHCP/BootP Header Format



The field names in the *DHCP Header* dialog conform to the labels in the header format diagram and are described in *Table:DHCP/BootP Header Fields Set by the DHCP Header Dialog*.

Table:DHCP/BootP Header Fields Set by the DHCP Header Dialog

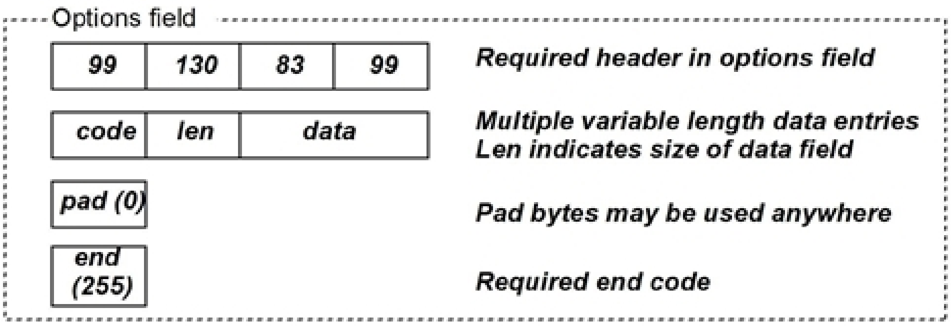
Field	Description
Op Code	One of: • 1 - Start Request. A request from a client to a server for information. • 2 - Start Reply. The server's response. • Unknown.
Hardware Type	The hardware address type. The default is '1' = 10Mb Ethernet. These numbers are drawn from the list of hardware types related to the ARP protocol. The most current version of this is found in *http://www.isi.edu/in-notes/iana/assignments/arp-parameters*.
Hardware Address Length	The length of address that corresponds to the Hardware Type. For example, '6' for Ethernet (MAC) addresses.
Hops	Number of hops. Clients set this to zero and servers may optionally use this in cross-gateway starting.
Transaction ID	A random number set by the client and used to match responses to requests.
Seconds	Filled in by the client and contains the number of seconds that have elapsed since the client started trying to start.
Flags	A single flag is defined:

Field	Description
	• 0000 - No Broadcast • 8000 - Broadcast • Unknown Broadcast is set by the client to indicate that it will require a broadcast response.
Client IP Address	Set by the client in a start request if it is known.
Local IP Address	Set by the server to indicate the client's IP address, if the client doesn't know its address.
Server IP Address	Returned by the server in its start reply.
Relay Agent IP Address	Set by the server, to be used in optional cross-gateway starting.
Client Hardware Address	The client's hardware address, the length of which is specified in the Hardware Address Length field.
Server Host Name	Set by the client to indicate the desired server it wishes to talk to.
Boot File Name	Set by the client to indicate a particular file name or operational mode. This is often used by the server to initiate a TFTP download of software to a client.
Options	An optional area used to transmit additional parameters. Option parameters are set using the 'Options' box in the center of the *DHCP Header* dialog and are discussed below.

DHCP Options

The DHCP options field is used to hold a wide variety of data. Its internal format, within the DHCP header, is shown in *Figure:DHCP Options Field Format*.

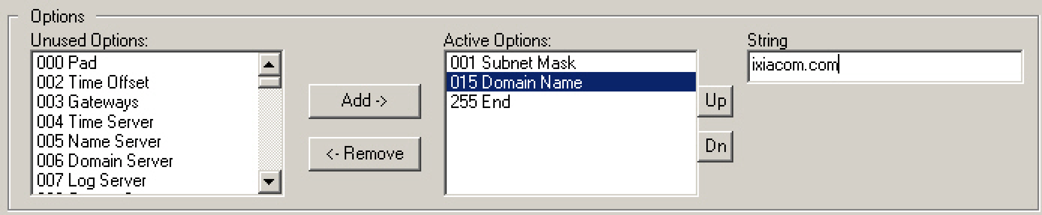
Figure:DHCP Options Field Format



If a DHCP packet uses its options field it must start with the four octets 99.130.83.99 (decimal, or 63.82.53.63 hex). This is followed by any number of coded entries. Each entry has a one-byte opcode, followed by a length byte and the code dependent data indicated by the length field. A special opcode (pad = 0) is reserved to pad data to any needed boundary. An end opcode (255) must terminate all of the data. The particular codes in that may be used are described in RFC 2132 which can be located at http://info.internet.isi.edu/in-notes/rfc/files/rfc2132.txt.

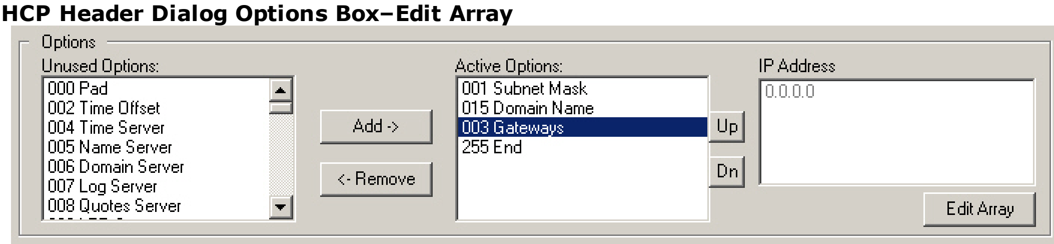
The options box, pictured in *Figure:DHCP Header Dialog Options Box*, may be used to set the options field of DHCP packets.

Figure:DHCP Header Dialog Options Box



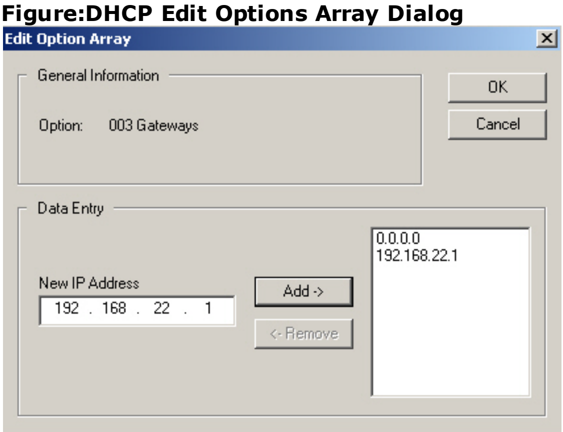
Unused Option codes are selected from the left list and moved into the Active Options code with the *Add* button. Active Options may be moved back into the unused category with the *Remove* button. Active options are rearranged through the use of the *Up* and *Dn* buttons. Each option may be configured by selecting the option and filling in the data in the right hand column, which asks for and formats data in a manner appropriate for the option selected. Where a list of data is called for, the Options box appears as shown in *Figure:DHCP Header Dialog Options Box–Edit Array*.

Figure:DHCP Header Dialog Options Box–Edit Array



To specify the number and content of the options data, select the *Edit Array* button. This presents the edit dialog shown in *Figure:DHCP Edit Options Array Dialog*.

Figure:DHCP Edit Options Array Dialog



This dialog allows to enter and remove array elements in the *Data Entry* box. New elements are entered in the edit box, whose format varies depending on the option under construction, and are added to the array with the *Add* button. Existing elements must be edited by removing them with the *Remove* button and adding them again.

DHCP Encoding

The bottom part of the *DHCP Header* dialog is the DHCP Encoding window (*Figure:DHCP Header Dialog*). The DHCP header is decoded in three columns: the hex offset from the beginning of the packet, the data interpreted in hex, and the data interpreted in ASCII. In order for data entered in the other parts of the screen to be reflected in the DHCP Encoding panel, it is necessary to move the cursor out of the data field using the TAB key, for example. DHCP data may be entered directly into the Encoding panel (hexadecimal or

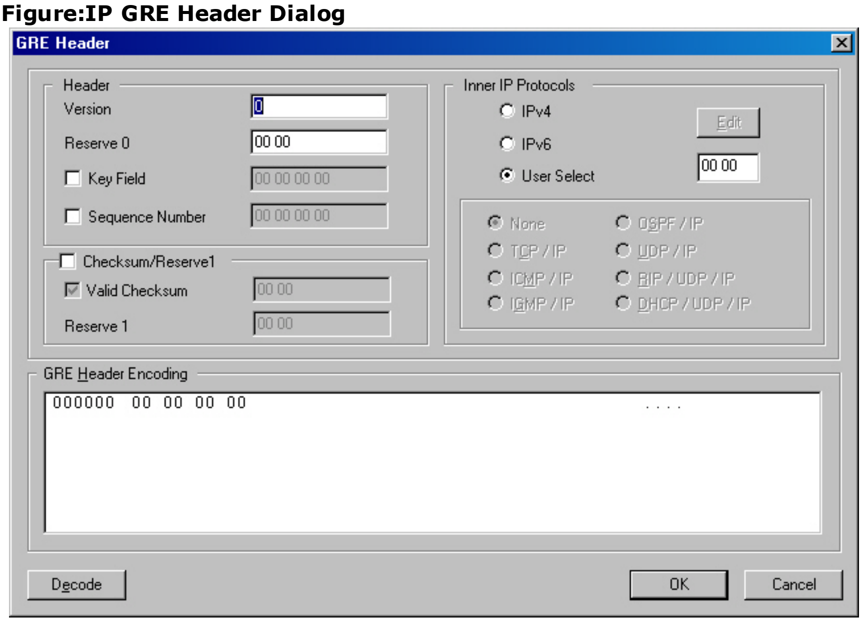
ASCII display) if desired. It is necessary to press the *Decode* button after editing in this manner.

GRE Header Dialog

General Routing Encapsulation (GRE) attempts to provide a simple, general purpose mechanism which reduces the problem of encapsulation from its current size to a more manageable size. Refer to the GRE—Generic Routing Encapsulation section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

The GRE Header dialog is accessed by selecting IPv4 and GRE in the protocol sub-tab of the Frame Data tab and selecting the Edit button. From the IP Header dialog, select the Edit GRE button. The GRE Header dialog is shown in *Figure:IP GRE Header Dialog*.

Figure:IP GRE Header Dialog



The format for a GRE message header (the default setting) is shown in *Figure:GRE Message Header*.

Figure:GRE Message Header

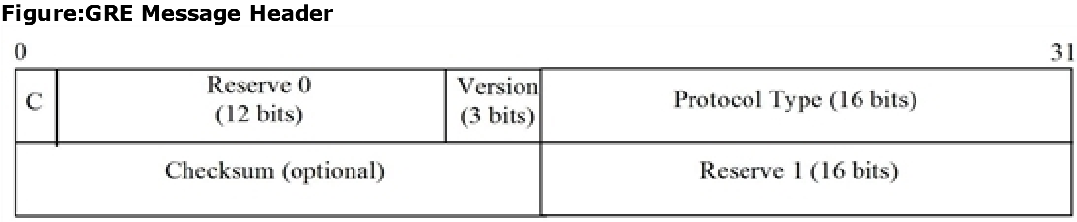


Table:GRE Configuration describes the controls for configuring the GRE header information.

Table:GRE Configuration

Section	Field/Control	Description
Header		Sets basic GRE header information
	Version	The version of GRE used. GRE headers are organized differently and contain varying information, depending on the version number.

Section	Field/Control	Description
	Reserve 0	Allows to set the Reserved 0 bits in the GRE header.
	Key Field	The GRE key is an authentication key used by the receiving router to validate the GRE packets. This check box allows to edit the GRE key.
	Sequence Number	The Sequence Number is used by the receiving router to establish the order in which packets have been transmitted. This check box allows to set the sequence number bits.
Inner IP Protocol		Sets the IP protocol used in the GRE.
	IPv4	Selects IPv4. This option enables the inner IP transport protocol option buttons as well.
	IPv6	Selects IPv6. This option enables the inner IP transport protocol option buttons as well.
	User Selected	Allows to set the IP field bits directly, using the edit box.
	Edit	Allows to edit the IPv4, IPv6, and transport options selected for the inner IP protocol.
Checksum/Reserve1		Allows to set the checksum value and the Reserve 1 value.
	Valid Checksum	Selecting this check box ensures the GRE checksum value is a valid value, and will return a 'Good' packet evaluation.
	Reserve1	Allows to set the Reserve 1 bits in the GRE header.
GRE Header Encoding		Displays the GRE bit information.

Protocol Padding

This dialog allows to added data padding between the Protocol Header and Payload Data patterns. It is accessed by selecting the *Protocol Pad* check box and then selecting the *Edit Data* button in the *Protocols* sub-tab of the *Frame Data* tab.

The Protocol Pad dialog is shown in *Figure:Protocol Pad Dialog*.

Figure:Protocol Pad Dialog

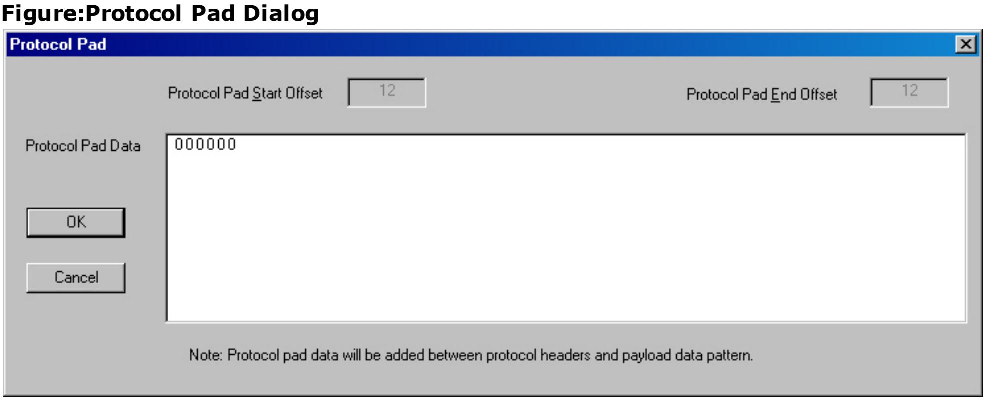


Table:Protocol Padding Configuration explains the controls in this dialog.

Table:Protocol Padding Configuration

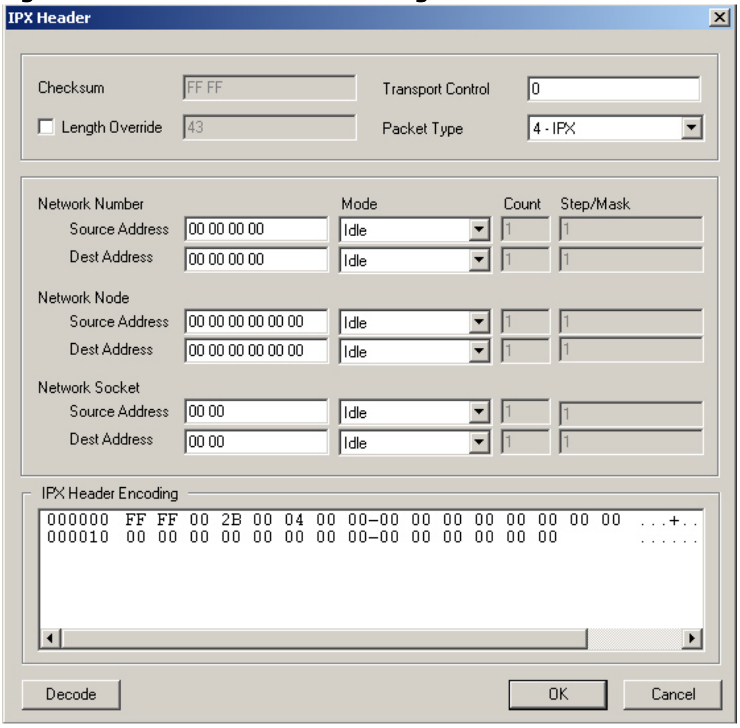
Field/Control	Description
Protocol Pad Start Offset	**Read Only.** Shows the offset for the beginning of the padding data, from the beginning of the packet.
Protocol Pad End Offset	**Read Only.** Shows the end of the padding data, from the beginning of the packet.
Protocol Pad Data	Allows to enter hexadecimal data that is used as padding data.

IPX Protocol

The protocol specific headers may be conveniently specified using the *Edit* button in the Protocols section. To access the IPX protocol header configuration controls, select the *IPX* option in the *Protocols* sub-tab, then select the *Edit* button.

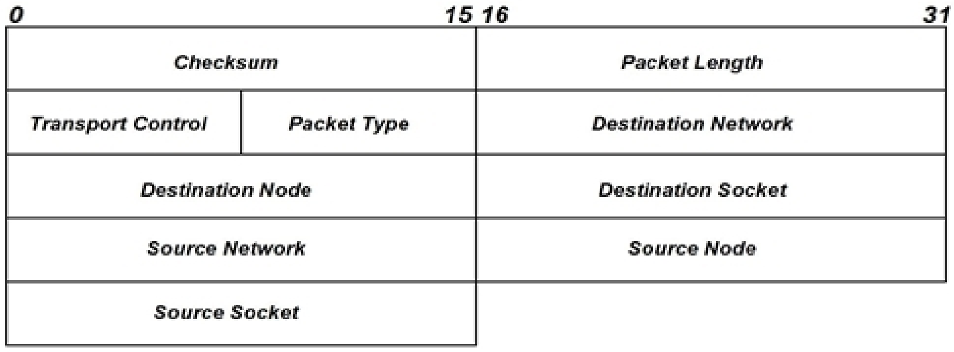
IPX protocols may not be used with Packet over SONET modules. The IPX selection shows the dialog in *Figure:Protocols: IPX Header Dialog*.

Figure:Protocols: IPX Header Dialog



The format of an IPX header is shown in *Figure:Protocols: IPX Header Dialog*.

Figure:Protocols: IPX Header Dialog



The correlation between the fields of an IPX header and the elements of the *IPX Header* dialog which set those fields are described in *Table:IPX Header Fields Set by the IPX Dialog*.

Table:IPX Header Fields Set by the IPX Dialog

Header Field	Dialog Field	Description
Checksum	Checksum	Automatically calculated checksum of the IPX header and packet data.
Packet Length	Length Override	If selected, the length field becomes active, and you may specify the length of the IPX datagram. If cleared, the length of the IPX datagram is automatically calculated.
	(Length field)	Length of the IPX datagram (in bytes).
Transport Control	Transport Control	Number of routers that the packet has passed through.
Packet Type	Packet Type	The type of IPX packet: • 0 - Unknown • 1 - Routing Info • 2 - Echo • 3 - Error • 4 - IPX • 5 - SPX • 17 - NCP NOTE Types 16, and 18-31 are reserved for Experimental Protocols.
Destination Network	Network Number - Dest Address	IPX Network number for the destination.
Source Network	Network Number - Source Address	IPX Network number for the source.
Destination Node	Network Node - Dest Address	Destination node number within the Destination Network.
Source Node	Network Node -	Source node number within the source network.

Header Field	Dialog Field	Description
	Source Address	
Destination Socket	Network Socket - Dest Address	Socket on the destination node within the destination network.
Source Socket	Network Socket - Source Address	Socket on the source node within the source network.
	Mode	The mode of modifying the IP address. Choose one of: • Idle • Increment • Decrement • Continuous Increment • Continuous Decrement.
	Count	The number of times to modify the IP Address using the mode—increment or decrement.
	Mask	Defines the network mask to be used for IP addresses, used with increment, decrement, continuous increment, and continuous decrement.

IPX Header Encoding

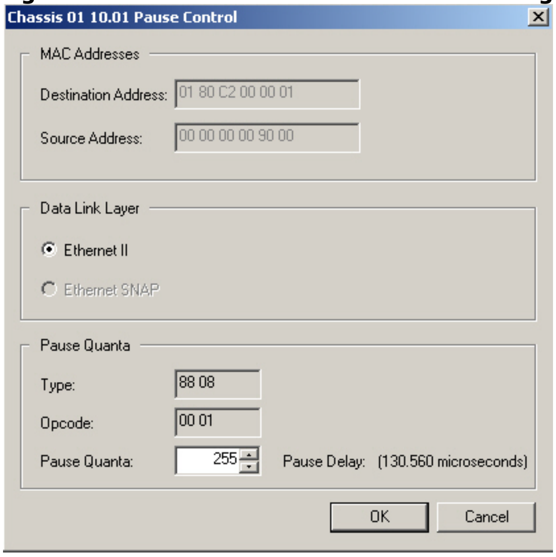
Values which are set in the dialog are reflected in the hexadecimal display of the IPX Header Encoding at the bottom of the dialog. It is also possible to edit the IPX Header directly from the display; all editing occurs in type-over mode. After any change, the *Decode* button should be clicked to reflect these changes back into the dialog fields.

Pause Control

The Pause control header is a means of implementing data flow control between attached devices, as defined in IEEE 802.3. The Pause control protocol is used only with the Ethernet II and Ethernet SNAP data link layer protocols.

The pause control message headers may be specified using the *Edit* button in the Protocols section of the *Frame Data* tab. The *Pause Control* dialog is shown in *Figure:Protocols: Pause Control Header Dialog*.

Figure:Protocols: Pause Control Header Dialog



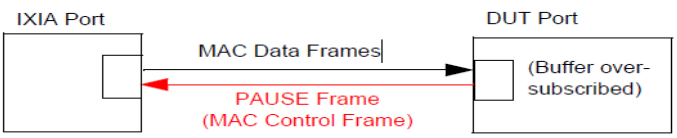
Pause Control is used to stop transmission of data frames for a certain length of time, as when a receiving port is becoming oversubscribed and cannot properly handle all of the incoming frames. This temporary delay prevents data frames from being lost. Pause control operates in full-duplex mode connections, and must be enabled on both ports on the link.

When the port transmitting the data frames receives a MAC PAUSE Control frame, it will stop sending data frames for the specified period of time. If frames were already in the process of being transmitted, their transmission will be completed, and then the PAUSE operation will begin.

NOTE IEEE specifications are followed for flow control when only auto negotiation is enabled.

A Pause Quanta unit is the time required for one bit to be transmitted (= one 'bit time') multiplied by 512. The Pause Delay is calculated based on the combination of the Pause Quanta counter value and the line rate of the port. Ixia ports act as the data transmit ports in this scenario. They are configured to listen for PAUSE frames from the DUT port which is receiving the data frames.

Figure:PAUSE Control—Example



The fields and controls in this dialog are described in *Table:Pause Control Dialog (shown for 10/100 module)*.

Table:Pause Control Dialog (shown for 10/100 module)

Category	Field/Control	Usage
MAC Addresses	Destination Address	(Read-Only except for 10GE modules) Set to the default Pause Control reserved multicast MAC address. When

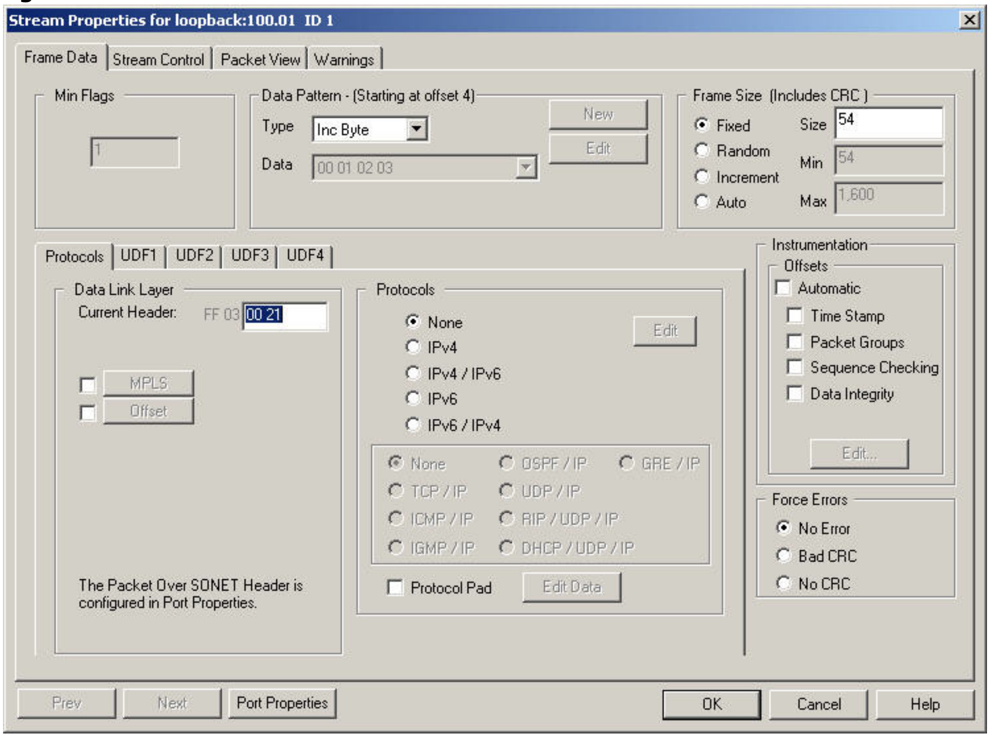
Category	Field/Control	Usage
		Pause Control is selected in the *Frame Data > Protocols > Protocols* box, this default address (0x01 80 C2 00 00 01) is entered automatically into the *MAC Destination Address* field in the DA/SA dialog. As long as Pause Control is enabled, the MAC address in the DA/SA dialog cannot be changed from this default address.
	Source Address	(Read-Only) This MAC address reflects the user-defined entry in the *MAC Source Address* field in the DA/SA dialog. It is the address of the MAC Control client sending the PAUSE frame to the directly connected port which is transmitting data frames.
Data Link Layer	Ethernet II	(Reflects the setting in the *Frame Data > Protocols > Data Link Layer* box, either Ethernet II or Ethernet SNAP protocol.)
	Ethernet SNAP	(Reflects the setting in the *Frame Data > Protocols > Data Link Layer* box, either Ethernet II or Ethernet SNAP protocol.)
Pause Quanta	Type	(Read-Only) The Length/Type for a MAC Control frame. The value is specified as '88-08' by IEEE 802.3.
	Opcode	(Read-Only) The MAC Control Opcode for the PAUSE control function. The value is specified as '00-01' by IEEE 802.3.
	Pause Quanta	The user-specified pause counter value, measured in Pause Quanta units. (1 Pause Quanta = 512 bit times.) The valid range is 0 to 65535 pause quanta.
	Pause Delay	(Read-Only) The pause delay time, measured in standard time units (for example, milliseconds), and based on the Pause Quanta counter value and the line speed of the port.

Frame Data for DCC

Packet flows, packet streams, and advanced streams for the optional SONET Data Communication Channel (DCC) feature on OC-192c POS modules are set up with special conditions for rate, frame size, and so on. The DCC frame data options are accessed by selecting one of the DCC options in the *Transmit Modes* tab of the *Port Properties* dialog.Chapter 20,*Port Properties–10 GE and UNIPHY Families* for more information.

The *Frame Data* tab for setting up DCC Packet Flows is shown in *Figure:Frame Data for DCC Packet Flows.*

Figure:Frame Data for DCC Packet Flows



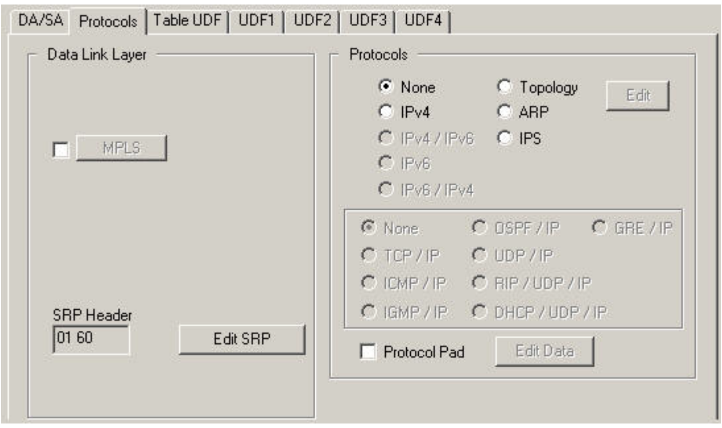
As shown in the figure, no timestamps can be added to the packets for DCC Packet Flows. However, for DCC Packet Streams the timestamp option is available. The valid range of frame sizes for DCC is 40 to 64K (65,535) bytes. Frame Data for SONET/POS Modules for information on the rest of the options in this dialog. Note that the *Protocols* > *Data Link Layer* > *MPLS* check box is not available for DCC Packet Flows, but it is available for DCC Packet Streams and DCC Advanced streams. It allows to insert MPLS labels after the POS header.

Frame Data for SRP

When the SRP feature is used on the OC-192c POS module, the usual POS header (PPP, and so on) is replaced by the SRP header, resulting in changed frame sizes. In addition, a special SRP CRC is calculated for each frame, in which the SRP header is excluded from the CRC calculation. The SRP frame data options are accessed by selecting the *SRP* option in the *SONET* tab of the *Port Properties* dialog. See, *Port Properties–10 GE and UNIPHY Families* for more information.

When Spatial Reuse Protocol (SRP) is enabled on an OC-192c POS module, the *Frame Data* tab Protocol section is modified, as shown in *Figure:Frame Data Protocols for SRP*. This dialog provides access to additional dialogs where headers for an SRP packet can be configured.

Figure:Frame Data Protocols for SRP



The fields and controls in the Protocols section are described in *Table:Frame Data Protocols for SRP*.

Table:Frame Data Protocols for SRP

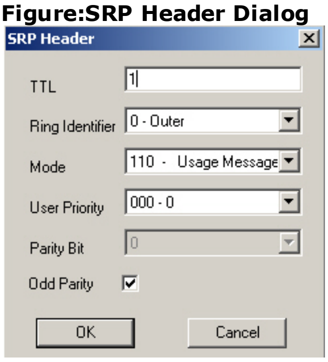
Section	Field/Control	Description
Data Link Layer	MPLS	Check this box to enable the use of MPLS labels in the header in SRP data frames. (Not available for use with SRP control frames: Topology, IPS, and SRP ARP.)
		Opens the *Edit MPLS* dialog. See the section on the *Edit MPLS for additional information.*
	SRP Header	(Read-only) Displays the two bytes of the generic SRP Header.
	Edit SRP button	Opens the *SRP Header* dialog. See the section on *SRP Header Dialog* for additional information.
Protocols (Choose one)	None	No Layer 3 protocol is selected.
	IPv4	Internet Protocol Version 4 is used. See the section on *Protocols—Network Layer for additional information.*
	Topology	When this protocol is selected and the *Edit* button is clicked, the *Topology Discovery Header* dialog will open. See the section on *SRP Topology Discovery Dialog* for additional information.
	ARP	Layer 2, Address Resolution Protocol (ARP) is used. See the section on *ARP Header Dialog for additional information.*
	IPS	Intelligent Protection Switching (IPS) is used.

Section	Field/Control	Description
		When this protocol is selected and the *Edit* button is clicked, the *IPS Header* dialog will open. See the section on *SRP Protection Switching (IPS) Dialog* for additional information.
	Edit	This button is active for all of the available protocols (not active for the *None* option). When the *Edit* button is clicked, a corresponding dialog will open to allow header configuration.
Sub-Protocols		*Table:Protocol Choices* for information on the Sub-Protocols.

SRP Header Dialog

This dialog is accessed by selecting the *Edit SRP* button in the *Protocols* section of the *Frame Data* tab. The headers for Spatial Reuse Protocol (SRP) frames can be configured using the *SRP Header* dialog, as shown in *Figure:SRP Header Dialog*.

Figure:SRP Header Dialog



NOTE (SRP Usage Frame headers are set in the *SRP Usage* dialog in Port Properties.) The fields and controls in this dialog are used to set the headers for SRP Discovery, IPS, and data frames, and are described in *Table:SRP Generic Header Dialog*.

Table:SRP Generic Header Dialog

Field/Control	Description
TTL	The 8-bit Time-To-Live field specifies the node hop count. The maximum number of nodes is 128 (rather than 256, the maximum value for this 8-bit field). The range of values is 0 to 255. An originating SRP node must set the TTL to at least twice the number of nodes in the ring, to allow for the possibility of a wrapped ring due to a failure condition.
Ring Identifier	Choose one of: • Outer (default) • Inner
Mode	The 3-bit field for the packet type. Choose one of: • 000 - Reserved • 001 - Reserved

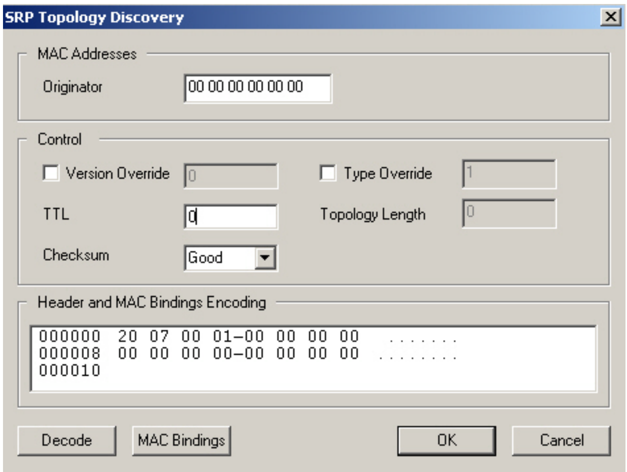
Field/Control	Description
	• 010 - Reserved • 011 - ATM cell • 100 - Control (pass): Control Message (Pass to host) used for SRP Discovery and SRP IPS frames • 101 - Control (local): Control Message (Locally buffered for host) • 110 - Usage Message: may be used when protocol is set to 'None' • 111 - Packet Data: used for IPv4 and ARP protocols NOTE When certain protocols are selected in the Frame Data - Protocols section, the type value in this field will be forced to the value which corresponds to the protocol. (for example, IPS protocol forces the value to 100 Control)
User Priority	The SRP User Priority (**not** IP TOS priority). Higher values have higher priorities. Choose one of: • 000 - 0 • 001 - 1 • 010 - 2 • 011 - 3 • 100 - 4 • 101 - 5 • 110 - 6 • 111 - 7
Parity Bit	(Read only) The Parity (P) bit field, used for data integrity over the preceding 15 bits of the SRP Usage frame header.
Odd Parity	If selected, odd parity will be used as a check on the SRP Usage frame header. The Parity bit will be forced to the value (1 or 0) that will be added to the value of the 15 preceding bits to create an odd value.

SRP Topology Discovery Dialog

Various types of control packets can be sent, including SRP Topology Discovery frames. The fields set in this dialog are used for an SRP Topology Discovery frame, and will follow the basic SRP standard. The Topology Discovery frame is used to build a topology map of each node. Each node sends out Discovery frames on both rings. Each node acts as the originator, in turn, by adding its MAC address to the MAC binding field and updating the topology length before passing the frame to the next node.

The controls in this dialog are accessed by first setting the port to use SRP (Chapter 19, Port Properties–POS and ATM Families for more information), selecting the Topology option in the *Protocols* sub-tab of the *Frame Data* tab, then selecting the *Edit* button. The *SRP Topology Discovery* dialog is shown in *Figure:SRP Topology Discovery Dialog*.

Figure:SRP Topology Discovery Dialog



The fields and controls in this dialog are described in *Table:SRP Topology Discovery Dialog*.

Table:SRP Topology Discovery Dialog

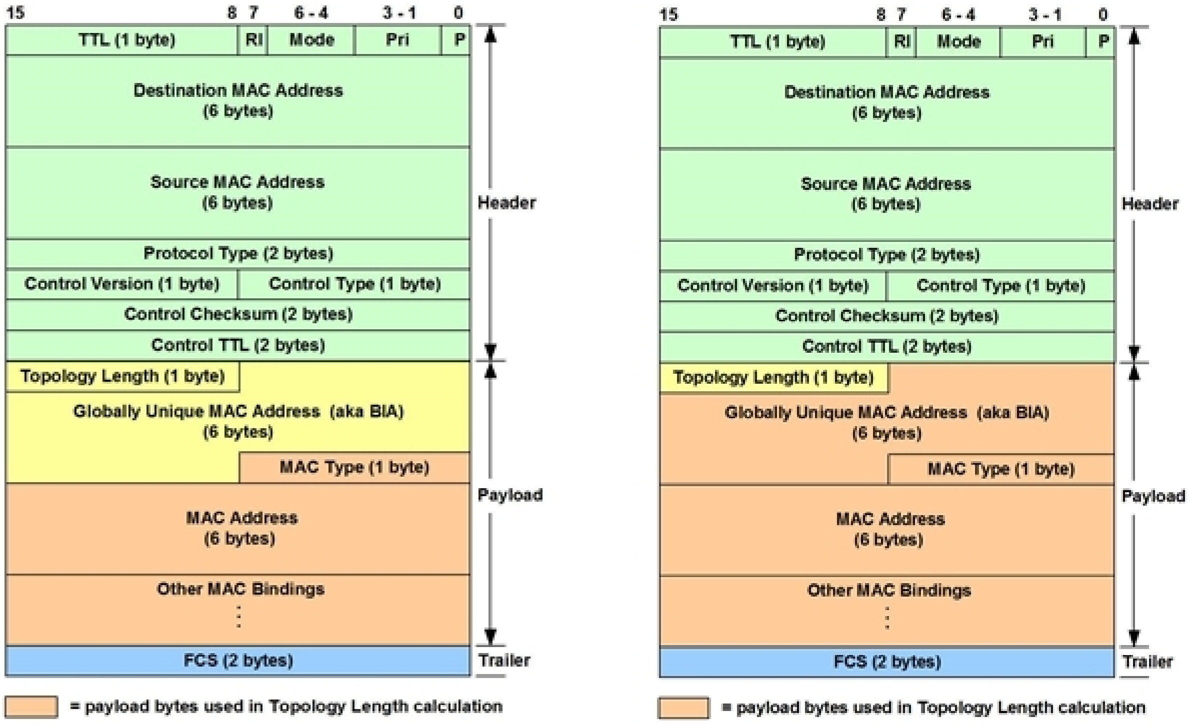
Section	Fields/Controls	Description
MAC Addresses	Originator	The 48-bit MAC address of the originating node.
Control (Defines the SRP 'Control Message' in the SRP Header)	Version Override (Control Version)	If selected, makes the corresponding field active, so a different version may be entered by you.
	TTL	Control Time-To-Live is the control layer node hop count. This value is decremented by each node that forwards the control frame.
	Checksum	32-bit CRC. Choose one of: • Bad • Good (default)
	Type Override (Control Type)	If selected, makes the corresponding field active, so a different Type value may be entered by you.
	Topology Length (Read Only)	(In bytes) This value is updated when MAC bindings are entered with 7 bytes added for each MAC binding. It is the calculated length value of the Topology frame payload. This value is found in the Length field of the Topology Discovery frame header. NOTE For Cisco SRP: If *Cisco SRP* is enabled in Port Properties, the length value calculation will include the 6 bytes for the originator MAC address. If *Cisco SRP* in NOT enabled in Port Prop-

Section	Fields/Controls	Description
		NOTE erties, the length value calculation will NOT include the 6 bytes for the originator MAC address. The SRP type used (Cisco SRP or non-Cisco SRP) for Topology frames must be the same for the transmitting port AND receiving port. If the type does not match, the frames will be decoded incorrectly upon receipt. See *SRP Topology Discovery Packet 'Length Calculations'* for diagrams showing how the Topology Length value is calculated for standard SRP and Cisco SRP. See *Frame Data for SRP* for additional information on Cisco SRP.
Header and MAC Bindings Encoding		This area contains the contents of the Topology Discovery Header and MAC Bindings. After changes have been made in the fields in this dialog, press the *Decode* button to apply the changes to the contents of this window area.
	Decode	Press this button to update the contents of the fields in the Encoding window area.
MAC Bindings		Press this button to edit the fields for the MAC bindings of the nodes on the SRP ring. See the section on the *MAC Bindings Dialog* for additional information.

SRP Topology Discovery Packet 'Length Calculations'

The topology Length in the SRP Topology Discovery packet header is calculated differently for 'Standard SRP' (per RFC 2892) and 'Cisco SRP' implementations, as shown in *Figure:Standard SRP and Cisco SRP 'Length Calculations'*. For Cisco SRP, the Topology Length is calculated over the Globally Unique originator MAC Address (BIA) plus the MAC bindings. For Standard SRP, only the MAC bindings are included.

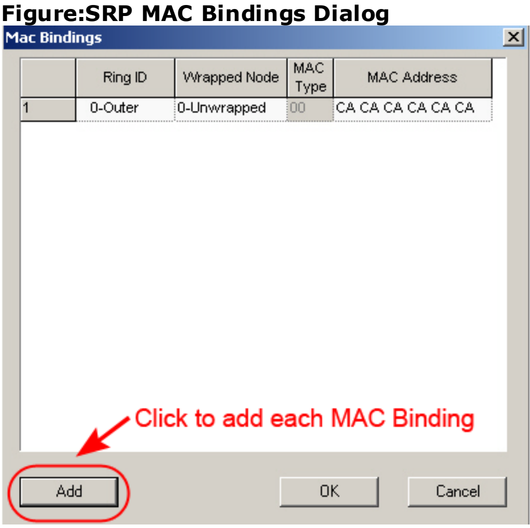
Figure:Standard SRP and Cisco SRP 'Length Calculations'



MAC Bindings Dialog

An SRP MAC Binding consists of a MAC address of a node, plus the associated MAC Type field for that address. To access this dialog, select the *MAC Binding* button from the *SRP Topology Discovery* dialog. The *MAC Binding* dialog is shown in *Figure:SRP MAC Bindings Dialog*.

Figure:SRP MAC Bindings Dialog



The fields and controls in this dialog are described in *Table:SRP MAC Bindings Dialog*.

Table:SRP MAC Bindings Dialog

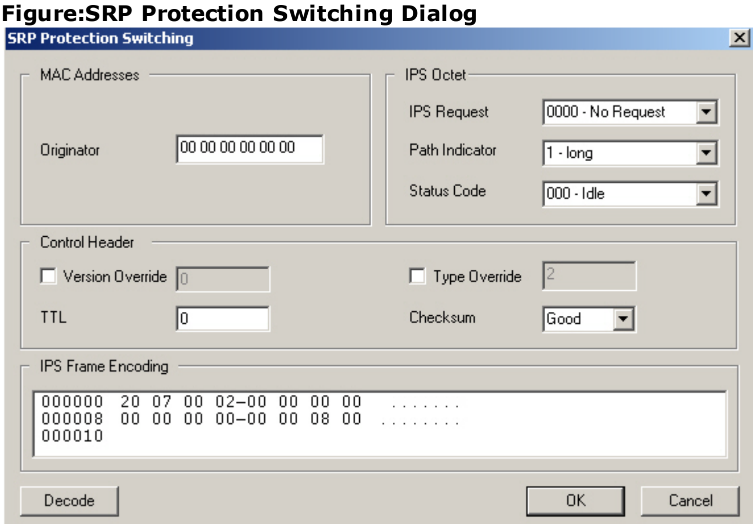
Field/Control	Description
Ring ID	The Ring Identifier. Choose one of: • 0 - Outer (default)

Field/Control	Description
	• 1 - Inner
Attached Node	The type of ring that the attached node is on. Choose one of: • 0 - Wrapped (Node) on an SRP ring where wrapping has been established for failure protection. • 1 - Unwrapped (Node) on a normal SRP dual ring configuration.
MAC Type	(Read-only) The hex value of the 8-bit MAC Type field associated with this particular MAC address. The value reflects the user-defined settings for the Ring ID bit and the Wrapped/Unwrapped bit in this table entry.
MAC Address	The 48-bit MAC SA of the node
Add	Press this button to add one entry to the list of MAC Bindings. Repeat for additional entries.

SRP Protection Switching (IPS) Dialog

The *SRP Protection Switching* dialog is shown in *Figure:SRP Protection Switching Dialog*. This dialog is reached by selecting the *IPS* option in the *Protocols* sub-tab of the *Frame Data* tab, and selecting the *Edit* button. This dialog allows to specify the header for an SRP IPS frame.

Figure:SRP Protection Switching Dialog



The fields and controls in this dialog are described in *Table:SRP Protection Switching Dialog*.

Table:SRP Protection Switching Dialog

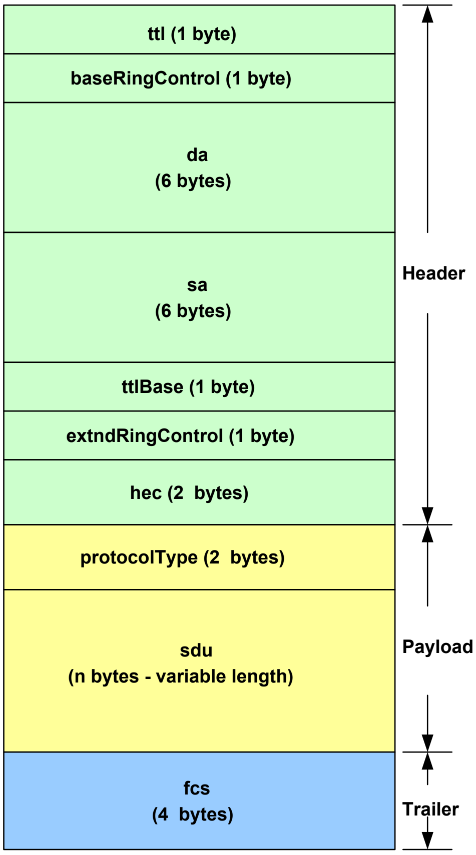
Section	Field/Control	Description
MAC Addresses	Originator	The 48-bit MAC address of the originating node.
IPS Octet	IPS Request	The IPS Request Type. Choose one of: • 0000 - No Request (IDLE) (default) • 0001 through 0100 - Invalid

Section	Field/Control	Description
		• 0101 - Wait to Restore (WTR) • 0110 - Manual Switch (MS) • 0111 - Invalid • 1000 - Signal Degrade (SD) • 1001 through 1010 - Invalid • 1011 - Signal Fail (SF) • 1100 - Invalid • 1101 - Forced Switch (FS) • 1110 through 1111 - Invalid
	Path Indicator	Choose one of: • 0 - short • 1 - long (default)
	Status Code	Choose one of: • 000 - Idle (default) • 010 - Traffic Wrapped (Protection Switch Completed) NOTE Values 001 through 111 are Invalid
Control Header	Version Override	If selected, makes the corresponding field active, so a different version may be entered by you.
	TTL	Control Time-To-Live is the control layer node hop count. This value is decremented by each node that forwards the control frame.
	Type Override	If selected, makes the corresponding field active, so a different type value may be entered by you.
	Checksum	Control checksum. Choose one of: • Bad • Good (default)
IPS Frame Encoding		This window area contains the contents of the IPS Frame. After changes have been made in the header fields in this dialog, press the *Decode* button to apply the changes to the contents of this area.
	Decode	Press this button to update the contents of the fields in the Encoding window area.

Frame Data for RPR

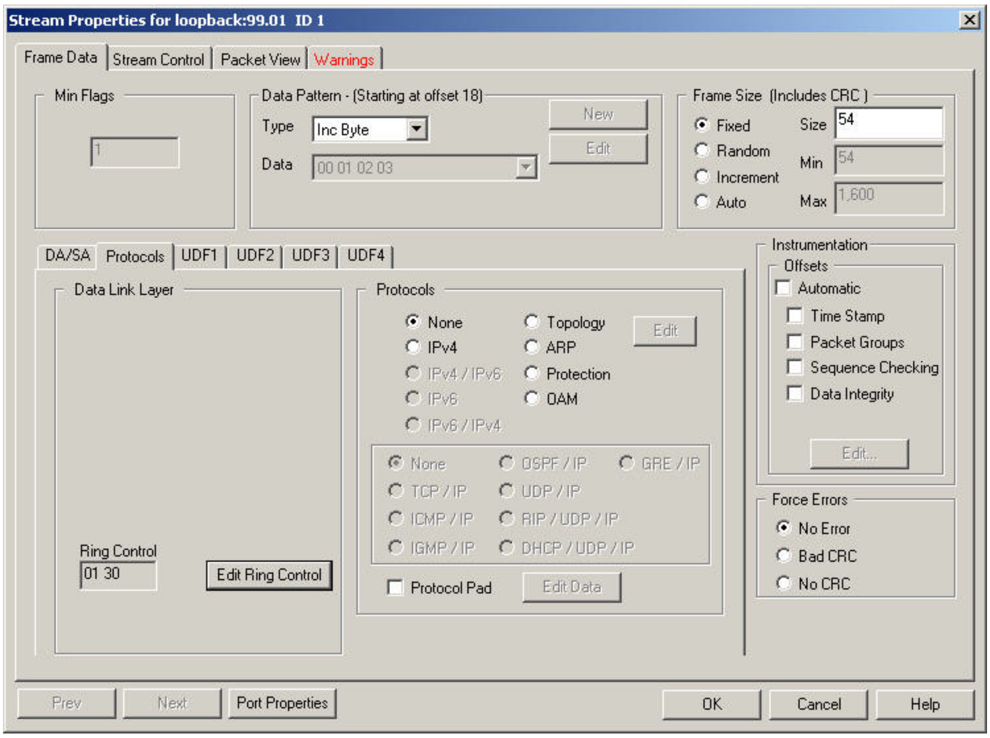
Ixia's optional Resilient Packet Ring (RPR) feature is implemented on the OC-48c and OC-192c POS modules, per IEEE P802.17/D2.1. A diagram of the format for an RPR data frame, based on that specification, is shown in *Figure:RPR Data Frame Format*.

Figure:RPR Data Frame Format



The Frame Data controls for RPR are displayed when the RPR option is selected in the *SONET* tab of the *Port Properties* dialog (See *Port Properties–POS and ATM Families* for more information). The *Frame Data* tab for use with RPR is shown in *Figure:RPR Frame Data Tab*.

Figure:RPR Frame Data Tab



The section of special interest to RPR in this dialog is 'Protocols.' The fields and controls in this section are described in *Table:RPR Frame Data—Protocols*.

Table:RPR Frame Data—Protocols

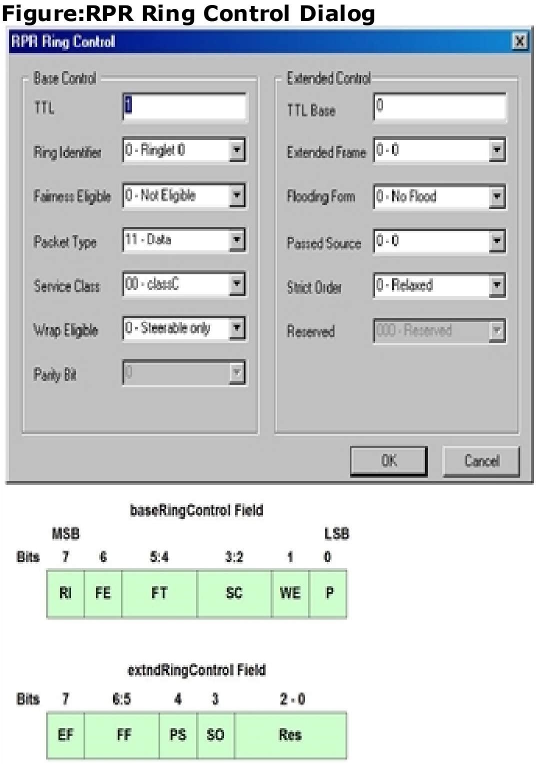
Section	Type	Description
Data Link Layer	Current Header	(Read-only) The current Data Link Layer header format, as selected in the Port Properties/SONET page. The hexadecimal format for the specific header is displayed in the field. This field cannot be directly edited unless the SONET header selection in Port Properties is set to *Other*.
	Ring Control	(Read-only) The value of the Ring Control header. The value displayed here is dependent on the settings in *Edit Ring Control* dialog. See *RPR Ring Control Dialog* for additional information. For standard use, when Resilient Packet Ring (RPR) is selected for the SONET frame header format, no header type is displayed here, but the first two octets configured for the header in the SONET page are displayed here (for Address and Control). The RPR header is available for use with IPv4 only (not IPv6). NOTE: FOR OPTIONAL RPR FEATURE: See *Port Properties for RPR* for information on the RPR feature for OC-48c and OC-192c POS modules. When the optional RPR feature is being used,

Section	Type	Description
		NOTE the RPR Header values are displayed in the Data Link Layer section (read-only), and an *Edit Ring Control* button is available.
	Edit Ring Control	Press this button to display the *Ring Control RPR Header* dialog. See *RPR Ring Control Dialog* for additional information. See *Port Properties for RPR* for information on the optional RPR feature on OC-48c and OC-192c POS modules. This button is available **ONLY** for use with the optional RPR feature on an Ixia OC-48c and OC-192c POS modules.
Protocols		For selection of a network layer protocol to be included in the frame header.
	None	If this option is selected, no network layer protocol is desired.
	IPv4	If this option is selected and the *Edit* button is clicked, IPv4 headers can be created for RPR data packets. When IPv4 is selected, the higher-level protocols, listed below in the dialog, are made available for header configuration. See *Configuring IPv4 Headers* for additional information.
	Topology	If this option is selected, and the *Edit* button is clicked, the *RPR Topology* dialog will be displayed. This dialog allows to configure headers for RPR Topology messages. See *RPR Topology Discovery* for additional information.
	ARP	If this option is selected, and the *Edit* button is clicked, the ARP dialog will be displayed. *ARP Header Dialog* for additional information.
	Protection	If this option is selected, and the *Edit* button is clicked, the *RPR Protection* dialog will be displayed. This dialog allows to configure headers for RPR Protection messages. See *RPR Protection Switching Dialog* for additional information.
	OAM	If this option is selected, and the *Edit* button is clicked, the *RPR OAM Control* dialog will be displayed. See *RPR OAM Dialog* for additional information.

RPR Ring Control Dialog

The *RPR Ring Control* dialog appears when the *Edit Ring Control* button is clicked in the Protocols section of the *Frame Data* tab. An RPR frame header contains a 1-byte baseRingControl field and a 1-byte extndRingControl field. This dialog allows to configure the contents and usage of both of those fields. The *RPR Ring Control* dialog is shown in *Figure:RPR Ring Control Dialog*.

Figure:RPR Ring Control Dialog



The fields and controls in this dialog are described in *Table:RPR Ring Control Dialog*.

Table:RPR Ring Control Dialog

Section	Field/Control	Description
Base Control	TTL	The first octet in an RPR frame header is the Time to Live hop count. The user indicates the maximum number of hops to the destination, to prevent an endless loop around the ring. In a Fairness Control Message, the originator sets the TTL to 255. When a single-choke FCM changes the SA to the local SA, it will also reset the TTL to 255.
	Ring Identifier (bit 7–RI)	The Ringlet Identifier (RI). The ringlet where the RPR frame was first transmitted. Choose one of: • 0 - Ringlet 0 • 1 - Ringlet 1
	Fairness Eligible (bit 6–FE)	Indicates RPR fairness eligibility (FE) status. Choose one of: • 0 - Not Eligible for fairness algorithm • 1 - Eligible for fairness algorithm
	Packet Type (bits 5-4–FT)	Corresponds to the RPR frame type (FT) field. Choose one of:

Section	Field/Control	Description
		• 01 - Control frame (excludes fairness frame) • 11 - Data frame
	Service Class (bits 3-2–SC)	The service class (SC) of the frame. Choose one of: • 00 - classC • 01- classB • 10 - classA1 • 11 - classA0
	Wrap Eligible (bit 1–WE)	To specify that the frame may be wrapped/wrap eligible (WE), as necessary. If it is not eligible for wrapping, it may be 'steered.' Choose one of: • 0 - Steerable (only) • 1 - Wrap Eligible
	Parity Bit (bit 0–P)	(1 bit - P field) (Read-only) Used for parity check of the ring control header, since there is no 'HEC' field in an RPR Fairness Frame.
Extended Ring Control	TTLBase	This 8-bit field should be set to the original TTL of the data packet before RPR encapsulation. • For data frames: This field is to be the same value as the TTL field upon transmission of the frame. • For all other frame types: This field is reserved for future use.
	Extended Frame (bit 1 - EF)	This bit indicates that this data frame is sent from a MAC source that is not a node on this ring, to a MAC destination that is not a node on this ring. If set to 1, the entire MAC layer packet is expected after the *hec* field in the RPR packet, including the destination and source MAC addresses. Choose one of: • 0 - 0 (default): frame not sent from a remote MAC source. • 1 - 1: indicates a frame with a remote MAC source address in the extended header.
	Flooding Form (bits 2-3 - FF)	This 2-bit field indicates whether the packet should be flooded, and the scope of the flooding. Choose one of: • 0 - No flood (default): no flooding. • 1 - Unidirectional Flooding: flood on in the ringlet specified in the ringIdentifier. • 2 - Bidirectional Flooding: flood on both ringlets.

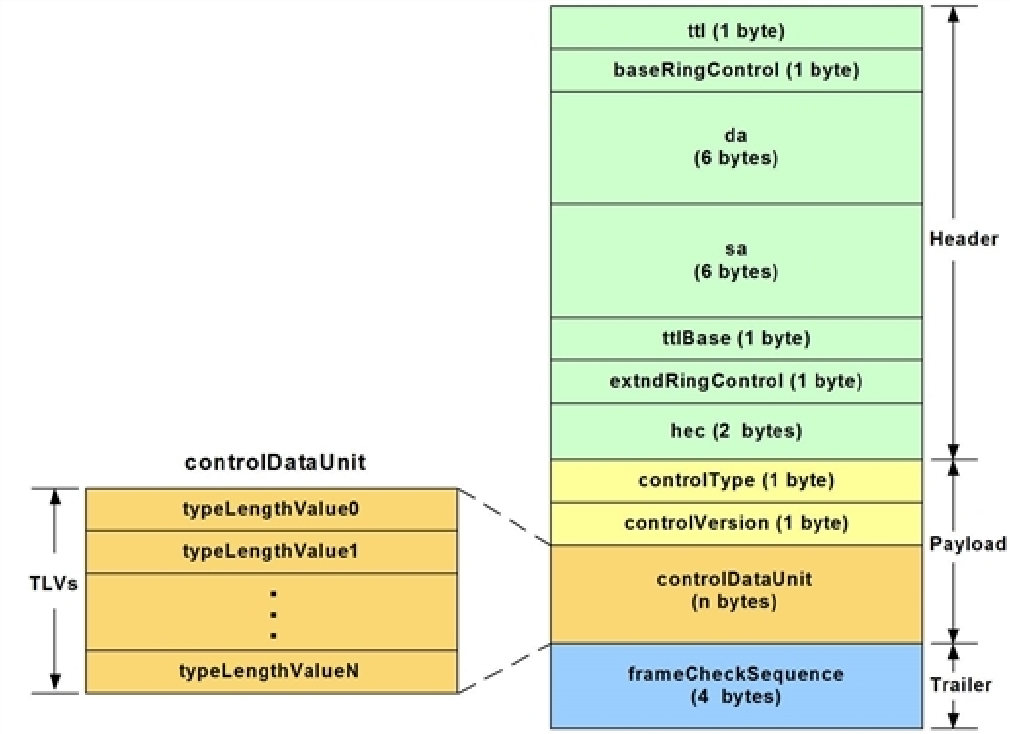
Section	Field/Control	Description
		• Reserved
	Passed Source (bit 4 - PS)	This 1-bit field is used by wrapping systems to prevent mis-order and duplication. It is normally set to 0 when a frame is first transmitted by a station and set to 1 when a wrapped frame passes the source station again. Choose one of: • 0 - 0 (default) • 1 - 1: wrapped frame passed the source station again.
	Strict Order (bit 5 - SO)	This 1-bit field indicates whether strict ordering or relaxed ordering requirements should be observed. Choose one of: • 0 - Relaxed (default) • 1 - Strict
	Reserved (bits 6-8 - res)	This 3-bit field is reserved for future use. It is: • Set to all 0s for transmission. • Ignored upon receipt.

RPR Topology Discovery

RPR Topology Discovery is handled with two types of messages, that are shown in *Figure:RPR Topology TLV Message Format*:

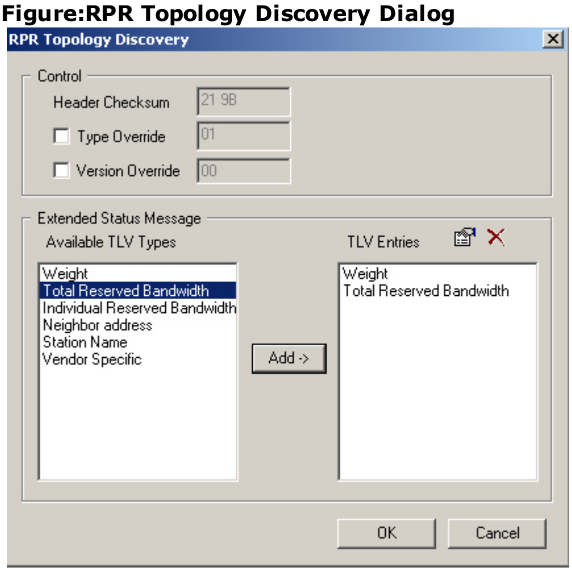
- **RPR Protection Message**—used for the discovery of the physical topology, due to its fast rate (sub-50 ms) and the fact that it is sent on triggers.
- **RPR Topology TLV Messages**—for the transmission of additional information from a source node/station about bandwidth and other configuration issues. The two types of TLV Messages are: Station TLV messages and Vendor-Specific TLV Messages.

Figure:RPR Topology TLV Message Format



The *RPR Topology Discovery* dialog is accessed by selecting *Topology* in the *Protocols* sub-tab of the *Frame Data* tab, and then selecting the *Edit* button. The *RPR Topology Discovery* dialog is shown in *Figure:RPR Ring Control Dialog*.

Figure:RPR Topology Discovery Dialog



The fields and controls in this dialog are described in *Table:RPR Topology Discovery Dialog*.

Table:RPR Topology Discovery Dialog

Section	Field/Control	Description
Control	Header Check-sum	(Read-only) The 16-bit header error (**hec**) calculated over the control header CRC16 checksum.

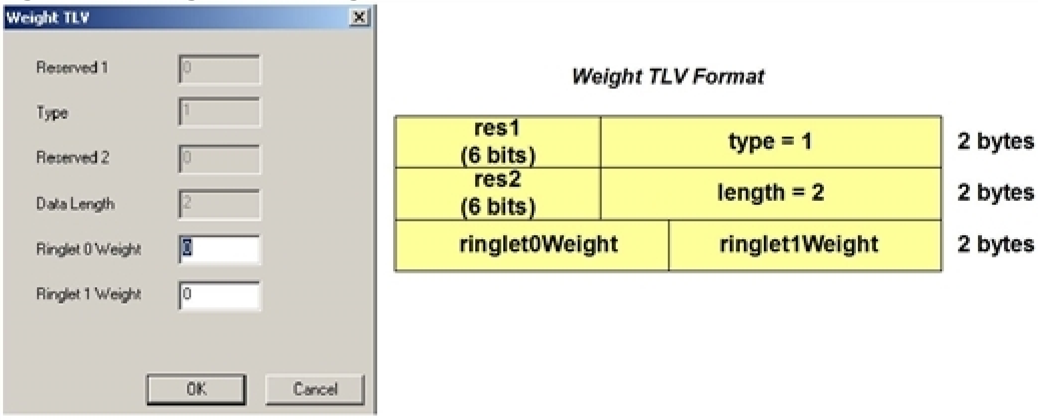
Section	Field/Control	Description
	Type Override	(Control type - override) If this option is selected, the type may be changed in the field to the right. If cleared, the value field is read-only. The one-byte Control Frame type (hex) values are: • 01 - Topology Discovery • 02 - Protection Message • 03 - OAM Control Frame • ---(other values) - Reserved
	Version Override	The one-byte Version number related to the control type. Currently, control types are version 0. If this option is selected, the version number may be changed in the field to the right. If not selected, the value field is read-only.
Extended Status Message	Available TLV Types	A list of TLV types that can be added to the header of an RPR Topology Extended status message packet. TLVs carry additional information about the sending node, and can be added in any order. The Station TLVs are: • Weight— *RPR Weight TLV Dialog*. • Total Reserved Bandwidth— *RPR Total Reserved Bandwidth TLV Dialog*. • Individual Reserved Bandwidth— *RPR Individual Reserved Bandwidth TLV Dialog*. • Neighbor address— *RPR Neighbor Address TLV Dialog*. • Station Name— *RPR Station Name TLV Dialog*. • The Vendor Specific TLV is: • Vendor Specific— *RPR Vendor Specific TLV Dialog*.
		Select (highlight) an available TLV Type in the list at the right. Then press the *Add* button to move it to the list of TLV Entries on the right. Some types of TLVs may be repeated in the list.
	TLV Entries	A user-defined list of the TLVs to be added to the header of the RPR Topology Discovery message packet currently being configured. Some types of TLVs may be repeated in the list. The TLVs in the list may be custom-configured by clicking the *Edit* button above the list.
		Edit TLV Header Click to display the *Edit* dialog corresponding to selec-

Section	Field/Control	Description
		ted (highlighted) TLV Entry in the list below.
		Remove TLV Header Click to delete a selected (highlighted) entry in the list of TLV Entries.

RPR Weight TLV Dialog

This dialog is accessed by highlighting the *Weight* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon (). Alternatively, double-click the *Weight* TLV entry. The RPR *Weight TLV* dialog is shown in *Figure:RPR Weight TLV Dialog*.

Figure:RPR Weight TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Weight TLV Dialog*.

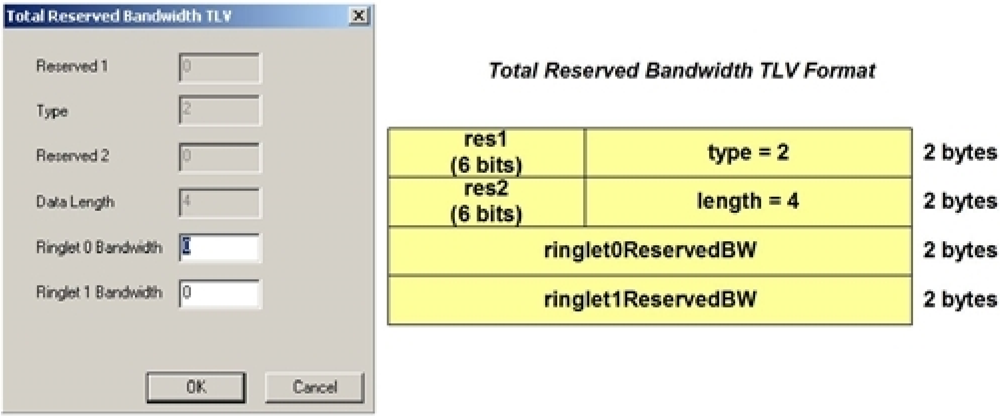
Table:RPR Weight TLV Dialog

Field/Control	Description
Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Type	(Read-only) 10 bits. The type value is 1.
Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Data Length	(Read-only) 10 bits. The combined length of the data fields = 2 bytes.
Ringlet 0 Weight	The weight value of the Ringlet 0 node.
Ringlet 1 Weight	The weight value of the Ringlet 1 node.

RPR Total Reserved Bandwidth TLV Dialog

This dialog is accessed by highlighting the *Total Reserved Bandwidth* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon (). Alternatively, double-click the *Total Reserved Bandwidth* TLV entry. The RPR *Total Reserved Bandwidth TLV* dialog is shown in *Figure:RPR Total Reserved Bandwidth TLV Dialog*.

Figure:RPR Total Reserved Bandwidth TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Total Reserved Bandwidth TLV Dialog*.

Table:RPR Total Reserved Bandwidth TLV Dialog

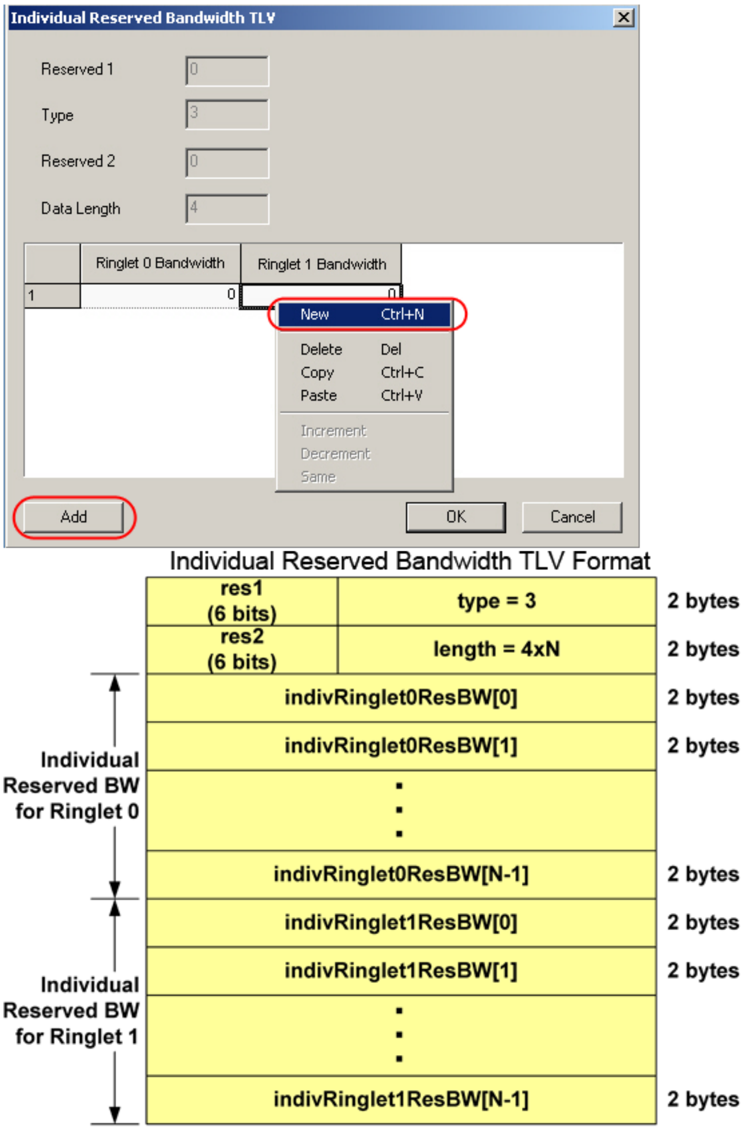
Field/Control	Description
Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Type	(Read-only) 10 bits. The type value is 2.
Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Data Length	(Read-only) 10 bits. The combined length of the data fields = 4 bytes.
Ringlet 0 Bandwidth	The total reserved subclassA0 bandwidth value of the Ringlet 0 node.
Ringlet 1 Bandwidth	The total reserved subclassA0 bandwidth value of the Ringlet 1 node.

RPR Individual Reserved Bandwidth TLV Dialog

The RPR *Individual Reserved Bandwidth TLV* dialog is used to set up the content of an RPR Individual Bandwidth TLV for use in an RPR Topology message. The data in this TLV is constructed by adding bandwidth pairs. Each bandwidth pair corresponds to the reserved bandwidth between this node and a node a number of hops away from this node. The first item in the pair represents the reserved bandwidth on Ringlet 0, and the second represents the reserved bandwidth on Ringlet 1. Bandwidth pairs must be added in order; that is, for the node one hop away, followed by the node two hops away, and so forth.

This dialog is accessed by highlighting the *Individual Reserved Bandwidth* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon (). Alternatively, double-click the *Individual Reserved Bandwidth* TLV entry. This dialog is shown in *Figure:RPR Individual Reserved Bandwidth TLV Dialog.*

Figure:RPR Individual Reserved Bandwidth TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Individual Reserved Bandwidth TLV Dialog*.

Table:RPR Individual Reserved Bandwidth TLV Dialog

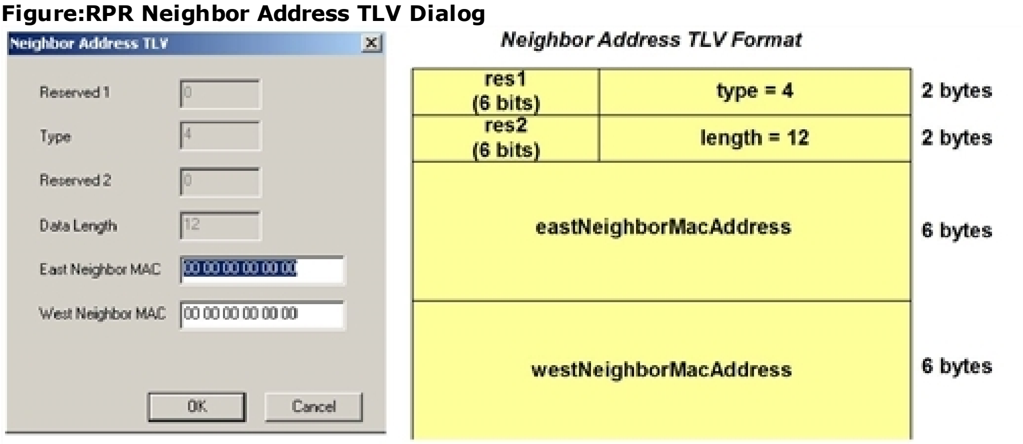
Section	Field/Control	Description
(Header)	Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
	Type	(Read-only) 10 bits. The type value is 3.
	Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
	Data Length	(Read-only) 10 bits. The combined length of the data fields = 4 x N bytes (4 times the number/N of hops). Each hop on the link is described by a 2-byte bandwidth field for each of the two ringlets = total of 4 bytes.

Section	Field/Control	Description
Window		Allows to create entries where the bandwidth can be reserved separately—for each one-hop link on the ring-let.
	Ringlet 0 Band-width	The reserved subclassA0 bandwidth reserved for a one-hop link on the Ringlet 0 node.
	Ringlet 1 Band-width	The reserved subclassA0 bandwidth reserved for a one-hop link on the Ringlet 1node.

RPR Neighbor Address TLV Dialog

This dialog is accessed by highlighting the *Neighbor Address* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon (). Alternatively, double-click the *Neighbor Address* TLV entry. The RPR *Neighbor Address TLV* dialog is shown in *Figure:RPR Neighbor Address TLV Dialog*.

Figure:RPR Neighbor Address TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Neighbor Address TLV Dia-log*.

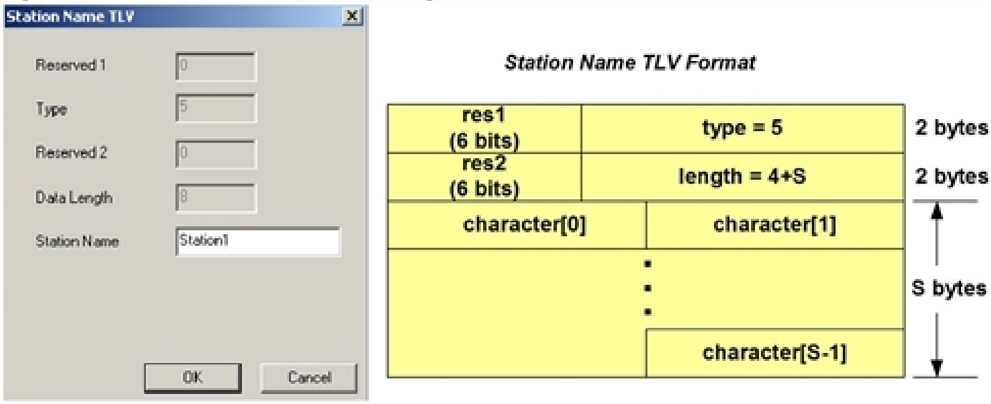
Table:RPR Neighbor Address TLV Dialog

Field/Control	Description
Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Type	(Read-only) 10 bits. The type value is 4.
Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Data Length	(Read-only) 10 bits. The combined length of the data fields = 12 bytes.
East Neighbor MAC	(6 bytes) The MAC address of the neighbor station connected to this station’s east interface. Set to all zeros when the MAC address is unknown.
West Neighbor MAC	(6 bytes) The MAC address of the neighbor station connected to this station’s west interface. Set to all zeros when the MAC address is unknown.

RPR Station Name TLV Dialog

This dialog is accessed by highlighting the *Station Name* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon ( ). Alternatively, double-click the *Station Name* TLV entry. The RPR *Station Name TLV* dialog is shown in *Figure:RPR Station Name TLV Dialog*.

Figure:RPR Station Name TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Station Name TLV Dialog*.

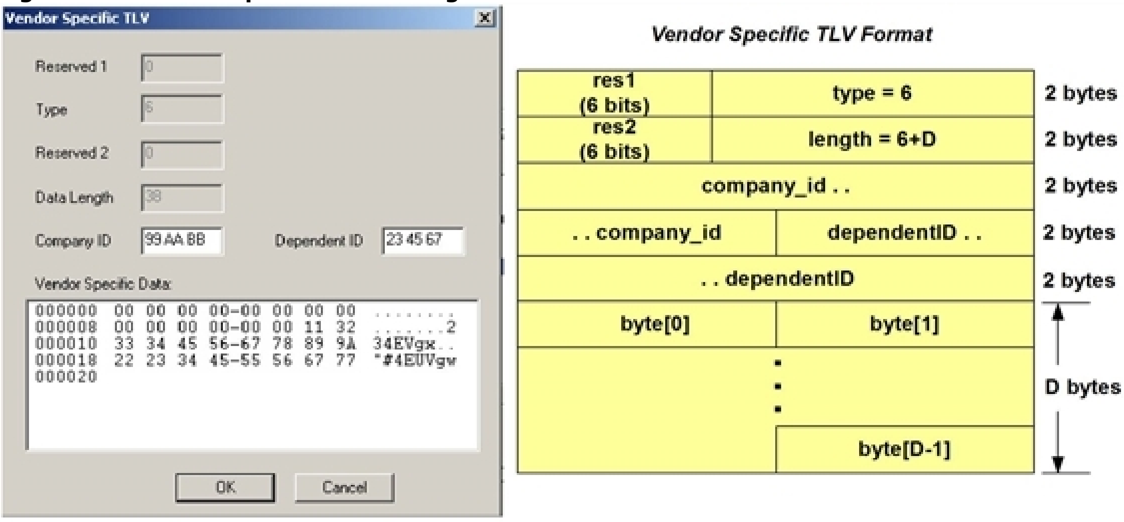
Table:RPR Station Name TLV Dialog

Field/Control	Description
Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Type	(Read-only) 10 bits. The type value is 5.
Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Data Length	(Read-only) 10 bits. The number of ASCII characters (S) in the station name, plus 4 bytes for the TLV header.
Station Name	The optional, user-defined name for this station, exclicked as a string of ASCII characters. The number of characters in the station name = 'S.'

RPR Vendor Specific TLV Dialog

This dialog is accessed by highlighting the *Vendor Specific* TLV entry from the list on the right, then selecting the *Edit TLV Header* icon ( ). Alternatively, double-click the *Vendor Specific* TLV entry. The RPR *Vendor Specific TLV* dialog is shown in *Figure:RPR Vendor Specific TLV Dialog*.

Figure:RPR Vendor Specific TLV Dialog



The fields and controls in this dialog are described in *Table:RPR Vendor Specific TLV Dialog*.

Table:RPR Vendor Specific TLV Dialog

Field/Control	Description
Reserved 1	(Read-only) The 6-bit Reserved1 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Type	(Read-only) 10 bits. The type value is 6.
Reserved 2	(Read-only) The 6-bit Reserved2 field is reserved for future use. It is set to 0, and is to be ignored by the receiving nodes.
Data Length	(Read-only) 10 bits. The Data Length value = 6 + D (bytes). It is the combined length of: • 6 bytes for the Company ID plus Dependent ID, plus • D bytes of user-entered, vendor-specific data.
Company ID	A 3-byte value (hex). It is the 24-bit IEEE/RAC company identifier, which is the first part of the globally unique EUI-64 identifier.
Dependent ID	A 3-byte value (hex). It is the 24-bit identifier which is the second part of the globally unique EUI-64 identifier. This ID is supplied by the company, and is unique within the company.
Vendor Specific Data	This window allows to enter raw data relevant to the vendor. The number of bytes of data (D) is part of the overall Data Length for value. The display consists of 3 sections: • Left column—first byte number in each row (in hex), for example, 0000 • Middle column—8 bytes of data (hex) per row • Right column—display of the data for that row, displayed in ASCII, if the byte can be displayed as such; otherwise, the byte is displayed as a dot (.).

RPR Protection Switching Dialog

The *RPR Protection Switching* dialog appears when the *Protection* option button is selected in the Protocols section of the *Frame Data* tab, and the *Edit* button has been clicked.

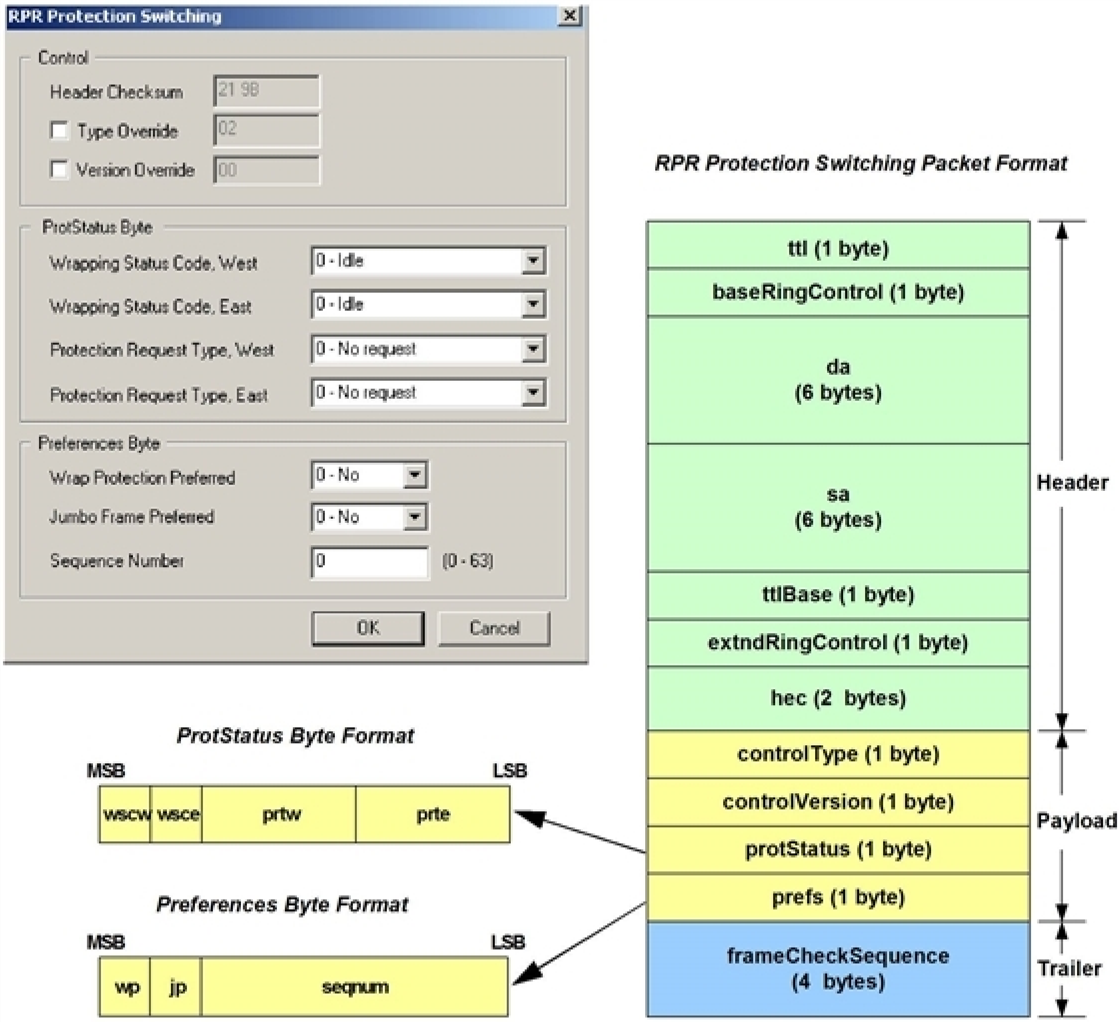
RPR operates over a dual-ring topology, with transmission from source station to destination station over a span of the ring. A single span or a single station can fail with a service interruption of only 50 milliseconds, if protection methods are employed, so that an alternate path can be used by the traffic.

Steering is supported by all stations. Steered traffic is discarded at the point of failure. To avoid continued discards, the source station redirects unicast traffic to the ringlet that retains connectivity to the destination. Multicast or broadcast traffic is normally directed to both ringlets, so as to reach all stations on the ring.

Wrapping is an optional capability that is only activated when all stations on the ring support this capability. Traffic is directed, at the point of failure, to the opposing ringlet. Wrapping is transparent to the source station and connectivity to all stations is retained.

The *RPR Protection Switch Packet* (message) dialog is shown in *Figure:RPR Protection Switching Dialog*.

Figure:RPR Protection Switching Dialog



The fields and controls in this dialog are described in *Table:RPR Protection Switching Dialog*.

Table:RPR Protection Switching Dialog

Section	Field/Control	Description
Control	Header Checksum	(Read-only) The 16-bit header error (hec) calculated over the control header—CRC16 checksum.
	Type Override	(Control type—override) If this option is selected, the type may be changed in the field to the right. If not selected, the value field is read-only. The one-byte Control Frame type (hex) values are: • 01 - Topology Discovery • 02 - Protection Message • 03 - OAM Control Frame • ---(other values) - Reserved
	Version Override	If this option is selected, the version number may be changed in the field to the right. If not selected, the value field is read-only. The one-byte Version number related to the control type. Currently control types are version 0.
ProtStatus Byte	Wrapping Status Code, West	The wrapping status for the traffic received on the west interface of this node/station. Choose one of: • 0 - Idle—Wrapping is not enabled. (This setting is used in steering rings.) • 1 - Wrapped—Traffic is wrapped on the ring (the Protection Switch has been completed). for traffic received on the east interface.
	Wrapping Status Code, East	The wrapping status for the traffic received on the east interface of this node/station. Choose one of: • 0 - Idle—Wrapping is not enabled. (This setting is used in steering rings.) • 1 - Wrapped—Traffic is wrapped on the ring (the Protection Switch has been completed) for traffic received on the west interface.
	Protection Request Type, West	(Binary values) The RPR Protection message type to report the protection state on the West receive interface of the node/station. Choose one of:

Section	Field/Control	Description
		• 0 - No request • 1 - Wait to restore • 2 - Manual switch—User specified command; indicated link should not be used (coerced) • 3 - Signal degrade—minor signal degrad-tioncondition. Link should not be used (coerced) • 4 - Signal fail—major signal degradation con-dition. Link cannot be used (forced) • 5 - Forced switch—User specified command; indicated link may not be used • 6 - Reserved • 7 - Reserved
	Protection Request Type, East	(Binary values) The RPR Protection message type to report the protection state on the East receive inter-face of the node/station. Choose one of: • 0 - No request • 1 - Wait to restore • 2 - Manual switch—User specified command; indicated link should not be used (coerced) • 3 - Signal degrade—minor signal degrad-tioncondition. Link should not be used (coerced) • 4 - Signal fail—major signal degradation con-dition. Link cannot be used (forced) • 5 - Forced switch—User specified command; indicated link may not be used • 6 - Reserved • 7 - Reserved
Preferences Byte	Wrap Protection Preferred	Indicates a station’s ability and/or preference to sup-port wrapping protection. Choose one of: • 0 - No—used by stations that cannot support wrap protection, and by stations that can support wrap protection but prefers not to do so. • 1 - Yes—used by a station which can support wrap protection and prefers to do so.
	Jumbo Frame Pre-ferred	Indicates a station’s ability and/or preference to sup-port jumbo frames. Choose one of: • 0 - No—used by stations that cannot support jumbo frames, and by stations that can support jumbo frames but prefer not to receive them.

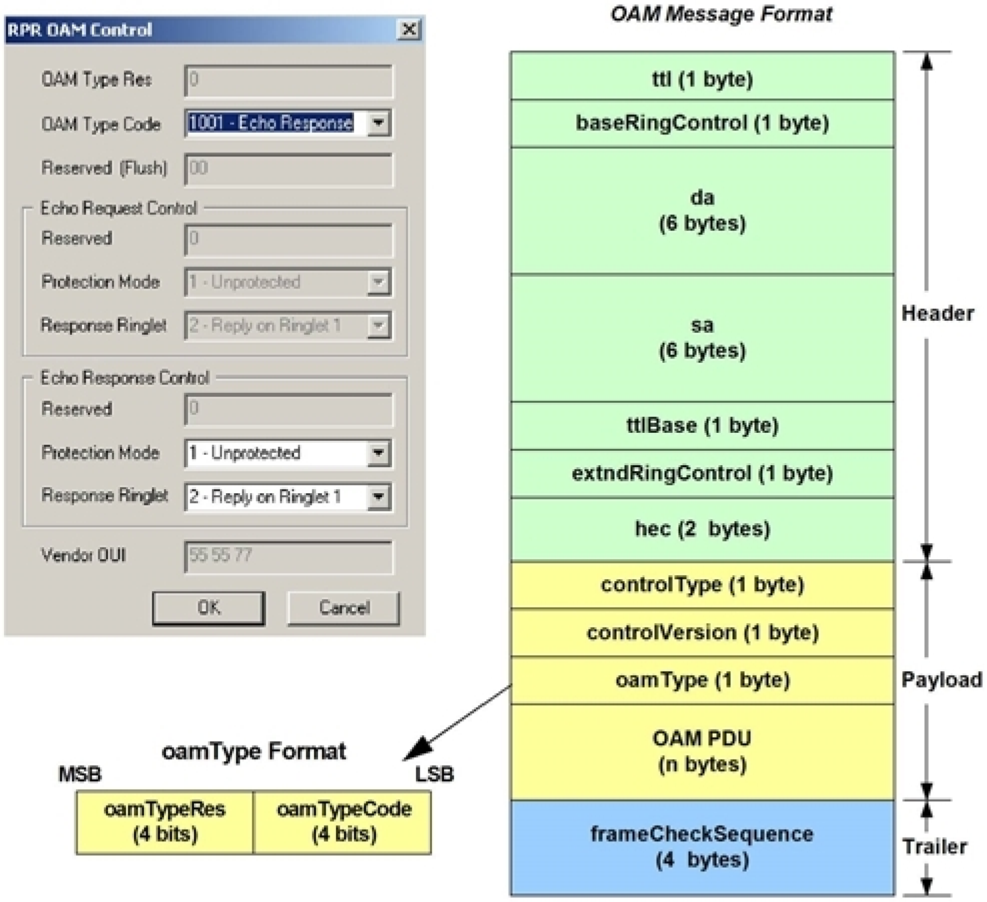
Section	Field/Control	Description
		• 1 - Yes—used by a station which can support jumbo frames and prefers to receive them.
	Sequence Number	(8 bits) Valid range is 0 to 63. This field indicates the sequence number used with all copies of a particular protection control message. The value is incremented only if the contents of the message packet change. It ensures that protection control messages will be processed in the correct order.

RPR OAM Dialog

The *RPR OAM Control* dialog (Operations, Administration, and Maintenance) is shown in *Figure:RPR OAM Dialog*. This dialog allows to configure the contents of the OAM Control Message, per the IEEE 802.17 Draft 2.1 specification. These messages/frames are sent between stations to determine the operational status of the connection. There are three types of messages: Echo Request and Response frames for determining connectivity; Flush frames to prevent misordering of frames; and Vendor Specific frames for carrying a vendor’s OAM information. All three types of frames can be configured in this dialog.

This dialog is accessed by selecting the OAM option in the *Protocols* sub-tab of the *Frame Data* tab. Note that the port must be set to use RPR as described in Chapter 19,*Port Properties–POS and ATM Families*.

Figure:RPR OAM Dialog



The fields and controls in this dialog are described in *Table:RPR OAM Dialog*.

Table:RPR OAM Dialog

Section	Field/Control	Description
	OAM Type Res	(Read-only) Reserved for future use.
	OAM Type Code	The OAM Type Code. This setting determines which of the fields in this dialog are active. Choose one of: • 0000 - Reserved • 0001 - Flush • 0010 through 0111 - Reserved • 1000 - Echo Request • 1001 - Echo Response • 1010 though 1110 - Reserved • 1111 - Vendor Specific
	Reserved (Flush)	This field is active only when OAM Type Code = 0001 - Flush
Echo Request Control		These fields are active only when OAM Type Code = 1000 - Echo Request. It indicates that an Echo Request OAM frame will be sent.

Section	Field/Control	Description
	Reserved	(Read-only) Reserved for future use.
	Protection Mode	Choose one of: • 0 - Protected • 1 - Unprotected
	Response Ringlet	Choose one of: • 0 - Reply on Default • 1 - Reply on Ringlet 0 • 2 - Reply on Ringlet 1 • 3 - Reserved
Echo Response Control		These fields are active only when OAM Type Code = 1001 - Echo Response. It indicates that an Echo Response OAM frame will be sent.
	Reserved	(Read-only) Reserved for future use.
	Protection Mode	Choose one of: • 0 - Protected • 1 - Unprotected
	Response Ringlet	Choose one of: • 0 - Reply on Default • 1 - Reply on Ringlet 0 • 2 - Reply on Ringlet 1 • 3 - Reserved
(Footer)	Vendor OUI	(Optional) This field is active only when OAM Type Code = 1111 - Vendor Specific. It indicates that a Vendor Specific OAM frame will be sent. This is the 3-octet IEEE company identifier for this vendor. OUI = Organizationally Unique Identifier.

Frame Data for FCoE Support

Fibre Channel over Ethernet (FCoE) has been implemented as an optional feature of NGY load modules (LSM10GXM family) and LSM1000XMVDC 4/8/12/ and 16-port load modules.

The load module will only show the FCoE feature if the EEPROM has been programmed.

1. To activate the FCoE feature, switch the port mode by selecting **Data Center Mode** in the Port Properties General tab (*Figure:Port Properties, NGY, Data Center Mode*) of the NGY module, or checking Enable Data Center Mode in the Port Properties General tab (*Figure:Port Properties, LSM1000XMVDC, Data Center Mode*) of the LSM1000XMVDC module.

   (A re-download of the FPGA occurs when the port mode is switched from Normal to Data Center, or vice-versa.)

Figure:Port Properties, NGY, Data Center Mode

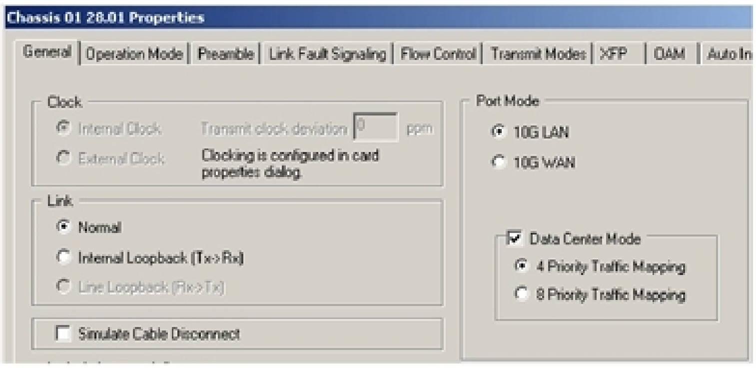
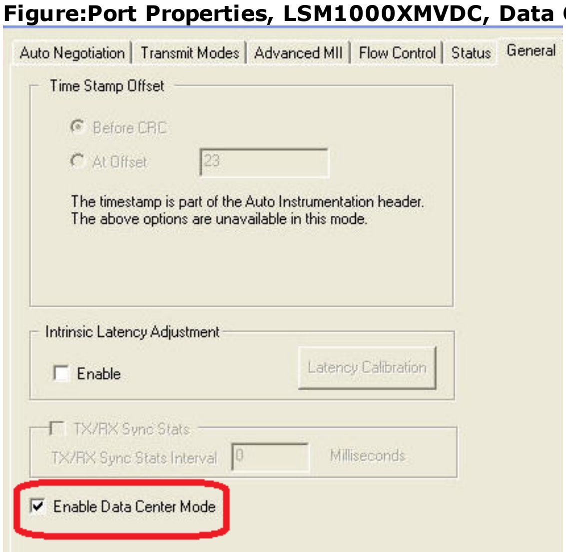


Figure:Port Properties, LSM1000XMVDC, Data Center Mode



2. Select 4- or 8-Priority traffic mapping option (NGY only).
3. Click **Apply**.

NOTE

When Data Center Mode is selected:

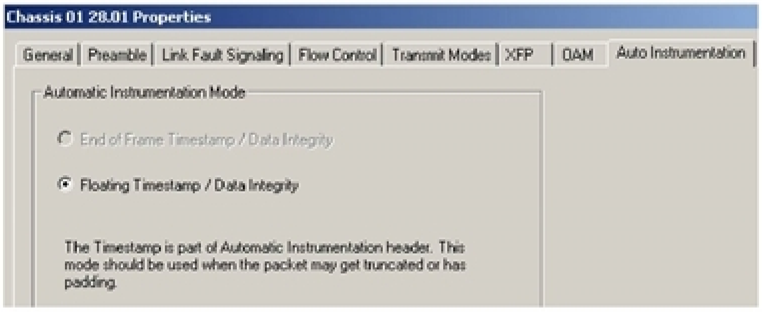
The port is automatically placed into Advanced Streams mode; Packet Stream mode is not supported.

Only Auto Instrumentation mode (Floating Timestamp / Data Integrity) is supported, both for transmit and receive (*Figure:Port Properties, Auto Instrumentation in Data Center Mode* below). End-of-frame Timestamp is not supported and PRBS is not supported.

4-Priority and 8-Priority traffic mapping (NGY module) have different features and limits. *NGY 4-PFC Mode* and *NGY 8-PFC Frame Size Limitation*.

Precision Time Protcol (PTP) is not enabled. (However, when Data Center Mode is not selected, PTP *is* enabled.)

Figure:Port Properties, Auto Instrumentation in Data Center Mode



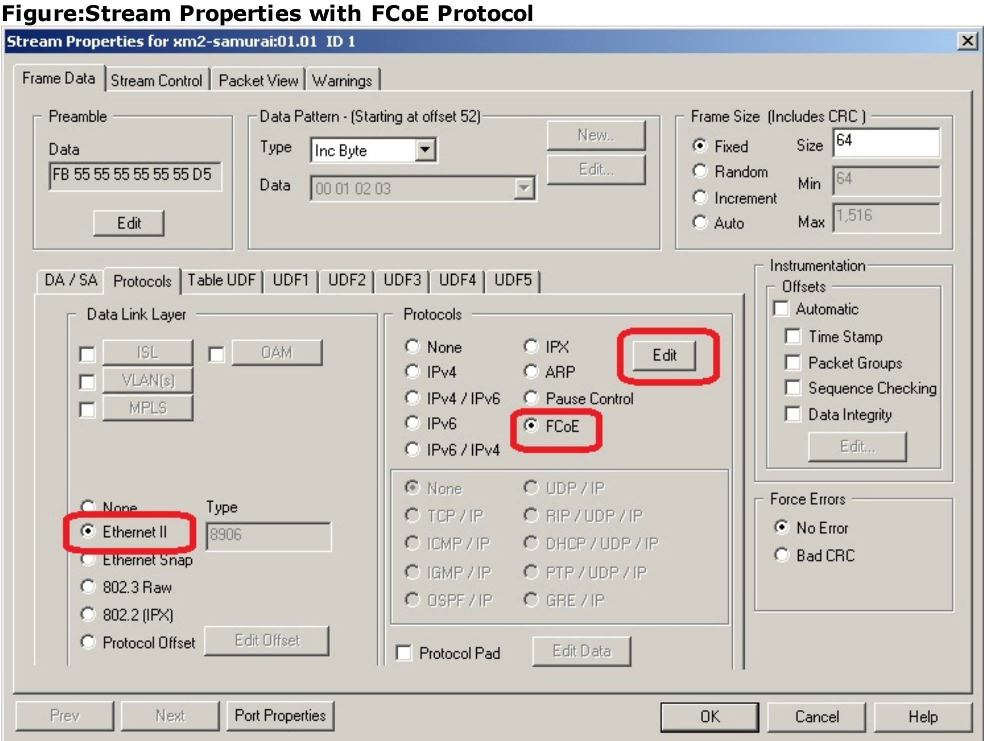
FCoE Configuration

After setting the port to Data Center Mode, the FCoE option is present in the list of selectable protocols (*Figure:Stream Properties with FCoE Protocol*).

NOTE When FCoE is enabled, only 256 advanced streams are supported. In normal mode (non-FCoE), 512 advanced streams are supported.

1. Open the Stream Properties window, Frame Data tab, and click **Ethernet II** in the Protocols tab.

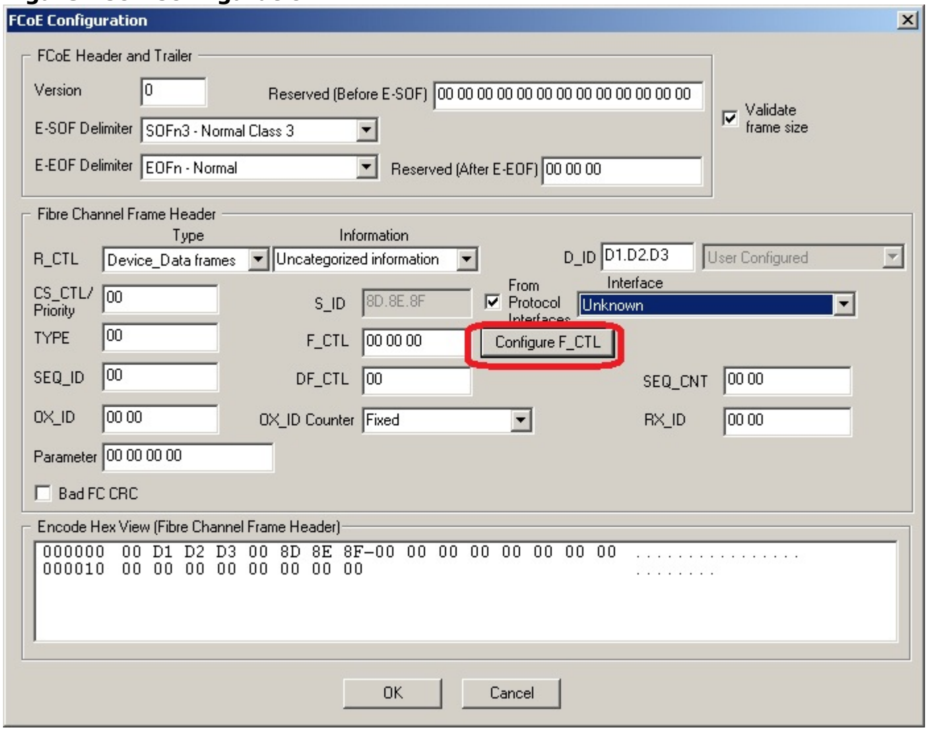
Figure:Stream Properties with FCoE Protocol



2. Click **FCoE** to select it, then click **Edit**.

   The FCoE Configuration dialog will display (*Figure:FCoE Configuration*).

Figure:FCoE Configuration

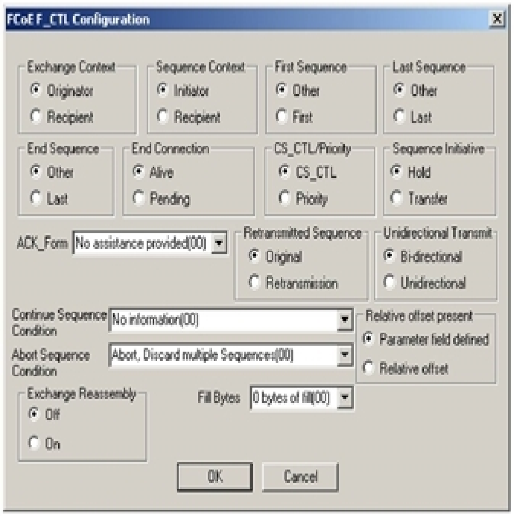


Field definitions for the FCoE Configuration dialog are provided in *Table:FCoE Configuration Dialog*.

3. Adjacent to the F-CTL field, click the Configure F_CTL button.

   The FCoE F_CTL Configuration dialog will display (*Figure:FCoE F_CTL Configuration*).

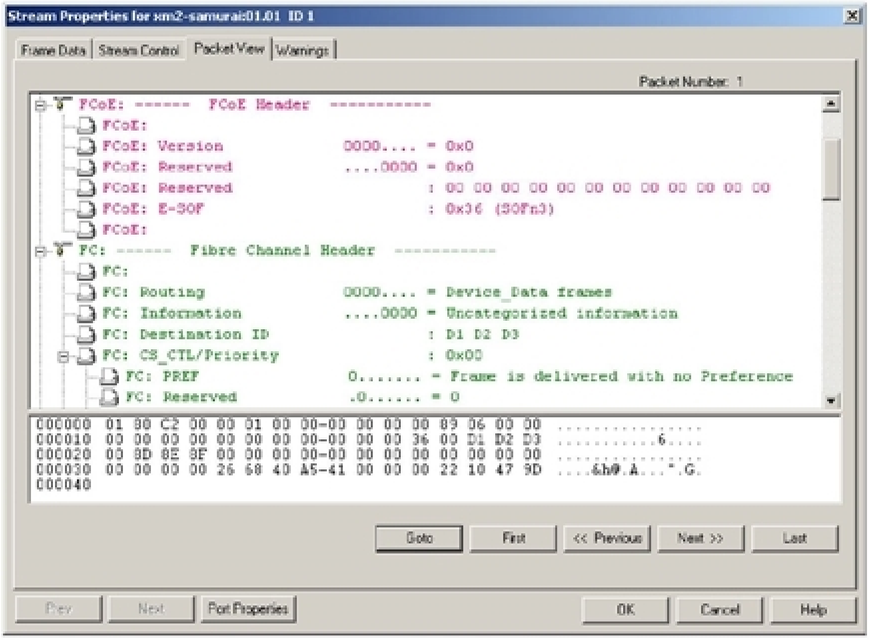
Figure:FCoE F_CTL Configuration



Field definitions for the F_CTL Configuration dialog are provided in *Table: F_CTL Configuration Dialog*.

The Stream Properties, Packet View tab will display the configured options (*Figure:Packet View Showing FCoE Header*).

Figure:Packet View Showing FCoE Header



FCoE Configuration

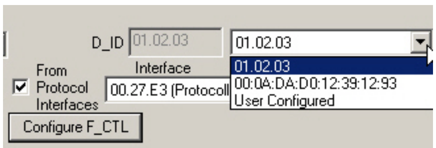
Field definitions for the FCoE Configuration dialog are listed in *Table:FCoE Configuration Dialog*.

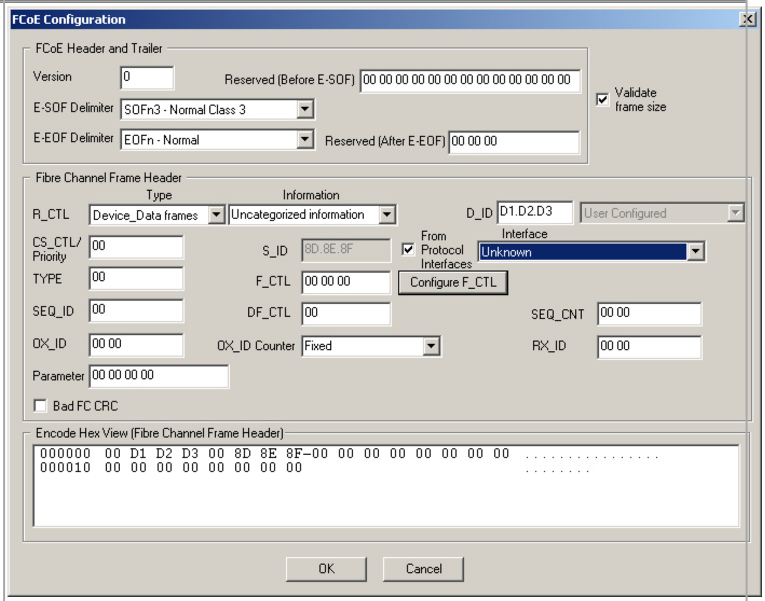
Table:FCoE Configuration Dialog

Section	Field/Control	Description
FCoE Header and Trailer	Version	Configures the version (*default = 1*)
	Reserved (Before E-SOF)	Start-of-Frame reserved value (*default = '00 ... 00'*)
	E-SOF Delimiter	The Start-of-Frame (SOF) delimiter is an Ordered Set that immediately precedes the frame content. There are multiple SOF delimiters defined for Sequence control. • SOFn1 - Normal Class 1 or 6 • SOFn2 - Normal Class 2 • SOFn3 - Normal Class 3 (*default*) • SOFn4 - Normal Class 4 • SOFi2 - Initiate Class 2 • SOFi3 - Initiate Class 3 • SOFi4 - Initiate Class 4 • SOFc4 - Connect Class 4 • SOFf - Fabric
	E-EOF Delimiter	The End-of-Frame (EOF) delimiter is an Ordered Set that immediately follows the CRC. The EOF delimiter

Section	Field/Control	Description
		designates the end of the frame content. All frames other than the last frame of a Sequence shall be terminated with an EOFn delimiter. Valid frame content: • EOFn - EOF Normal identifies the end-of-frame • EOFt - EOF Terminate indicates that the Sequence associated with this SEQ_ID is complete. (*default*) • EOFrt - EOF Remove Terminate • EOFni - EOF Normal Invalid replaces an EOFn or EOFt, indicating that the frame content is invalid. • EOFrti - EOF Remove Terminate Invalid • EOFa (EOF Abort) terminates a partial frame due to a malfunction in a link facility during transmission.
	Reserved (After E-EOF)	Specifies the 3 rescued bytes after End-of-Frame delimiter
Validate Frame Size (check box)		When cleared, you can do negative testing using non-multiple of '4' frame size
Fibre Channel Frame Header	R_CTL Type	The R_CTL field is a one-byte field that contains routing bits and information bits to categorize the frame function. When the R_CTL field is used in combination with the TYPE field, it provides an FC_Port with assistance in frame routing, data routing, or addressing. The R_CTL field is further subdivided into the ROUTING field and the INFORMATION field. Frame Types: • Device_Data frames • Extended Link Services • FC-4 Link_Data • Video_Data • Extended_Headers • Basic Link Services • Link_Control Frame • Extended Routing
	R_CTL Information	The INFORMATION field is included in R_CTL to assist the receiver of a Data frame in directing the Data Field content to the appropriate buffer pool. Information categories for R_CTL Type = *Device_Data*

Section	Field/Control	Description
		or *FC-4 Link_Data*: • Uncategorized Information • Solicited Data • Unsolicited Control • Solicited Control • Unsolicited Data • Data Descriptor • Unsolicited Command • Command Status • Reserved Information categories for R_CTL Type = *Extended Link Services:* • Solicited Data • Request • Reply • Reserved Information categories for R_CTL Type = *Video_Data:* • Unsolicited Data • Reserved Information categories for R_CTL Type = *Extended Headers:* • Virtual Fabric Tagging Head • Inter-Fabric Routing Header • Encapsulation Header • Reserved Information categories for R_CTL Type = *Basic Link Services:* • No Operation • Abort Sequence • Remove Connection • Basic_Accept • Basic_Reject • Dedicated Connection Preempted • Reserved (continued)
	R_CTL Information (continued)	Information categories for R_CTL Type = *Link Control Frame:* • Acknowledge_1

Section	Field/Control	Description
		• Acknowledge_0 • Nx_Port Reject • Fabric Reject • Nx_Port Busy • Fabric Busy to Data Frame • Fabric Busy to Link_Control Frame • Link Credit Reset • Notify • End • Reserved Information categories for R_CTL Type = *Extended Routing:* • Vendor Unique • Reserved
	D_ID	Three-byte field that contains the address identifier of the destination Nx_Port. If PLOGI Destination has been configured, the box will list these.  The first PLOGI Destination will be selected by default. If *User Configured* is selected, the D_ID field will become accessible (not grayed-out).
	CS-CTL/Priority	Class Specific Control/Priority (00 or 01) When set to zero, is interpreted to be CS_CTL information (containing management information for the class of service identified by the SOF). When set to one, is interpreted to be Priority information (containing priority information for the class of service identified by the SOF)
	S_ID	Three-byte field that contains the address identifier of the source Nx_Port or, click **From Protocol Interfaces** and the value will be supplied.
	From Protocol Interfaces (check box)	Selecting this check box synchronizes the S_ID with the values set in FCoE interfaces that have been created using the Protocol Interfaces wizards. Configured and Discovered VLAN IDs will also display. When selected, choose the desired FCoE interface from the listing.

<table>
<tr><th>Section</th><th>Field/Control</th><th>Description</th></tr>
<tr><td></td><td></td><td>


Protocol Interfaces for more information.

From Protocol Interfaces also shows up on the DA/SA page. From Protocol Interfaces Option.
</td></tr>
<tr><td></td><td>Type</td><td>
The data structure type is a one-byte field that identifies the protocol of the frame content for Data frames.

When R_CTL = *Basic* or *Extended Link_Data*:

- 00 = Basic Link Service
- 01 = Extended Link Service
- 01 to CF = Reserved
- D0 to FF = Vendor Specific

When R_CTL = *Video_Data*:

- 02 to 5F = Reserved
- 60 = FC-AV Container
- 61 = ARINC 818
- 62 to 63 = Reserved for FC-AV
- 64 to CF = Reserved
- D0 to FF = Vendor Specific

When R_CTL = *Device_Data* and *Link_Data*:

- 00 to 03 = Reserved
- 04 = Obsolete
- 05 = IPv4, IPv6, and ARP over Fibre Channel
- 06 to 07 = Reserved
- 08 = Fibre Channel Protocol (see FCP-3)
- 09 = Obsolete
</td></tr>
</table>

Section	Field/Control	Description
		• 0A to 0F = Reserved - SCSI • 10 = Reserved • 11 to 13 = Obsolete • 14 = Fibre Channel SATA Tunnelling Protocol (see FC-SATA)
	F_CTL	Frame Control is a three-byte field that contains control information relating to the frame content.*Table: F_CTL Configuration Dialog*.
	SEQ_ID	The SEQ_ID is a one-byte field assigned by the Sequence Initiator that shall be unique for a specific D_ID and S_ID pair while the Sequence is open.
	DF_CTL	Data Field Control (DF_CTL) is a one-byte field that specifies the presence of optional headers at the beginning of the Data_Field. See DF_CTL Bit Definition, below.
	DF_CTL Bit Definition:	

Word 3, Bit(s)	Optional Header	Applicability
23	Reserved	all frames
22	0 = Neither ESP_Header nor ESP_Trailer 1 = Both ESP_Header and ESP_Trailer	all frames
21	0 = No Network_Header 1 = Network_Header	Device_Data and Video_Data frames
20	0 = No Association_Header 1 = Association_Header	Device_Data and Video_Data frames
19-18	Reserved	all frames
17-16	00b = No Device_Header 01b = 16 Byte Device_Header 10b = 32 Byte Device_Header 11b = 64 Byte Device_Header	Device_Data and Video_Data frames

Section	Field/Control	Description
	SEQ_CNT	The sequence count is a two-byte field that indicates the sequential order of Data frame transmission within a single Sequence or multiple consecutive Sequences for the same Exchange. The SEQ_CNT of the first Data frame of the first Sequence of the Exchange transmitted by either the Originator or Responder is binary zero. The SEQ_CNT of each subsequent Data frame in the Sequence is incremented by one.
	OX_ID	The Originator Exchange_ID is a two-byte field that identifies the Exchange_ID assigned by the Originator of the Exchange. Each Exchange is assigned an identifier unique to the Originator or Originator-Responder pair.
	OX_ID Counter	The decrement/increment options enable changing the value for the Exchange IDs through UDFs instead of manually setting different values in the streams. Options are:

Section	Field/Control	Description
		Fixed Increment Decrement Continuous Increment Continuous Decrement Random
	RX_ID	The Responder Exchange_ID is a two byte field assigned by the Responder that provides a unique, locally meaningful identifier at the Responder for an Exchange established by an Originator and identified by an OX_ID.
	Parameter	The Parameter field has meanings based on frame type. For Link_Control frames, the Parameter field is used to carry information specific to the individual Link_Control frame. For Data frames with the relative offset present bit set to 1, the Parameter field specifies relative offset. For Data frames with the relative offset Present bit set to zero, the Parameter field is set and interpreted in a protocol specific manner that may depend on the type of Information Unit carried by the frame.
	Bad FC CRC (check box)	When selected, will ensure that the inner FC CRC that is generated by hardware will be wrong. If cleared, then the FC CRC should be a valid CRC.
Encode Hex View	Fibre Channel Frame Header	This display shows the configuration of the header, based on the options selected in the fields above.

F_CTL Configuration

NOTE Refer *F_CTL Configuration* for information on Fibre Channel Module (FCM) specific F_CTL Configuration explanation.

Field definitions for the F_CTL Configuration dialog are listed in *Table:F_CTL Configuration Dialog*.

Table:F_CTL Configuration Dialog

Field/Control	Description
Exchange Context	0 = Originator of exchange 1 = Recipient (responder) of exchange
Sequence Context	0 = Sequence Initiator 1 = Sequence Recipient
First Sequence	0 = Other sequence other than first of exchange 1 = First sequence of exchange
Last Sequence	0 = Other sequence other than last of exchange 1 = Last sequence of exchange

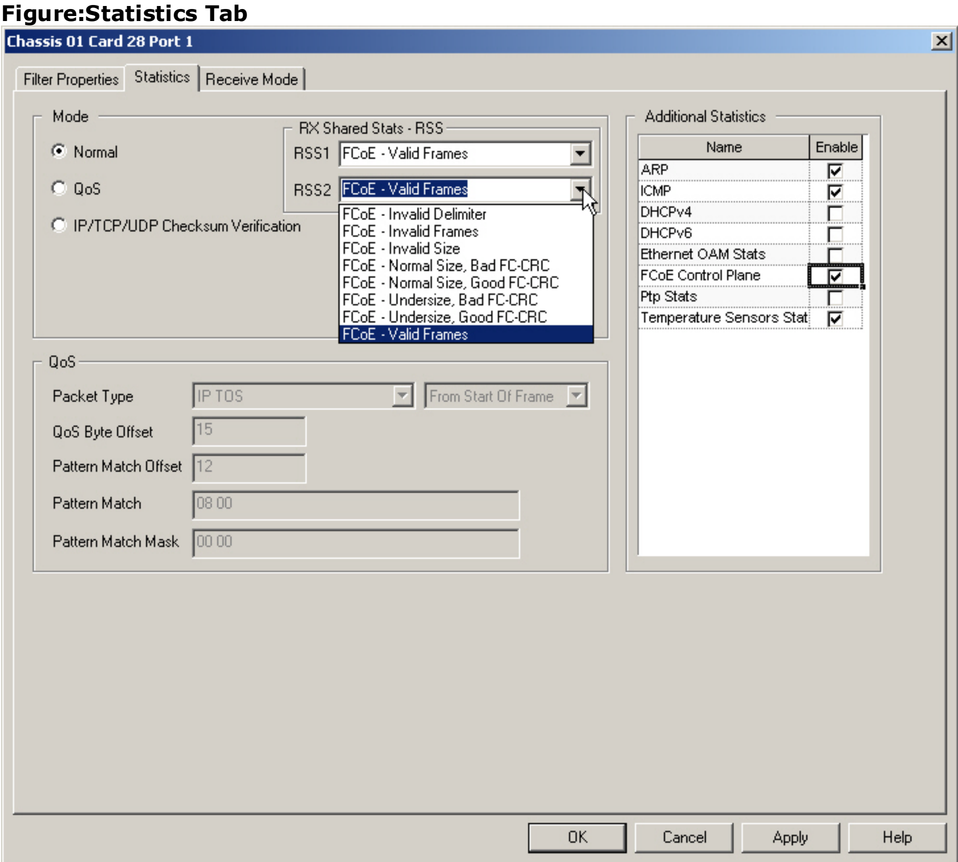
Field/Control	Description
End Sequence	0 = Other data frame other than last of sequence 1 = Last data frame of sequence
End Connection	0 = Alive connection active 1 = Pending end of connection pending
CS_CTL/Priority	0 = CS_CTL 1 = Priority
Sequence Initiative	0 = Hold sequence initiative 1 = Transfer sequence initiative
ACK_Form	00 = No assistance provided 01 = Ack_1 Required 10 = reserved 11 = Ack_0 Required
Retransmitted Sequence	0 = Original Sequence transmission 1 = Retransmission of sequence
Unidirectional Transmit	0 = Bi-directional transmission 1 = Unidirectional transmission
Continue Sequence Condition	Last Data frame Sequence Initiator 00 = No information 01 = Sequence to follow-immediately 10 = Sequence to follow-soon 11 = Sequence to follow-delayed
Abort Sequence Condition	*ACK frame (Sequence Context = Recipient)* 00 = Continue sequence 01 = Abort Sequence, Perform ABTS 10 = Stop Sequence 11 = Immediate Sequence retransmission requested *Data frame (1st of Exchange) (Sequence Context = Initiator)* 00 = Abort, Discard multiple Sequences 01 = Abort, Discard a single Sequence 10 = Process policy with infinite buffers 11 = Discard multiple Sequences with immediate retransmission
Exchange Reassembly	Off On
Fill Bytes	End of Payload - bytes of fill (following Payload) 00 = 0 bytes of fill 01 = 1 byte of fill 10 = 2 bytes of fill

Field/Control	Description
	11 = 3 bytes of fill
Relative offset present	0 = Parameter field defined for some frames 1 = Relative offset

FCoE Statistics

Two additional dedicated statistics are provided with FCoE: RX Shared Stats1 and RX Shared Stats2. These two stats can be mapped to any of the stats defined below.

Figure:Statistics Tab



The fields and controls in this dialog are described in *Table:RX Shared Stats Configuration*.

Table:RX Shared Stats Configuration

Option	Description
FCoE Invalid Delimiter	Frame with invalid FC frame delimiter
FCoE Invalid Frames	Illegal size FCoE frame or Bad FC-CRC FCoE frame or Bad Ethernet CRC FCoE frame or invalid FC frame delimiter
FCoE Invalid Size	Frame size is not a multiple of 4 bytes with EType field set to FCoE frame.
FCoE Normal Size, Bad FC-CRC	Size of FCoE frame is legal, FC-CRF is bad Normal size FCoE frame = frame size is multiple of 4 bytes with EType field set to FCoE: 64 <= FrameSize <= 2176 NonVLAN 64 <= FrameSize <= 2180 VLAN

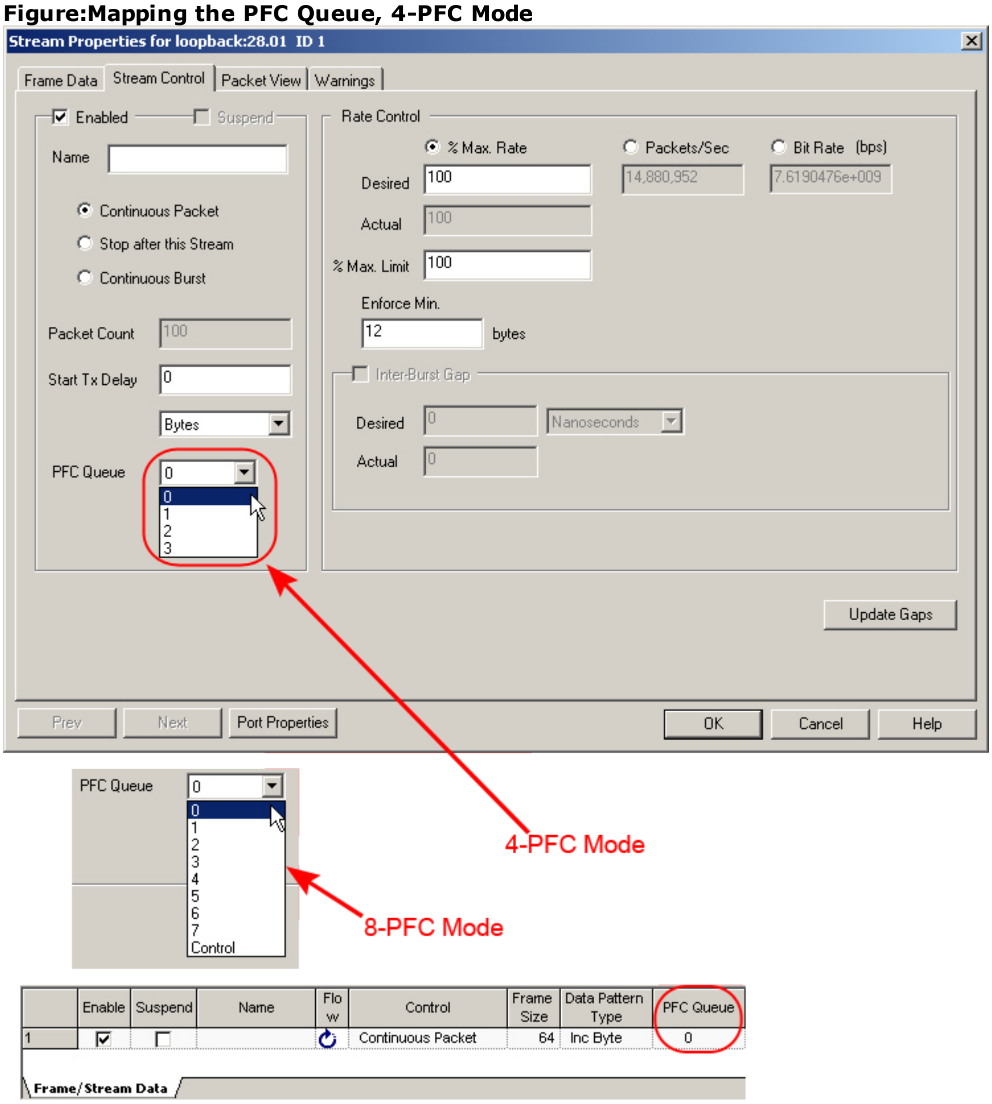
Option	Description
FCoE Normal Size, Good FC-CRC	Size of FCoE frame is legal, FC-CRF is good
FCoE Undersize, Bad FC-CRC	Undersize = legal size FCoE frame, FrameSize < 64 FC-CRC is bad.
FCoE Undersize, Good FC-CRC	Undersize = legal size FCoE frame, FrameSize < 64 FC-CRC is good.
FCoE Valid Frames	Frame size is multiple of 4 bytes with EType field set to FCoE frame.

Priority-based Flow Control

The Ixia port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. The flow control type is determined by the selection made on the Flow Control tab of the Port Properties dialog (*Figure:Port Properties, Flow Control, 4-PFC Mode*).

The PFC scheduling function is based on the existing Advanced Scheduler.
A new parameter **PFC Queue** is added to each stream (*Figure:Mapping the PFC Queue, 4-PFC Mode*). The PFC Queue can be mapped to the priority field in the frame. Four or eight priorities of traffic can be implemented, with frame size up to 9216 bytes. This applies to both FCoE and non-FCoE frames.

Figure:Mapping the PFC Queue, 4-PFC Mode

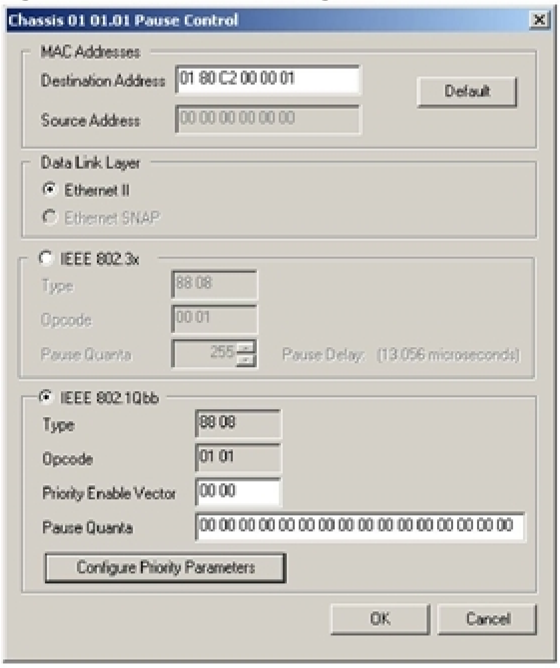


Pause Control Dialog

Priority parameters can be configured directly in the Pause Control dialog or by using the PFC Configuration dialog.

To access the Pause Control dialog, from the Stream Properties window, Frame Data tab, Protocols tab, click **Ethernet II** and click **Pause Control**, then click **Edit**. The Pause Control dialog will open (*Figure:Pause Control Dialog*).

Figure:Pause Control Dialog



You can configure priority parameters directly in the Priority Enable Vector field (which allows editing the pause timer) or click the **Configure Priority Parameters button**.

When the **Configure Priority Parameters** button is clicked, the PFC Configuration dialog shown in *Figure:PFC Configuration Dialog* will display, allowing the direct configuration of the detailed parameters (Pause Quanta).

Figure:PFC Configuration Dialog

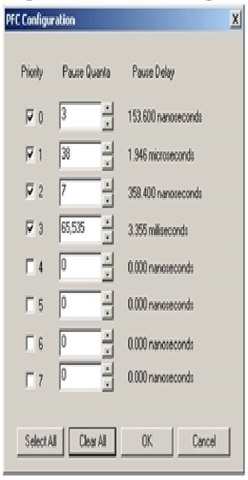
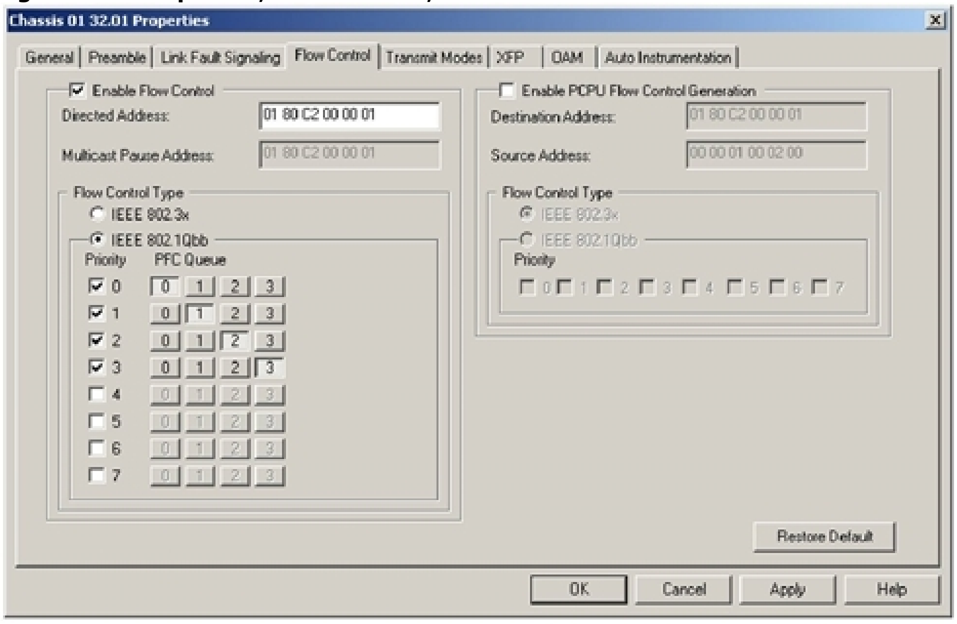


Figure:Port Properties, Flow Control, 4-PFC Mode shows how to configure the port to respond to PFC, in the Flow Control tab of the Port Properties window.

NGY 4-PFC Mode

The NGY load module in Data Center Mode—with 4-Priority traffic mapping selected—supports only four PFC queues, with frame size 48 to 9K bytes on all four.

Figure:Port Properties, Flow Control, 4-PFC Mode



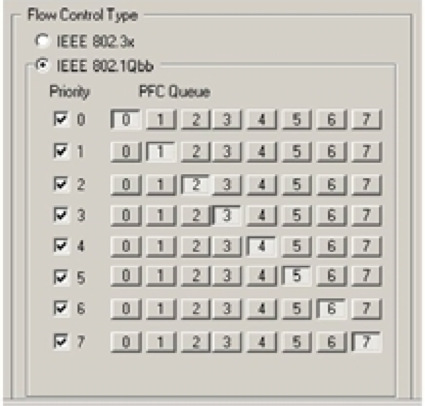
NGY 8-PFC Frame Size Limitation

The NGY load module in Data Center Mode—with 8-Priority traffic mapping selected—supports the following frame size for each PFC queue:.

Table:NGY 8-PFC Frame Sizes

PFC Queue	Min Frame Size	Max Frame Size
0	48 Byte	9216 Byte
1	48 Byte	2500 Byte
2	48 Byte	2500 Byte
3	48 Byte	2500 Byte
4	48 Byte	2500 Byte
5	48 Byte	2500 Byte
6	48 Byte	2500 Byte
7	48 Byte	2500 Byte
8	48 Byte	2500 Byte
Control traffic	48 Byte	2500 Byte

Figure:Port Properties, Flow Control, 8-PFC Mode



LSM XMVDC Frame Size Limitation

There is limitation in LSM1000XMVDC load modules that all PFC queues will have a minimum frame size 48 bytes and maximum frame size 2500 bytes.

Frame Data for PTP Support

Precision Time Protocol (IEEE 1588v2) has been implemented as an optional feature of these load modules:

- NGY load modules (LSM10GXM family
- LSM1000XMV(R) 4/8/12/16 (not in Data Center Mode)
- LSM1000XMVDC 4/8/12/16 (not in Data Center Mode)

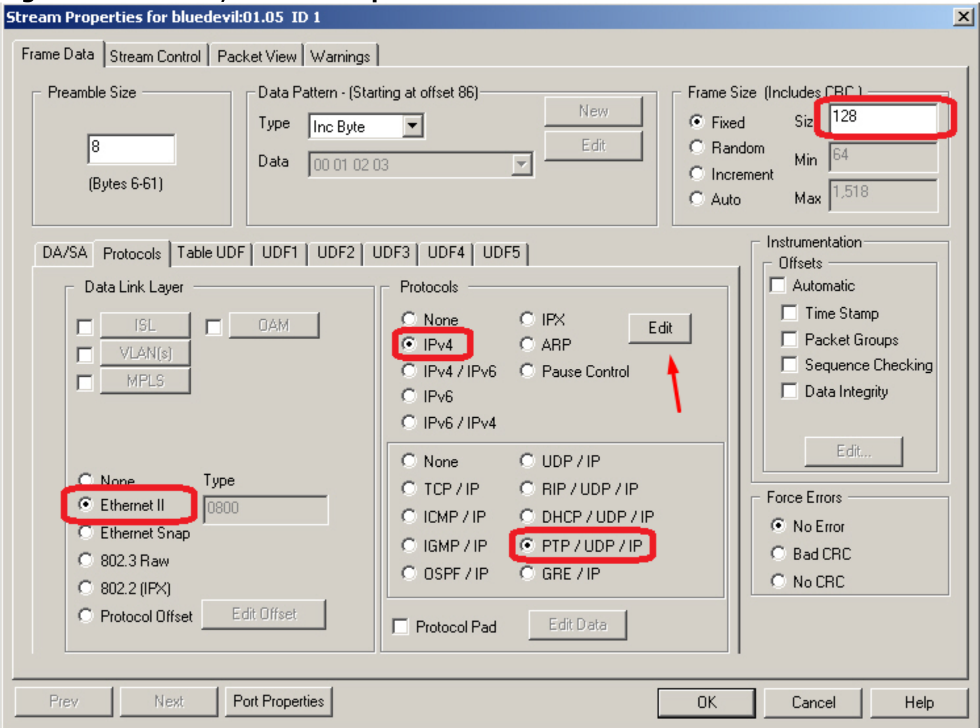
NOTE PTP support in LSM1000XMVDC cards is available only if you purchase EEProm option.

- ASM1000XMV12V
- Xcellon-Ultra XP and NP

For a discussion of PTP theory, see Chapter 3 of the *Ixia Hardware and Reference Guide*.

1. To activate the PTP feature, begin at the Frame Data tab of the Stream Properties page (*Figure:Frame Data, Stream Properties*).

Figure:Frame Data, Stream Properties



2. Choose Ethernet II, IPv4, and PTP/UDP/IP.

   (A Warning message will occur, regarding frame size.)

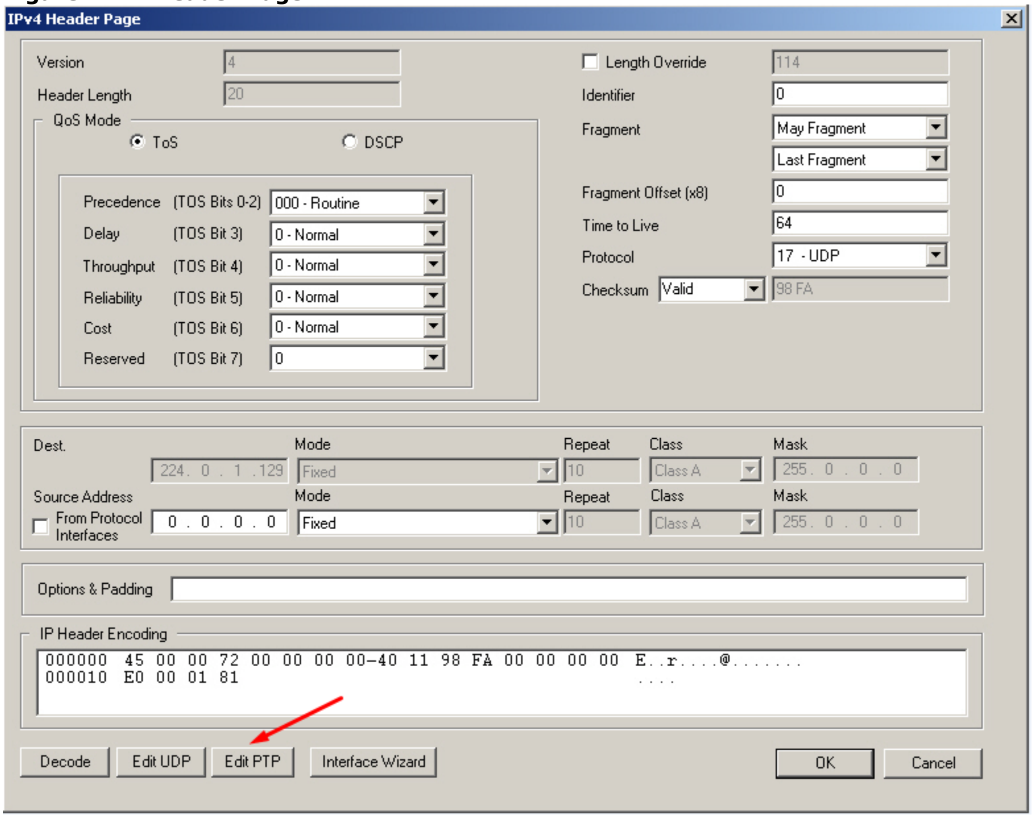
3. Change the Frame Size to 128 (so that it is long enough to accommodate the PTP header).

4. Click **Edit**.

   The IPv4 Header configuration dialog will display (*Figure:IPv4 Header Page*).

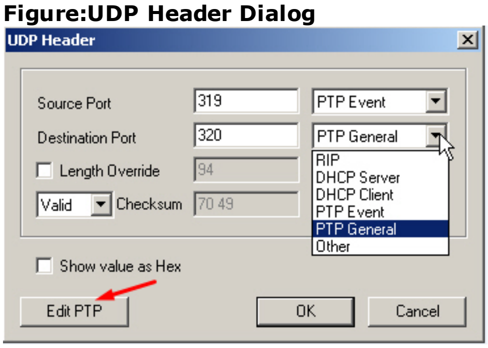
NOTE When a stream is configured as PTP, the Destination Address on the Streams properties DA/SA tab will be deactivated and grayed out, due to the fact that Ethernet, IPv4 and UDP transmission of PTP packets relies on a reserved Destination Address.

Figure:IPv4 Header Page



5. Click **Edit PTP** to access the PTP Header configuration dialog (Figure:PTP Header Configuration Dialog).
6. Click **Edit UDP** to access the UDP Header dialog (*Figure:UDP Header Dialog*, to set up the source and destination ports for PTP traffic. (The PTP Header config dialog can also be accessed from the UDP config dialog.)

Figure:UDP Header Dialog



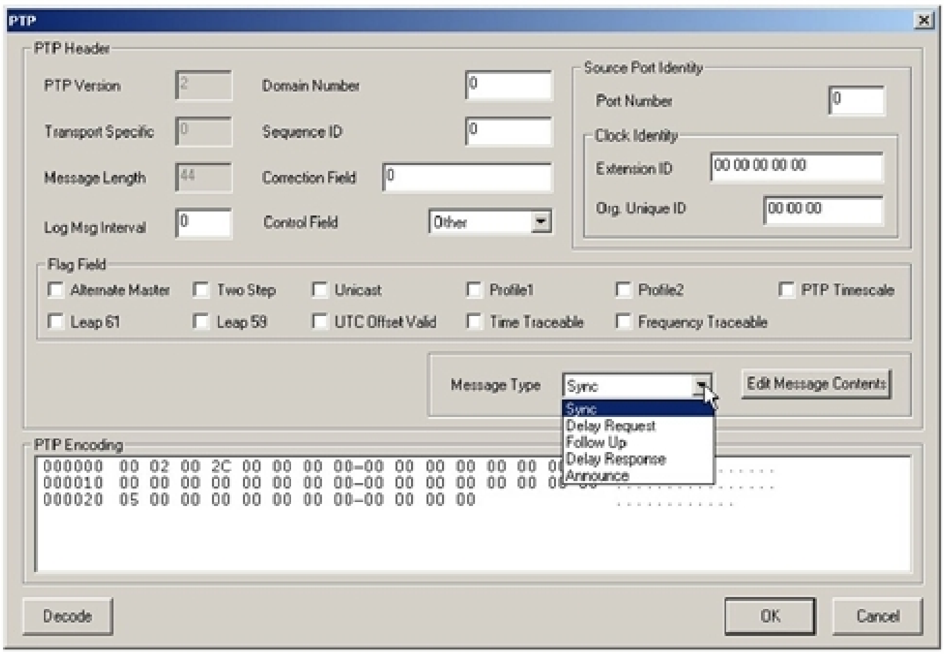
Two PTP ports are available for both source and destination: PTP Event (port 319) and PTP General (port 320). The full range of choices appear in *Table:UDP Header for PTP*.

Table:UDP Header for PTP

Field	Description
Source Port	Protocol source port number. One of: • RIP (Port 520) • DHCP Server (Port 67)

Field	Description
	• DHCP Client (Port 68) • PTP Event (Port 319) • PTP General (Port 320) • Other (Port 63)—If Other is selected, the *Edit Protocol* button is disabled (dimmed).
Destination Port	Protocol destination port number. One of: • RIP (Port 520) • DHCP Server (Port 67) • DHCP Client (Port 68) • PTP Event (Port 319) • PTP General (Port 320) • Other (Port 63)—If Other is selected, the *Edit Protocol* button is disabled (dimmed).
Length Override	See *Table:UDP Header Fields Set by the IPv4 UDP Dialog*.
Checksum	See *Table:UDP Header Fields Set by the IPv4 UDP Dialog*.

Figure:PTP Header Configuration Dialog



7. Configure the desired PTP header using the fields on this page. *Table:PTP Header Configuration* contains field descriptions.
8. Choose a **Message Type** and click the **Edit Message Contents** button.

A message-specific configuration dialog will open (*Table:PTP Message Configuration Dialogs*).

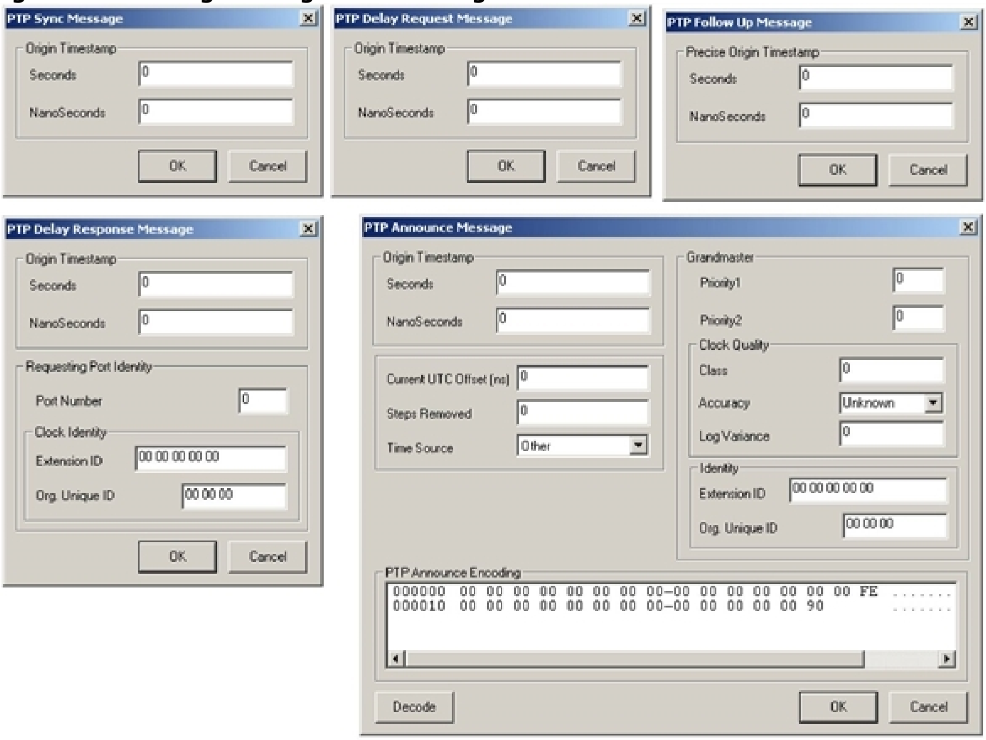
Table:PTP Header Configuration

Section	Field/Control	Description
PTP Header	PTP Version	(Read only) Displays the PTP version.

Section	Field/Control	Description
	Domain Number	A domain consists of one or more PTP devices communicating with each other as defined by the protocol. Range 0 - 255. (*default = 0*)
	Transport Specific	(Read only) The Transport Specific field. (*default = 0*)
	Sequence ID	The sequence ID of the message shall be one greater than the sequence ID of the previous message of the same message type sent to the same message destination address by the transmitting port. (*default = 0*)
	Message Length	(Read only) The total number of octets that form the PTP message. The counted octets start with the first octet of the header and include and terminate with the last octet of any suffix or, if there are no suffix members with the last octet of the message. (*default = 44*)
	Correction Field	Exclicked in nanoseconds and fractions thereof. (*default = 0*) Transparent clocks forward PTP timing messages through the clock in the manner of an ordinary bridge or router but, in addition, measure the time spent by a PTP timing message within the transparent clock. These 'residence' times are accumulated in the Correction Field in the PTP timing messages, which allows the subordinate to correct the timestamps, effectively removing the timing fluctuations that would otherwise be introduced by the bridges.
	Log Msg Interval	The value is determined by the type of the message. (*default = 0*)
	Control Field	The value depends on the message type defined in the **Message Type** field. Select from pull-down: Sync Delay Request Follow-up Delay Response Management Other (*default*)
Source Port Identity	Port Number	Identifies a specific Precision Time Protocol (PTP) port on a PTP node.
	Clock Identity Extension ID	Extension identifier. (*default = '00 00 00 00 00'*)
	Org. Unique ID	Organization Unique Identifier (OUI): the value of the OUI assigned to the vendor or standards organization by the IEEE. The most significant 3 octets of

Section	Field/Control	Description
		the Clock Identity shall be an OUI. (*default* = *'00 00 00'*)
Flag Field	Alternate Master	Selected = Alternate Master
	Leap 61	Selected = Leap 61
	Two Step	Cleared = a one-step clock Selected = a two-step clock.
	Leap 59	Selected = Leap 59
	Unicast	Selected = the transport layer protocol address to which this message was sent is a unicast address. Cleared = the transport layer protocol address to which this message was sent is a multicast address.
	UTC Offset Valid	Selected = UTC Offset Valid
	Profile 1	Selected = Profile 1
	Time Traceable	Selected = Time Traceable
	Profile 2	Selected = Profile 2
	Frequency Trace-able	Selected = Frequency Traceable
	PTP Timescale	Selected = PTP Timescale
	Message Type	Select type of PTP message from pulldown, then click **Edit Message Contents** button. Sync (*default*) Delay Request Follow-up Delay Response Announce
	PTP Encoding	This window displays the encoding of the con-figuration choices made above. Click the **Decode** button to refresh this window.

Figure:PTP Message Configuration Dialogs



Field definitions for PTP messages are provided in *Table:PTP Message Configuration*.

Table:PTP Message Configuration

Section	Field/Control	Description
PTP Sync Message	Origin Timestamp	Seconds: The time interval, exclicked in seconds. (*default = 0*) Nanoseconds: The time interval, exclicked in nanoseconds. (*default = 0*)
PTP Delay Request Message	Origin Timestamp	Seconds: The time interval, exclicked in seconds. (*default = 0*) Nanoseconds: The time interval, exclicked in nanoseconds. (*default = 0*)
PTP Follow-Up Message	Precise Origin Timestamp	Seconds: The time interval, exclicked in seconds. (*default = 0*) Nanoseconds: The time interval, exclicked in nanoseconds. (*default = 0*)
PTP Delay Response Message	Origin Timestamp	Seconds: The time interval, exclicked in seconds. (*default = 0*) Nanoseconds: The time interval, exclicked in nanoseconds. (*default = 0*)
	Requesting Port Identity	Port Number: 16-bit port number associated with the clock. (*default = 0*) Clock Identity: Extension ID: Extension identifier.

Section	Field/Control	Description
		(*default = ‘00 00 00 00 00’*) Org. Unique ID - Organization Unique Identifier (OUI) - the value of the OUI assigned to the vendor or standards organization by the IEEE. The most significant 3 octets of the Clock Identity shall be an OUI. (*default = ‘00 00 00’*)
PTP Announce Message	Origin Timestamp	Seconds - The time interval, exclicked in seconds. (*default = 0*) Nanoseconds - The time interval, exclicked in nanoseconds. (*default = 0*)
	Current UTC Offset (ns)	Current UTC Offset (ns) - The UTC time differs from the TAI time by a constant offset. This is calculated as follows: TAI - UTC. (*default = 0*) Steps Removed - In addition to this precedence order, the distance measured by the number of boundary clocks between the local clock and the foreign master is used when two Announce messages reflect the same foreign master. (*default = 0*) Time Source - (select from pulldown) Indicates the source of time used by the grandmaster clock. • Other (*default*) • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP • Hand Set • Internal Oscillator • Alternate PTP Profile (0 to 14)
	Grandmaster	Priority 1 - A user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected. (*default = 0*) Priority 2 - A user configurable designation that provides finer grained ordering among otherwise equivalent clocks. (*default = 0*)
	Clock Quality	Class (*default = 0*) The clockClass attribute of an ordinary or boundary clock denotes the traceability of the time or frequency distributed by the grandmaster clock.
		Accuracy (select from pulldown)

Section	Field/Control	Description
		• Unknown (*default*) • 25 nanoseconds (ns) • 100 ns • 250 ns • 1 microsecond (us) • 2.5 us • 10 us • 25 us • 100 us • 250 us • 1 millisecond (ms) • 2.5 ms • 10 ms • 25 ms • 100 ms • 250 ms • 1 second • 10 seconds • greater than 10 seconds
		Log Variance (*default = 0*) Defines the stability of a clock.
	Identity	Extension ID - Extension identifier. (*default = '00 00 00 00 00'*) Org. Unique ID - Organization Unique Identifier (OUI) - the value of the OUI assigned to the vendor or standards organization by the IEEE. The most significant 3 octets of the Clock Identity shall be an OUI. (*default = '00 00 00'*)
	PTP Announce Encoding	Shows the coding based on the choices in the fields above. Click the **Decode** button to refresh this display.

PTP Statistics

PTP port-level statistics can be collected by checking the appropriate check box in the Statistics tab (*Figure:PTP Statistics*).

Figure:PTP Statistics

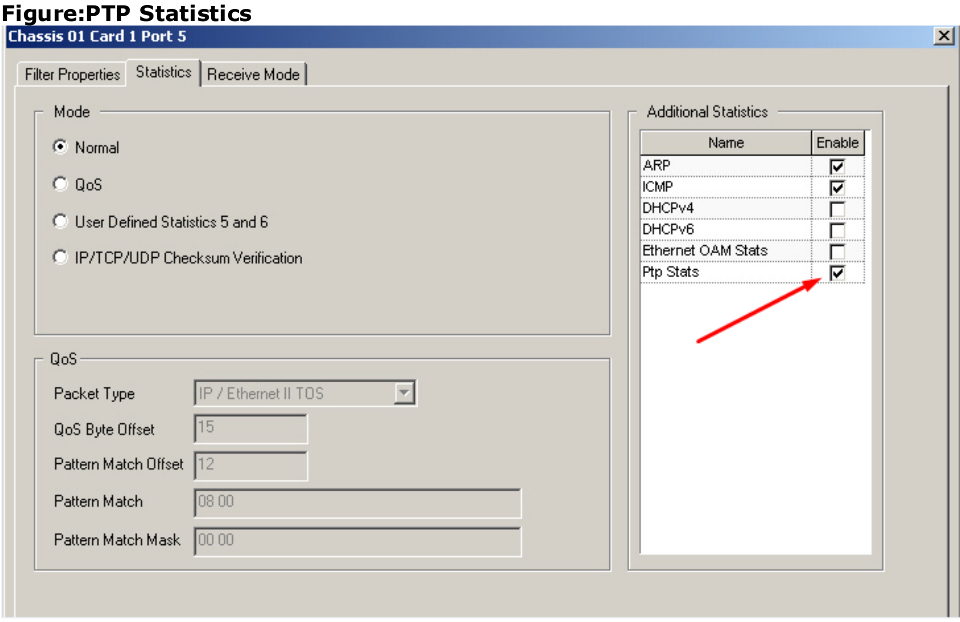
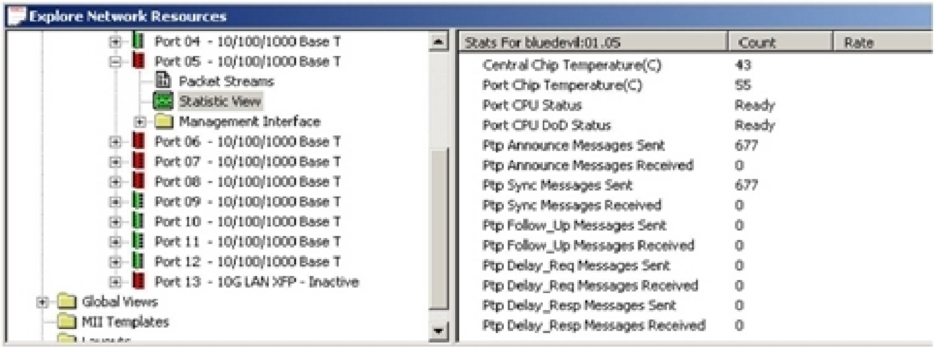


Figure:PTP Statistic View shows the Statistics View with PTP statistics listed.

Figure:PTP Statistic View



Frame Data for Fibre Channel Support

The *Protocols* tab in the Frame Data section for Fibre Channel has been implemented to configure protocol standards for Fibre Channel load module.

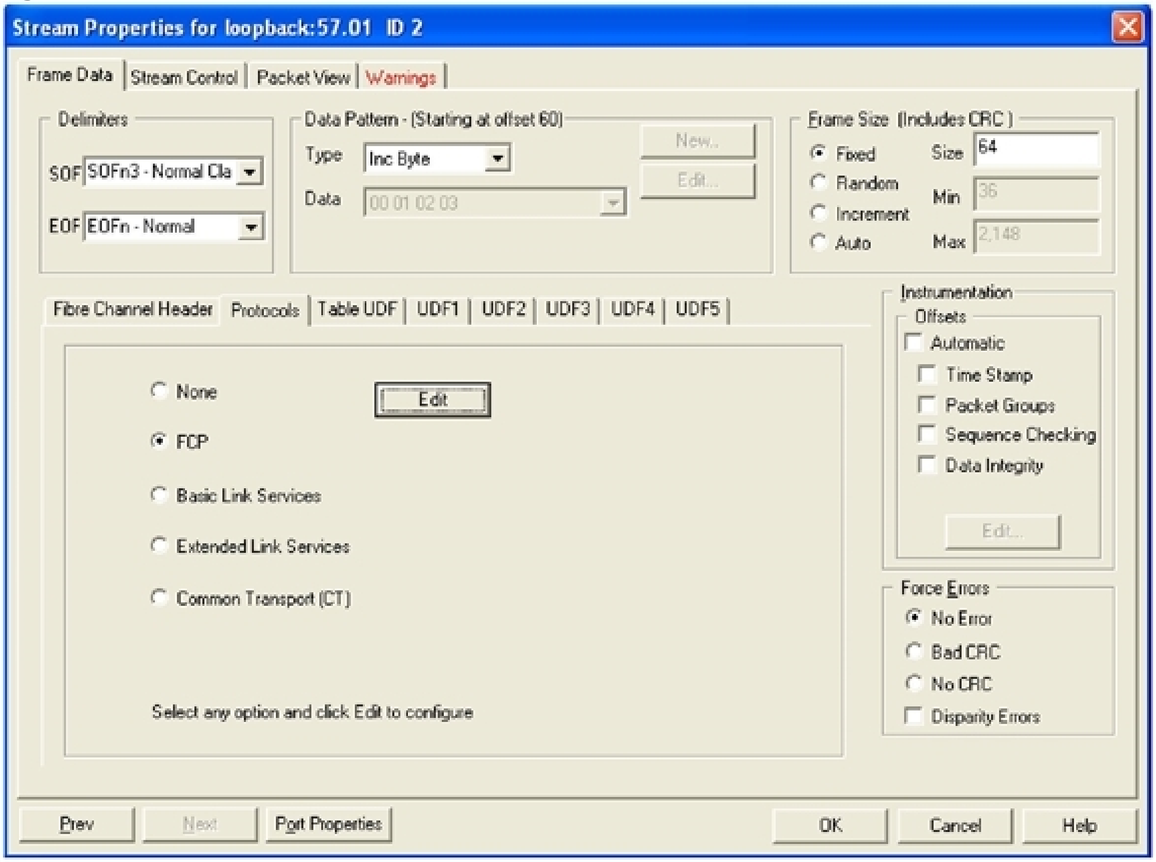
The protocol options are as follows:

- *Fibre Channel Protocol (FCP)*
- *Basic Link Services*
- *Extended Link Services (ELS)*
- *Common Transport (CT)*

To activate the *Protocols* tab, do the following:

1. Begin at the *Frame Data* tab of the *Stream Properties* window (*Figure:Frame Data Protocol tab*).

Figure:Frame Data Protocol tab



2. Click the *Protocols* tab in the *Frame Data* section to access the Protocols section.
3. Select the option button for the protocol you want to configure and click the 

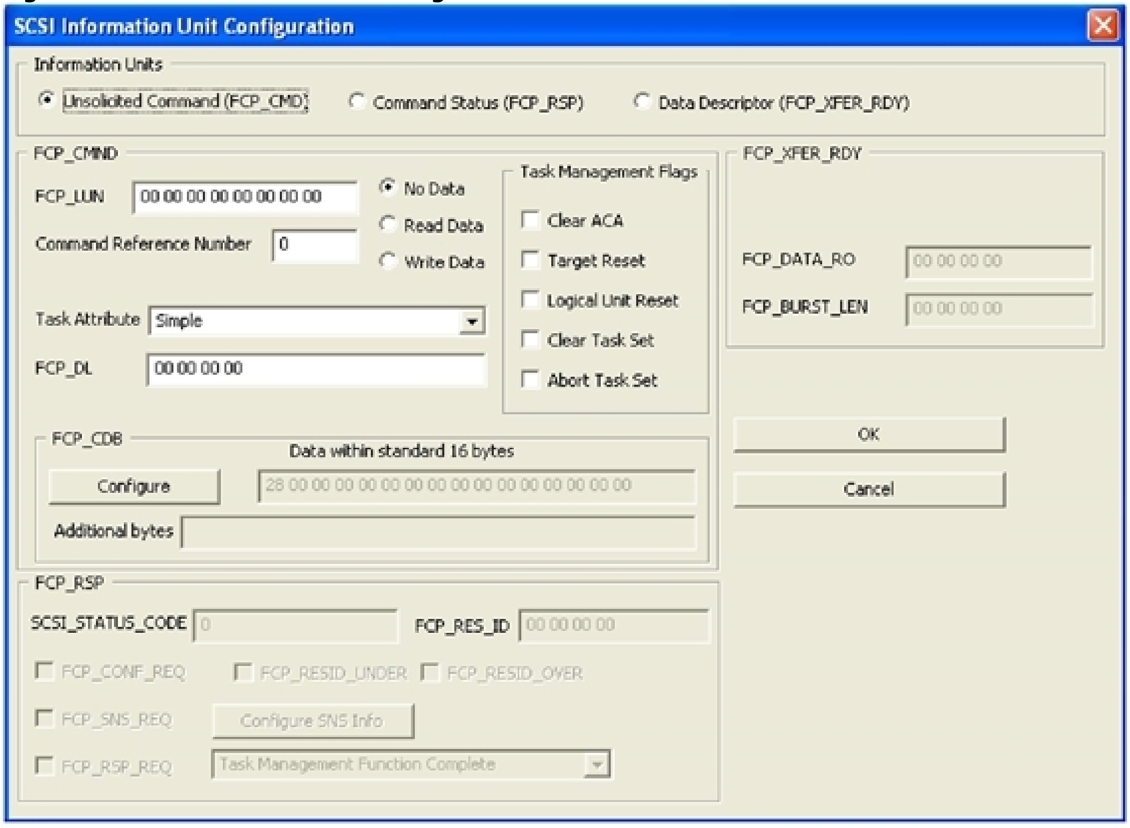
button to open the selected protocol in the edit mode.

Fibre Channel Protocol (FCP)

Fibre Channel Protocol (FCP) is a standard SCSI device interface using Fibre Channel communication. The Fibre Channel protocol provides a range of implementation possibilities extending to maximum performance. The transmission medium is isolated from the control protocol so that each implementation may use a technology best suited to the environment of use.

The SCSI Information Unit Configuration dialog is shown in *Figure:SCSI Information Unit Configuration.*

Figure:SCSI Information Unit Configuration



The fields and controls in this dialog are described in *Table:SCSI Information Unit Configuration dialog*.

Table:SCSI Information Unit Configuration dialog

Section	Fields/Controls	Description
Information Units	Unsolicited Command (FCP_CMD)	If selected, enables the *FCP_CMND* section.
	Command Status (FCP_RSP)	If selected, enables the *FCP_RSP* section.
	Data Descriptor (FCP_XFER_RDY)	If selected, enables the *FCP_XFER_RDY* section.
FCP_CMND	The options in this section are enabled only if *Unsolicited Command (FCP_CMD)* option is selected as the information unit.	
	FCP_LUN	The FCP Logical Unit Number (FCP_LUN) contains the address of the destination logical unit in the attached sub system. The default value is 00 00 00 00 00 00 00 00. If this field contains a valid logical unit address, the INQUIRY command is forwarded to the addressed logical unit.
	Command Reference Number	This field contains the number sent by the initiator to assist in performing precise delivery checking for FCP commands.

Section	Fields/Controls	Description
		The default value is 0.
	Task Attribute	This field contains values that specify the task attribute associated with the Command Descriptor Block (CDB). The options in the list are as follows: • Simple: This task attribute requests that the task be managed according to the rules for a SIMPLE task attribute. • Head of Queue: This task attribute requests that the task be managed according to the rules for a HEAD OF QUEUE task attribute. • Ordered: This task attribute requests that the task be managed according to the rules for an ORDERED task attribute. • Automatic Contingent Allegiance: This task attribute requests that the task be managed according to the rules for an Automatic Contingent Allegiance (ACA) task attribute.
	FCP_DL	This field contains a count of the maximum number of data bytes that is transferred to or from the application client data buffer by the SCSI CDB. The default value is 00 00 00 00.
	No Data	If selected, no data read or write operation is set.
	Read Data	This is a SCSI read operation. When the Read Data bit is set to one, it specifies that the frame data initiator expects FCP_DATA IUs to be in the direction opposite to the direction of the FCP_CMND IU.
	Write Data	This is a SCSI write operation. When the Write Data bit is set to one, it specifies that the initiator expects FCP_DATA IUs to be in the same direction as the FCP_CMD IU.
Task Management Flags	This field contains flags that request for the execution of certain task management functions for the SCSI. The options in the list are as follows: • Clear ACA • Target Reset • Logical Unit Reset	

Section	Fields/Controls	Description
	• Clear Task Set • Abort Task Set	
	Clear ACA	If selected, clears the Automatic Contingent Allegiance (ACA) condition.
	Target Reset	If selected, performs a TARGET RESET task management function to the FCP device. This flag is mandatory for the Fibre Channel protocol.
	Logical Unit Reset	If selected, performs a LOGICAL UNIT RESET task management function. It aborts all tasks in the task set for the logical unit and performs a LOGICAL UNIT RESET for all the dependent logical units. This flag is mandatory for the Fibre Channel protocol.
	Clear Task Set	If selected, aborts all tasks from all initiators in the specified task. A unit attention condition is created for all initiators other than the initiator that sent the CLEAR TASK SET that had tasks in the task set. This flag is mandatory for the Fibre Channel protocol.
	Abort Task Set	If selected, aborts all tasks in the task set from the initiator requesting the ABORT TASK SET. This flag is mandatory for the Fibre Channel protocol.
FCP_CDB	Fibre Channel Protocol Command Descriptor Block (FCP_CDB) field contains the CDB that is sent to the addressed logical unit.	
		Click to open the *CDB Configuration* dialog. Refer *CDB Configuration* for more information.
	Data within standard 16 bytes	This is the maximum CDB length. 16 bytes is the maximum length.
	Additional bytes	This field contains additional bytes of data beyond the maximum 16 bytes limit of FCP_CDB. **NOTE** This field is disabled if any task management flag is set to one.
FCP_RSP	The options in this section are enabled only if *Command Status (FCP_RSP)* option is selected as the information unit. The FCP_RSP provides information on FCP operations that includes SCSI status, protocol verification, and any other applicable autosense data.	
	SCSI_STATUS_CODE	This field contains the status code for the completion of the SCSI command code.
	FCP_RES_ID	This field contains a count of the number of

Section	Fields/Controls	Description
		residual data bytes that were not transferred in the FCP_DATA for this SCSI command. The FCP_RES_ID is functional only if the FCP_RESID_OVER or FCP_RESID_UNDER bit is set to one.
	FCP_CONF_REQ	If selected, transmits an FCP_CONF to confirm receipt of the FCP_RSP Sequence.
	FCP_RESID_UNDER	If selected, indicates that the FCP_RESID field is valid and contains the number of bytes that were expected to be transferred, but were not transferred. The application client examines the FCP_RESID field in the context of the command to determine whether or not an error condition occurred.
	FCP_RESID_OVER	If selected, indicates that the FCP_RESID field is valid and contains the count of bytes that cannot be transferred because the FCP_DL was not sufficient. The application client should examine the FCP_RESID field in the context of the command to determine whether or not an error condition occurred.
	FCP_SNS_REQ	If selected, specifies the number of valid bytes of FCP_SNS_INFO.
		Click to open the *SNS_Info Configuration* dialog. NOTE This button is enabled if FCP_SNS_REQ check box is selected. Refer *SNS_Info Configuration* for more information.
	FCP_RSP_REQ	If selected, specifies the number of valid bytes of FCP_RSP_INFO. The options in the list are as follows: • Task Management Function Complete • FCP_DATA length different than FCP_BURST_LEN • FCP_CMND fields invalid • FCP_DATA Parameter mismatch with FCP_DATA_RO • Task Management Function Rejected • Task Management Function Failed
FCP_XFER_RDY	The options in this section are enabled only if *Data Descriptor (FCP_XFER_RDY)* option is selected as the information unit. FCP_XFER_RDY indicates that the target is ready to receive a part or	

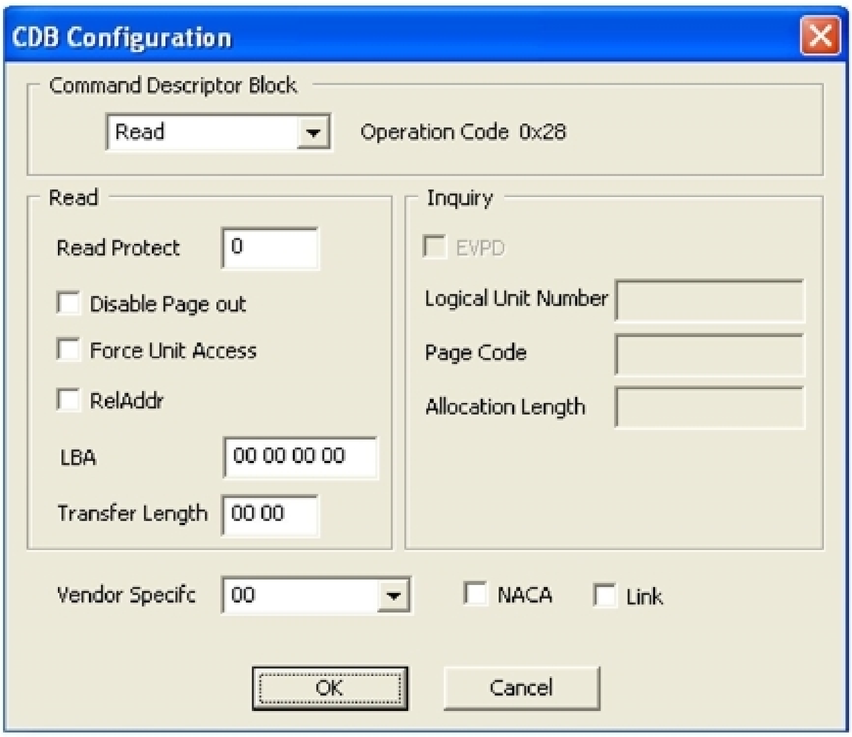
Section	Fields/Controls	Description
	all of the data for a write command. The FCP_XFER_RDY contains parameters such as the length and initial relative offset of the FCP_DATA as requested and required by the initiator.	
	FCP_DATA_RO	This field contains the value that specifies the relative offset in the PARAMETER field for the first data byte of the requested FCP_DATA. The default value is 00 00 00 00.
	FCP_BURST_LEN	This field contains the value that specifies the amount of buffer space prepared for the next FCP_DATA and requests the transfer from the initiator of an IU of that length. The value in the FCP_BURST_LEN field is the same as the SCSI data delivery request byte count. The default value is 00 00 00 00.

CDB Configuration

The Command Descriptor Block (CDB) is a structure that is used to communicate a command from an application client to a device server. The SCSI CDB defines the operation to be performed by the device server. If an invalid parameter is detected in the CDB by the logical unit, no command is processed by the logical unit.

The *CDB Configuration* dialog is shown in *Figure:CDB Configuration dialog*.

Figure:CDB Configuration dialog



The fields and controls in this dialog are described in *Table:CDB Configuration dialog*.

Table:CDB Configuration dialog

Section	Fields/Controls	Description
Command Descriptor Block	The CDB command options in the list are as follows: • Read • Write • Inquiry	
	Operation Code 0x28	The first byte in the CDB.
Read	Read Protect	Sends a READ command to return data to an application client. NOTE This section is enabled only if *Read* option is selected in the *Command Descriptor Block* list.
	Disable Page Out	If selected, allows the initiator to warn the target that the data being read is unlikely to be requested again soon and so is not worth keeping in the target's data cache.
	Force Unit Access	If selected, initiates the target to fetch data from the media surface and not to use a cached copy of data.
	RelAddr	If selected, this bit is used to indicate that the LBA value is relative.
	LBA	The Logical Block Addressing value.
	Transfer Length	The 16 bit Transfer Length field used by the Read command.
Write	Write Protect	Sends a WRITE command to return data to an application client. NOTE This section is enabled only if *Write* option is selected in the *Command Descriptor Block* list.
	Disable Page Out	If selected, allows the initiator to warn the target that the data being written is unlikely to be requested again soon and so is not worth keeping in the target's data cache.
	Force Unit Access	If selected, initiates the target to fetch data from the media surface and not to use a cached copy of data.
	RelAddr	If selected, this bit is used to indicate that the LBA value is relative.
	LBA	The Logical Block Addressing value.
	Transfer Length	The 16 bit Transfer Length field used by the Read command.
Inquiry	Sends an ENQUIRY command to return data to an application client. NOTE This section is enabled only if *Inquiry* option is selected in the *Command Descriptor Block* list.	

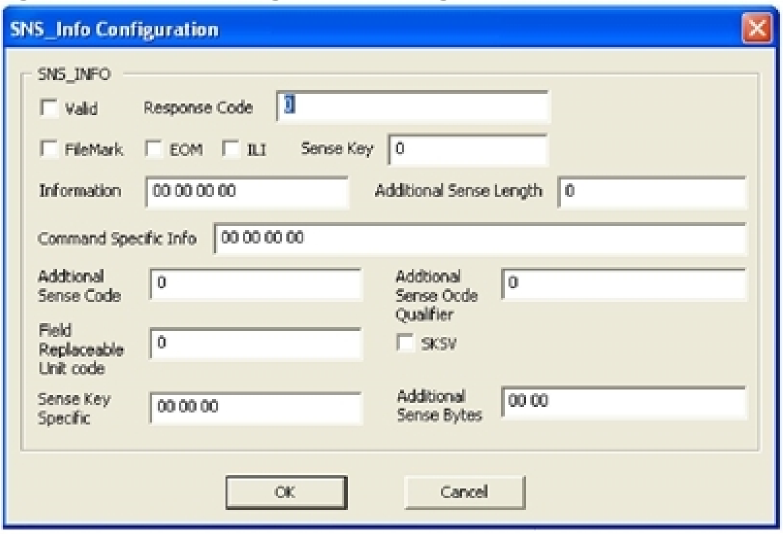
Section	Fields/Controls	Description
	EVPD	If selected, enables Vital Product Data.
	Logical Unit Number	The 3 bit identifier for a logical unit.
	Page Code	The page code parameter byte. If EVPD parameter bit is zero and the Page Code parameter byte is zero, the target returns the standard enquiry data.
	Allocation Length	The allocation length of the Inquiry command.
Vendor Specific		Specification of the referenced item is determined by the SCSI device vendor. The options in the list are as follows: • 00 • 01 • 10 • 11
NACA		The Normal Automatic Contingent Allegiance (NACA) bit specifies whether an ACA is established if the command returns with CHECK CONDITION status. If selected and NACA bit is set to one, an ACA is established. If cleared and NACA bit is set to zero, ACA is not established.
Link		If selected, establishes the link.

SNS_Info Configuration

The SNS_Info field for FCP contains the autosense data. The proper SNS_INFO is presented when the SCSI status byte of CHECK CONDITION is presented. If no condition requiring the presentation of SCSI sense data has occurred, the SNS_INFO field is not included in the FCP_RSP IU. The FCP_SNS_LEN_VALID bit is then zero. In this case, FCP devices to perform autosense.

The *SNS_Info Configuration* dialog is shown in *Figure:SNS_Info Configuration dialog*.

Figure:SNS_Info Configuration dialog

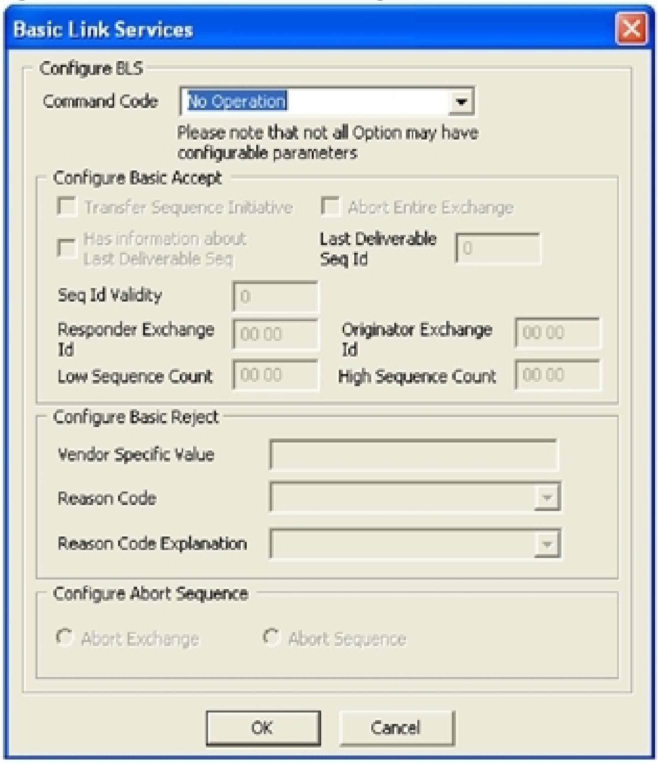


Basic Link Services

Basic Link Services are single frame, single sequence commands that are embedded in an unrelated exchange. Basic Link Services commands consist of only a single Basic Link_ Data frame and are interspersed or are a part of a Sequence for an Exchange performing a specific protocol other than Basic Link Service. Basic Link Service commands support low-level functions and login is not required before using such commands.

The *Basic Link Services* dialog is shown in *Figure:Basic Link Services dialog*.

Figure:Basic Link Services dialog



The fields and controls in this dialog are described in *Table:Basic Link Services dialog*.

Table:Basic Link Services dialog

Section	Fields/Controls	Description
Command Code	The Command Code list contains the Basic Link Service commands. The options in the list are as follows: • No Operation • Abort Sequence • Remove Connection • Basic_Accept • Basic_Reject • Dedicated Connection Preempted NOTE Not all command options have configurable parameters. 'No Operation', 'Remove Connection', and 'Dedicated Connection Preempted', do not have configurable parameters in the present scope of Basic Link Service configuration.	
Configure Basic Accept	Basic Accept is a single frame Link Service Reply Sequence that notifies the transmitter of a Basic Link Service Request frame that the request has been completed. NOTE This section is enabled only if *Basic Accept* is selected as the Basic Link Service command.	
	Transfer Sequence Initiative	If selected, the Basic Accept Link Service Reply Sequence transfers the Sequence Initiative by setting the Sequence Initiative bit (Bit 16) to one in F_CTL on the last Data frame of the Reply Sequence.
	Abort Entire Exchange	If selected, aborts the transfer of Sequence Initiative.
	Has Information about Last Deliverable Seq	If selected, provides information about the last delivered Sequence Initiative.
	Last Deliverable Seq Id	Sets the last deliverable Sequence Identifier assigned by the Sequence Initiator.
	Seq Id Validity	The value validating the Sequence Identifier.
	Responder Exchange Id	Exchange Identifiers are used to uniquely identify an Exchange. The Responder assigns Responder ID (RX_ID) that is unique to the Responder or Responder-Originator pair and communicates it to the Originator before the end of the first Sequence of the Exchange.
	Originator Exchange Id	The Originator assigns each new Exchange an Originator Exchange ID (OX_ID) unique to the Originator or Originator-Responder pair and embeds it in all frames of the Exchange.
	Low Sequence Count	Indicates low Sequence Count. The sequence count (SEQ_CNT) is a two-byte field that indicates the sequential order of Data frame transmission within a single Sequence or multiple consecutive Sequences for the same

Section	Fields/Controls	Description
		Exchange.
	High Sequence Count	Indicates high Sequence Count.
Configure Basic Reject	Basic Reject is a single frame Link Service Reply Sequence that notifies the transmitter of a Basic Link Service Request frame that the request has been rejected. NOTE This section is enabled only if *Basic Reject* is selected as the Basic Link Service command.	
	Vendor Specific Value	Specification of the referenced item is determined by the SCSI device vendor. The default value is 0.
	Reason Code	The Basic Reject reason codes in the list are as follows: • Invalid Command Code: The Command code in the Sequence being rejected is invalid. • Logical Error: The request identified by the Command code is invalid or logically inconsistent for the conditions present. • Logical Busy: The Basic Link Service is logically busy and unable to process the request at this time. • Protocol Error: This indicates that an error has been detected that violates the rules of FC-2 protocol that are not specified by other error codes. • Unable To Perform Command Request: The Recipient of a Link Service command is unable to perform the request at this time.
	Reason Code Explanation	The Basic Reject reason codes explanation in the list are as follows: • No Additional Explanation • Invalid OxId-RxId Combination • Sequence Aborted/No Sequence Information Provided
Configure Abort Sequence	Abort Sequence (ABTS) frame is used by the Sequence Initiator to request that the Sequence Recipient abort one or more Sequences and by the Sequence Recipient to request that the ABTS Recipient abort the entire Exchange. NOTE This section is enabled only if *Abort Sequence* is selected as the Basic Link Service command.	
	Abort Exchange	If selected, the Sequence Recipient elects to abort one or more Sequences or elect to abort

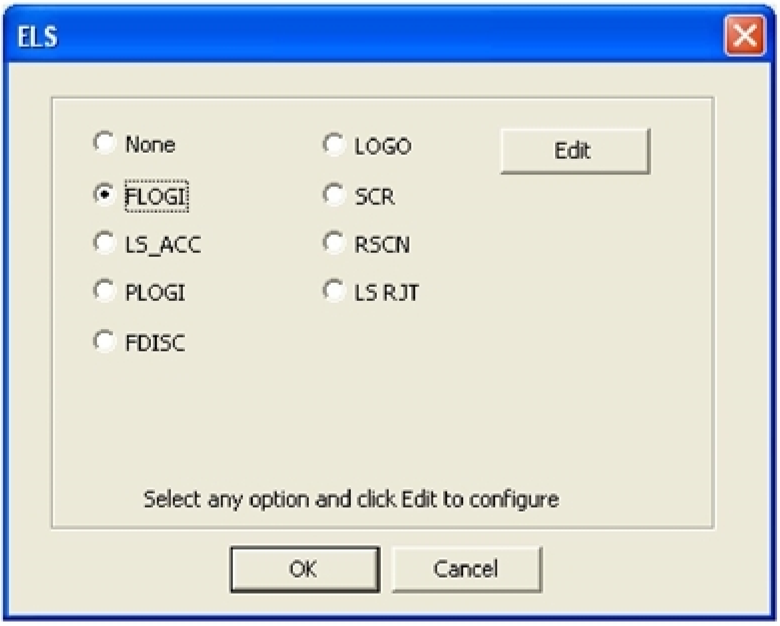
Section	Fields/Controls	Description
		the entire Exchange in a protocol specific manner.
	Abort Sequence	If selected, Sequence Recipient requests that one or more Sequences in progress be aborted by setting the Abort Sequence Condition bits to a value of 01b on an ACK frame.

Extended Link Services (ELS)

An Extended Link Service (ELS) request solicits a destination Nx_Port to perform a function. An ELS reply is transmitted in response to an ELS request, unless otherwise specified. Each request or reply is composed of a single Sequence with the ELS_Command code being specified in the first word of the Payload of the first frame of the Sequence.

The *ELS* dialog is shown in *Figure:Extended Link Services dialog*.

Figure:Extended Link Services dialog



The fields and controls in this dialog are described in *Table:Extended Link Services dialog*.

Table:Extended Link Services dialog

Field	Description
FLOGI	Select the *Flogi* option button and click *Edit* button to open the *FLOGI* configuration dialog. Refer *FLOGI* for more information.
LS_ACC	Select the *LS_ACC* option button and click *Edit* button to open the *Ls_Acc* configuration dialog. Refer *LS_ACC* for more information.
PLOGI	Select the *PLOGI* option button and click *Edit* button to open the *PLOGI* configuration dialog. Refer *PLOGI* for more information.

Field	Description
FDISC	Select the *FDISC* option button and click *Edit* button to open the *F-DISC* configuration dialog. Refer *FDISC* for more information.
LOGO	Select the *LOGO* option button and click *Edit* button to open the *ELS LOGO* configuration dialog. Refer *ELS Logo* for more information.
SCR	Select the *SCR* option button and click *Edit* button to open the *ELS SCR* configuration dialog. Refer *SCR* for more information.
RSCN	Select the *RSCN* option button and click *Edit* button to open the *ELS RSCN* configuration dialog. Refer *RSCN* for more information.
LSRJT	Select the *LSRJT* option button and click *Edit* button to open the *ELS LS_RJT* configuration dialog. Refer *LS RJT* for more information.

FLOGI

NOTE Refer *LS_ACC*, *PLOGI*, and *FDISC* for detailed information on each of these Extended Link services.

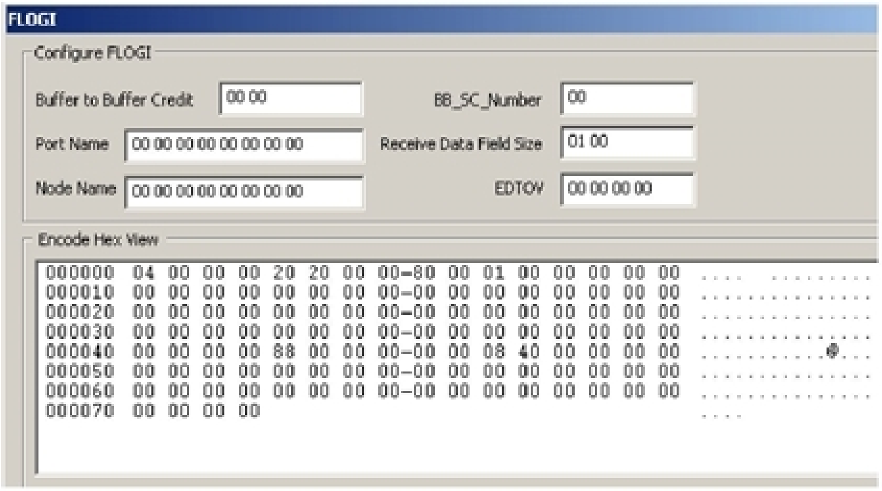
The Fabric Login (FLOGI) ELS transfers Service Parameters from the initiating Nx_Port to the FC_Port associated with the D_ID. The FLOGI frame provides the means by which an Nx_Port requests Login with the Fabric. Login with the Fabric is required for all Nx_Ports, regardless of the class supported. Communication with other Nx_Ports is not attempted until the Fabric Login procedure is complete.

The functions accomplished by a FLOGI login are as follows:

- It determines the presence or absence of a Fabric.
- If a Fabric is present, it provides the Nx_Port with the specific set of operating characteristics associated with the entire Fabric, F_Port_Name and Fabric_Name.
- If a Fabric is present, it provides the Fabric with the specific set of operating characteristics, N_Port_Name and Node_Name of the Nx_Port.
- If a Fabric is present, the Fabric optionally assigns or confirms the N_Port_ID of the Nx_Port that initiated the Login.
- If a Fabric is present, it initializes the buffer-to-buffer Credit.
- If the Nx_Port and the Fabric support Authentication, it enables the subsequent Nx_Port to Fabric Authentication.
- If the N_Port and the Fabric support Virtual Fabrics, it enables the subsequent negotiation of Virtual Fabrics parameters.

The *FLOGI* dialog is shown in *Figure:FLOGI dialog.*

Figure:FLOGI dialog



The fields and controls in this dialog are described in *Table:FLOGI dialog*.

Table:FLOGI dialog

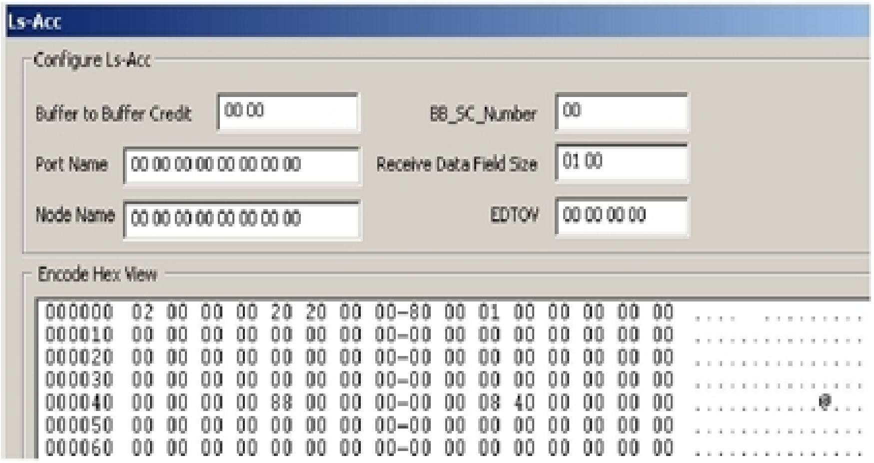
Field	Description
Buffer to Buffer Credit	It is the limiting value for BB_Credit_CNT in the buffer-to-buffer flow control model. If a Fabric is present, FLOGI initializes the buffer-to-buffer Credit.
BB_SC_ Number	The Buffer-to-buffer State Change Number (BB_SC_N) field specifies the Buffer-to-buffer State Change Number. It indicates that the sender of the FLOGI frame is requesting BB_SC_N number of frames to be sent between two consecutive BB_SCs primitives, and 2BB_SC_ N number of R_RDY primitives to be sent between two consecutive BB_SCr primitives.
Port Name	The eight-byte field that identifies an FC_Port.
Node Name	The eight-byte name identifier associated with a node.
Receive Data Field Size	The field size of the data received from the FC_Port.
EDTOV	The EDTOV value.
Encode Hex View	The coded hexadecimal view.
	Click this button to decode.

LS_ACC

The Link Service Accept (LS_ACC) ELS reply Sequence notifies the originator of an ELS request that the ELS request Sequence has been completed. The Responder terminates the Exchange by setting the Last Sequence bit (Bit 20) in F_CTL on the last Data frame of the reply Sequence. The first byte of the Payload contains 02h. The remainder of the Payload is unique to the ELS request.

The Ls_Acc dialog is shown in *Figure:LS_ACC dialog*.

Figure:LS_ACC dialog



The fields and controls in this dialog are described in *Table:LS_ACC dialog*.

Table:LS_ACC dialog

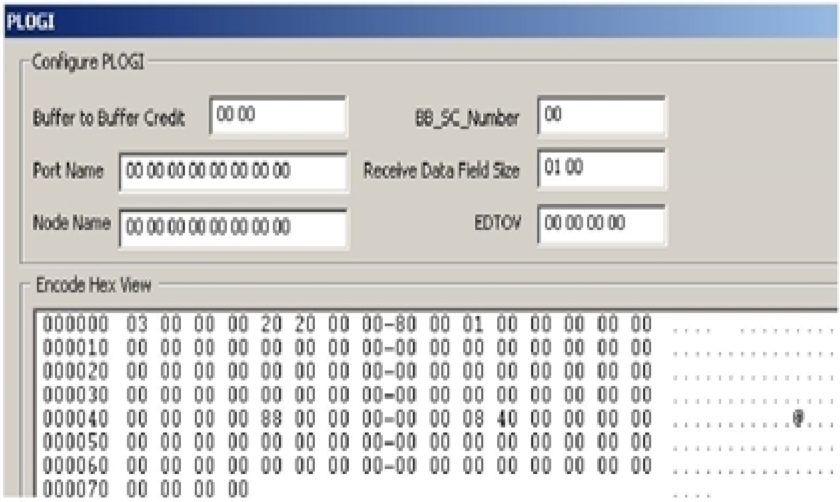
Field	Description
Buffer to Buffer Credit	It is the limiting value for BB_Credit_CNT in the buffer-to-buffer flow control model.
BB_SC_ Number	The Buffer-to-buffer State Change Number (BB_SC_N) field specifies the Buffer-to-buffer State Change Number. It indicates that the sender of the FLOGI frame is requesting BB_SC_N number of frames to be sent between two consecutive BB_SCs primitives, and 2BB_SC_ N number of R_RDY primitives to be sent between two consecutive BB_SCr primitives.
Port Name	The eight-byte field that identifies an FC_Port.
Node Name	The eight-byte name identifier associated with a node.
Receive Data Field Size	The field size of the data received from the FC_Port.
EDTOV	The EDTOV value.
Encode Hex View	The coded hexadecimal view.
Decode	Click this button to decode.

PLOGI

The PLOGI ELS transfers Service Parameters from the initiating Nx_Port to the FC_Port associated with the D_ID. The PLOGI frame provides the means by which an Nx_Port requests Login with another Nx_Port before other Data frame transfers.

The *PLOGI* dialog is shown in *Figure:PLOGI dialog*.

Figure:PLOGI dialog



The fields and controls in this dialog are described in *Table:PLOGI dialog*.

Table:PLOGI dialog

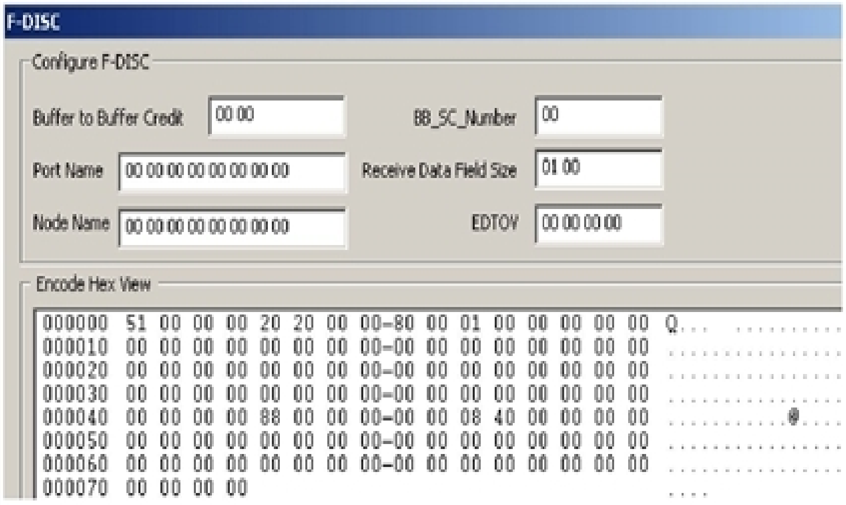
Field	Description
Buffer to Buffer Credit	It is the limiting value for BB_Credit_CNT in the buffer-to-buffer flow control model.
BB_SC_ Number	The Buffer-to-buffer State Change Number (BB_SC_N) field specifies the Buffer-to-buffer State Change Number. It indicates that the sender of the FLOGI frame is requesting BB_SC_N number of frames to be sent between two consecutive BB_SCs primitives, and 2BB_SC_ N number of R_RDY primitives to be sent between two consecutive BB_SCr primitives.
Port Name	The eight-byte field that identifies an FC_Port.
Node Name	The eight-byte name identifier associated with a node.
Receive Data Field Size	The field size of the data received from the FC_Port.
EDTOV	The EDTOV value.
Encode Hex View	The coded hexadecimal view.
	Click this button to decode.

FDISC

The Discover F_Port Service Parameters (FDISC) ELS transfers Service Parameters from the initiating Nx_Port to the Fx_Port at well-known F_Port_ID. This provides the means for the exchange of Service Parameters and the assignment of an additional N_Port_IDs without changing service parameters.

The *F-DISC* dialog is shown in *Figure:F-DISC dialog*.

Figure:F-DISC dialog



The fields and controls in this dialog are described in *Table:F-DISC dialog*.

Table:F-DISC dialog

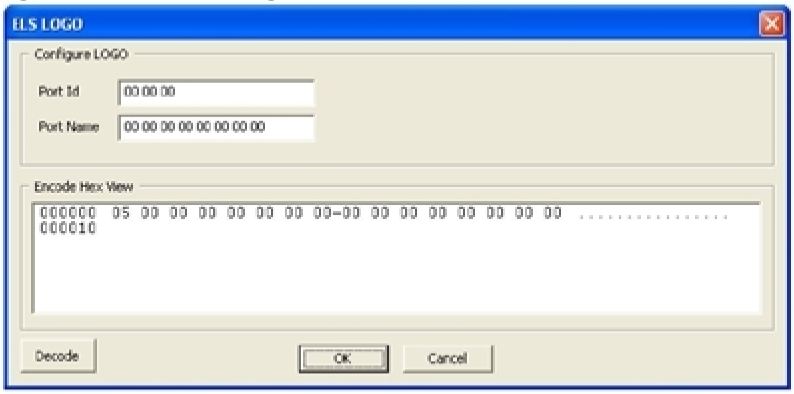
Field	Description
Buffer to Buffer Credit	It is the limiting value for BB_Credit_CNT in the buffer-to-buffer flow control model.
BB_SC_ Number	The Buffer-to-buffer State Change Number (BB_SC_N) field specifies the Buffer-to-buffer State Change Number. It indicates that the sender of the FLOGI frame is requesting BB_SC_N number of frames to be sent between two consecutive BB_SCs primitives, and 2BB_SC_ N number of R_RDY primitives to be sent between two consecutive BB_SCr primitives.
Port Name	The eight-byte field that identifies an FC_Port.
Node Name	The eight-byte name identifier associated with a node.
Receive Data Field Size	The field size of the data received from the FC_Port.
EDTOV	The EDTOV value.
Encode Hex View	The coded hexadecimal view.
Decode	Click this button to decode.

ELS Logo

The LOGO ELS provides a method for explicitly removing service between two Nx_Port_IDs or between an N_Port_ID and a Fabric. Logout releases resources, identifiers, and relationships associated with maintaining service between an Nx_Port_ID and a destination Nx_Port_ID or Fabric.

The ELS LOGO dialog is shown in *Figure:ELS LOGO dialog*.

Figure:ELS LOGO dialog



The fields and controls in this dialog are described in *Table:ELS LOGO dialog*.

Table:ELS LOGO dialog

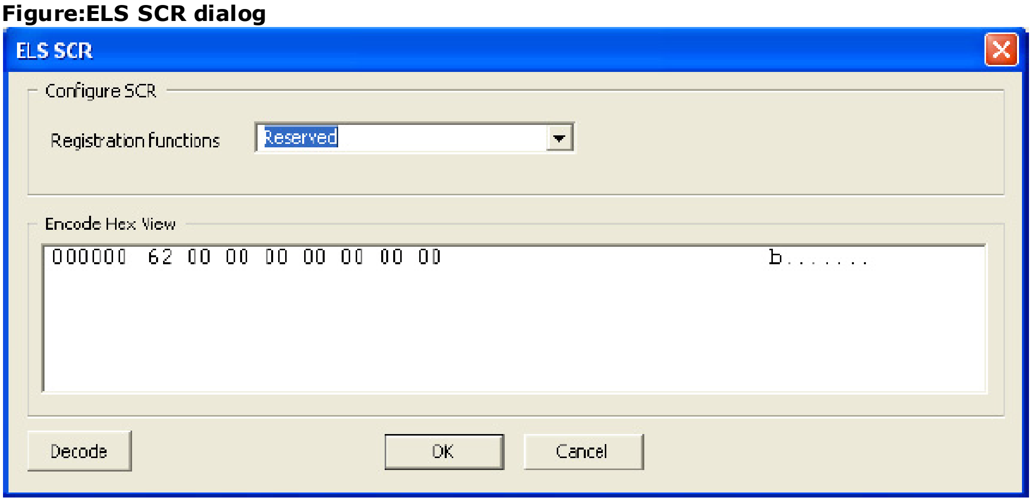
Field	Description
Port Id	The unique address identifier of the FC Port.
Port Name	The eight-byte field that identifies the FC Port.
Encode Hex View	The coded hexadecimal view.
	Click this button to decode.

SCR

The State Change Registration (SCR) ELS requests the Fabric Controller or Nx_Port to add the Nx_Port that is sending the SCR Request to the list of Nx_Ports registered to receive the RSCN ELS.

The *ELS SCR* dialog is shown in *Figure:ELS SCR dialog*.

Figure:ELS SCR dialog



The fields and controls in this dialog are described in *Table:ELS SCR dialog*.

Table:ELS SCR dialog

Field	Description
Registration functions	The Registration Functions for SCR are available in the following formats:

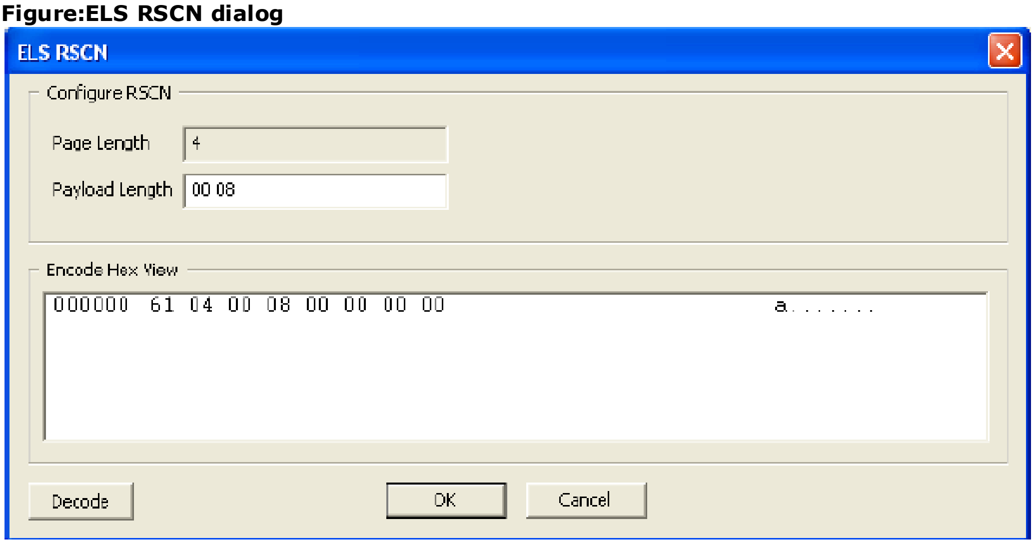
Field	Description
	• Reserved: The reserved format with value 0. • Fabric Detection Registration: Register to receive all RSCN Requests issued by the Fabric Controller for events detected by the Fabric. • Nx-Port Detected Registration: Register to receive all RSCN Requests issued for events detected by the affected Nx_Port. • Full Registration: Register to receive all RSCN Requests issued. The RSCN Request returns all affected N_Port_ID pages. • Clear Registration: Removes any current RSCN registrations.
Encode Hex View	The coded hexadecimal view.
	Click this button to decode.

RSCN

The Registered State Change Notification (RSCN) ELS is sent to registered Nx_Ports when an event occurs that may have affected the state of one or more Nx_Ports, or the ULP state within the Nx_Port. The term, state, is used here to refer to any condition of an Nx_Port that is considered important enough to notify other Nx_Ports of a change in that state. The RSCN provides an indication of the change of state that is being reported.

RSCN is intended to provide a timely indication of changes in nodes to avoid the considerable traffic that polling may generate. RSCN may be used to indicate a failed node, allowing the release of resources tied up by the failed node. RSCN may also be used to notify interested nodes of new devices coming online, and of changes within an online node that affect the operation of the system. The sender of the RSCN Request may coalesce several events into a single report.

Figure:ELS RSCN dialog



The fields and controls in this dialog are described in *Table:ELS RSCN dialog*.

Table:ELS RSCN dialog

Field	Description
Page Length	This field is the length in bytes of an affected Port_ID page. This value is fixed at 04h.

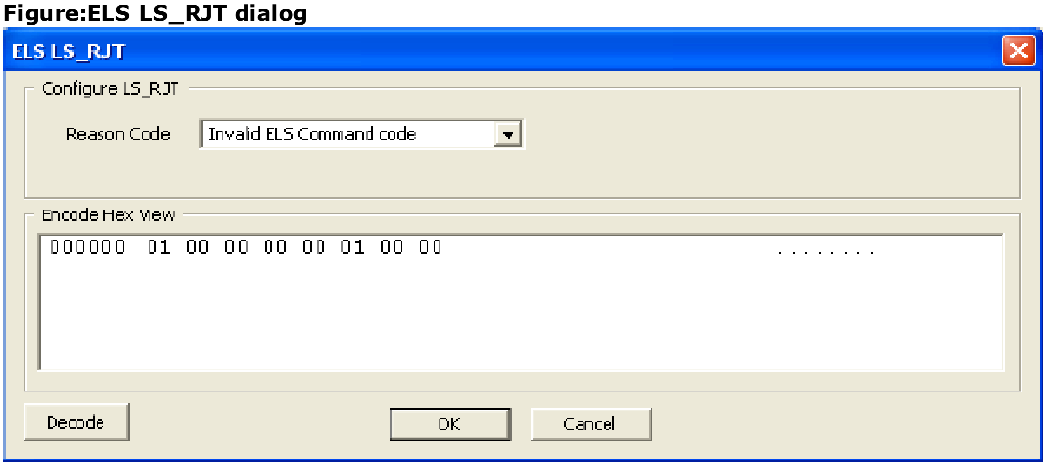
Field	Description
Payload Length	This field is the length in bytes of the entire Payload, inclusive of the word 0. This value is a multiple of 4 bytes. The minimum value of this field is 8 bytes. The maximum value of this field is 1024 bytes.
Encode Hex View	The coded hexadecimal view.
	Click this button to decode.

LS RJT

The Link Service Reject (LS_RJT) notifies the transmitter of a Link Service request that the Link Service request Sequence has been rejected. A four-byte reason code is contained in the Data Field. Link Service Reject is transmitted for a variety of conditions that are unique to a specific Link Service request. For example, if the Service Parameters specified in a Login frame were logically inconsistent or in error, a P_RJT frame would not be transmitted in response, but rather a Link Service Reject.

The ELS LS_RJT dialog is shown in *Figure:ELS LS_RJT dialog*.

Figure:ELS LS_RJT dialog



The fields and controls in this dialog are described in *Table:ELS LS_RJT dialog*.

Table:ELS LS_RJT dialog

Field	Description
Reason Code	The ELS LS_RJT reason codes are as follows: • Invalid ELS Command code: The ELS_Command code in the Sequence being rejected is invalid. • Logical Error: The request identified by the ELS_Command code and Payload content is invalid or logically inconsistent for the conditions present. • Logical busy: The Link Service is logically busy and unable to process the request at this time. • Protocol Error: This indicates that an error has been detected that violates the rules of the ELS Protocol that are not specified by other error codes. • Unable to Perform Command: The Recipient of a Link Service command is unable to perform the request at this time.

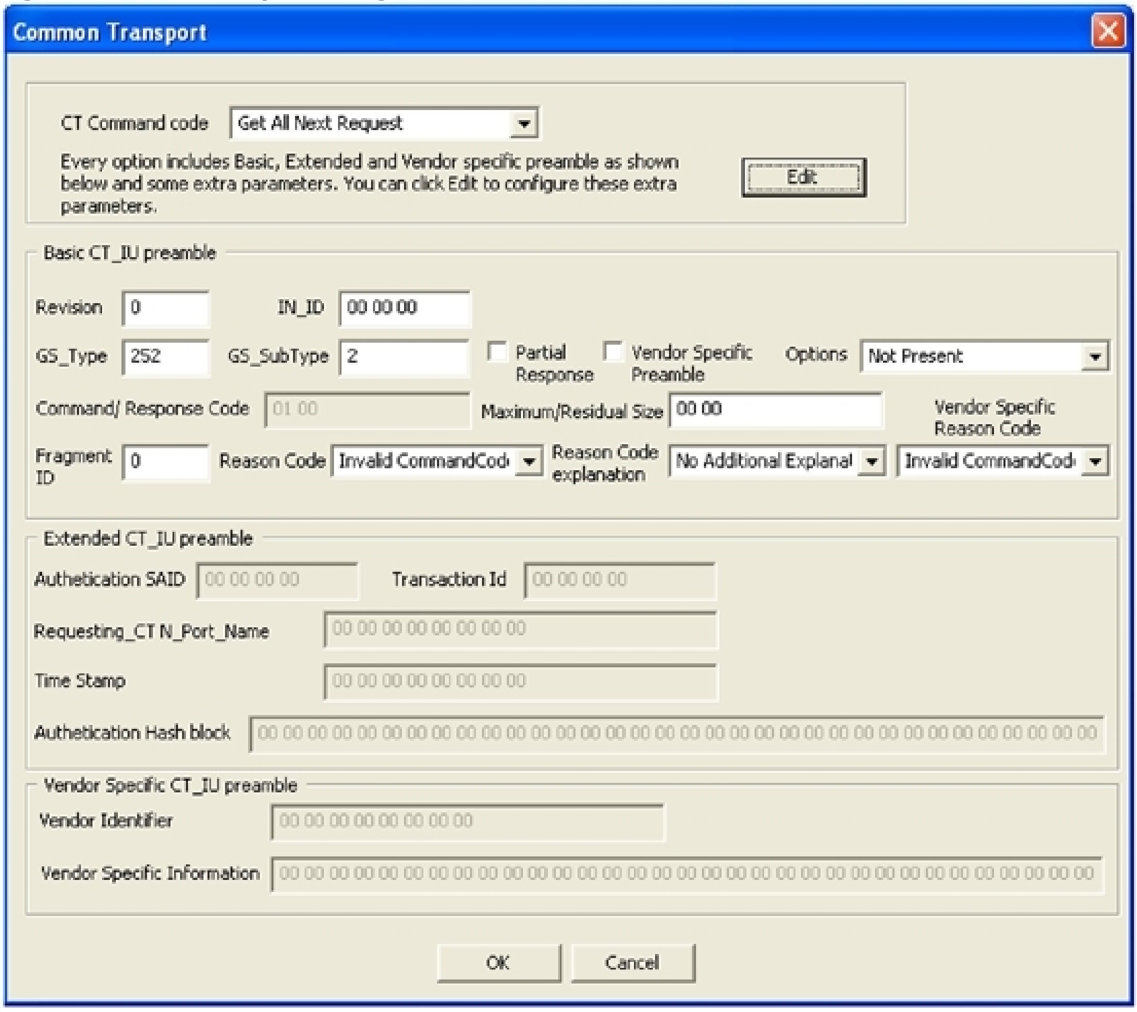
Field	Description
	• Command Not Supported: The Recipient of a Link Service command does not support the command requested. • Command Already In Progress: The command progress is tracked. • Vendor Specific Error: The Vendor specific error bits may be used by Vendors to specify additional reason codes.
Encode Hex View	The coded hexadecimal view.
Decode	Click this button to decode.

Common Transport (CT)

Fibre Channel Generic Services share a Common Transport (CT) at the FC-4 level. The CT provides access to a Service with a set of service parameters that facilitates the usage of Fibre Channel properties. It also provides another level of multiplexing that simplifies the Server-to-Server communication for a distributed Service.

The Common Transport dialog is shown in *Figure:Common Transport dialog*.

Figure:Common Transport dialog



The fields and controls in this dialog are described in *Table:Common Transport dialog*.

Table:Common Transport dialog

Section	Fields/Controls	Description
CT Command Code	The Common Transport Command code options. The options in the list are as follows: • Get All Next Request • Get All Next Accept • Get Port Name Request • Get Port Name Accept • Get Node Name Request • Get Node Name Accept • Get FC4 Type Request • Register Node Name Request NOTE Each CT Command code is included in Basic, Extended, and Vendor Specific preamble.	
	Edit	Click to open the *Common Transport Configuration* dialog where you can configure various parameters for the selected CT Command Code.
Basic_CT_IU preamble	The 16-byte basic format in the Common Transport Information Unit preamble. It is shown as follows:	

Basic_CT_IU Preamble Format

Word Bits	3322 2222 1098 7654	2222 1111 3210 9876	1111 1100 5432 1098	0000 0000 7654 3210
0	Revision	IN_ID		
1	GS_Type	GS_Subtype	Options	Reserved
2	Command/Response code		Maximum/Residual Size	
3	Fragment ID	Reason code	Reason Code Explanation	Vendor Specific

Section	Fields/Controls	Description
	Revision	This field denotes the revision of the CT protocol. If the revision version is 01h or 02h, it denotes a prior revision of the protocol. The default value is 0.
	GS_Type	This field denotes the type of Generic Service. The default value is 252.
	Command/Response Code	This field indicates whether the CT IU is a request or a response. If the CT_IU is a request, this field specifies the command to be performed. If the CT_IU is a response, this field indicates whether the request was accepted or rejected.

Section	Fields/Controls	Description
		The valid Command/Response code values are as follows: • Request CT_IU (0001-03FF) • Reserved for FC-SW-3 (0400-05FF) • Request CT_IU (0600-7EFF) • Common Request CT_IU (7F00-7FFF) • Reject Response CT_IU (8001) • Accept Response CT_IU (8002) • Reserved for FC-SW-3 (E000-FFFF) • Reserved (other values)
	Fragment ID	This field contains a value that identifies the fragment contained in the IU. The value contained in this field in the Request CT_IU is echoed by the service in the associated Response CT_IU.
	IN_ID	This field is provided to allow distributed Servers to communicate the identity of the original requestor. This field is not intended to enable third-party responses by distributed Servers. This field is set to zero by the Requesting_CT.
	GS_SubType	This field is used to indicate second level routing behind the N_ Port. It indicates the specific Server behind the Generic Service. The values in this field are provided by the individual service.
	Reason Code	This field contains the reason code associated with a Reject CT_IU. This field is reserved when the Command/Response code field indicates the CT_IU is not a Reject CT_IU. The Reason Code options in the list are as follows: • Invalid CommandCode: The command code passed in the Request CT_IU is not defined by the Server. • Invalid VersionLevel: The specified version level is not supported by the Server. • Logical Error: The request identified by the Request CT_IU command code and additional

Section	Fields/Controls	Description
		information content is invalid or logically inconsistent for the conditions present. • Invalid Ct Iu Size: The CT IU size is invalid for the Request CT IU command code. • Logical Busy: The Server is logically busy and unable to process the request at this time. • Protocol Error: This indicates that an error has been detected that violates the rules of the Server protocol that are not specified by other error codes. • Unable to PerformCommand Request: The Server is unable to perform the request. • Command Not Supported: The Server does not support the command requested. • Server Not Available: The server identified by the GS_Type and GS_Subtype is not available. • Session Could Not Be Established: A server session could not be established. • Vendor Specific Error: The Vendor Specific Field may be used by Vendors to specify additional reason codes.
	Partial Response	If selected, indicates that the response is incomplete. For example, when a Server is distributed amongst several switches, if one or more of the switches fails to respond, the Partial Response bit is used to indicate that those switches did not participate in the response cycle.
	Maximum/Residual Size	This field manages the size of the information returned in an Accept CT_IU. The default value is 00 00.
	Reason Code explanation	This field contains a reason code explanation associated with a Reject CT_IU. This field is reserved when the Com-

Section	Fields/Controls	Description
		mand/Response code field indicates that the CT_IU is not a Reject CT_IU. The options in the field are as follows: • No Additional Explanation • Authorization Exception • Authentication Exception • DataBase Full • DataBase Empty • Processing Request • Unable To Verify Connection • Devices Not In Common Zone
	Vendor Specific Preamble	If selected, enables the *Vendor Specific CT_IU Preamble* section in the *Common Transport* section. This field contains a vendor specific reason code associated with a Reject CT_IU. This field is reserved when the Command/Response code field indicates that the CT_IU is not a Reject CT_IU.
	Options	This field denotes options used by the Requesting_CT or Responding_CT. The options are as follows: • Not Present • Retain Residual Info1 • Retain Residual Info2 • Transaction Id Valid1 • Transaction Id Valid2
	Vendor Specific reason Code	This field is associated with a Reject CT_IU.
Extended CT_IU preamble	The 88-byte extended format in the Common Transport Information Unit preamble. It is preceded by the 16-bytes basic CT IU preamble. NOTE This section is enabled if any option, other than 'Not Present,' is selected in the *Options* list in *Basic_CT_IU preamble* section.	
Extended_CT_IU Preamble Format		

Section	Fields/Controls	Description

Word Bits	3322 2222 1098 7654	2222 1111 3210 9876	1111 1100 5432 1098	0000 0000 7654 3210
4	Authentication SAID			
5	transaction_id			
6...7	Requesting_CT N_Port_Name			
8...9	Time Stamp			
10...25	Authentication Hash Block			

Section	Fields/Controls	Description
	Authentication SAID	This field denotes the Secured Association Identifier that uniquely identifies the algorithm and key used to generate the Authentication Hash Block, as prearranged between the Requesting_CT and the Responding_CT. The default value is 00 00 00 00.
	Requesting_CT N_Port_Name	This field contains the value of the N_Port_Name of the Requesting_CT. The Responding_CT responds by using the same encoded N_Port_Name value in the Accept CT_IU or Reject CT_IU as is supplied in the Request CT_IU.
	Time Stamp	This field contains a time stamp value set by the CT sending the CT_IU. The Requesting_CT sets this value according to its time reference when it sends the CT_IU. The Responding_CT sets this value according to its time reference when it sends the CT_IU, or it may echo the value sent by the Requesting_CT. In all cases, the value of the time stamp consistently increases.
	Authentication Hash block	This field contains the encoded value of the hash generated by the identified algorithm and key.
	Transaction Id	This field contains an opaque value. The opaque value is not validated by the Responding_CT. The Responding_CT responds by using the same encoded transaction_id value in the Accept CT_IU or Reject CT_IU as is supplied in the Request CT_IU.
Vendor Specific CT_IU preamble	The vendor specific format in the Common Transport Information	

Section	Fields/Controls	Description
	Unit preamble. The *Options* field in the Basic CT IU preamble indicates whether the Vendor Specific preamble is present. If the Vendor Specific preamble is present, it immediately follows the Basic CT_IU preamble if no Extended CT_IU preamble exists, or it immediately follows the Extended CT_IU preamble if that preamble exists. NOTE This section is enabled if Vendor Specific Preamble check box in *Basic_CT_IU preamble* section is selected.	

Vendor Specific_CT_IU Preamble Format

Word Bits	3322 2222 1098 7654	2222 1111 3210 9876	1111 1100 5432 1098	0000 0000 7654 3210
0..1	Vendor Identifier			
2...33	Vendor Specific Information			

Section	Fields/Controls	Description
	Vendor Identifier	This field contains the T10 Vendor ID of the vendor that defines the content of the Vendor Specific Information field.
	Vendor Specific Information	This field contains 32 words of vendor specific information.

Chapter 7 - Frame Data–User Defined Fields (UDF)

The *Frame Data* tab in the *Stream Properties* dialog provides control over all aspects of packets transmitted by the Ixia hardware. These frames are also referred to as datagrams or packets in some contexts. Many frames may be generated in the processing of a stream. Many of the controls available allow the specification of a series of values applied to subsequent frames.

This chapter discusses UDF frame data structure. For other parts of frame data construction, see:

- Chapter 5, *Frame Data–Basic Frame Structure*
- Chapter 6, *Frame Data–Protocol Control*

This chapter covers:

- *User Defined Fields*
- *UDF Counters for Individual Bytes*
- *UDF for XDM10G32S Load Module*
- *UDF for Lava Load Module*
- *UDF Configurable Step Size*
- *Standard UDF Configuration*
- *Advanced UDFs*
- *Table UDF*

User Defined Fields

The User Defined Fields (UDF) control an independent 32-bit counter. There are several variations for the UDF fields, depending on the module. For all modules, at least four UDFs can be configured. For newer modules, five UDFs can be configured.

For many modules a *Table UDF* is available. *Table UDF* for more information. For a breakdown of which modules have specific UDF features, see Table 1-7 part 3 in the *Ixia Platform Reference Manual*.

For some modules there is a special set of UDFs with additional options. *Advanced UDFs* for additional information.

Table:UDF Characteristics per Module summarizes these variations.

Table:UDF Characteristics per Module

Module	Has UDF5	Has UDF8	Has Table UDF	Advanced UDFs
LM100TX / LM100TX3				
LM100TX8	X			X
LM100TXS8	X			X
LM100MII				
ALM1000T8 (no packet streams)				
ASM1000XMV12X-01	X		X	X
CPM1000T8 (no packet streams)				

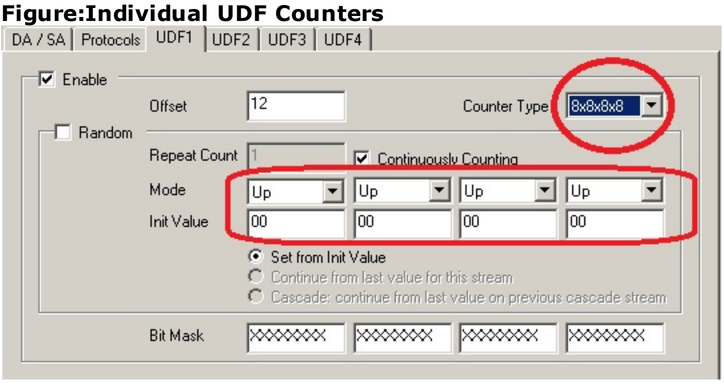
Module	Has UDF5	Has UDF8	Has Table UDF	Advanced UDFs
ELM1000ST2 (no packet streams)				
LM1000T-5				
LM1000TX4 / LM1000TXS4	X		X	X
LM1000STX2	X		X	X
LM1000STX4	X		X	X
LM1000STXS2	X		X	X
LM1000STXS4	X		X	X
LSM1000XMS12-01 / LSM1000XMSR12-01	X		X	X
LSM1000XMV16-01 / LSM1000XMVR16-01	X		X	X
OLM1000STX24 / OLM1000STXS24	X		X	X
LM100FX / LM100FXSM				
LM1000SX / LM1000SX3				
LM1000LX				
LM1000GBIC / LM1000GBIC-P1				
LM1000SFP4 / LM1000SFPS4	X		X	X
LM622MR / LM622MR-512	X		X	X
LMOC12c / LMOC3c				
LMOC48c POS / LMOC48c POS-M				
LMOC48c BERT / LMOC48 POS BERT				
LMOC48VAR				
LMOC192cPOS			X	
LMOC192c VSR-POS			X	
LMOC192c BERT				
LMOC192c VSR-BERT				
LMOC192c POS+BERT			X	
LMOC192c VSR-POS+BERT			X	
LMOC192c POS+WAN			X	
LMOC192c POS+BERT+WAN			X	
LM10GE LAN / LM10GE LAN-M			X	
LM10GE WAN			X	
LSM10G1-01	X		X	X
LSM10GL1-01	X		X	X
LSM10GXL6-01	X		X	X
LM10GE XAUI			X	
LM10GE XAUI+BERT			X	
LM10GE XAUI BERT only			X	
LM10GE XENPAK / LM10GE XENPAK-M			X	
LM10GE XENPAK+BERT / LM10GE XENPAK-MA+BERT			X	

Module	Has UDF5	Has UDF8	Has Table UDF	Advanced UDFs
LM10GE XENPAK BERT only			X	
LM10G			X	
LSM10GXM3-01 / LSM10GXMR3-01	X		X	X
LSM10GXM4-01 / LSM10GXMR4-01	X		X	X
LSM10GXM8-01 / LSM10GXMR8-01	X		X	X
MSM2.5G1-01	X		X	X
MSM10G1-01	X		X	X
PLM1000T4-PD (no packet streams)				
LSM1000POE4-02 (no packet streams)				
AFM1000SP-01 (no packet streams)				
XDM10G32S		X		

UDF Counters for Individual Bytes

The Gigabit, LM-GBIC, LM100TX, LMOC12c/LMOC3c POS and LM1000T-5 modules have an option for configuring complex variations of the 32-bit counter, byte-by-byte, as shown for a Gigabit module in *Figure:Individual UDF Counters*. In this example, the counter has been divided into four 8-bit counters, each with an 8-bit mask.

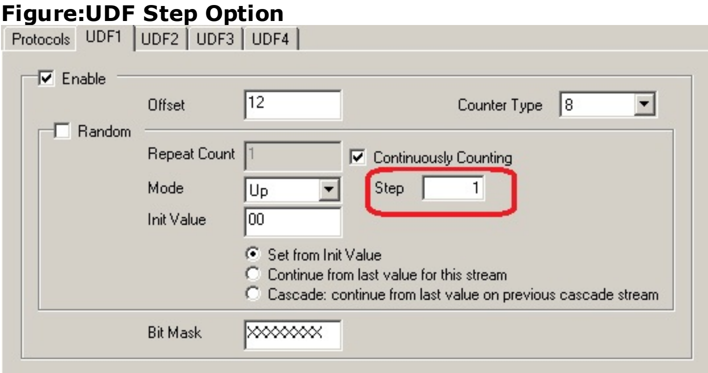
Figure:Individual UDF Counters



UDF Configurable Step Size

Some load modules also have a configurable step size for counting, as shown in *Figure:UDF Step Option*.

Figure:UDF Step Option



The fields and controls in these dialogs are described in *Table:User Defined Fields, Standard*.

Standard UDF Configuration

For load modules with 4 UDFs, the fields are defined in the following table. (**Note**: Not all modules have all these fields.) Refer to *Table:UDF Characteristics per Module*to identify modules that do not have 5 UDFs..

Table:User Defined Fields, Standard

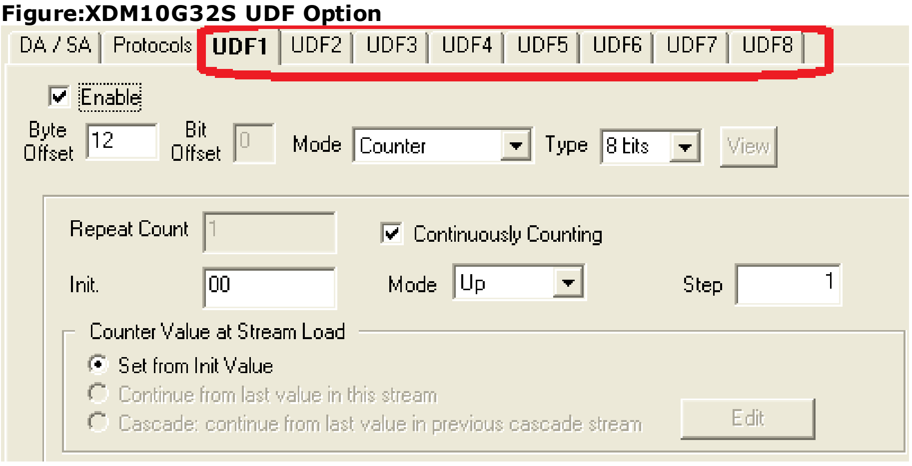
Field/Control	Description
Enable	Must be selected for the particular UDF to be active.
Offset	The offset from the start of the frame (in bytes).
Counter Type	The use and division of the 32-bit counter. The values '8,' '16,' '24,' and '32' indicate counters of their respective lengths. For modules that support configuration of individual bytes, the following counter types are available: • 8 • 16 • 8x8 • 24 • 16x8 • 8x16 • 8x8x8 • 32 • 24x8 • 16x16 • 16x8x8 • 8x24 • 8x16x8 • 8x8x16 • 8x8x8x8
Random	If selected, the counter values will change randomly, and the configuration fields in the box will be dimmed.
Repeat Count/Continuous Counting	If the Continuous Counting check box is selected, then the counter will continuously count. If not, then the value in the Repeat Count field is used to control the number of times that the counter will increment. When the Repeat Count is exhausted, the value resets to 0 and counting is continued.
Mode	Up or Down controls the direction of counting.
Step	(LMOC48c, LMOC-192c, & 10 Gig modules) The increment step for Up or Down increment mode can be specified. (Default = 1).
Init Value	The initial value for the counter, as masked by the Bit Mask Value.

Field/Control	Description
	This value will be incremented or decremented by the value specified in the *Step* field.
Set from Init Value	If selected, the counter resets and starts counting from the specified initial value.
Continue from last value for this stream	If selected, the counter will continue from the last value that was used for this stream.
Cascade: continue from last value on previous cascade stream	If selected, the Cascading UDF option will be enabled. This allows a UDF counter for a 'cascade' stream to continue from the value at the end of the previous cascade stream, rather than being reset.
Bit Mask	For each of the counters, a correspondingly large set of bit values which control whether each value will be held at '0,' '1' or allowed to change ('X').

UDF for XDM10G32S Load Module

XDM10G32S consists of eight UDFs (UDFs 1 - 8) that provide additional counter modes and types. The structure is shown in the following figure:

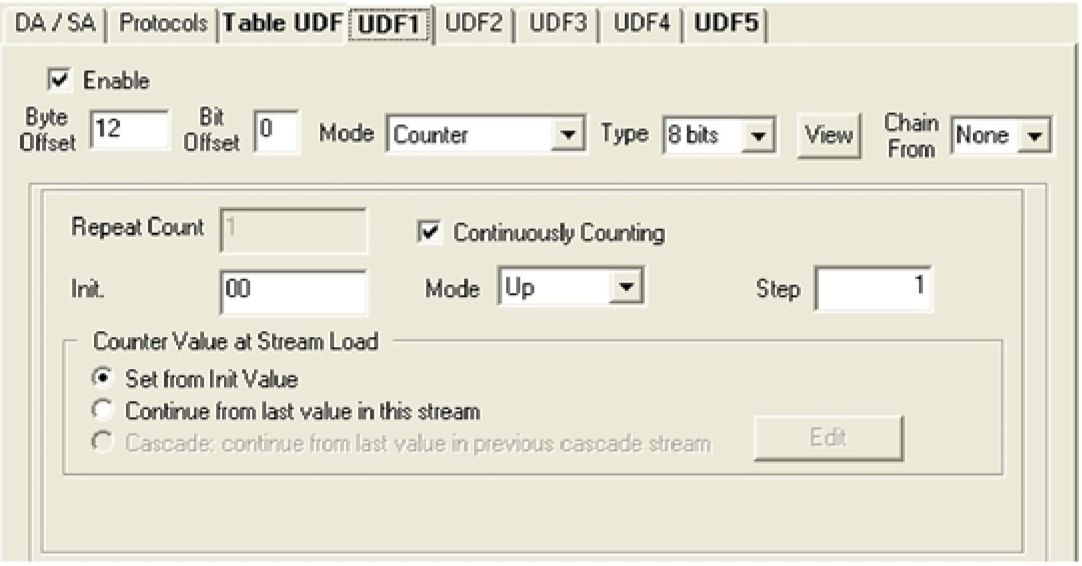
Figure:XDM10G32S UDF Option



UDF for Lava Load Module

Lava consists of five UDFs (UDFs 1 - 5) that provide additional counter modes and types. The structure is shown in the following figure:

Figure:Lava UDF Option



Refer to the following table for the UDFs supported by load module:

Table:User Defined Fields for Load Module

Field/Control	Description
Enable	Must be selected for the particular UDF to be active.
Byte Offset	The offset from the start of the frame (in bytes). The default value is 12 bytes.
Bit Offset	Adds another offset just after the bytes specified in Byte Offset. The range is 0 to 7 bits. Default = 0.
Mode	The available modes are the following: • Counter • Value List (For more information, see *UDF Counter Mode–Value List*) • Nested Counter (For more information, see UDF *Counter Mode–Nested Counter*) • Random • IPV4
Type	The choices of '8,' '16,' '24,' and '32' indicate single counters of their respective lengths.
Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop). • Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from.

Field/Control	Description
	• UDFs in random mode cannot be chained to. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count. • If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.

UDF for Xcellon-Multis Load Module

Xcellon-Multis consists of ten UDFs (UDFs 1 - 10) that provide additional counter modes and types. The structure is shown in the following figure:

figure:Xcellon-Multis UDF Option

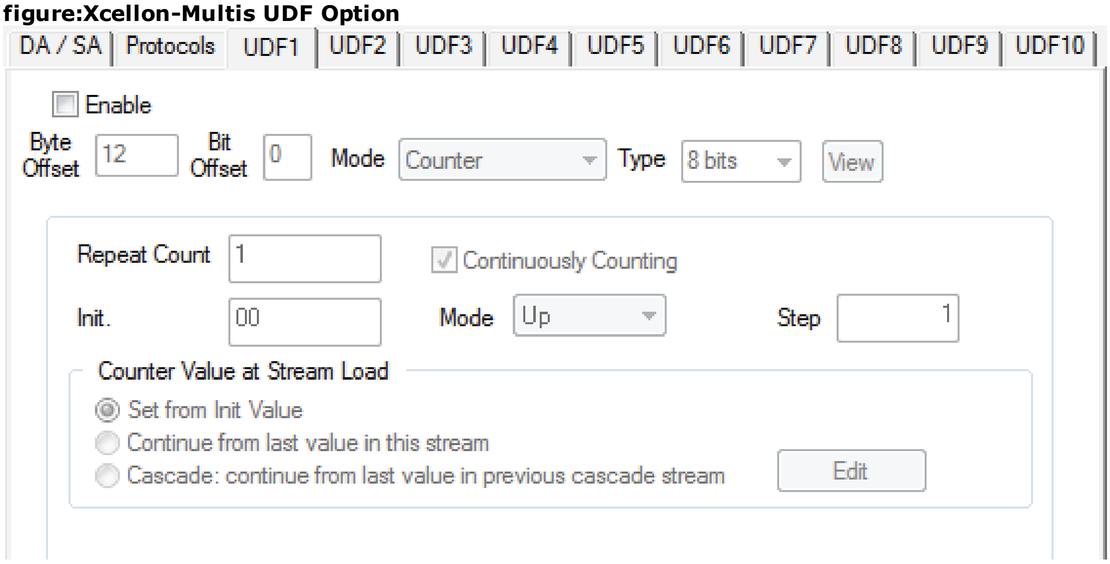


table:User Defined Fields for Load Module

Section	Field/Control	Usage
Header	Enable	Must be selected for the particular UDF to be active.
	Byte Offset	The offset from the start of the frame (in bytes).
	Bit Offset	Adds another offset just after the bytes specified in Byte Offset. The range is 0 to 7 bits. Default = 0.
	Mode	The available modes are the following:Counter Value List (For more information, see *UDF Counter*

Section	Field/Control	Usage
		Mode–Value List) Nested Counter (For more information, see *UDF Counter Mode–Nested Counter*) Random
	Type	The choices of '8,' '16,' '24,' and '32' indicate single counters of their respective lengths.
	View	Click to view the Affected Bits display. This is the UDF layout as currently configured. See *View UDF Layout* .
Window	Repeat Count	The Repeat Count field is active only when the Continuously Counting check box is not selected. This field is used to control the number of times
	Continuously Counting	If the Continuously Counting box is selected, then the counter will continuously count, with default increment step = 1.
	Init. (Initial Value)	The initial value for the counter, as masked by the Bit Mask Value. It is incremented or decremented by a value specified in the Step field. The default value in Tcl is 08 00.
	Mode	Up or Down increment mode controls the direction of counting.
	Step	The increment step for Up or Down increment mode can be specified. (Default = 1).
	Set from Init Value	Select to reset the counter to the Initial Value for each stream.
	Continue from last value in this stream	('Self-cascading UDFs') Select to reset the counter to the last value of this stream.

Advanced UDFs

For some modules there are five UDFs (UDFs 1 - 5) that provide advanced counter modes and types. Refer to *Table:UDF Characteristics per Module*to identify modules with this feature.

Availability depends on the UDF number. Furthermore, older OC-48c/OC-192c load modules can use two of the advanced UDFs. (*UDF Counter Modes for Advanced UDFs* for details.)

The contents of the lower part of the UDF are different depending on the setting in the Counter Mode field. The available counter modes are:

- *UDF Counter Mode–Counter*—The format for this mode is similar to those for the typical UDF. This mode is available for OC-48c and OC-192c cards.
- *UDF Counter Mode–Random*—This mode provides a configurable field for a Bit Mask. This mode is available for OC-48c and OC-192c cards.
- *UDF Counter Mode–Value List*—This mode allows to define data values for the UDF.
- *UDF Counter Mode–Range List*—This mode allows to define ranges of values for the UDF.
- *UDF Counter Mode–Nested Counter*—This mode allows to set up inner and outer counting loops for the UDF.
- *UDF Counter Mode–IPv4*—This mode allows to set up inner and outer counting loops for the UDF. For LM622MR cards, it is only available in POS mode.

Bit Size Counter

For some modules, the Counter Type parameter has been modified so that the size is exclicked in bit level, from 1 bit to 32 bits. The Offset Option can also specify the offset in bit level.

Affected modules include the following:

- LM1000STXS4, LM1000STXS24, LM1000XMS12,
- LM622MR / LM622MR-512
- LSM10G1-01, LSM10GL1-01, LSM10GXL6-01
- MSM2.5G1-01 and MSM10G1-01
- LSM1000XMV16-01

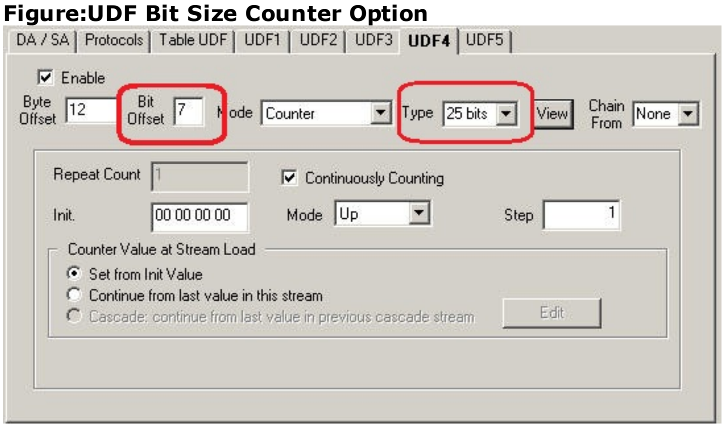
The following Advanced UDF Counter modes are affected, and field definitions are located in the respective topics:

- Counter Mode: *UDF Counter Mode–Counter*
- Range List Mode: *UDF Counter Mode–Range List*
- Nested Counter Mode: *UDF Counter Mode–Nested Counter*

The offset option has two components for these modules:

- **Byte Offset**: Origins from beginning of the packet, which is 0. The range is 0 to (FrameSize - 1) bytes.
- **Bit Offset**: Adds another offset just after the bytes specified in *Byte Offset*. The range is 0 to 7 bits.

Figure:UDF Bit Size Counter Option



The maximum size of the UDF (a 32-bit counter) is 32 bits, so the size of the UDF depends on the Bit Offset. See *Table:Maximum Size of UDF*.

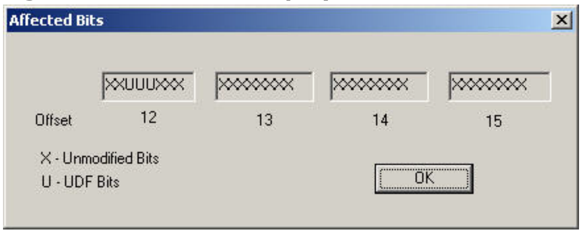
Table:Maximum Size of UDF

Bit Offset	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Maximum Size (bits)	**32**	**31**	**30**	**29**	**28**	**27**	**26**	**25**

View UDF Layout

Click the **View** button (when active) to view the 32 bit map layout of the selected UDF.

Figure:Affected Bits Display



For example if you select Bit Offset 2, Type (width) 3 bits and Byte Offset 12, then the UDF layout appears as shown above.

- X = unmodified bits from original packet
- U = UDF bits

So at Byte Offset 12, the first 2 bits (XX) are unmodified bits (from the packet). Then the next 3 bits UUU are from the UDF. And rest are again unmodified bits.

UDF Counter Modes for Advanced UDFs

The number and types of Counter Modes available for these UDFs vary depending on the UDF number, as shown in *Table:UDF Counter Modes for Advanced UDFs*.

Table:UDF Counter Modes for Advanced UDFs

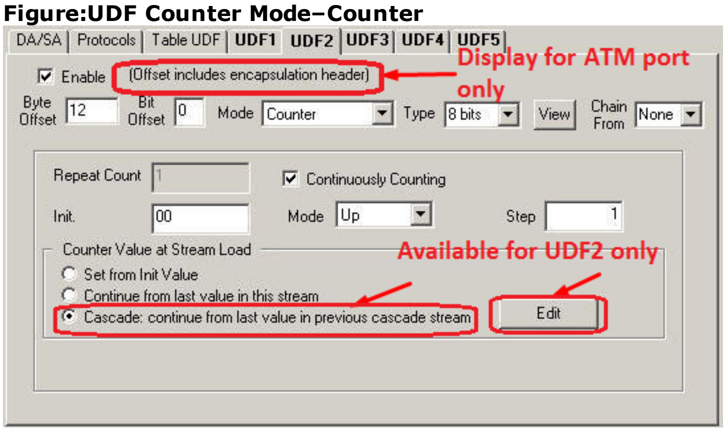
UDF Number	Counter Modes
UDF1	• Counter • Random • Value List • Range List (not available for ATM)

UDF Number	Counter Modes
UDF2	• Counter • Random • Value List
UDF3	• Counter • Random • Value List
UDF4	• Counter • Random • Value List • Nested Counter • IPv4
UDF5	• Counter • Random • Value List • Nested Counter • IPv4

UDF Counter Mode–Counter

When the Counter Mode field is set to *Counter*, the UDF appears as shown in *Figure:UDF Counter Mode–Counter*.

Figure:UDF Counter Mode–Counter



The fields and controls in this dialog are described in *Table:UDF Counter Mode–Counter*.

Table:UDF Counter Mode–Counter

Section	Field/Control	Usage
Header	Enable	This check box enables the UDF. NOTE For ATM ports, the note displays 'Offset includes encapsulation header'
	Byte Offset	The offset (in bytes) from the start of the frame. The default is 12 bytes.
	Bit Offset	For modules with *Advanced UDFs*: Enter the offset in bits. This will add another offset

Section	Field/Control	Usage
		just after the bytes specified in *Byte Offset*. The range is 0 to 7 bits. Default = 0.
	Mode	Selects the UDF Counter mode. In this case, **Counter**. The configuration options change depending on the mode selected. The options are shown in *Table:UDF Counter Modes for Advanced UDFs*.
	Type	The use and division of the 32-bit counter. For modules with *Advanced UDFs*: 1 bit to 32 bits. The values '8,' '16,' '24,' and '32' indicate counters of their respective lengths. For modules that support configuration of individual bytes, the following counter types are available: • 8 • 16 • 8x8 • 24 • 16x8 • 8x16 • 8x8x8 • 32 • 24x8 • 16x16 • 16x8x8 • 8x24 • 8x16x8 • 8x8x16 • 8x8x8x8
	View	Click to view the Affected Bits display. This is the UDF layout as currently configured. *View UDF Layout*.
	Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop).

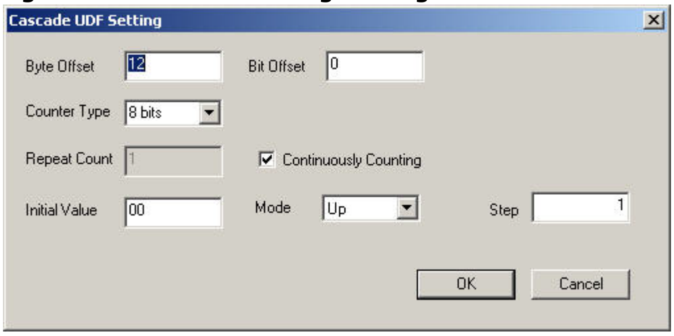
Section	Field/Control	Usage
		• Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from. • UDFs in random mode cannot be chained to. • For ATM ports, a UDF cannot be chained from if it is in Value List mode. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count. • If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.
Window	Repeat Count	The *Repeat Count* field is active only when the *Continuously Counting* check box is not selected. This field is used to control the number of times that the counter will increment. When the Repeat Count is exhausted, the value resets to 0 and counting is continued.
	Continuously Counting	If the *Continuously Counting* box is selected, then the counter will continuously count, with default increment step = 1.
	Init. (Initial Value)	The initial value for the counter, as masked by the Bit Mask Value. It is incremented or decremented by a value specified in the *Step* field. NOTE The default value in Tcl is 08 00.
	Mode	Up or Down increment mode controls the direction of counting.
	Step	The increment step for Up or Down increment mode can be specified. (Default = 1).
	Set from Init Value	Select to reset the counter to the Initial Value for each stream.
	Continue from last value in this stream	('Self-cascading UDFs') Select to reset the counter to the last value of this stream.
	Cascade: continue from last value in previous cascade stream	**(For use with UDF2 ONLY on modules with Advanced UDFs)** If selected, the Cascading UDF option will be enabled. This allows a UDF counter for a cascade stream to

Section	Field/Control	Usage
		continue from the last value of the previous cascade stream, rather than having the counter reset to the Initial value.
	Edit	**(For use with UDF2 ONLY on on modules with Advanced UDFs)** Press this button to display the *Cascade UDF Settings* dialog. *Cascade UDF Settings* for additional information.
		For each of the counters, a correspondingly large set of bit values which control whether each value will be held at '0,' '1' or allowed to change ('X'). The length of this field matches the number of bits selected in the *Counter Type* field (8, 16, 24, or 32 bits).

Cascade UDF Settings

The *Cascade UDF Settings* dialog is shown in *Figure:Cascade UDF Settings Dialog*.

Figure:Cascade UDF Settings Dialog



The fields and controls in this dialog are described in *Table:Cascade UDF Settings Dialog*.

Table:Cascade UDF Settings Dialog

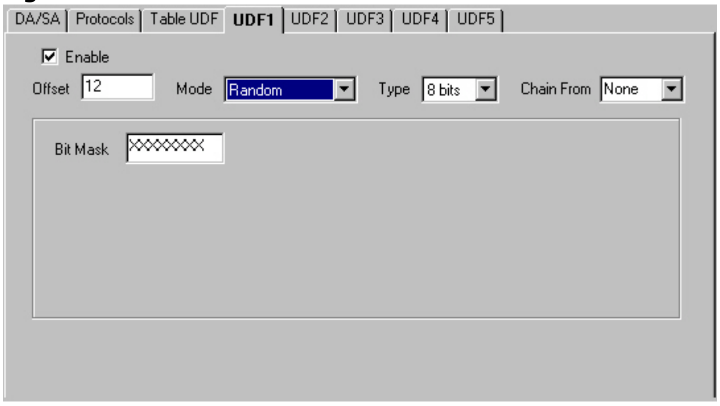
Field/Control	Usage
Byte Offset	The offset from the start of the frame—where the cascading UDF will be inserted.
Bit Offset	Enter the offset in bits. This will add another offset just after the bytes specified in *Byte Offset*. The range is 0 to 7 bits. Default = 0.
Counter Type	The use and division of the 32-bit counter. The choices '8,' '16,' '24,' and '32' indicate counters of their respective lengths.
Repeat Count	The *Repeat Count* field is active only when the *Continuously Counting* check box is not selected. This field is used to control the number of times that the counter will increment. When the Repeat Count is exhausted, the value resets to 0 and counting is continued.
Continuously Counting	If the *Continuously Counting* check box is selected, then the counter will continuously count, with default increment step = 1.
Init Value	The initial value for the counter, as masked by the Bit Mask

Field/Control	Usage
	Value. It is incremented or decremented by a value specified in the *Step* field.
Mode	Up or Down increment mode controls the direction of counting.
Step	The increment step for Up or Down increment mode can be specified. (Default = 1).

UDF Counter Mode–Random

The Random counter mode is shown in *Figure:UDF Counter Mode–Random*.

Figure:UDF Counter Mode–Random



When the Random counter mode is selected, a Bit Mask field is displayed. The length of this field matches the number of bits selected in the Counter Type field (8, 16, 24, or 32 bits). Random values, the selected number of bits in length, will be used in conjunction with the bit mask. You can control which mask bit values will be set to '0,' '1' or allowed to change ('X').

UDF Counter Mode–Value List

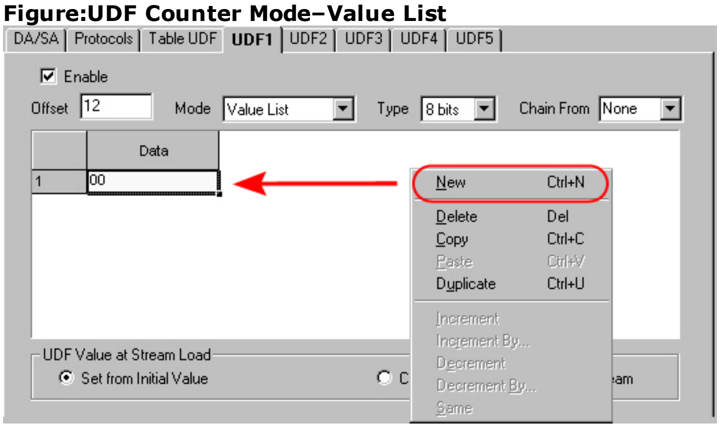
The Value List counter mode is shown in *Figure:UDF Counter Mode–Value List*.

NOTE

For LSM1000XMV and ASM1000XMV load modules, full feature versions, in Wide Packet Group–Wide Bin Mode, the PGID count has been increased to 1 million. Also,the memory for Value List and Range List has been separated (whereas for other load modules, these are combined). So the Value List UDF counter mode can handle up to 1048576 individual entries, and the Range List can handle up to 32767 entries.

However, the Value List entries on the different UDFs, when added together, cannot exceed this 1 million limit.

Figure:UDF Counter Mode–Value List



By using the right-click menu for the window, entries may be added and/or edited in the Value list.

The fields and controls in this window are described in *Table:UDF Counter Mode–Range List*.

Table:UDF Counter Mode–Value List

Section	Field/Control	Usage
Header	Enable	Must be selected for the particular UDF to be active.
	Offset	The offset from the start of the frame (in bytes). The default is 12 bytes.
	Mode	**Value List**—This mode allows to define specific values for the UDF.
	Type	The use of the 32-bit counter. The choices of '8,' '16,' '24,' and '32' indicate single counters of their respective lengths.
	Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop). • Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from. • UDFs in random mode cannot be chained to. • For ATM ports, a UDF cannot be chained from if it is in Value List mode. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count.

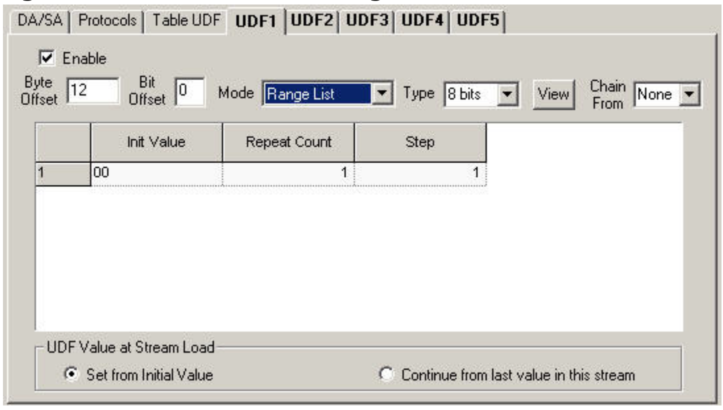
Section	Field/Control	Usage
		• If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.
List/Table	Data	This is the first value for the 32-bit counter. (This value is inserted into the packet at the specified offset. The first Init value in the list is inserted into the first packet in the stream - at the specified UDF offset, the second Init value in the second packet in the stream, and so on.)
UDF Value at Stream Load	Set from Initial Value	If selected, each new stream uses the UDF starting (initial) value for beginning the sequence of UDFs in the packets for the stream. The counting process starts over with the initial value.
	Continue from last value for this stream	If selected, each new stream starts counting from the last UDF value in the previous stream. The counting process does not start over, but continues across the group of streams.

UDF Counter Mode–Range List

The Range List counter mode is shown in *Figure:UDF Counter Mode–Range List*.

NOTE For LSM1000XMV and ASM1000XMV load modules, full feature versions, in Wide Packet Group–Wide Bin Mode, the PGID count has been increased to 1 million. Also,the memory for Value List and Range List has been separated (whereas for other load modules, these are combined). So the Range List UDF counter mode can handle up to 32767 individual entries.

Figure:UDF Counter Mode–Range List



By using the right-click menu for the window, entries may be added and/or edited in the Range list. The fields and controls in this window are described in *Table:UDF Counter Mode–Range List*.

Table:UDF Counter Mode–Range List

Section	Field/Control	Usage
Header	Enable	This check box enables the UDF.
	Byte Offset	The offset (in bytes) from the start of the frame. The default is 12 bytes.
	Bit Offset	For modules with *Advanced UDFs*: Enter the offset in bits. This will add another offset just after the bytes specified in *Byte Offset*. The range is 0 to 7 bits. Default = 0.
	Mode	**Range List**—This mode allows to define ranges of values for the UDF. The configuration options change depending on the mode selected. The options are shown in *Table:UDF Counter Modes for Advanced UDFs*.
	Type	The use and division of the 32-bit counter. For modules with *Advanced UDFs*: 1 bit to 32 bits. The values '8,' '16,' '24,' and '32' indicate counters of their respective lengths. For modules that support configuration of individual bytes, the following counter types are available: • 8 • 16 • 8x8 • 24 • 16x8 • 8x16 • 8x8x8 • 32 • 24x8 • 16x16 • 16x8x8 • 8x24 • 8x16x8 • 8x8x16 • 8x8x8x8
	View	Click to view the Affected Bits display. This is the UDF layout as currently configured. *View UDF Layout*.
	Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF

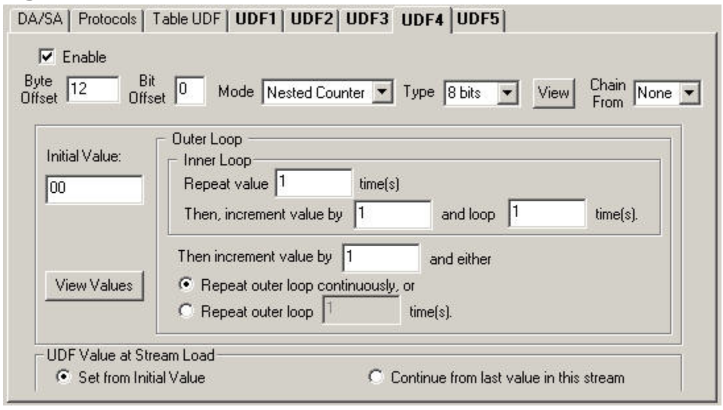
Section	Field/Control	Usage
		will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop). • Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from. • UDFs in random mode cannot be chained to. • For ATM ports, a UDF cannot be chained from if it is in Value List mode. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count. • If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.
List/Table	Init Value	This is the first value in a range of values for the 32-bit counter. The successive values in this stream are defined by the number of repeats and the size of the increment/decrement steps. (This value is inserted into the packet at the specified offset. The first value in the list is inserted into the first packet in the stream - at the specified UDF offset, the second value in the second packet in the stream, and so on.)
	Repeat Count	The number of times that the initial value will be incremented, by an amount equal to the Step size. The default is ‘1.’
	Step	The increment step for the repeat count can be specified.
UDF Value at Stream Load	Set from Initial Value	If selected, each new stream uses the UDF starting (initial) value for beginning the sequence of UDFs in the packets for the stream. The counting process starts over with the initial value.

Section	Field/Control	Usage
	Continue from last value for this stream	If selected, each new stream starts counting from the last UDF value in the previous stream. The counting process does not start over, but continues across the group of streams.

UDF Counter Mode–Nested Counter

This counter mode applies only for use with UDFs 4 and 5, and is shown for UDF4 in *Figure:UDF Counter Mode–Nested Counter*.

Figure:UDF Counter Mode–Nested Counter



The fields and controls in this window are described in *Table:UDF Counter Mode–Nested Counter*.

Table:UDF Counter Mode–Nested Counter

Section	Field/Control	Usage
Header	Enable	This check box enables the UDF.
	Byte Offset	The offset (in bytes) from the start of the frame. The default is 12 bytes.
	Bit Offset	For modules with *Advanced UDFs*: Enter the offset in bits. This will add another offset just after the bytes specified in *Byte Offset*. The range is 0 to 7 bits. Default = 0.
	Mode	**Nested Counter**—This mode allows to create inner and outer counting loops for the UDF.
	Type	The use and division of the 32-bit counter. For modules with *Advanced UDFs*: 1 bit to 32 bits. The values '8,' '16,' '24,' and '32' indicate counters of their respective lengths. For modules that support configuration of individual bytes, the following counter types are available: • 8 • 16 • 8x8

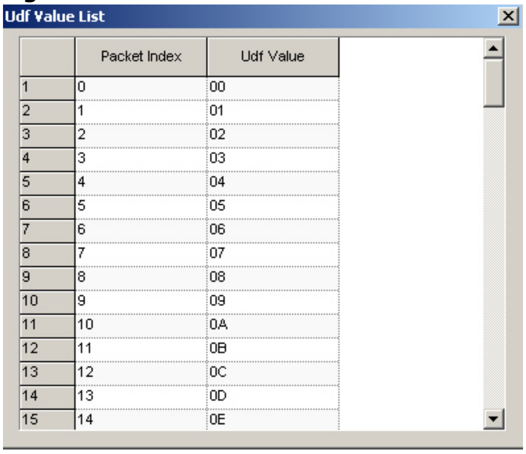
Section	Field/Control	Usage
		• 24 • 16x8 • 8x16 • 8x8x8 • 32 • 24x8 • 16x16 • 16x8x8 • 8x24 • 8x16x8 • 8x8x16 • 8x8x8x8
	View	Click to view the Affected Bits display. This is the UDF layout as currently configured. *View UDF Layout*.
	Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop). • Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from. • UDFs in random mode cannot be chained to. • For ATM ports, a UDF cannot be chained from if it is in Value List mode. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count. • If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.
Initial Value:		(hex value)

Section	Field/Control	Usage
		This is the starting UDF value.
View Values		Press this button to see the UDF Value List. It shows the list of UDF values that will be placed into the packets. *UDF Value List* for additional information.
Outer Loop	Inner Loop	(integers) Repeat Value ___ time(s)
		Then increment value by ___ and loop __ time(s). Enter the hex value for the increment size, and enter the integer for the number of times to repeat the inner loop.
	(For the Outer Loop) Then, increment value by __ and either	Enter the hex value for the increment size for the outer loop. Then the select the type of outer looping desired. Choose one of: • Repeat outer loop continuously (with increasing values), or • Repeat outer loop ___ time(s): Repeating the outer looping sequence a specified number of times before restarting the counting sequence with the initial value. The entire counting sequence starts over with the initial value.
UDF Value at Stream Load	Set from Initial Value	If selected, each new stream uses the UDF starting (initial) value for beginning the sequence of UDFs in the packets for the stream. The counting process starts over with the initial value.
	Continue from last value for this stream	If selected, each new stream starts counting from the last UDF value in the previous stream. The counting process does not start over, but continues across the group of streams.

UDF Value List

The UDF Value List is shown in *Figure:UDF Value List*.

Figure:UDF Value List



The fields and columns in this window are described in *Table:UDF Value List*.

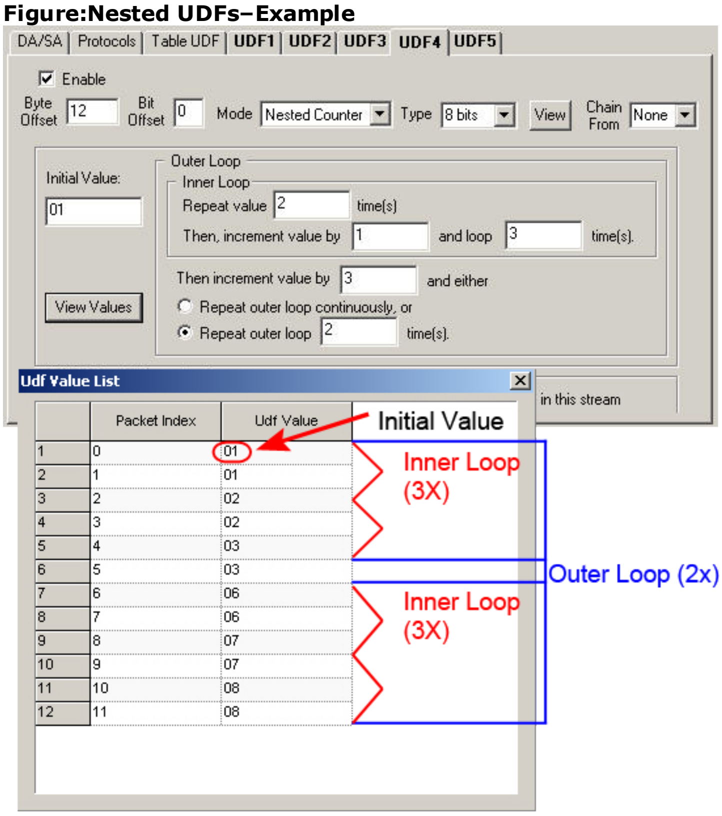
Table:UDF Value List

Field/Column	Description
Packet Index	The index number for the packet in the stream.
UDF Value	The hex value inserted into the UDF.

Nested UDFs–Example

An example of a simple configuration setup for use of the Nested Counter Mode is shown in *Figure:Nested UDFs–Example*. The configuration values in the dialog and the corresponding values in the UDF Value List are shown.

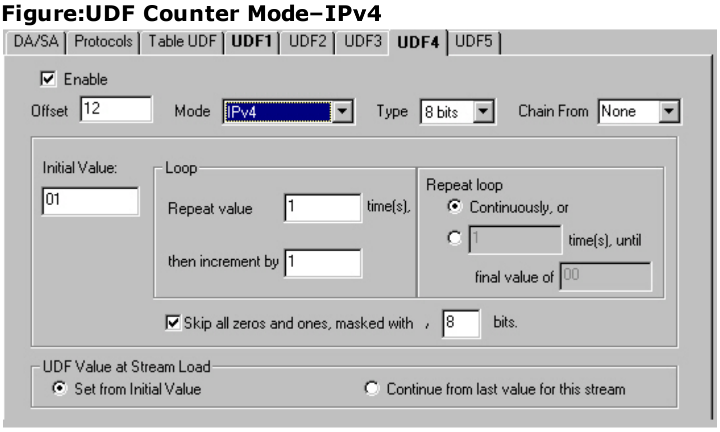
Figure:Nested UDFs–Example



UDF Counter Mode–IPv4

This counter mode applies only to use with UDFs 4 and 5, and is shown for UDF5 in *Figure:UDF Counter Mode–IPv4*.

Figure:UDF Counter Mode–IPv4



The fields and controls in this window are described in *Table:UDF Counter Mode–IPv4*.

Table:UDF Counter Mode–IPv4

Section	Field/Control	Usage
Header	Enable	Must be selected for the particular UDF to be active.
	Offset	The offset from the start of the frame (in bytes). The default is 12 bytes.
	Mode	**IPv4**—This mode allows to create counting loops to be used with IPv4 addresses.

Section	Field/Control	Usage
	Type	The use and division of the 32-bit counter. Choose one of: • 8 bits • 16 bits • 24 bits • 32 bits
Initial Value:	Chain From	Allows to select what UDF the current UDF should chain from. When this option is employed, the UDF will stay in its initial value until the UDF it is chained from reaches its terminating value. The following rules apply to chaining UDFs: • Chain loops should not be created as it will cause data failures (that is, UDF 5 from UDF 3 from UDF 1 from UDF 5 is an illegal chain, as it creates a loop). • Only one UDF can be chained from, though multiple UDFs can chain from the same UDF. • Table UDFs cannot be chained from. • UDFs in random mode cannot be chained to. • For ATM ports, a UDF cannot be chained from if it is in Value List mode. • For Nested Counter/IPv4 mode, the chain will trigger from the inner loop count and NOT the outer loop count. • If Cascade UDF (UDF2) uses the Chained From option, Cascade will be turned off. • UDF2 cannot be chained to if Cascade is enabled. • If UDF(n) is chained from a continuous mode UDF, the chained UDF will reach its terminating count after 2^32 iterations. Hence, UDF(n) will start after 2^32 iterations. The pull-down list always shows all UDFs, but only enabled UDFs can be chained to.
	Loop (for Inner Loop)	(integer) Repeat Value ___ time(s)
		then increment value by ___, (For the Inner Loop) Enter the hex value for the increment size, and enter the integer for the number of times to repeat the inner loop.
	Repeat loop	Choose one of:

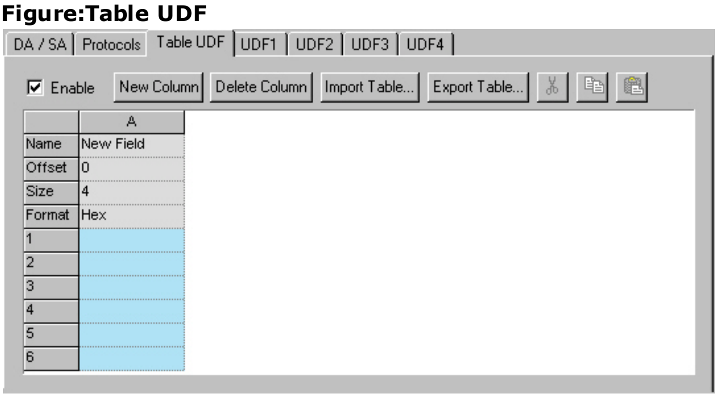
Section	Field/Control	Usage
	(for Outer Loop)	• Continuously, or • ___ times until final value of __ (final value is read-only) The final value of the count, based on values entered in the Initial Value, Loop, and Repeat loop fields.
		Select the desired type of outer loop. Choose one of: • Continuous looping with increasing values. • Repeating the outer looping sequence a specified number of times before restarting the counting sequence with the initial value. The entire counting sequence starts over with the initial value.
Skip all zeros and ones, masked with _ _ bits		If selected, values with all '1's and '0's in a particular part of the value may be skipped so as to avoid broadcast addresses.
UDF Value at Stream Load	Set from Initial Value	If selected, each new stream uses the UDF starting (initial) value for beginning the sequence of UDFs in the packets for the stream. The counting process starts over with the initial value.
	Continue from last value for this stream	If selected, each new stream starts counting from the last UDF value in the previous stream. The counting process does not start over, but continues across the group of streams.

Table UDF

Certain modules have a Table UDF option (refer to *Table:UDF Characteristics per Module*). Table UDFs allows to specify a number of lists of values to be placed at designated offsets within a stream. Each list consists of an Offset, a Size, and a list of values.

The *Table UDF* tab is shown in *Figure:Table UDF*.

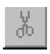
Figure:Table UDF



You may create any number of lists, subject to implementation restrictions such as available memory, and import or export those lists.

Table: UDF Configuration describes the configuration options in the *Table UDF* tab.

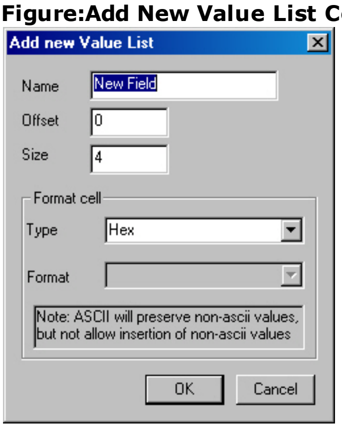
Table: UDF Configuration

Field/Control	Usage
Enable	This check box enables the Table UDF.
New Column	Selecting this button allows to create a value list. The parameters of the value list are set in the *Add a Value List* dialog, as discussed in *Creating a Value List*.
Delete Column	Selecting this button deletes the selected value list. Note the column letter at the very top of the column must be selected to use this function.
Import Table	Selecting this button allows to import table values from an Excel file.
Export Table	Selecting this button allows to export table values as an Excel file.
Name	Descriptive text for a value list. The name is set using the *Add a Value List* dialog, as discussed in *Creating a Value List*.
Offset	Offset is the beginning point for value insertion relative to byte 0 of the frame. Offset is measured in bytes. The Offset is set using the *Add a Value List* dialog, as discussed in *Creating a Value List*.
Size	Size is the length of each value in a value list, measured in bytes. The size is set using the *Add a Value List* dialog, as discussed in *Creating a Value List*.
Format	The Format is set using the *Add a Value List* dialog, as discussed in *Creating a Value List*.
	Selecting this icon cuts highlighted text in the data portion of the value list.
	Selecting this icon copies highlighted text in the data portion of the value list.
	Selecting this icon pastes text copied or cut from the data portion of the value list.

Creating a Value List

The *Add New Value List* dialog allows to configure the parameters of a value list. The *Add New Value List* dialog is shown in *Figure:Add New Value List Configuration*.

Figure:Add New Value List Configuration



The configurable parameters in this dialog are described in *Table:New Value List Configuration*.

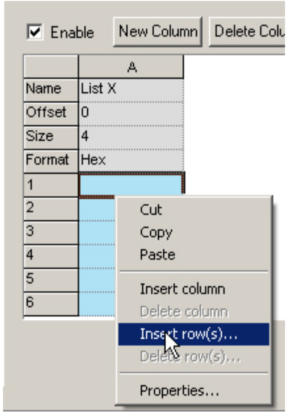
Table:New Value List Configuration

Field/Control	Usage
Name	Descriptive text for a value list. A value list name has no functional meaning in the implementation, but is useful for descriptive documentation of the packet field. Name may be blank and need not be unique across value lists in a value list group.
Offset	Offset is the beginning point for value insertion relative to byte 0 of the frame. Offset is measured in bytes and must be between 0 and 247.
Size	Size is the length of each value in a value list, measured in bytes. Size must be between 1 and 256. The offset + size must be less than or equal to 248.
Type	Sets the type of information that is to be inserted into the packet stream. • Hex • ASCII • Binary • Decimal • MAC • IPv4 • IPv6 • Custom The type of data selected assists in creating the data. For example, selecting ‘IPv4’ will force the data into dotted decimal notation (1.1.1.1). Selecting ‘Custom’ enables the Format field, described below.
Format	Allows to specify the data format for custom Table UDFs. Select from the following list: • 32d—thirty-two bit decimal format. • 32x—thirty-two bit hexadecimal format. • 32b—thirty-two bit binary format. • 32a—thirty-two bit ASCII format. • 8d.8d.8d.8d—Dotted decimal format, in eight bit sections. • 8x.8x.8x.8x—Dotted hex format, in eight bit sections. • 16d.16d—Dotted decimal format, in sixteen bit sections. • 16x.16x—Dotted hex format, in sixteen bit sections. Note that the Type setting must be ‘Custom’ for this field to be active.

Adding Rows (Table UDF Entries)

After creating a column, right-click in the body of the column and select **Insert Row(s)** from the action menu, as shown in *Figure:Insert Rows*.

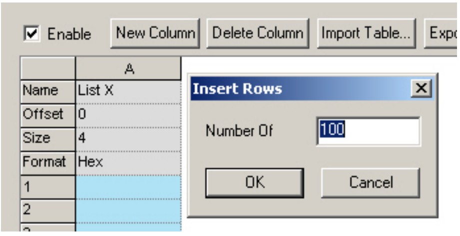
Figure:Insert Rows



A dialog box will appear, prompting you to specify the number of rows (Table UDF entries). Different types of load modules have different limitations on the maximum number that can be created, depending of number and size of streams and frame size.

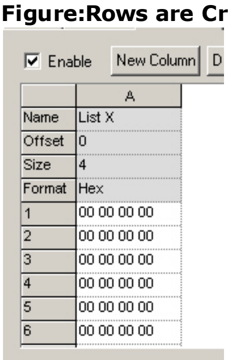
Enter the number of rows (entries), then click OK (*Figure:Enter the Number of Rows*).

Figure:Enter the Number of Rows



The newly created rows will appear, as shown in *Figure:Rows are Created*.

Figure:Rows are Created



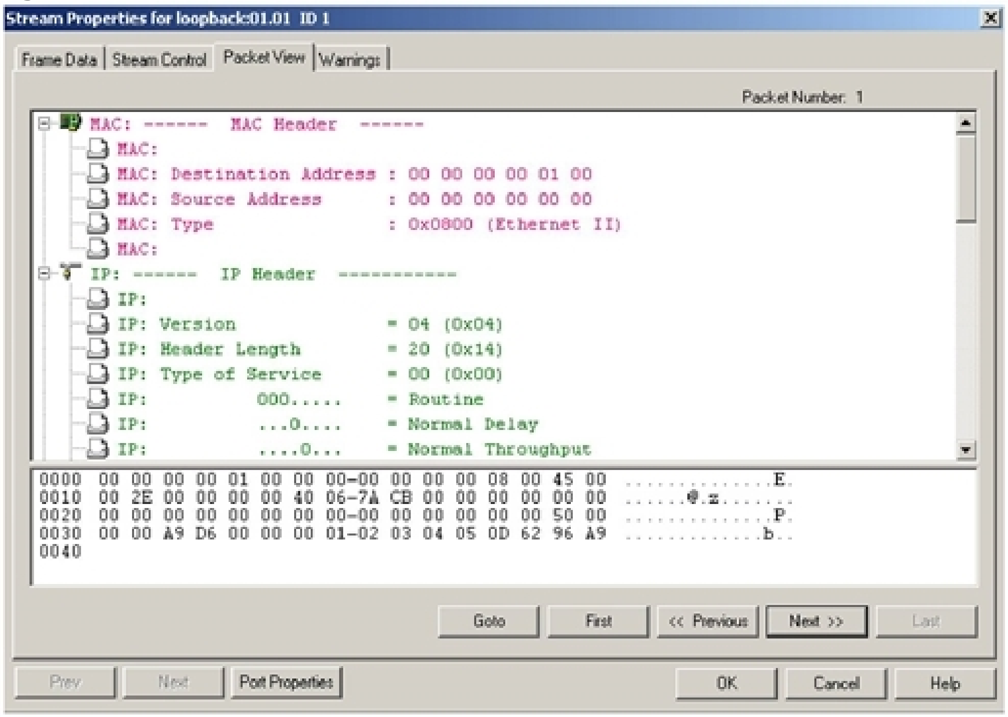
[This page intentionally left blank]

Chapter 8 - Packet View

Packet View Tab

The results of constructing packets through the *Frame Data* tab (as described in Frame Data Tab *are displayed in the Packet View. The Packet View tab is pictured in Figure:Packet View Tab.*

Figure:Packet View Tab



The parts of the display are:

- *Decode Panel*—shows the packet decoded header contents.
- *Raw Packet Panel*—shows the hexadecimal and ASCII interpretation of the first packet of a stream region.
- *Controls for Use with Packet View*—shows the additional controls available for use with ports configured for flows.

Decode Panel

The Decode Panel is a protocol dependent decode of the selected packet's contents. It reflects programming performed through the *Protocols* sub-tab (Frame Data–Protocol Control *for more information) from the* Frame Data Tab*. The data in the display can be scrolled by conventional means: up/down arrow keys, up/down page keys, and use of the scroll bar.*

Raw Packet Panel

The Raw Packet Panel shows the entire contents of the packet up to, but not including, the FCS. The left-hand column contains the packet offset, exclicked in hexadecimal. The middle column contains sixteen bytes of data, exclicked in hexadecimal. The right-hand column contains a display of the data in ASCII, if the byte can be displayed as such; otherwise the byte is displayed as a dot (.). The data in the display can be scrolled by conventional means: up/down arrow keys, up/down page keys, and use of the scroll bar.

Controls for Use with Packet View

The *Packet View* tab is able to look at the fields of any individual packet configured by you. The controls that are available are described in *Table:Packet View Controls for Use with Flows*.

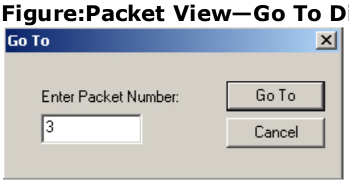
Table:Packet View Controls for Use with Flows

Control	Description
Go To	When clicked, the *Go To* dialog is displayed. For additional information, *Go To Dialog*.
First	Click once to go to the First packet in the flow. See Note 2 below.
<< Previous	Click once to go to the Previous packet in the flow. See Note 2 below.
Next >>	Click once to go to the Next packet in the flow. See Note 1 below.
Last	Click once to go to the Last packet in the flow. See Note 1 below.
Port Properties	Displays the *Port Properties* dialog for this port.

Go To Dialog

The *Go To* dialog allows to enter a positive integer that identifies the target packet, as shown in *Figure:Packet View—Go To Dialog*.

Figure:Packet View—Go To Dialog



Chapter 9 - IxRouter Window

In This Chapter

This chapter covers the following topics:

Introduction to IxRouter

Most Ixia card types offer a Protocol Server. The Protocol Server includes a complete TCP/IP stack, allowing different forms of high-level protocol-based DUT testing. The Protocol Server is accessed through the IxRouter window in IxExplorer and can be configured to test a set of Level 2 and Level 3 protocols, which include MAC and IPv4/IPv6 addressing and routing. The information gathered by the IxRouter Window is used within generated frame data, also.

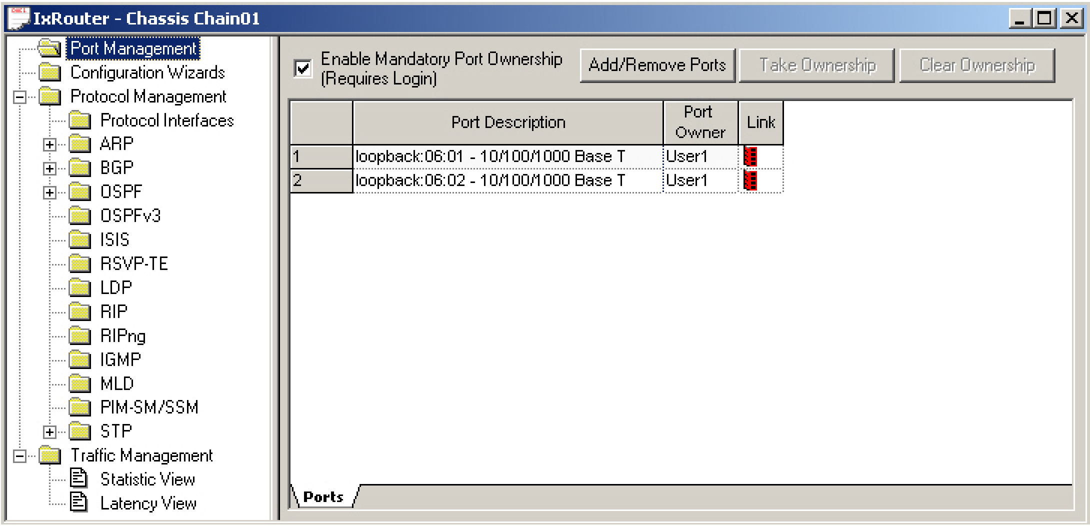
- The IxRouter Window is available by default in IxExplorer—for Ixia modules that support Internet traffic. This window provides a location for configuring protocol interfaces on selected ports. In addition, the IxRouter Protocol Management window allows to enable PING (ICMP) for IPv4 and ARP on the selected ports.
- Routing protocols are available in the IxRouter Window after installation of protocol emulation software bundles and/or individual protocol emulations. The protocols that are supported vary by load module type. Refer to the *Ixia Platform Reference Manual* for details. Refer to *Protocols Supported by the IxRouter Window for a list of the available protocols and the chapters covering those protocol emulations in detail.*

NOTE For information on installation of the IxRouter protocol emulation software, see

NOTE the IxRouter Installation Chapter of the *IxNetwork User Guide*.

The IxRouter Window, with IxRouter Protocol Emulations installed, is shown in *Figure:IxRouter Window with IxRouter Protocol Emulations Installed*.

Figure:IxRouter Window with IxRouter Protocol Emulations Installed



IxRouter Window Architecture

In general, the IxRouter window 'tree' in the left pane displays the list of windows and protocol emulations that can be configured, while the details view in the right pane shows information, in spreadsheet or dialog format, for the item selected in the tree.

There is a hierarchy for configuring services within each protocol, specialized for each protocol. For complex routing protocols such as OSPF, there are many levels in the hierarchy; those relationships are described in detail in the applicable sections. Once a protocol has been enabled for a selected port, the port name/number will appear in the tree below that protocol.

The IxRouter Window consists of the main divisions which are described in the sections listed in *Table:IxRouter Window Sections*.

Table:IxRouter Window Sections

Section	Description
Port Management Window	For Login, Port Selection, and Port Ownership functions. Refer to *Port Management Window* for additional information.
Configuration Wizards	(Available when IxNetwork protocol emulations are installed.) Sets of dialogs for easily configuring Layer 2 VPNs, Layer 3 VPNs, and test topologies for individual, or multiple, routing protocols. Refer to the Configuration Wizards Chapter in the *IxNetwork User Guide* for additional information.
Protocol Management Window	For enabling available protocol emulations on specific ports, and configuring protocols through sub-windows (in the protocol tree) for each protocol.

Section	Description
	Refer to *Protocol Management Window* for additional information.
Protocol Interfaces Window	For creating interfaces that can be configured for use with network protocols. Refer to *Protocol Interfaces Window* for additional information.
Protocol List	Protocol 'Tree'—list of IxRouter protocol emulations. • ARP and ICMP (PINGv4) are available by default. • Additional routing protocols are installed separately. Refer to *Protocols Supported by the IxRouter Window* for additional information.
Protocol Traffic Management Window	(Available when IxRouter protocol emulations are installed.) Protocol Traffic Management Window—for automatically generating (constructing) streams based on protocol configurations. Refer to the Protocol Traffic Management Window Chapter in the *IxNetwork User Guide.*

Protocols Supported by the IxRouter Window

NOTE The protocols supported by the IxRouter Window vary by load module type. Refer to the *Ixia Platform Reference Guide*for details.

The IxRouter Window supports the protocols listed in *Table:Protocols Supported by IxRouter Window*. ARP and ICMP (PING for IPv4) are available in the IxExplorer IxRouter Window; additional protocol emulations are available separately.

Table:Protocols Supported by IxRouter Window

Protocol	Description
ARP	Address Resolution Protocol (non-POS only) (Includes the IP table for IP to MAC addressing.) Refer to *ARP* for additional information.
PING for IPv4	'Packet Internet Groper/PING'—uses Internet Message Control Protocol (ICMP) echo messages and responses. Refer to ICMP/PINGv4 for additional information.
BGP	Border Gateway Protocol version 4—for IPv4 and IPv6, L3 VPNs, MVPNs. Refer to the BGP Chapter in the *IxNetwork Users Guide* for additional information.
OSPFv2	Open Shortest Path First Protocol Version 2—for IPv4. Refer to the OSPF Chapter in the *IxNetwork User Guide* for additional information.
OSPFv3	Open Shortest Path First Protocol Version 3—for IPv6. Refer to the OSPF Chapter in the *IxNetwork Users Guide* for additional information.

Protocol	Description
ISIS	Intermediate System to Intermediate System Protocol - for IPv4 and IPv6. Refer to the ISIS Chapter in the *IxNetwork Users Guid*e for additional information.
RSVP-TE	Resource ReServation Protocol with Traffic Engineering—for IPv4. Refer to the RSVP-TE Chapter in the *IxNetwork Users Guide* for additional information.
LDP	Label Distribution Protocol—for IPv4 and IPv6, L2 VPNs. Refer to the LDP Chapter in the *IxNetwork User Guid*e for additional information.
RIP	Routing Information Protocol—for IPv4. Refer to the RIP Chapter in the *IxNetwork User Guid*e for additional information.
RIPng	Routing Information Protocol—Next Generation (IPv6). Refer to the RIPng Chapter in the *IxNetwork User Guid*e for additional information.
IGMP	Internet Group Management Protocol—versions 1, 2, and 3, for IPv4. Refer to the IGMP Chapter in the *IxNetwork User Guid*e for additional information.
MLD	Multicast Listener Discovery—versions 1 and 2, for IPv6. Refer to the MLD Chapter in the *IxNetwork User Guid*e for additional information.
PIM-SM/SSM	Protocol Independent Multicast - Sparse Mode / Protocol Independent Multicast - Source Specific Multicast - for IPv4 and IPv6, MVPNs Refer to the PIM-SM/SSM Chapter in the *IxNetwork User Guid*e for additional information.

Opening the IxRouter Window

The IxRouter window provides a location in IxExplorer for configuring the routing protocol services. The IxRouter window is accessed in the IxExplorer window by using one of the following methods, which are shown in *Figure:Opening the IxRouter Window*:

- Click a port and then select 'IxRouter' in the Port Details list in the right pane, or
- Click the *IxRouter* icon in the toolbar, or
- Right-click a port or chassis to display the shortcut menu and select 'IxRouter.'

Figure:Opening the IxRouter Window

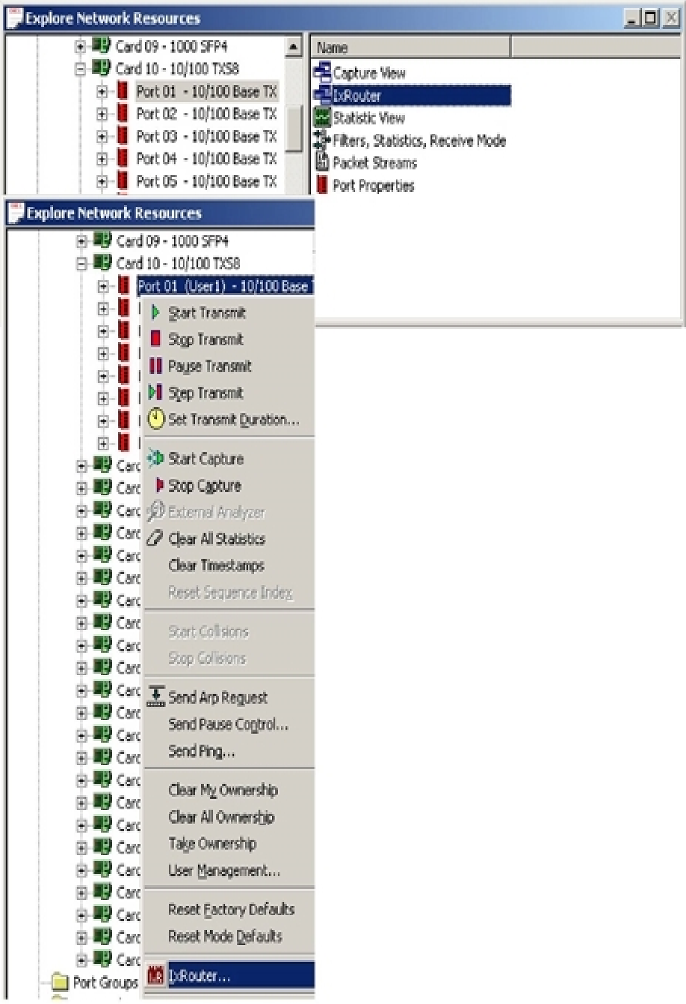


Figure:Opening the IxRouter Window

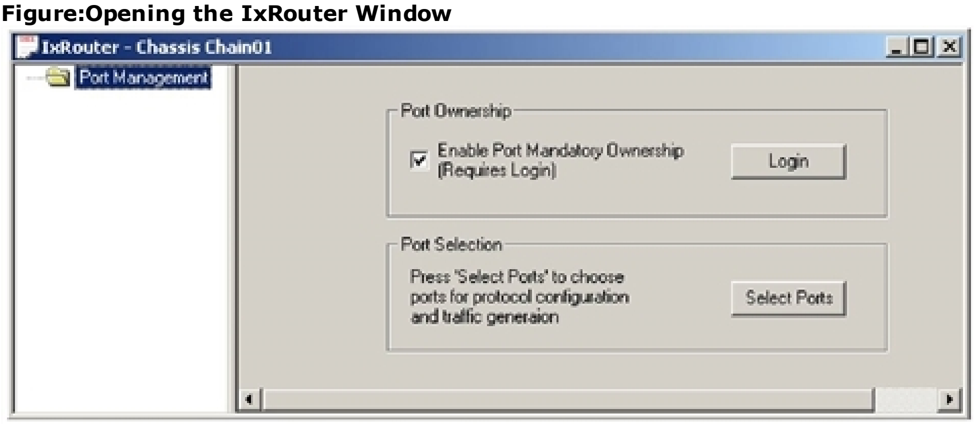
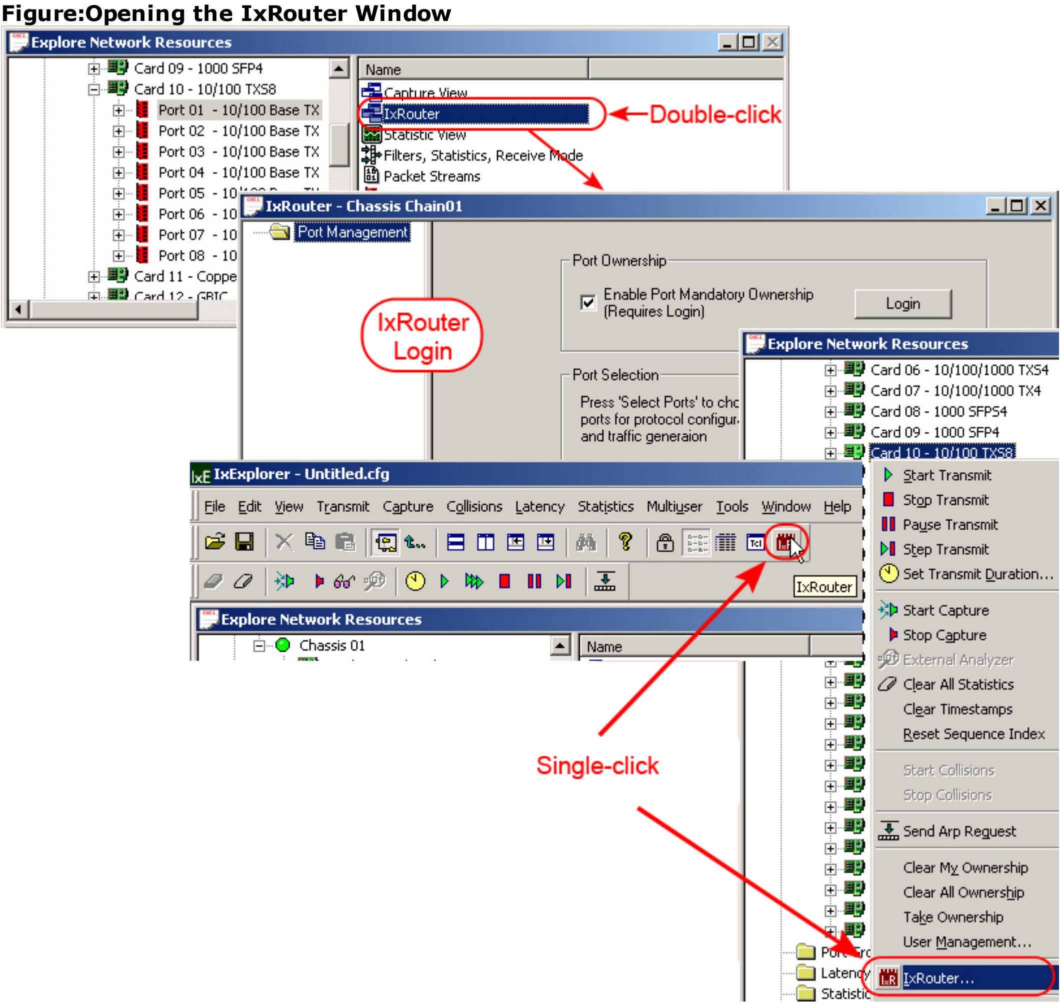


Figure:Opening the IxRouter Window



Port Management Window

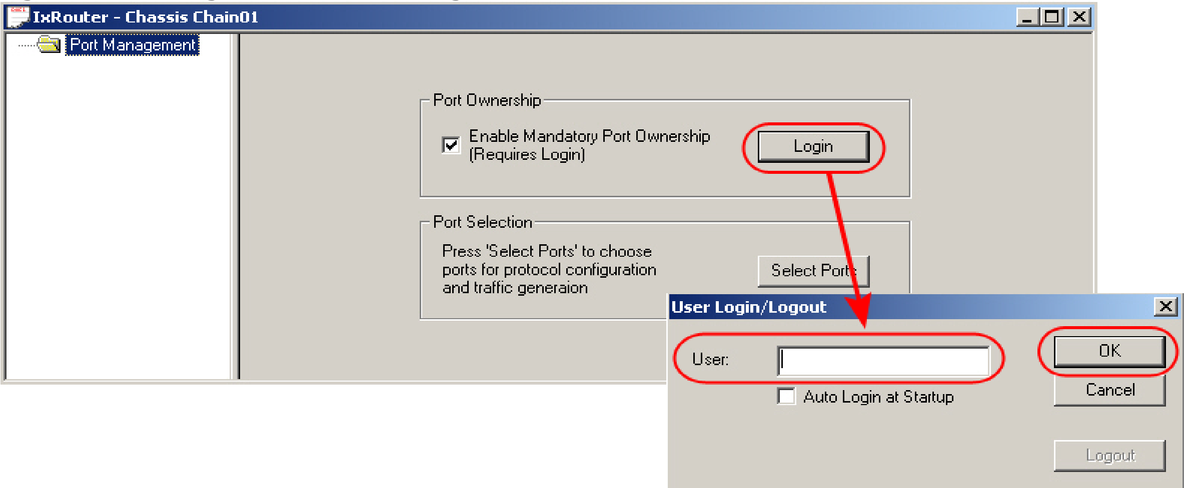
The IxRouter Port Management window is described in the following sections:

- *Login Window*
- *Selecting Ports*
- *Mandatory Port Ownership*

Login Window

When the IxRouter Window first opens, as shown in *Figure:Port Management Window—Login*, the Port Management window, in Login mode, is displayed by default—with no additional items listed in the protocol tree (left pane).

Figure:Port Management Window—Login



Login requirements depend on the setting for the Mandatory Port Ownership feature. *Mandatory Port Ownership* for additional information on Mandatory Port Ownership feature. There are two modes for the Mandatory Port Ownership—enabled or disabled, as described below:

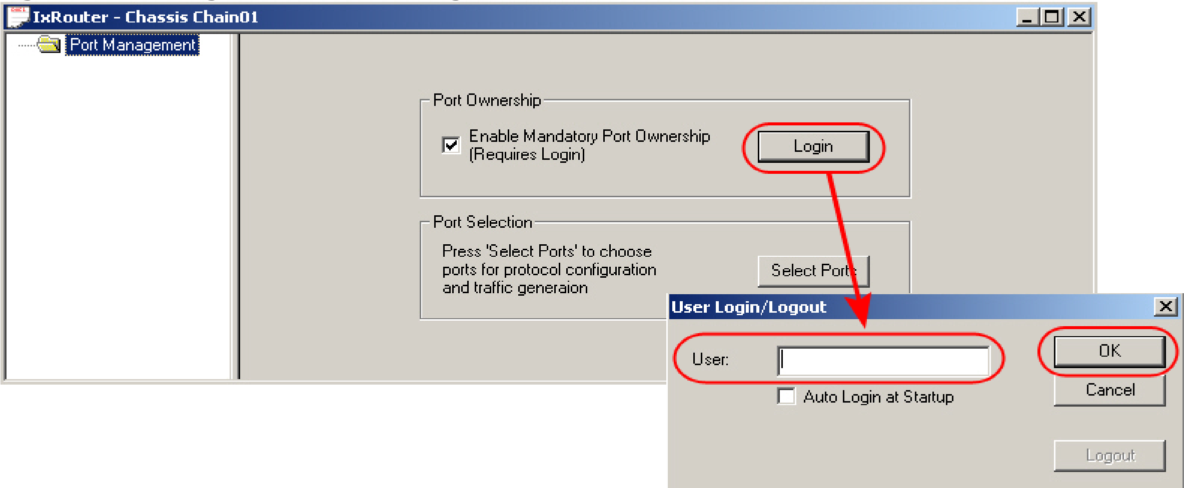
- If the 'Enable Mandatory Port Ownership' option is selected (the default setting), Login is **required**. Click the *Login* button to log on as the user. Click *OK* to close the dialog. After logging in, click the *Select Ports* button to display the Select Ports dialog, which lists all of the available ports on the current chassis. Go to *Selecting Ports* for information on selecting ports.
- If the 'Enable Mandatory Port Ownership' option is NOT selected, no Login is required. Click the *Select Ports* button to display the Select Ports dialog, which lists all of the available ports on the current chassis. Go to *Selecting Ports* for information on selecting ports.

Enabling the 'Auto Login at Startup' option allows to close and open IxRouter without logging in each time, as long as the IxExplorer window remains open. If the IxExplorer window is closed, and then re-opened, you must log on to IxRouter again.

Login Window

When the IxRouter Window first opens, as shown in *Figure:Port Management Window—Login*, the Port Management window, in Login mode, is displayed by default—with no additional items listed in the protocol tree (left pane).

Figure:Port Management Window—Login



Login requirements depend on the setting for the Mandatory Port Ownership feature. *Mandatory Port Ownership* for additional information on Mandatory Port Ownership feature. There are two modes for the Mandatory Port Ownership—enabled or disabled, as described below:

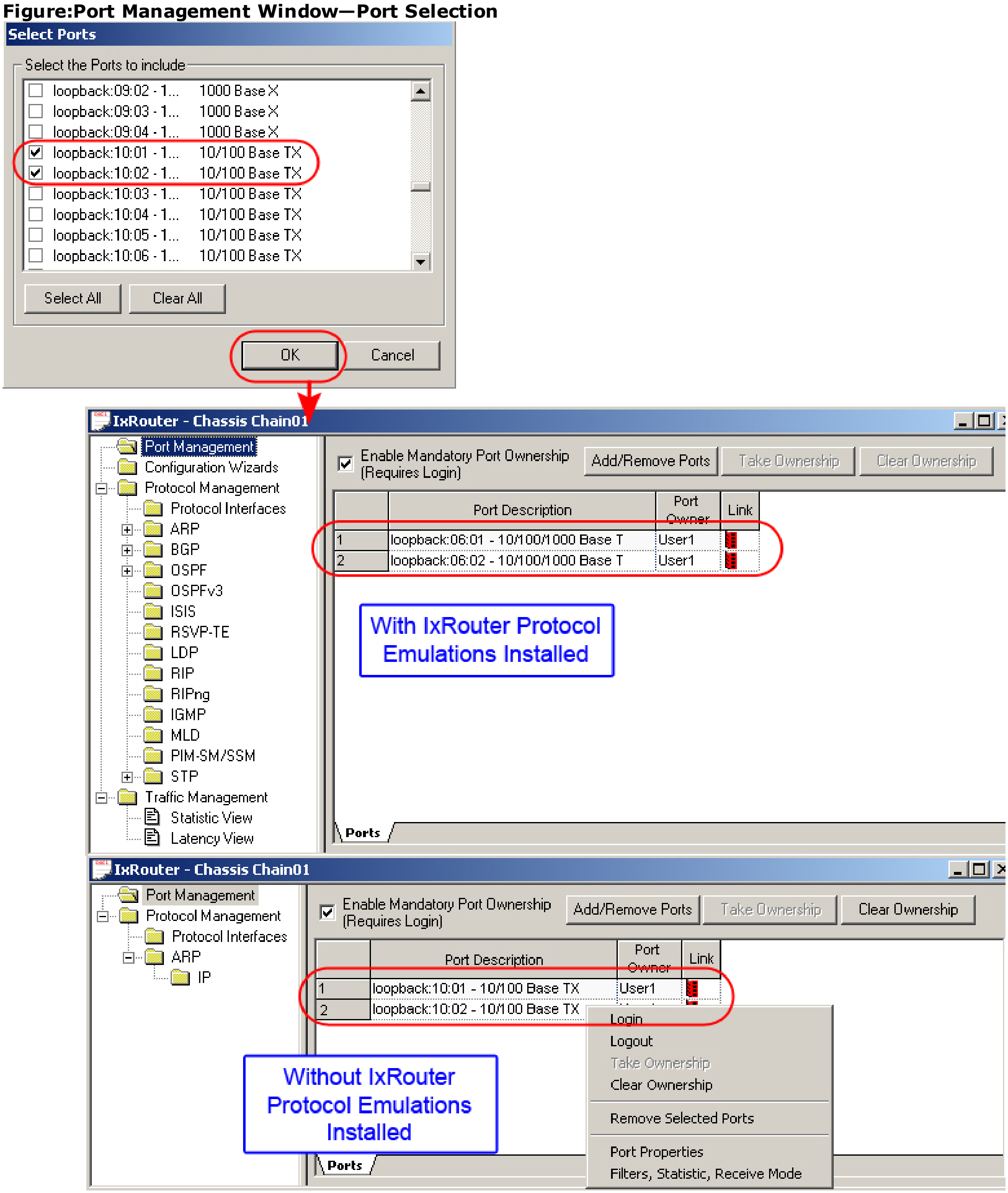
- If the 'Enable Mandatory Port Ownership' option is selected (the default setting), Login is **required**. Click the *Login* button to log on as the user. Click *OK* to close the dialog. After logging in, click the *Select Ports* button to display the Select Ports dialog, which lists all of the available ports on the current chassis. Go to *Selecting Ports* for information on selecting ports.
- If the 'Enable Mandatory Port Ownership' option is NOT selected, no Login is required. Click the *Select Ports* button to display the Select Ports dialog, which lists all of the available ports on the current chassis. Go to *Selecting Ports* for information on selecting ports.

Enabling the 'Auto Login at Startup' option allows to close and open IxRouter without logging in each time, as long as the IxExplorer window remains open. If the IxExplorer window is closed, and then re-opened, you must log on to IxRouter again.

Selecting Ports

The Select Ports dialog is shown in *Figure:Port Management Window—Port Selection*. In the dialog, select the check boxes for the port(s) that will be configured for protocols. Click *OK* to close the Select Ports and Login dialogs. The Port Management window will be displayed with the selected ports listed in the port grid (right pane). Examples are shown for IxRouter window configurations, with and without IxRouter Protocol emulations installed.

Figure:Port Management Window—Port Selection



The fields and controls available in this window and in the shortcut menu are described in *Table:Port Management Window*.

Table:Port Management Window

Section	Fields/Controls	Description
Header	Enable Mandatory Port Ownership	If this check box is selected, you MUST Login and take ownership of the port(s) to configure and use the port(s). If this check box is not selected, Login and port ownership are not required to configure and use the

Section	Fields/Controls	Description
		port(s). The default is selected. *Mandatory Port Ownership* for additional information.
	Add/Remove Ports	Click the *Add/Remove* button to display the Select Ports dialog and select (add ports) or deselect (remove ports) the check boxes for desired ports, as shown in *Figure:Port Management Window—Port Selection*. NOTE If ALL of the ports are removed from the table, the Port Management grid will be closed immediately, and the Login window will be displayed.
	Take Ownership	NOTE You must already be logged in for this feature to be available. Click the *Take Ownership* button to reserve the ownership and use of the port(s) that have been selected in the table.
	Clear Ownership	Click the *Clear Ownership* button to release the ownership and use of the port(s) that have been selected in the table.
Table	Port Description	The description (port name, type, and so forth) of the port is listed.
	Port Owner	The name of the user who has taken ownership of this port. NOTE Port ownership is mandatory if the 'Enable Mandatory Port Ownership' option is enabled through the check box.
	Link	The color of this icon indicates the state of the link for this port: • **Green**—Link is Up. • **Red**—Link is Down. • **Yellow**—Link is in loopback mode. • **Gray** —Link is unavailable because it is busy or it is an unsupported link type.
Shortcut Menu	Login	Click 'Login' to display the *User Login/Logout* dialog for the Protocol Window. Enter the user name and click *OK*. The protcol tree will expand to display all of the available protocols.
	Logout	Click 'Logout' to logout from the Protocol Window. The port entries in the table will become unavailable, and the protocol tree will close—only 'Port

Section	Fields/Controls	Description
		Management' will be visible.
	Take Ownership	NOTE You must already be logged in for this feature to be available. Click 'Take Ownership' to reserve the ownership and use of the port(s) that have been selected in the table.
	Clear Ownership	Click 'Clear Ownership' to release the ownership and use of the port(s) that have been selected in the table.
	Remove Selected Ports	Click 'Remove Selected Ports' to immediately delete the selected port(s) from the table. NOTE If ALL of the ports are removed from the table, the Port Management grid will be closed immediately, and the Login window will be displayed.
	Port Properties	(Operates for only **one port** at a time.) Click 'Port Properties' to display the Port Properties dialog for the selected/highlighted port. Refer to *IxExplorer Users Guide - Port Properties* chapter, for additional information on Port Properties dialogs.
	Filter, Statistic, Receive Mode	(Operates for only **one port** at a time.) Click 'FIlter, Statistic, Receive Mode' to display the Filter, Statistic, Receive Mode dialogs for the selected/highlighted port. Refer to *IxExplorer Users Guide - Filter, Statistics, Receive Mode* chapter, for additional information on Filter, Statistic, Receive Mode dialogs.

Mandatory Port Ownership

The Mandatory Port Ownership feature prevents other users from overwriting port configurations and interrupting the test process on the port.

If the mandatory port ownership feature is enabled (the default setting), you must log on through the Port Management window—Login window, or, through the IxExplorer Login dialog box, available from the 'Multiuser' menu in the IxExplorer main toolbar).

New IxExplorer/IxRouter Session

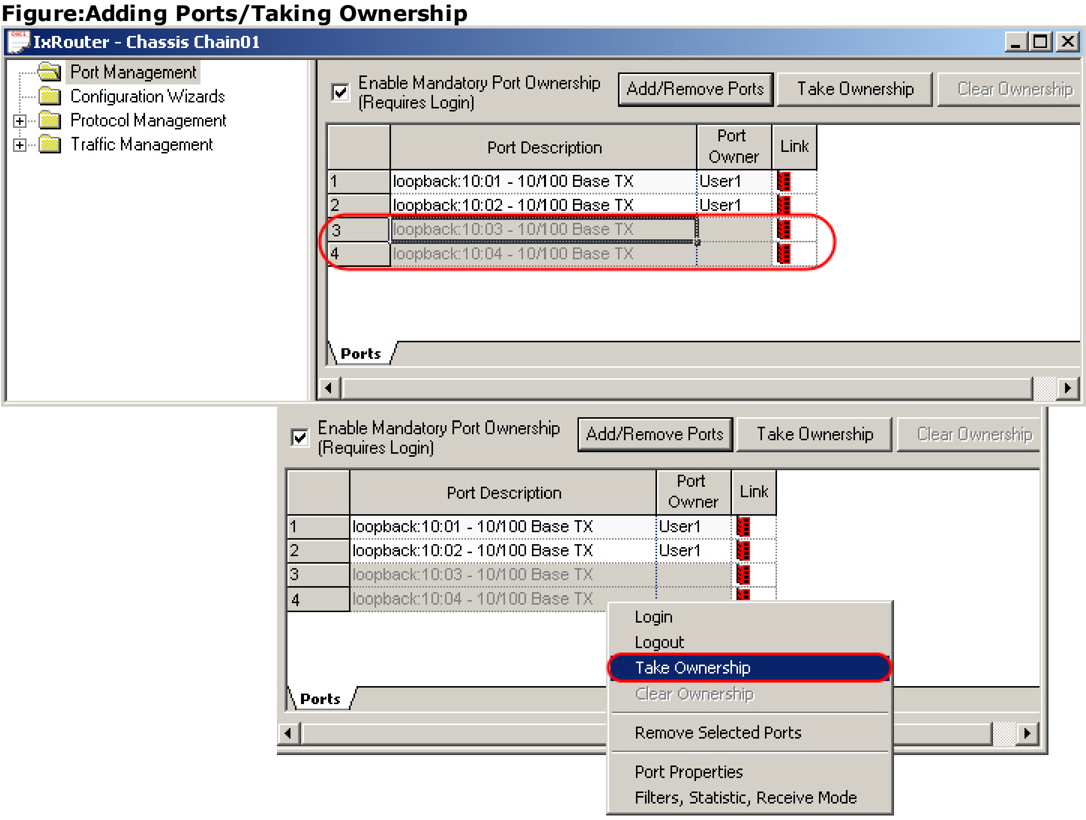
The procedure for logging in and setting up ports, when IxExplorer and IxRouter are first opened for a new session, or when all ports have been removed from the Port Management table, is covered in the following sections:

- *Login Window*
- *Selecting Ports*

Adding Ports/Taking Ownership

When ports are added after the initial (active) port selection, the new ports are listed in the Port Management window table, but are unavailable (dimmed), as shown in *Figure:Adding Ports/Taking Ownership*. Use the right-click shortcut menu and click 'Take Ownership' to make the selected ports available for configuration.

Figure:Adding Ports/Taking Ownership



Reopening IxRouter Window

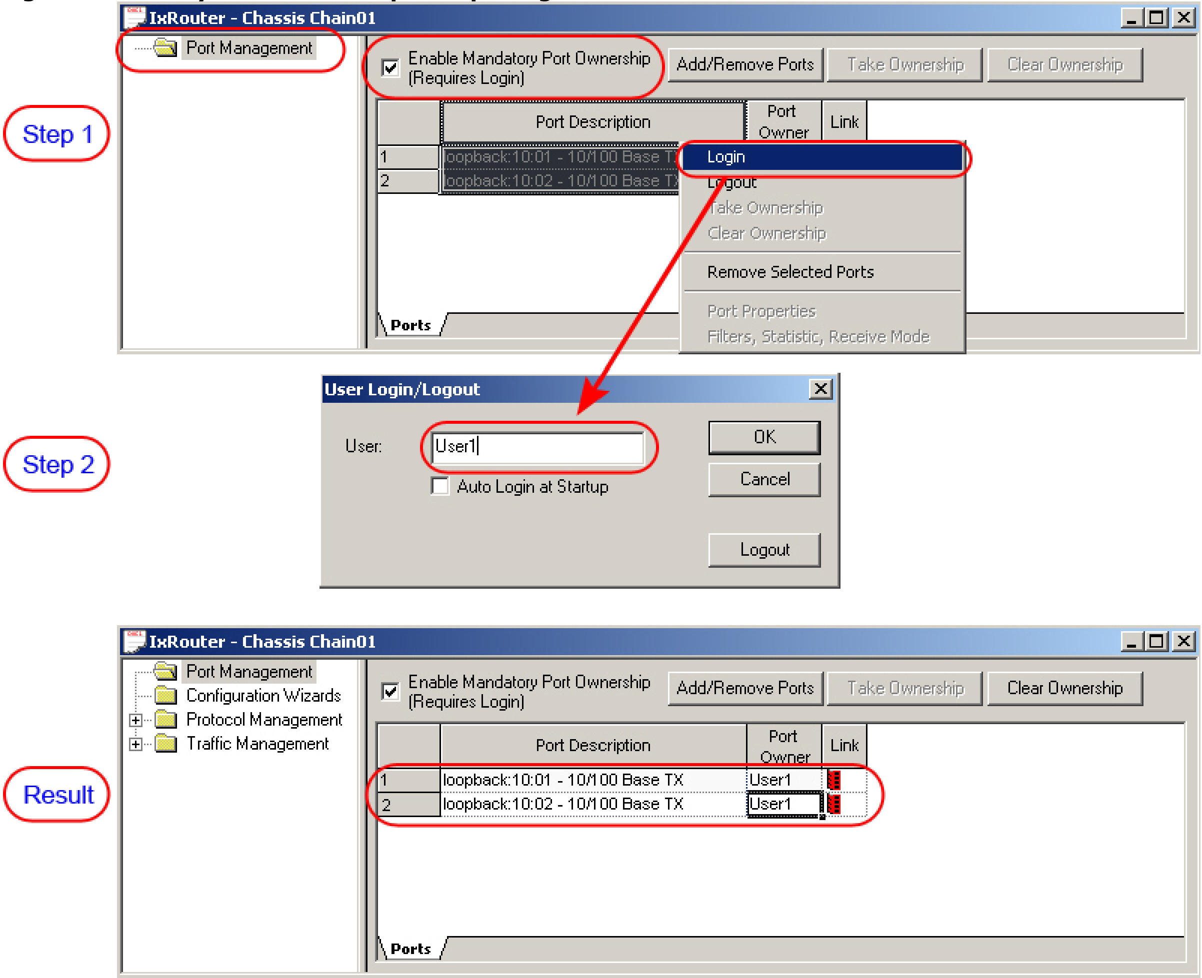
If the IxExplorer Window is closed, IxRouter is also closed. When IxExplorer is reopened while Mandatory Port Ownership is enabled, you will have to follow the procedure shown in *Figure:Mandatory Port Ownership—Reopening IxRouter Window* to regain access to IxRouter and the previously selected ports.

After logging in, right-click in a port entry in the Port Management window to open the shortcut menu, as shown in *Figure:Mandatory Port Ownership—Reopening IxRouter Window*. Click 'Take Ownership,' or click the *Take Ownership* button in the window header, to assign the Login User name to the port.

NOTE

Enabling the 'Auto Login at Startup' option allows to close and open IxRouter without logging in each time, as long as the IxExplorer window remains open. If the IxExplorer window is **closed**, and then re-opened, you must log on to IxRouter again.

Figure:Mandatory Port Ownership—Reopening IxRouter Window



Protocol Management Window

The Protocol Management window allows to enable routing protocol emulations on a specified port, as shown in *Figure:Protocol Management Window*. Examples are shown for IxRouter window configurations with and without IxRouter protocol emulations installed. The available routing protocols listed will depend on which protocol emulations have been purchased and installed.

The protocols can be enabled one at a time by selecting the check boxes. Or, all of the protocols available for the port can be enabled simultaneously by right-clicking the number field at the left end of the row and clicking 'Enable Selection' in the shortcut menu, as shown in the figure.

Note that when a protocol is selected and enabled for one or more ports, a '+' sign appears next to the name of the protocol 'tree' in the left pane of the window. This symbol indicates that configuration windows are available for that protocol—in a tree structure below the protocol name.

Figure:Protocol Management Window

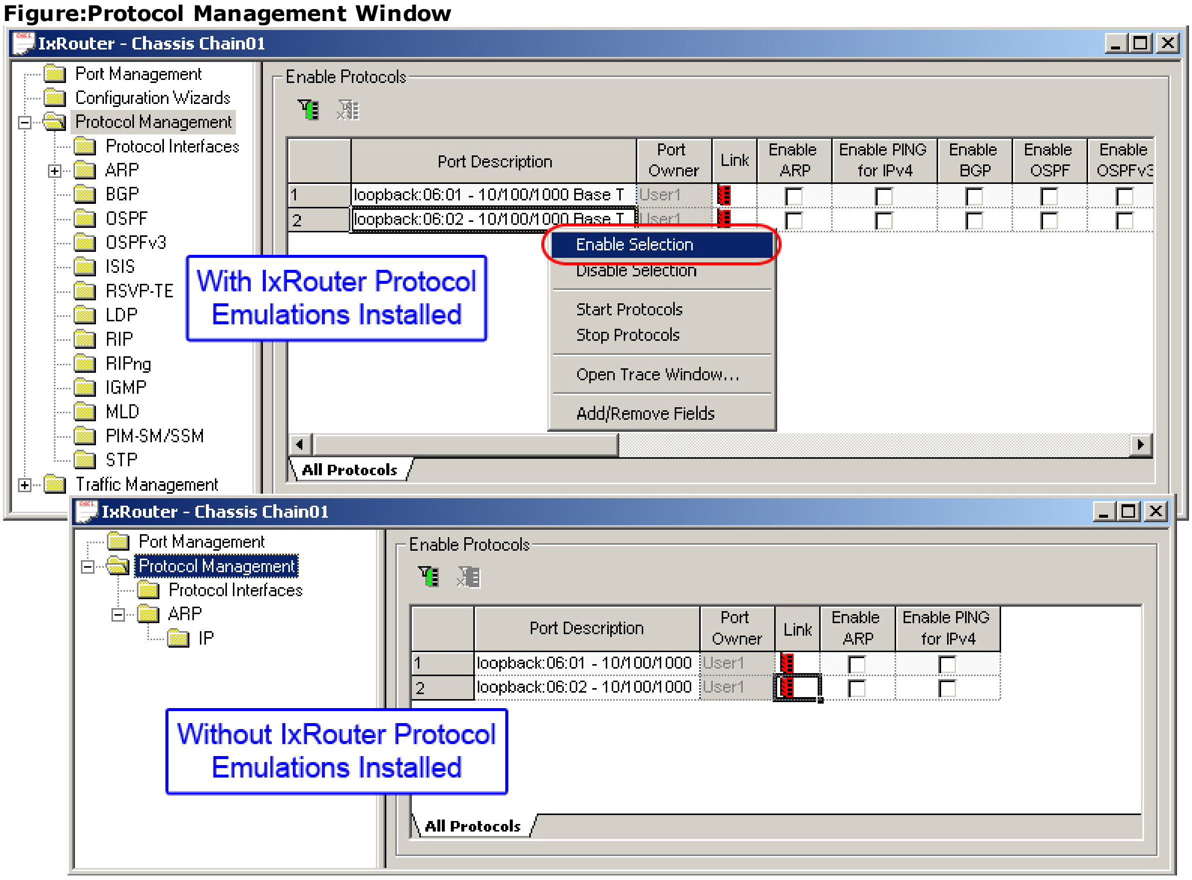
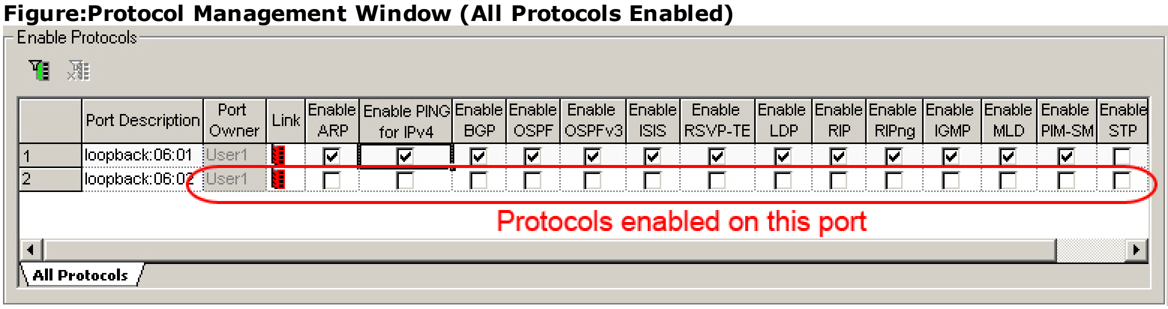
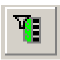
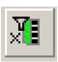


Figure:Protocol Management Window (All Protocols Enabled)



The fields and controls in the Protocol Management window, including the shortcut menu for the protocol grid, are described in *Table:Protocol Management Window*.

Table:Protocol Management Window

Section	Fields/Controls	Description
(Header)		Press the *Filter Selected Ports* button to display the Filter Ports dialog. Ports selected in the Filter Ports dialog will be displayed in the grid, but any non-selected ports will be removed from the grid as long as the Filter Ports feature is enabled. *Filter Ports Dialog* for additional information.
		Press the *Remove Port Filter* button to disable the Filter Ports feature, and non-filtered ports will reappear in the grid. *Filter Ports Dialog* for additional information.

Section	Fields/Controls	Description
(Table/Grid)	Port Description	The description (port name, type, and so forth) of the selected ports are listed.
	Port Owner	(Read-Only) The name of the user who has taken ownership of this port. NOTE Port ownership is mandatory if the 'Enable Mandatory Ownership' option is enabled through the check box in the Port Management window
	Link	The color of this icon indicates the state of the link: • **Green**—Link is Up. • **Red**—Link is Down. • **Yellow**—Link is in loopback mode. • **Gray**—Link is unavailable because it is busy or it is an unsupported link type.
	Enable ARP	(Non-POS cards only) If selected, enables ARP requests and responses for this port. ARP requests are received at the MAC level. For additional information on configuring the ARP protocol,*ARP*.
	Enable PING for IPv4	If selected, enables IPv4 PING transmission and reception for this port. PING messages are IPv4 ICMP messages of type *Echo Request.* Responses are IPv4 ICMP message of type *Echo Response*. For additional information on configuring the ICMP/PING protocol, ICMP/PINGv4.
	Enable BGP	If selected, enables BGP testing for this port. Refer to the BGP Chapter in the *IxNetwork User Guide* for additional information.
	Enable OSPF(v2)	If selected, enables OSPF testing for this port. Refer to the OSPF Chapter in the *IxNetwork User Guide* for additional information.
	Enable OSPFv3	If selected, enables OSPFv3 testing for this port. Refer to the OSPF Chapter in the *IxNetwork User Guide* for additional information.
	Enable ISIS	If selected, enables ISIS testing for this port. Refer to the ISIS Chapter in the *IxNetwork User Guide* for additional information.
	Enable RSVP-TE	If selected, enables RSVP-TE testing for this port. Refer to the RSVP-TE Chapter in the *IxNetwork User Guide* for additional information.
	Enable LDP	If selected, enables LDP testing for this port.

Section	Fields/Controls	Description
		Refer to the LDP Chapter in the *IxNetwork User Guide* for additional information.
	Enable RIP	If selected, enables RIP testing for this port. Refer to the RIP Chapter in the *IxNetwork User Guide* for additional information.
	Enable RIPng	If selected, enables RIPng testing for this port. Refer to the RIPng Chapter in the *IxNetwork User Guide* for additional information.
	Enable IGMP	If selected, enables IGMP testing for this port. Refer to the IGMP Chapter in the *IxNetwork User Guide* for additional information.
	Enable MLD	If selected, enables MLD testing for this port. Refer to the MLD Chapter in the *IxNetwork User Guide* for additional information.
	Enable PIM-SM	If selected, enables PIM-SM testing for this port. Refer to the PIM-SM/SSM Chapter in the *IxNetwork User Guide* for additional information.
Shortcut Menu	Enable Selection	If one protocol is selected for a port, clicking 'Enable Selection' enables the configuration and use of that particular protocol on the port. If the entire row of protocols is selected for a port, clicking 'Enable Selection' enables the configuration and use of ALL of the listed protocols on that port.
	Disable Selection	If one protocol is selected for a port, clicking 'Disable Selection' disables the configuration and use of that particular protocol on the port. If the entire row of protocols is selected for a port, clicking 'Disable Selection' disables the configuration and use of ALL of the listed protocols on that port.
	Start Protocols	Starts all protocols on any of the ports in this window which have been configured for the protocols.
	Stop Protocols	Stops all protocols on any ports in this window which are currently running protocols.
	Open Trace Window...	NOTE Available only when Protocol emulations are installed. Clicking 'Open Trace Window...' opens the *Trace and Statistics Window*, plus one *Port Trace* window for each port that has been selected. *Port Trace Window* for additional information.
	Add/Remove Fields	NOTE Available only when Protocol emulations are installed.

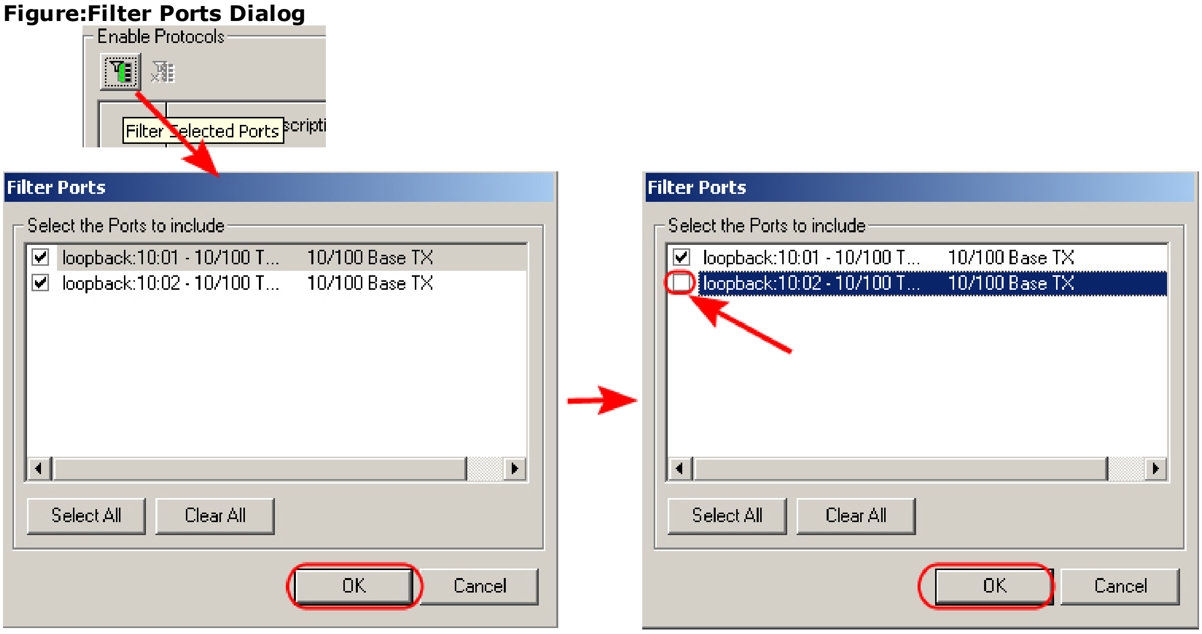
Section	Fields/Controls	Description
		Clicking 'Add/Remove Fields' displays the Add/Remove Field dialog for this window, where you may add or remove fields displayed in the grid, to customize the window. *Add/Remove Dialog* for additional information on the use of an Add/Remove Fields dialog.

Filter Ports Dialog

The Filter Ports feature allows only the specific ports selected (enabled) in the Filter Ports dialog to be displayed in the Protocol Management Window grid, when working with a sub-set of available ports is preferred.

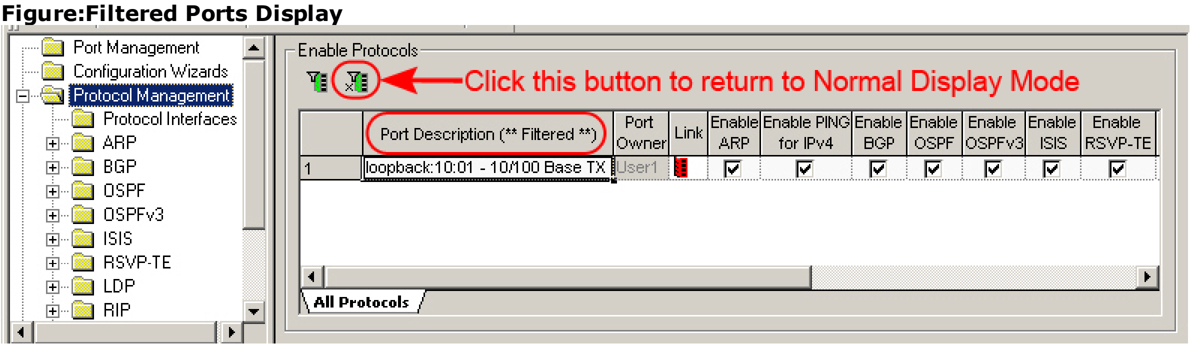
Click the *Filter Selected Ports* button in the Protocol Management window header, to display the Filter Ports dialog, as shown in *Figure:Filter Ports Dialog*. By default, all ports that have been selected in the Port Management window will be listed in the dialog. Deselect (uncheck) any ports that are not to be displayed in the Protocol Management window.

Figure:Filter Ports Dialog



Only the specific ports selected in the Filter Ports dialog will be displayed in the Protocol Management Window grid, as shown in *Figure:Filtered Ports Display* listed under ***'Port Description (**Filtered**)'***. Click the *Remove Port Filter* button to restore the original list of ports.

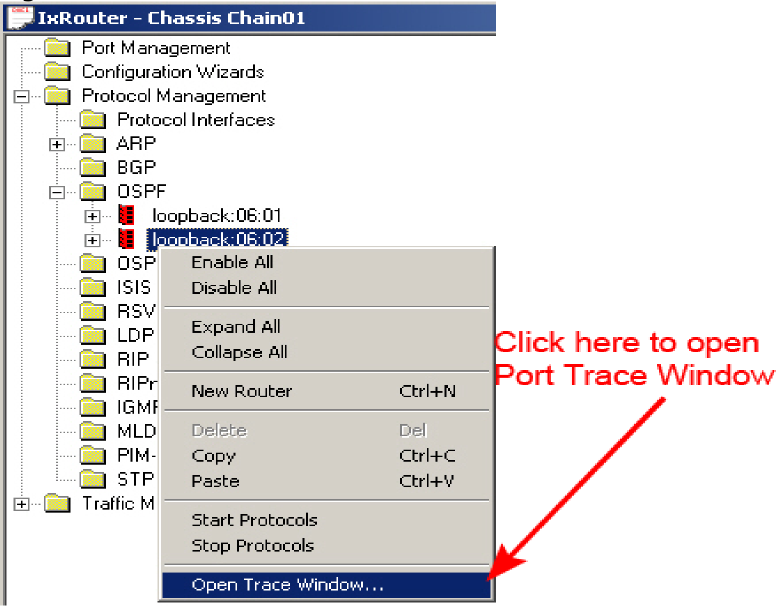
Figure:Filtered Ports Display



Port Trace Window

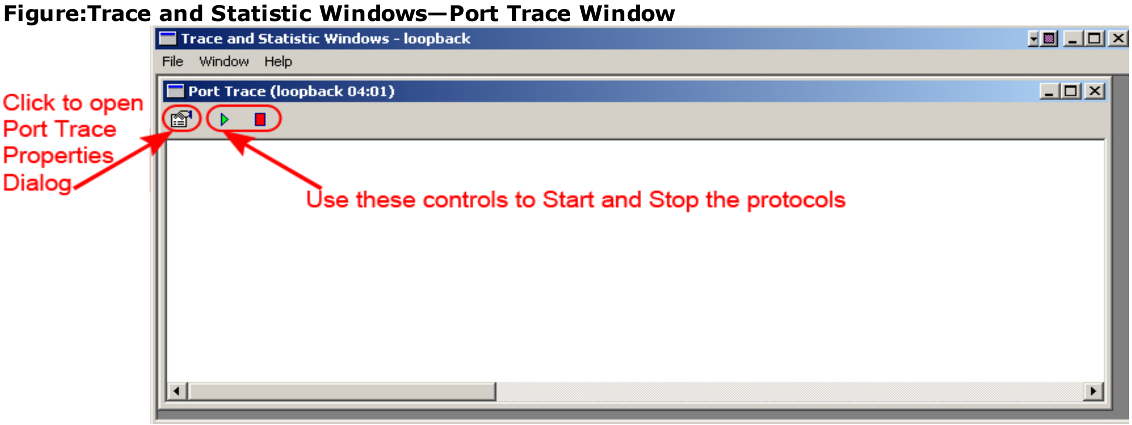
The Port Trace window can be accessed from a port item listed in the Protocol Window, or from the Protocol Management window pop-up menu. Right-clicking the port item displays a pop-up menu with a selection for 'Open Trace Window...,' as shown in *Figure:Port Trace Command*.

Figure:Port Trace Command



Clicking this menu option displays the Trace and Statistic Windows, with the Port Trace window included, as shown in *Figure:Trace and Statistic Windows—Port Trace Window*.

Figure:Trace and Statistic Windows—Port Trace Window

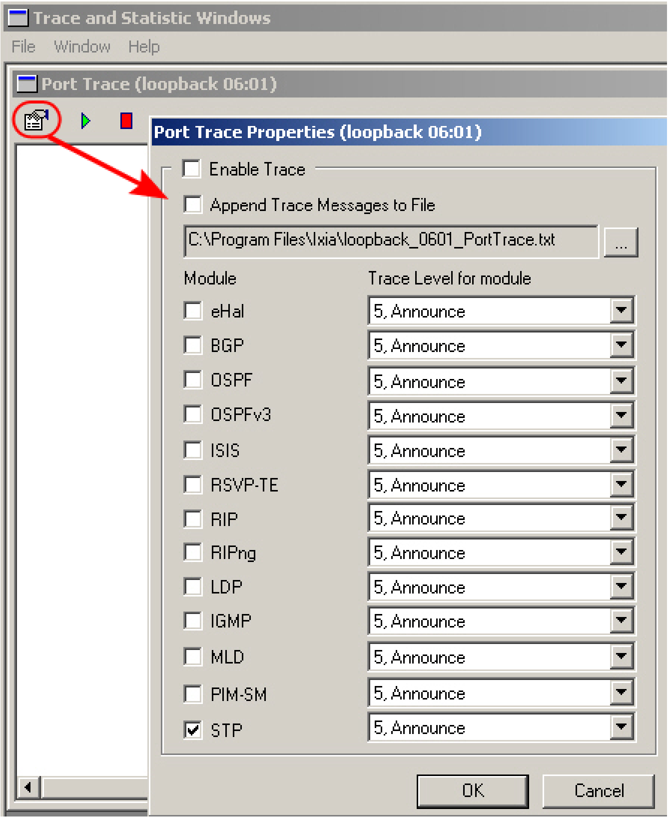


The information displayed in this window about the status of a port depends on the selections made in the Port Trace Properties dialog. *Port Trace Properties Dialog* for additional information on this dialog.

Port Trace Properties Dialog

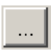
Click the *Edit* button in the Port Trace window toolbar to display the Port Trace Properties dialog, which is shown in *Figure:Port Trace Properties Dialog*.

Figure:Port Trace Properties Dialog



The fields and controls in this dialog are described in *Table:Port Trace Properties*.

Table:Port Trace Properties

Field/Control	Description
Enable Trace	Enables the Port Trace option for this port.
Append Trace Messages to File	Enables the saving of the port trace information to a file with the name automatically based on chassis/card/port plus '_ PortTrace.txt.'
	Press this button to display the Save As dialog, where the port trace information can be saved to a 'Trace' file, with the extension '.txt.'
Module	Choice of protocol to monitor in the Port Trace. Select one or more of the following protocols: • **eHal**—IxExplorer to IxServer communication • **BGP**—Border Gateway Protocol Version • **OSPF**—Open Shortest Path First • **ISIS**—Intermediate System - Intermediate System • **RSVP-TE**—Resource ReSerVation Protocol - Traffic Engineering • **RIP**—Routing Information Protocol • **LDP**—Label Distribution Protocol • **RIPng**—Routing Information Protocol Next Generation • **IGMP**—Internet Gateway Multicast Protocol

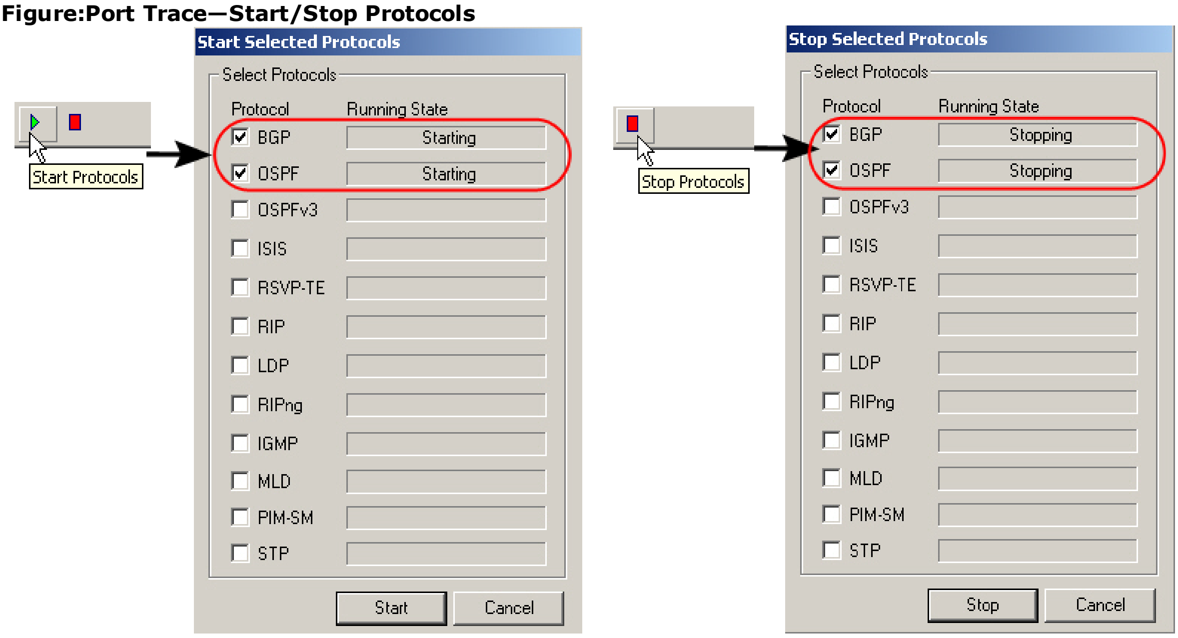
Field/Control	Description
	• **MLD**—Multicast Listener Discovery Protocol • **PIM-SM/SSM**—Protocol Independent Multicast - Sparse Mode, Protocol Independent Multicast–Source-Specific Multicast
Trace Level for Module	Select one of: • **1, Critical**—Unexpected occurrences, such as running out of memory on system. • **2, Error**—Indicates legitimate error condition (such as incorrect protocol configuration) that will most likely prevent the test from running. • **3, Alert**—Reserved for future use. • **4, Warning**—Situations that are some sort of error condition for the current protocol that is running, but not due to user configuration, such as a line cut. • **5, Announce**—(Default setting) All messages and protocol states of a non-periodic nature (Start, Stop, and so on.) • **6, Info**—All protocol events with some level of details displayed. • **7, Debug**—Same as info plus Hex dumps of frames received from the network. • **8, LowDebug**—Internal states of Ixia's protocol engine.
(Message)	'Trace is not enabled for the selected protocol(s). Select 'OK' to enable trace, 'Cancel' to leave it disabled.' The first time that you click 'Open Port Trace' for one of the port items listed under a particular protocol, this dialog appears automatically, with a checkmark entered for the protocol. This indicates that the Port Trace function is not yet enabled—you must click *OK* button to enable Port Trace for that protocol.

NOTE 'Announce' level (the default) should be sufficient for most uses. Info, Debug, and Low Debug decrease performance due to increased processing.

Port Trace Window–Start/Stop Protocols

The Port Trace Window provides toolbar controls for starting and stopping *enabled* protocols, as shown in *Figure:Port Trace—Start/Stop Protocols*.

Figure:Port Trace—Start/Stop Protocols



Additional Features in IxRouter

Additional features available in the IxRouter window are covered in the following sections:

- *IxRouter Window Display Options*
- *Add/Remove Dialog*
- *Add View*
- *IxRouter Window 'Refresh'*

IxRouter Window Display Options

The number and type of options in a shortcut menu will vary, depending on the type of parameters available for the window. An example showing the shortcut menu for the BGP port-level grid is shown in *Figure:IxRouter Window—Grid Shortcut Menu Example*.

Figure:IxRouter Window—Grid Shortcut Menu Example

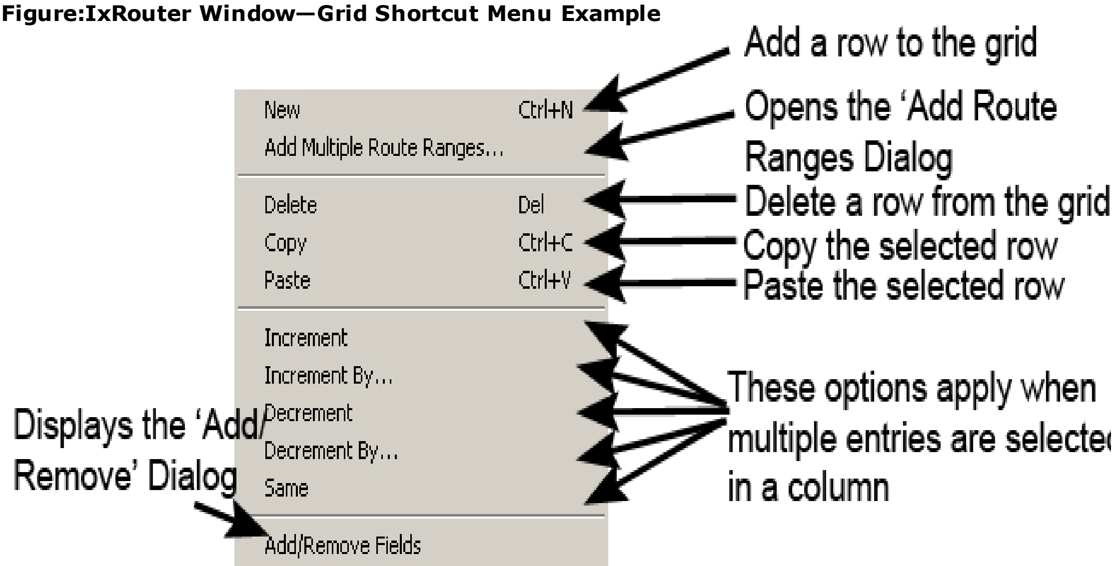
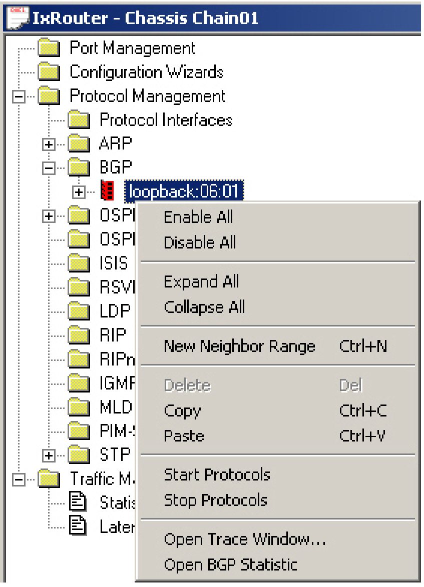


Figure:IxRouter Protocol Tree Shortcut Menu Example (for BGP Neighbor level)



The fields and controls in this dialog are described in *Table:IxRouter Protocol Tree Shortcut Menu Example (for BGP Neighbor level)*.

Table:IxRouter Protocol Tree Shortcut Menu Example (for BGP Neighbor level)

Field/Control	Description
Enable All	Enable all protocol items that have been configured for this level and levels below it in the tree.
Disable All	Disable all protocol items that have been configured for this level and levels below it in the tree.
Expand All	Open the protocol tree for all items below the selected item.
Collapse All	Close the protocol tree for all items below the selected item.
New Neighbor Range - Ctrl + N	(Other, different protocol items may be available depending the protocol and the level in the protocol tree.) In this example, adds a new BGP Neighbor Range for this port (in the grid to the right).
Delete - Del	If available, the selected item and all items below it in the tree will be deleted.
Copy - Ctrl + C	If available, copy the selected item and all of the items configured below it in the tree. For example, a BGP Neighbor configuration can be copied and pasted under the port.
Paste - Ctrl + V	If available, the selected item and all of the items configured below it in the tree can be pasted into the same level. For example, a BGP Neighbor configuration can be copied and pasted under the port.
Start Protocols	Starts the protocol engines for all enabled, configured items on this port.
Stop Protocols	Stops the protocol engines for all enabled, configured items on this port.

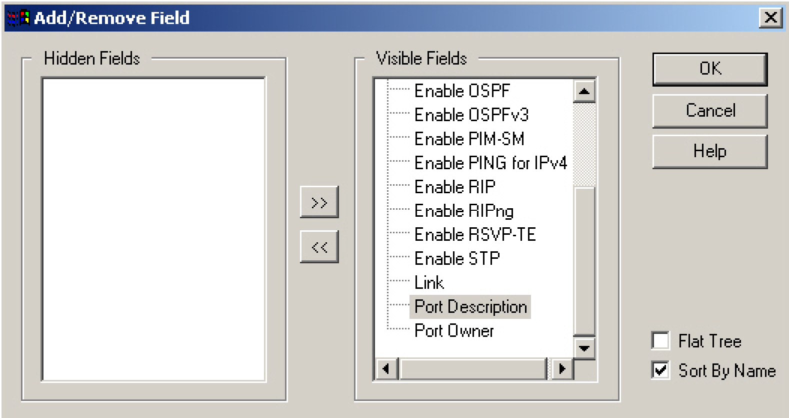
Field/Control	Description
Open Trace Window	Open the Port Trace Window for this port. Port Trace Window for additional information.
Open BGP Statistics	(This feature applies to BGP only) Open the BGP Port Stat Window for this port.

Add/Remove Dialog

The Add/Remove Field dialog allows to customize a spreadsheet/grid view in the IxRouter window. An example of the Add/Remove Field dialog is shown in *Figure:IxRouter Window—Add/Remove Fields (shown for Protocol Management Window)*.

NOTE This feature is available when protocol emulations have been installed.

Figure:IxRouter Window—Add/Remove Fields (shown for Protocol Management Window)



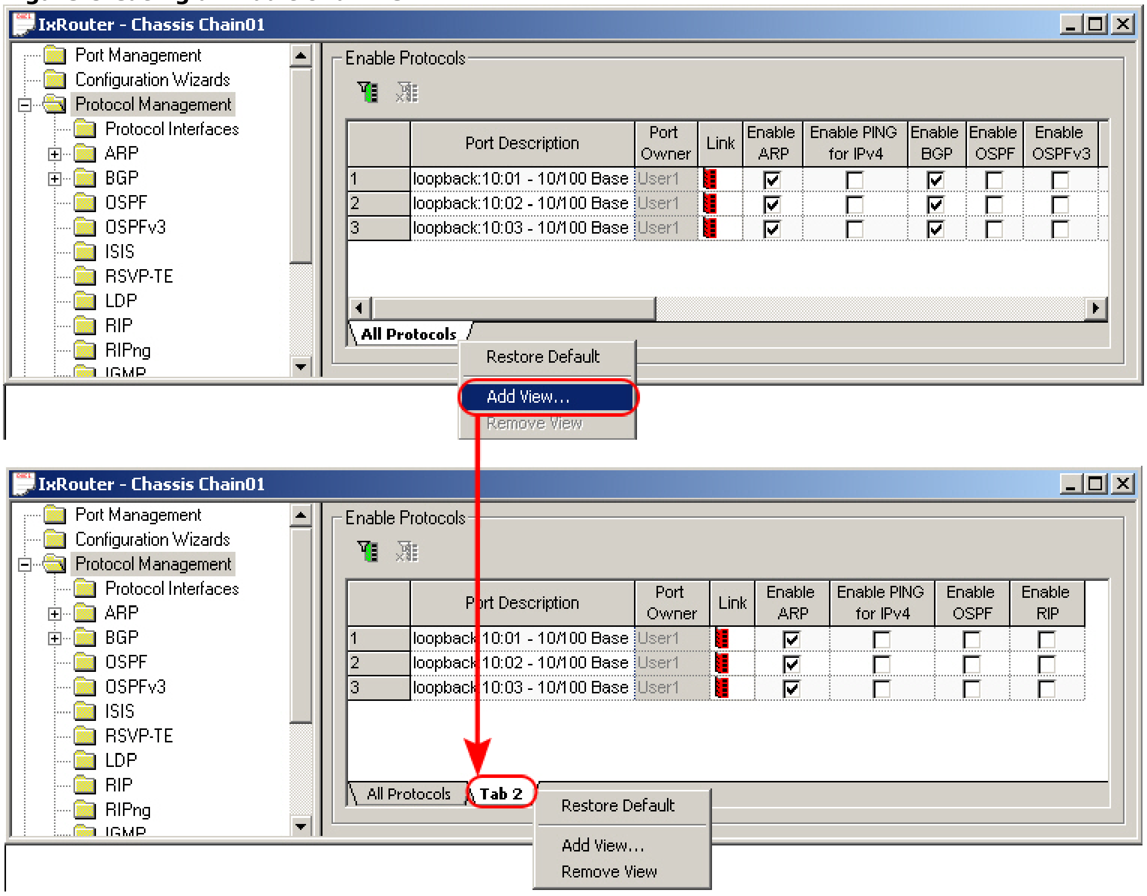
To create or modify a customized spreadsheet view, use the '>>' arrow to move a hidden field to the Visible Fields column and the '<<' arrow to move a visible field to the Hidden Fields column. Columns and rows may be rearranged by selecting the entire row or column and moving it (using the 'drag and drop' method) to its new location. The fields available depend on the particular protocol being configured, and the level of configuration within that protocol. The 'Flat Tree' check box allows to view lists which include all possible fields, without a hierarchy. The 'Sort by Name' check box allows to view lists with the field names in alphabetical order.

Add View

In the Protocol Management window, by default there is one tabbed spreadsheet view named 'All Protocols,' which lists all available protocols.

An additional tabbed view with a subset of the listed items can be created. Right-click the tab name, and select 'Add View.' The Add/Remove dialog (Add/Remove Dialog) will open so items can be moved to the 'Hidden Fields' list in the left pane. A subset of items will remain in the Visible Fields list. Click *OK* to close the dialog. The new subset view, 'Tab 2,' is displayed in the Protocol Management window.

Figure:Creating an Additional View

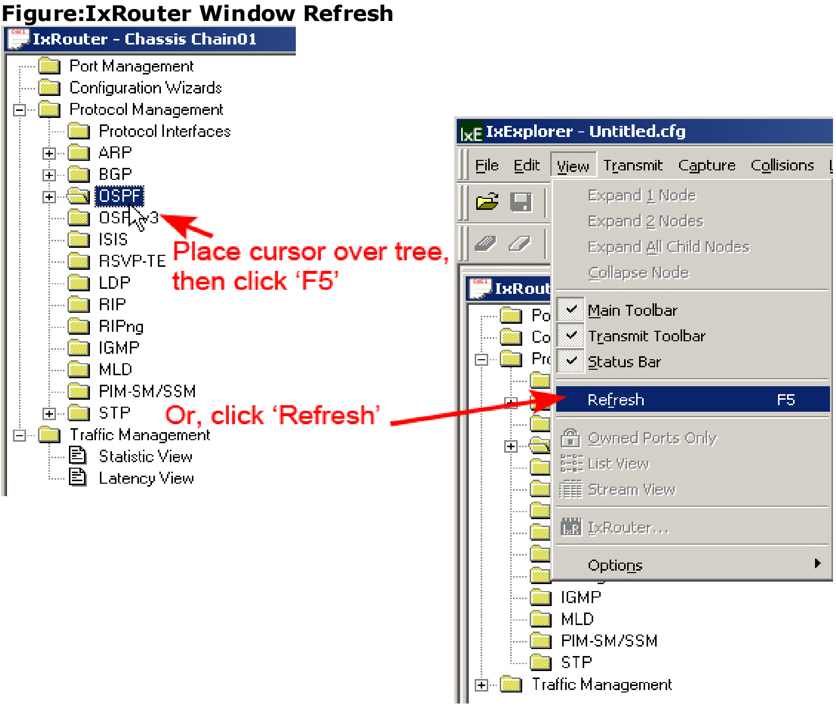


IxRouter Window 'Refresh'

The chassis configuration display can be 'refreshed' (updated) in the Protocol Window by:

- Pressing the *F5 (Refresh)* button when the focus is on the tree in the Protocol Window, or
- Going to the IxExplorer Main menu bar > View menu > Refresh, and clicking 'Refresh.'

Figure:IxRouter Window Refresh

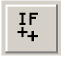


[This page intentionally left blank]

Chapter 10 - Protocol Interfaces

Multiple protocol interfaces can be configured for Ixia ports that support this capability, with the number of protocol interfaces being dependent on the amount of memory available on the Ixia port.

There are two methods available for creating one or more Protocol Interfaces for an Ixia port:

Configuration Method	Access Via	Description
Protocol Interfaces Wizard	 Click this button to display the Protocol Interfaces Wizard. Available in Protocol Interfaces window and in various windows for individual protocols.	Enter configuration information in the dialogs of the Protocol Interfaces Wizard. *Protocol Interface Wizard* for additional information.
Manual	Open Protocol Interfaces window in IxRouter Window tree.	Enter configuration information directly in the Protocol Interfaces window/grid. *Protocol Interfaces Window* for additional information.

Protocol Interfaces Window

The main Protocol Interfaces window is made up of multiple tabbed views. The window with combined views for Protocol Interfaces is shown in *Figure:Protocol Interfaces Tab*. The default Interface Description for the port is '[Empty],'until a protocol interface is created by you. The sets of tabbed windows are described in the following sections:

- *Protocol Interfaces Tab*
- *PTP Clock Configuration*
- *Unconnected Interfaces*
- *GRE Tunnels*
- *NPIV Protocol Interface*
- *Discovered Neighbors*
- *Interface Addresses*
- *DHCPv4 Discovered Information*
- *DHCPv6 Discovered Information*
- *FCoE Discovered Information*
- *PTP Discovered Information*

NOTE
You will not be able to select DHCPv4-enabled interfaces for use with protocol emulations, with the exception of IGMP.
You will not be able to select DHCPv6-enabled interfaces for use with protocol

NOTE emulations.

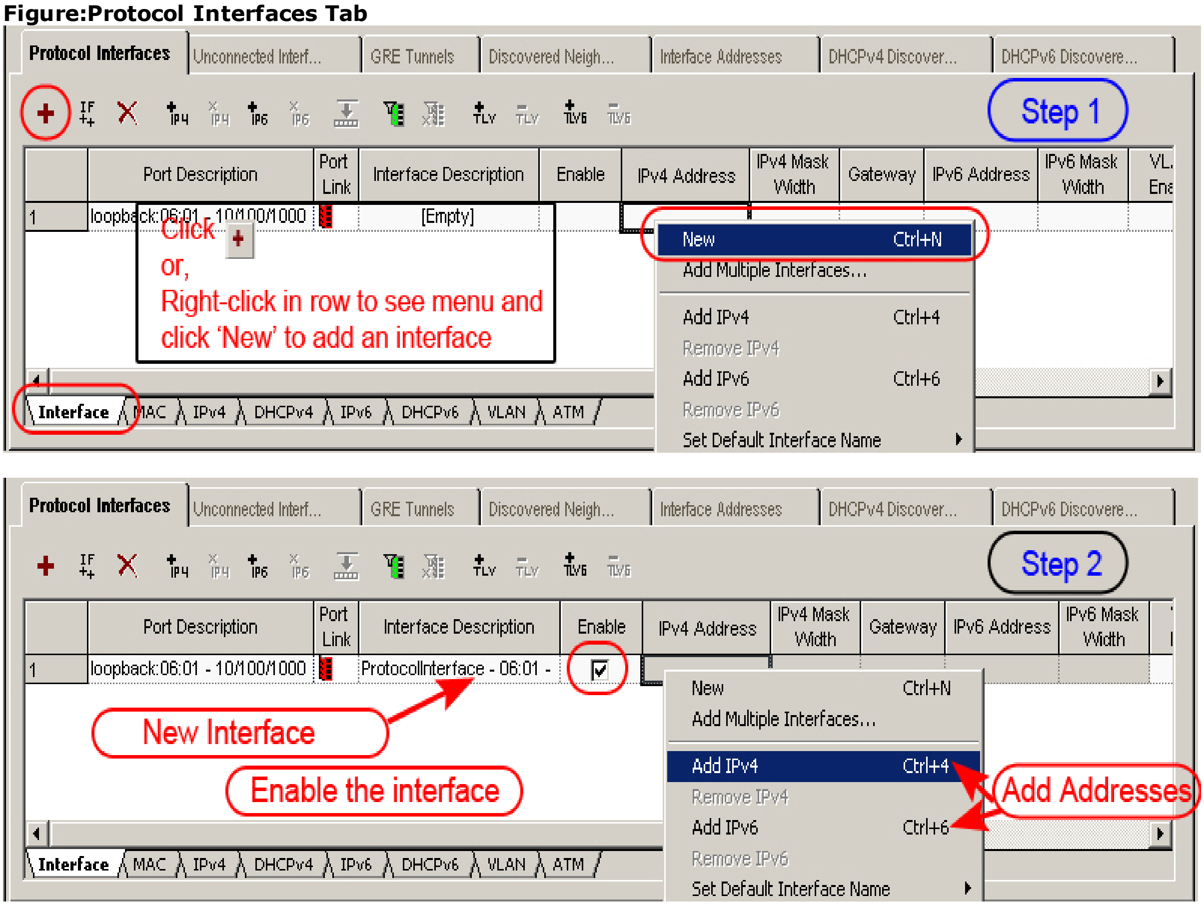
DHCP is applicable only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.

Protocol Interfaces Tab

The Protocol Interfaces tab (for ‘connected’ protocol interfaces) is shown in *Figure:Protocol Interfaces Tab*, below. Steps 1 and 2 show how to create a protocol interface for the port, add addresses, and then enable the interface.

NOTE The ‘Enable’ box MUST be selected to make a protocol interface active and available for configuration with routing protocols.

Figure:Protocol Interfaces Tab



Individual views for MAC, IPv4, DHCPv4, IPv6, DHCPv6, and VLAN are shown in *Figure:Protocol Interfaces (Views for MAC, IPv4, DHCPv4, IPv6 & DHCPv6)* and *Figure:Protocol Interfaces—VLAN*. The ATM View, available for configuration for ATM-capable modules only, is shown in *Figure:Protocol Interfaces—ATM (active for ATM ports ONLY)*. The FCoE View is shown in *Figure:Protocol Interfaces—FC/FCoE* and the PTP View is shown in *Figure:Protocol Interfaces—PTP*. The DCBX view is shown in *Figure:Protocol Interfaces—DCBX / LLDP*.

NOTE IPv6 has a minimum frame size of 1280 bytes. When creating IPv6 protocol interfaces for POS ports, it is important that the desired negotiated port Transmit MRU value is set to 1280 bytes or higher. If this is not done, protocol

NOTE

interfaces cannot be associated with the port.

For more information on setting the desired Transmit MRU value, see the 'PPP Properties' section of the 'Port Properties—POS and ATM Families' chapter.

Figure:Protocol Interfaces (Views for MAC, IPv4, DHCPv4, IPv6 & DHCPv6)

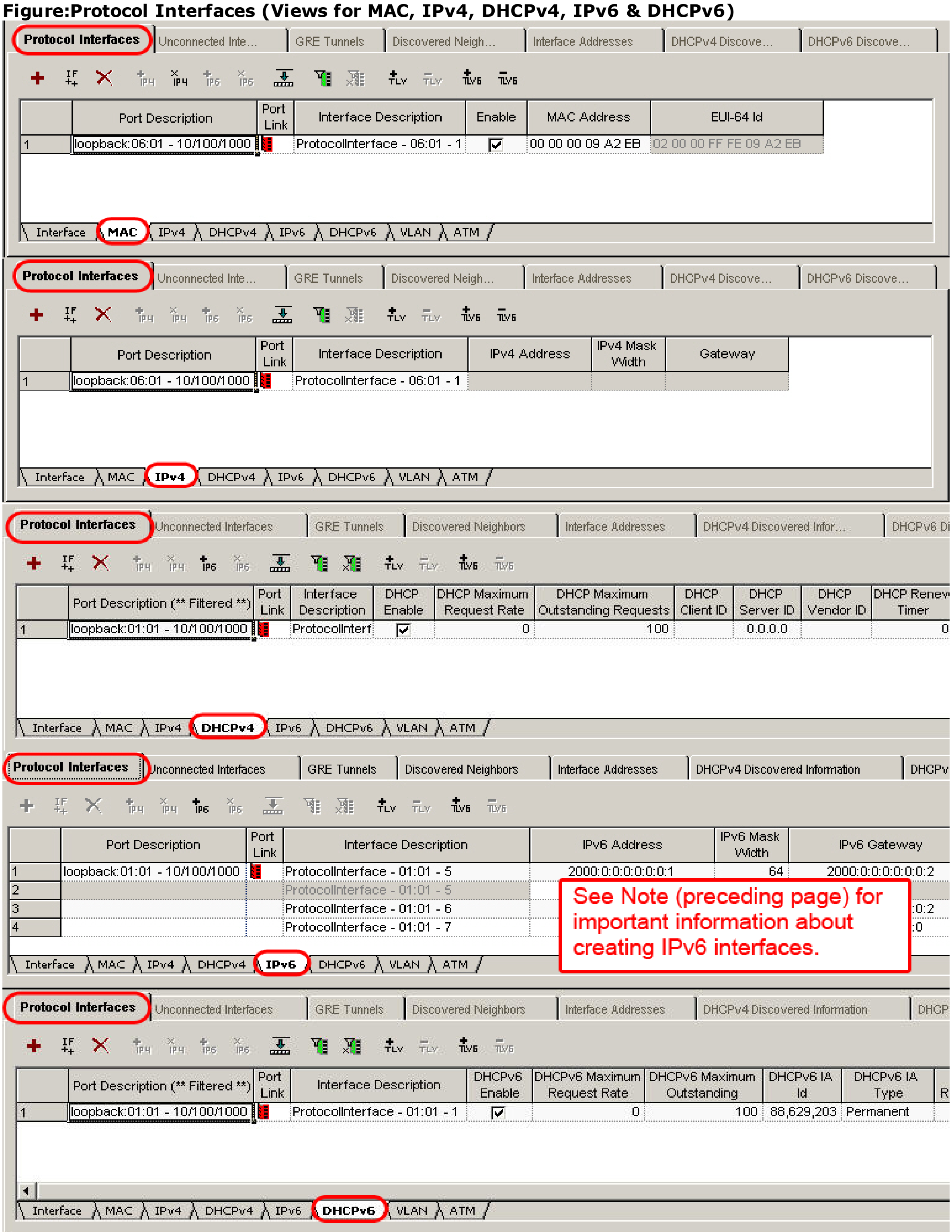


Figure:Protocol Interfaces—VLAN

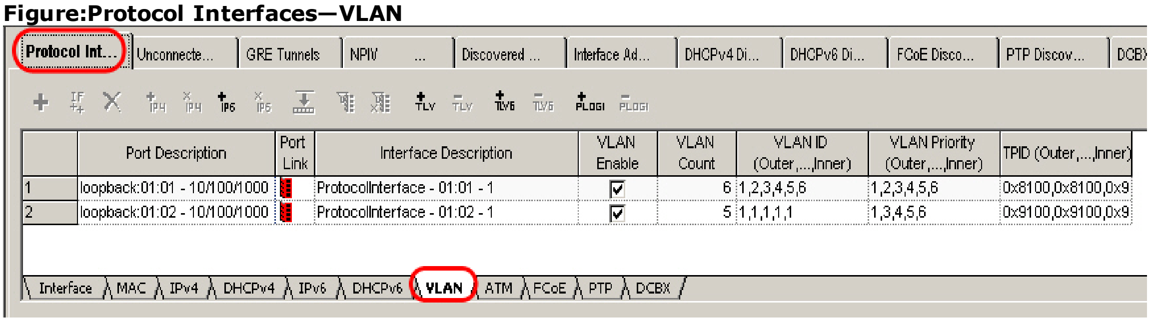


Figure:Protocol Interfaces—ATM (active for ATM ports ONLY)

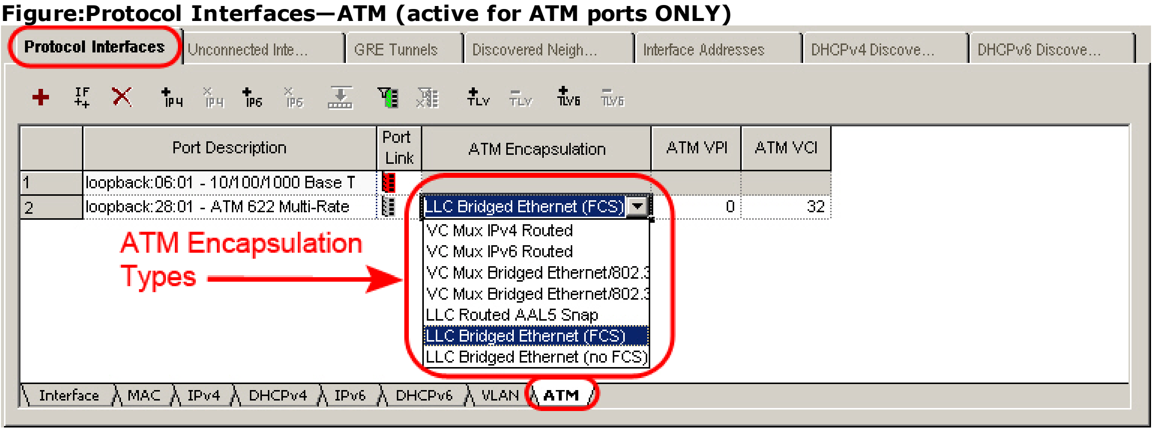


Figure:Protocol Interfaces—FC/FCoE

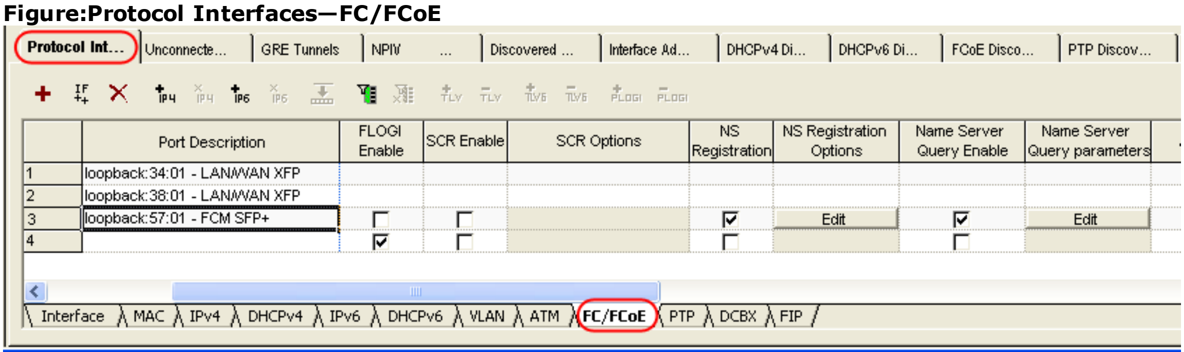


Figure:Protocol Interfaces—PTP

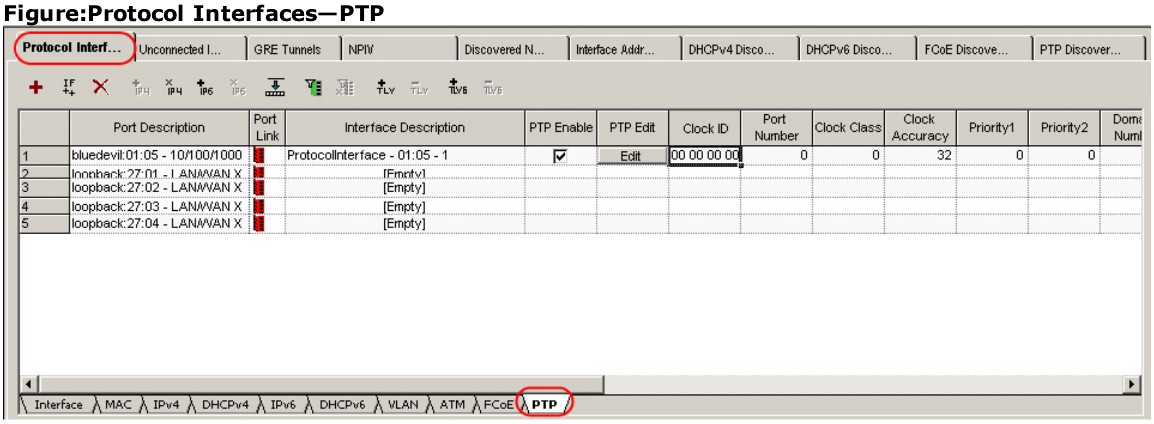
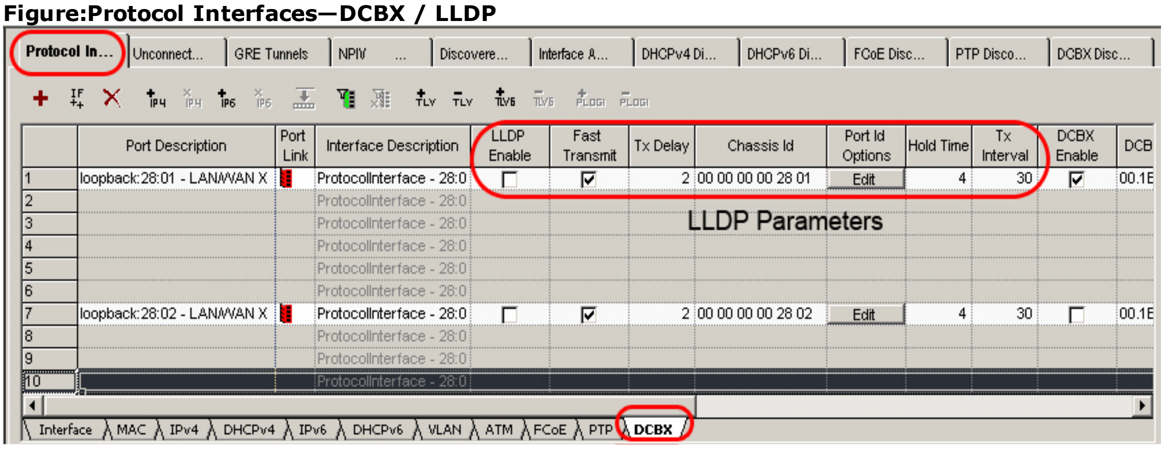


Figure:Protocol Interfaces—DCBX / LLDP



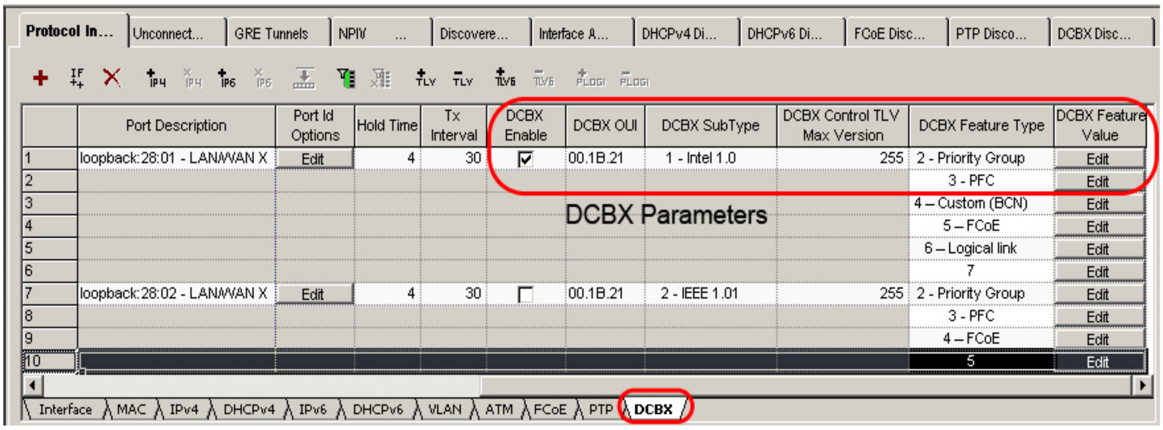
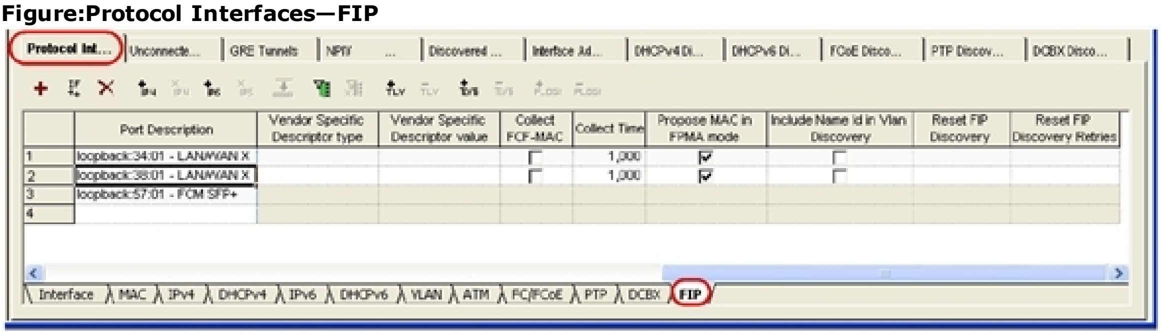


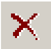
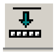
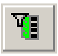
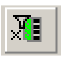
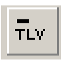
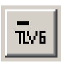
Figure:Protocol Interfaces—FIP



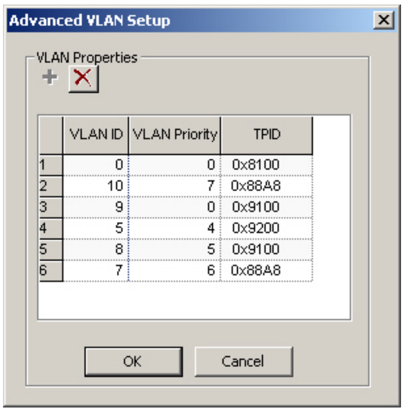
The fields and controls shown in these views are described in *Table:Protocol Interfaces tab*. You may manually edit any of the available entries in the view by placing the cursor over the value field or table cell and pressing the ***F2*** key.

Table:Protocol Interfaces tab

View/Section	Field/Control	Description
Protocol Interfaces - Header		Click this button to add a protocol interface to the selected port in the Interface view. NOTE The number of protocol interfaces that can be added depends on the amount of memory available.
		Click this button to display the Protocol Interfaces wizard dialog for configuring one or more protocol interfaces.

View/Section	Field/Control	Description
		Protocol Interface Wizard for additional information.
		Click this button to delete the selected interface entry (ies) from the table.
		Click this button to add an IPv4 Address to a Selected Interface.
		Click this button to delete the IPv4 Address from a Selected Interface.
		Click this button to add an IPv6 Address to a Selected Interface.
		Click this button to delete the selected IPv6 Address(es) from a Selected Interface.
		For Ethernet type ports only. Click this button to transmit an ARP request for the selected entry(ies).
		Filter Selected Ports. Click this button to display the Filter Port dialog. This dialog allows to specify which of the available ports will be displayed in the table. Then the Port Description column will be automatically relabeled as 'Port Description (** Filtered **). *Filter Ports Dialog* for additional information on Port Filtering.
		Remove Port Filter. Click this button to disable the Port Filter feature, and all available ports are displayed in the table.
		Add DHCPv4 TLV. Add a DHCPv4 TLV entry to the table.
		Remove DHCPv4 TLV. Delete the selected DHCPv4 TLV entry(ies) from the table.
		Add DHCPv6 TLV. Add a DHCPv6 TLV entry to the table.
		Remove DHCPv6 TLV. Delete the selected DHCPv6 TLV entry(ies) from the table.
Fields for all Protocol Interface Views	Port Description	The identifier for the port including card and port numbers, and the port type.
	Port Link	The color of this icon indicates the state of the link: • **Green**—Link is Up. • **Red**—Link is Down.

View/Section	Field/Control	Description
		• **Yellow**—Link is in loopback mode. • **Gray**—Link is unavailable because it is busy or it is an unsupported link type.
	Interface Description	When an interface is added to the port in this window, the new Interface description consists of three items: • The interface number on this port. • The card number / port number. • Protocol Interface. (You may manually edit the Interface Description.)
Interface View	Enable	Select this box to enable the selected protocol interface.
	IPv4 Address	When an interface is selected, an IPv4 address may be added to that interface, using the *Add* button, or 'Add' from the Interfaces pop-up menu. Adding the IPv4 Address also automatically adds an IPv4 Mask Width and a Gateway address to the interface, using the default values.
	IPv4 Mask Width	The length of the IPv4 network mask to be used with the IPv4 address, in bits. The default IPv4 mask width is 24 bits.
	Gateway	The IPv4 address of the 'Gateway' to the network, typically an interface on the DUT.
	IPv6 Address	When an interface is selected, an IPv6 address may be added to that interface, using the *Add* button or 'Add' from the Interfaces pop-up menu. Adding the IPv6 Address also automatically adds an IPv6 Mask Width to the interface, using the default values. Multiple IPv6 addresses may be added to each interface.
	IPv6 Mask Width	The number of bits for the IPv6 network mask to be used with the IPv6 address, starting with the most significant bit of the address (at the left). These bits (n bits) comprise the network part of the address. The remaining bits in the address (128 minus n) comprise the host part of the address. The default IPv6 Mask width is 64 bits.
	IPv6 Gateway	(Optional) There can be one gateway per IPv6 interface.
VLAN View	VLAN Enable	(For IPv4 only) If selected, enables the VLAN option on this port, with one VLAN ID per interface. Double-click this field or any of the following VLAN fields to open the Advanced VLAN Setup dialog, in which these values can be configured.

View/Section	Field/Control	Description
		
	VLAN Count	The number of VLANs (up to 6)
	VLAN ID	(For IPv4 only) If the VLAN option is enabled for the current interface, a VLAN ID may be added to the packet, to identify the VLAN that the packet belongs to.
	VLAN Priority (Outer, ..., Inner)	The user priority of the VLAN tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
	TPID (Outer, ..., Inner)	Tag Protocol ID: Ether types identify the protocol that follows the VLAN header. Select from available hex options: 0x8100, 0x88A8, 0x9100, 0x9200
MAC View	MAC Address	For non-POS ports/interfaces only. When a New interface is added to the port, a MAC (Layer 2/Ethernet) address is automatically assigned to that interface.
	EUI-64 Id	This is the 64-bit IEEE Modified EUI Id value for the Interface Identifier portion of the IPv6 address. For **Ethernet** modules, this field is not editable. The value is automatically calculated, based on the 48-bit MAC address. For more information on how this value is calculated, refer to the IPv6 Interface Identifiers (IIDs) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*. For OC48 and OC192 POS modules, you can edit the value.
IPv4 View	IPv4 Address	When an interface is selected, exactly one IPv4 address may be added to that interface, using the *Add* button, or 'Add' option in the Interfaces pop-up menu. Adding the IPv4 Address also automatically adds an IPv4 Mask Width and a Gateway address to the interface, using the default values.
	IPv4 Mask Width	The length of the IPv4 network mask to be used with the IPv4 address, in bits. The default IPv4 mask width is 24 bits.
	Gateway	The IPv4 address of the 'Gateway' to the network, typ-

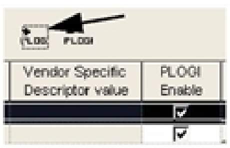
View/Section	Field/Control	Description
		ically an interface on the DUT.
	Auto Arp	If selected and then MAC interface is enabled, the Learned IP Addresses and Learned MAC Addresses are automatically shown in the ARP Table.
DHCPv4 View	DHCP Enable	**(Applies only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.)** NOTE You will not be able to select DHCPv4-enabled interfaces for use with protocol emulations, with the exception of IGMP. If selected, the IPv4 DHCP client feature will be enabled. DHCP negotiation will be started and an IPv4 address learned from the DHCP server will be assigned automatically to the protocol interface. When this feature is enabled, the fields in the IPv4 view will be dimmed and unavailable for configuration by you. If an IPv4 address has already been assigned to the port, a warning message will open, requiring a choice by you to continue with DHCP address assignment to replace the existing IPv4 address, or to keep the existing address.
	DHCP (DHCPv6) Maximum Request Rate	(For rate control) The user-specified maximum number of Request messages that can be sent per second from the client to the server, requesting an IPv4 address. A value of zero (0) indicates that there will be no rate control, that is, requests will be sent as fast as possible.
	DHCP (DHCPv6) Maximum Outstanding	The maximum number of DHCP requests that can be pending, waiting replies from the server. If this number is reached, no further requests can be sent until an acknowledgment is received for a pending request.
	DHCP Client ID	(string) You may optionally assign an identifier for the Client. This value must be unique on the subnet where the DHCP Client is located. If this value is *not* configured by you, the MAC address of the Protocol Interface will automatically be used as the Client ID.
	DHCP Server ID	(4-octet IPv4 address) If this value is configured by you, the DHCP client state machine will perform negotiations only with this specified DHCP server. This value is used to identify the DHCP Server and as a destination address from the client.
	DHCP Vendor ID	(string)

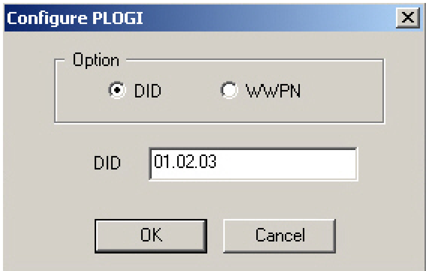
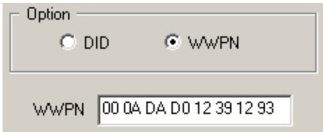
View/Section	Field/Control	Description
		The optional, user-assigned Vendor ID (vendor class identifier).
	DHCP Renew Timer	(in seconds) The user-specified value and the lease timer (from the DHCP Server) are compared. The lowest value is used as the release/renew timer. After this time period has elapsed, the address will be renewed. Maximum is 4,294,967,295 (decimal) = 0xFFFFFFF (hex). This value equals 'infinity,' and indicates that the IP address allocation is 'permanent.'
	Relay Agent Address	Set by the server, to be used in optional cross-gateway starting.
(DHCP TLVs)		DHCP TLVs (tuples) for custom DHCP options. Additional TLV entries may be added by pressing the  button.
	DHCP Type	(integer) The identifier or 'tag' for this DHCP option.
	DHCP Value	The DHCP option value field may contain data for configuration information such as IPv4 addresses, time server information, and so on.
IPv6 View	NOTE IPv6 has a maximum transmission unit (MTU) minimum of 1280. When creating IPv6 protocol interfaces for POS ports, it is important that the desired negotiated port Transmit MRU value is 1280 bytes or greater. If this is not done, protocol interfaces cannot be associated with the port. For more information on setting the desired Transmit MRU value, see the 'PPP Properties' section of the 'Port Properties–POS and ATM Families' chapter in the *IxExplorer User Guide*.	
	IPv6 Address	When an interface is selected, an IPv6 address may be added to that interface, using the *Add* button or the 'Add' option from the Interfaces pop-up menu. Adding the IPv6 Address also automatically adds an IPv6 Mask Width to the interface, using the default values. Multiple IPv6 addresses may be added to each interface.
	IPv6 Mask Width	The number of bits for the IPv6 network 'mask' to be used with the IPv6 address, starting with the most significant bit of the address (at the left). These bits (n bits) comprise the network part of the address. The remaining bits in the address (128 minus n) comprise the host part of the address. The default IPv6 Mask width is 64 bits.

View/Section	Field/Control	Description
	IPv6 Gateway	(Optional) There can be one gateway per IPv6 interface.
	Auto Neighbor Discovery	If selected and then MAC interface is enabled, the Discovered Neighbors parameters are automatically shown.
DHCPv6 View	DHCPv6 Enable	**(Applies only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.)** NOTE You will not be able to select DHCPv6-enabled interfaces for use with protocol emulations. If selected, the IPv6 DHCP client feature will be enabled. DHCPv6 negotiation will be started and an IPv6 address learned from the DHCPv6 server will be assigned automatically to the protocol interface. When this feature is enabled, the fields in the IPv6 view will be dimmed and unavailable for configuration by you. If an IPv6 address has already been assigned to the port, a warning message will open, requiring a choice by you to continue with DHCPv6 address assignment to replace the existing IPv6 address, or to keep the existing address.
	DHCPv6 Maximum Request Rate	(For rate control) The user-specified maximum number of Request messages that can be sent per second from the client to the server, requesting an IPv6 address. A value of zero (0) indicates that there will be no rate control, that is, requests will be sent as fast as possible.
	DHCPv6 IA Id	(string) The unique identifier value for the Identity Association.
	DHCPv6 IA Type	The Identity Association type. Choose one of: • Temporary (IA_TA)—A group of temporary IPv6 addresses identified by a unique Identity Association Id (IAID)—Assigned by the DHCP server to the client. Each IA_TA may be associated with only one interface. (The DHCPv6 server sends complete IPv6 addresses to the client.) • Permanent (IA_NA)—A group of non-temporary (permanent) IPv6 addresses identified by a unique Identity Association Id (IAID) - assigned by the DHCP server to the client. Each IA_NA may be associated with only one interface. (The DHCPv6 server sends complete IPv6 addresses to the client.) • Prefix Delegation (IA_PD)—Collection of prefixes. The delegating router (server) assigns the prefix (es) to the requesting router, instead of individual, complete addresses. For example, prefixes of length /64. The requesting router can then assign

View/Section	Field/Control	Description
		128-bit address(es) or subnets to its interfaces. Currently, each IA_PD may be associated with one interface. NOTE Address assignment may also be used by the requesting router—in addition to prefix delegation.
	DHCPv6 Renew Time	(In seconds) The amount of time that the DHCPv6 Client will wait before sending a Renew message to the server. The Renew message is sent by the client to request an extension of the lifetime for the IPv6 address that was assigned by the server.
	Relay Destination	Set by the server, to be used in optional cross-gateway starting.
(DHCPv6 TLVs)		DHCPv6 TLVs (tuples) for custom DHCPv6 options. Additional TLV entries may be added by pressing the  button.
	DHCPv6 Tlv Type	(decimal) The identifier for this DHCPv6 option.
	DHCPv6 Tlv Value	(hex) The DHCPv6 option value field may contain data for configuration information such as time server information, and so forth.
VLAN View	VLAN Enable	If selected, enables the VLAN option on this port, with one VLAN ID per interface.
	VLAN ID	If the VLAN option is enabled for the current interface, a VLAN ID may be added to the packet, to identify the VLAN to which the packet belongs.
	VLAN Priority	The user priority of the VLAN tag: a value from 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.
ATM View (applies to ATM ports only)	ATM Encapsulation	The type of RFC 2684 ATM multiplexing encapsulation (bridging or routing) protocol to be used. Choose one of: • VC Mux IPv4 Routed • VC Mux IPv6 Routed • VC Mux Bridged Ethernet/802.3 (FCS)—(the default) • VC Mux Bridged Ethernet/802.3 (no FCS) • LLC Routed AAL5 Snap

View/Section	Field/Control	Description
		• LLC Bridged Ethernet (FCS) • LLC Bridged Ethernet (no FCS) NOTE See the information below regarding the general types of ATM encapsulation. • **VC Mux**—VC MUX Routed Protocol. For ATM Virtual Connection (VC) Multiplexing. Each ATM VC carries routed PDUs for only one protocol. Multiple VCs are required for multiple protocols. Helps to reduce fragmentation overhead. • **LLC Snap**—LLC/SNAP Routed Protocol. For ATM LLC Encapsulation. Each ATM VC carries routed PDUs for multiple protocols. Helps to reduce the number of separate VCs required if multiple protocols are used.
	ATM VPI	Virtual Path Identifier (VPI) for the VC over which information is being transmitted. The minimum value = 0. See the *Ixia Platform Reference Manual* for additional information about ATM VPI/VCI pairs.
	ATM VCI	Virtual Circuit/Channel Identifier (VCI) for the VC over which information is being transmitted. The minimum value = 32. (Values less than 32 are reserved.) See the *Ixia Platform Reference Manual* for additional information about ATM VPI/VCI pairs.
FC/FCoE View	FLOGI Enable	If selected, enables Fabric login (FLOGI). The FLOGI frame provides the means by which an Nx_Port requests Login with the Fabric.
	SCR Enable	If selected, enables State Change Registration. SCR requests the Fabric Controller or Nx_Port to add the Nx_Port that is sending the SCR Request to the list of Nx_Ports.
	SCR Options	If *SCR Enable* check box is enabled, the field for SCR Options become available. The registration function options for SCR are as follows: • Fabric Detected: Register to receive all Registered State Change Notification (RSCN) Requests issued by the Fabric Controller for events detected by the Fabric. • Nx Port Detected: Register to receive all RSCN Requests issued for events detected by the affected Nx_Port. • Full Registration: Register to receive all RSCN

View/Section	Field/Control	Description
		Requests issued. The RSCN Request returns all affected N_Port_ID pages.
	NS Registration	If selected, enables Name Server Registration for this port.
	NS Registration Options	If *NS Registration* check box is selected, the *NS Registration Options* field becomes active and the *Edit* button is available. Click *Edit* to open the *Name Server Registration Configuration* dialog to configure NS Registration options. Refer *Name Server Registration* for more information.
	Name Server Query Enable	If selected, enables Name Server Query parameters for this Fibre Channel Name Server.
	Name Server Query parameters	If *Name Server Query Enable* check box is selected, the *Name Server Query parameters* field becomes active and the *Edit* button is available. Click *Edit* button to open the *FC Name Server Query* dialog to configure FC name server options. Refer *FC Name Server Query* for more information.
	Automatic PLOGI	If selected, automatically enables PLOGI to all the ports that are advertised by the fabric, or to PLOGI to a subset of the available ports that belong to a specified domain.
	PLOGI Enable	Enables PLOGI. The PLOGI transfers Service Parameters from the initiating Nx_Port to the FC Port associated with the Destination Identifier. The PLOGI frame provides the means by which an Nx_Port requests Login with another Nx_Port before other Data frame transfers. If +PLOGI is activated (in the toolbar, as shown in the figure)  enables Port login to specified Destination ID.
	PLOGI Destination	The PLOGI Destination Identifier. When +PLOGI is activated, a dialog opens for configuring the Port login.

View/Section	Field/Control	Description
		 
	PRLI Enable	If selected, enables the Process Login parameters used by this port. The Process Login (PRLI) ELS request is used to establish the operating environment between a group of related processes at the originating Nx_Port and a group of related processes at the responding Nx_Port. If enabled, this option causes the state machine to attempt a process login.
	Number of Retries	Number of retries before being marked as *Failure*.
	Request Rate	Maximum rate (packets/second). This value is configured per port. The port CPU state machine uses this value to determine the rate at which it should send out the control plane packets. This option is not configurable per interface, and all the interfaces on the port uses this configured value.
	Retry Interval	The interval between retries, when a packet is sent and no response received. The default value is 2000 (milliseconds).
	Source Port WWN	The Source Port Worldwide Name is a Name_Identifier that is unique worldwide. It is represented by a 64-bit value.
	Source Node WWN	The Source Node Worldwide Name is a Name_Identifier that is unique worldwide. It is represented by a 64-bit value.
	Source OUI	The three bytes Source Organization Unique Identifier.
	Buffer to Buffer Rx Size	The size, in bytes, of the buffer-to-buffer capacity. It is the maximum buffer-to-buffer Receive_Data_Field specified by the Fabric.
PTP View	PTP Enable	Enables PTP
	PTP Edit	Click **Edit** button to open *PTP Clock Configuration* dia-

View/Section	Field/Control	Description
		log.
	Clock ID	(See *Table:PTP Clock Configuration* for definitions.)
	Port Number	(See *Table:PTP Clock Configuration* for definitions.)
	Clock Class	(See *Table:PTP Clock Configuration* for definitions.)
	Clock Accuracy	(See *Table:PTP Clock Configuration* for definitions.)
	Priority1	(See *Table:PTP Clock Configuration* for definitions.)
	Priority2	(See *Table:PTP Clock Configuration* for definitions.)
	Domain Number	(See *Table:PTP Clock Configuration* for definitions.)
	Announce Interval	(See *Table:PTP Clock Configuration* for definitions.)
	Sync Interval	(See *Table:PTP Clock Configuration* for definitions.)
	Delay Request Interval	(See *Table:PTP Clock Configuration* for definitions.)
	Announce Receipt Timeout	(See Announce Receipt Timeout in *Table:PTP Clock Configuration* for definitions.)
	Delay Mechanism	(See *Table:PTP Clock Configuration* for definitions.)
	Master Slave Flag	(See *Table:PTP Clock Configuration* for definitions.)
	Start Offset	(See *Table:PTP Clock Configuration* for definitions.)
	% Bad Timestamp	(See *Table:PTP Clock Configuration* for definitions.)
	Timestamp Error	(See *Table:PTP Clock Configuration* for definitions.)
	% Bad CRC	(See *Table:PTP Clock Configuration* for definitions.)
	% Drop Follow-up Messages	(See *Table:PTP Clock Configuration* for definitions.)
	% Delay Resp Messages	(See *Table:PTP Clock Configuration* for definitions.)
DCBX / LLDP View	LLDP Enable	Enables LLDP Tx and Rx NOTE Since DCBX is an acknowledged protocol which uses LLDP, for the protocol to operate correctly, both LLDP Rx and Tx are enabled on the interface on which DCBX runs.
	Fast Transmit	Enables Fast Transmit. The interval for the LLDP transmission time to refresh the timer (Tx Interval) is set to 1 second for the first five transmissions after LLDP initialization and then reset to the administratively configured value.
	Tx Delay	Minimum delay between successive transmitted LLDP frames. Set to 2 seconds as a DCBX default.
	Chassis Id	MAC address of the chassis.

View/Section	Field/Control	Description
	Port Id Options	Click **Edit** to configure. *DCBX Port Id*.
	Hold Time	Tx Hold is the multiplier on Tx Interval that determines the actual TTL that is sent in the LLDP message. Hold Time x Tx Interval = TTL.
	Tx Interval	If Fast Transmit is enabled, the interval for the LLDP transmission time to refresh the timer (msgTxInterval) is set to 1 second for the first five transmissions after LLDP initialization and then reset to the administratively configured value. Hold Time x Tx Interval = TTL. Default = 30.
	DCBX Enable	Enables DCBX.
	DCBX OUI	The OUI used for the DCBX TLV is 0x001B21. The default is the Intel OUI, but can be changed to any 3-byte value.
	DCBX SubType	Select one of two DCBX types, either Intel 1.0 or IEEE 1.01. Based on the selection, the TLV differs.
	DCBX Control TLV Max Version	Set to 255. Highest DCBX protocol version supported by the system. Version numbers range from 0 to 255.
	DCBX Feature Type	Click the TLV+ icon (above) to add a TLV, and then the DCBX Feature Type becomes active: For SubType 1 (Intel) the first Feature Type entry is 2 Priority Group, next is 3-PFC, then 4-Custom (BCN), then 5-FCoE, then 6-Logical Link, then customizable 7, 8, and so on. The first 5 types are the 'known' TLVs. For SubType 2 IEEE, the first is 2-Priority Group, then 3-PDF, then 4-FCoE, then customizable 5,6, and so on. The first 3 types are the 'known' TLVs.
	DCBX Feature Value	For each DCBX Feature Type, click **Edit** to configure values. See *Table:DCBX Feature Values*.
FIP View	FIP Version	The version of FCoE Initialization Protocol (FIP) used.
	FIP enable	If selected, enables FIP. If enabled, the interface uses FIP for its initialization. Otherwise, it uses Cisco adhoc standard.
	Max FCoE size	Enter the maximum FCoE size (default - 2,158).
	Addressing Mode	Specifies the addressing mode to be used by the n-port. The options in the list are as follows: • Fabric Provided (default) • Server Provided • Both
	VLAN Discovery Enable	If selected, VLAN Discovery is performed.

View/Section	Field/Control	Description
	Untagged VLAN Discovery	If *VLAN Enable* is selected, this field becomes available. It enables untagged FIP VLAN discovery.
	VN_Port Keep Alive Enable	If enabled, VN_Port sends periodic keep alives.
	ENode Keep alive	If enabled, ENode sends periodic keep alives.
	Vendor ID	This value is used in the vendor specific descriptor.
	Vendor Specific Descriptor type	A user-specified entry.
	Vendor Specific Descriptor value	A user-specified entry.
	Collect FCF-MAC	If selected, sends collect FCF MAC address.
	Collect Time	The collect time for FCF MAC address. The default value is 1000 milliseconds.
	Propose MAC in FPMA mode	If selected, sends proposal for MAC address in FPMA mode.
	Include Name Id in VLAN Discovery	If selected, includes Name Identifier in VLAN Discovery tag.
	Reset FIP Discovery	If selected, resets FIP Discovery tag.
	Reset FIP Discovery Retries	If set, retries FIP Discovery for the selected number of times.

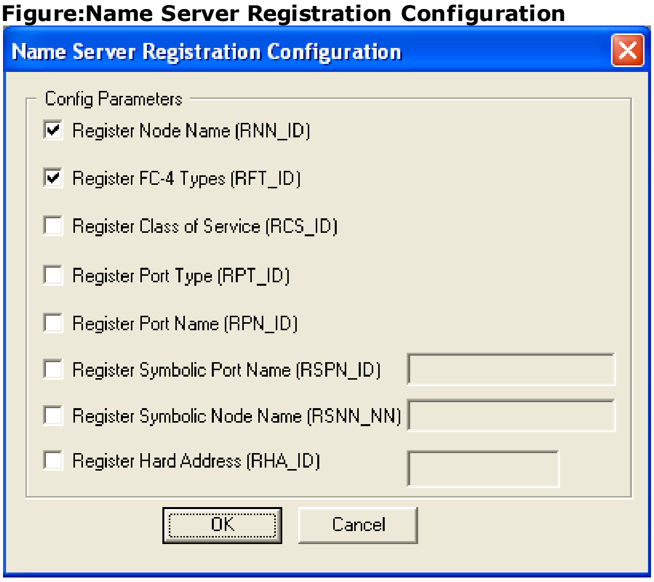
Name Server Registration

The Name Server Registration Configuration option enables to set up the configurable parameters for the name server registration. Once configured, it sends name server query to the Fibre Channel Name Server.

To access the *Name Server Registration Configuration* dialog, select the *NS Registration* check box in FC/FCoE view. The *NS Registration Options* field becomes active and the *Edit* button is available. Click *Edit* to open the *Name Server Registration Configuration* dialog to configure NS Registration options.

The *Name Server Registration Configuration* dialog box is shown in *Figure:Name Server Registration Configuration*.

Figure:Name Server Registration Configuration



The options available in this dialog are described in *Table:Name Server Registration Configuration*.

Table:Name Server Registration Configuration

Options	Description
Register Node Name (RNN_ID)	The RNN_ID Name Server request is used to associate a Node Name with a given Port Identifier.
Register FC-4 Types (RFT_ID)	The RFT_ID Name Server request is used to record the FC-4 TYPEs that are supported by a given Port Identifier.
Register Class of Service (RCS_ID)	The RCS_ID Name Server request is used to record the Classes of Service that are supported by a given Port Identifier.
Register Port Type (RPT_ID)	The RPT_ID Name Server request is used to record the Port Type that is supported by a given Port Identifier.
Register Port Name (RPN_ID)	The RPN_ID Name Server request is used to record the Port Name that is supported by a given Port Identifier.
Register Symbolic Port Name (RSPN_ID)	The RSPN_ID Name Server request is used to associate a Symbolic Port Name with a given Port Identifier.
Register Symbolic Node Name (RSNN_NN)	The RSNN_NN Name Server request is used to associate a Symbolic Node Name with a given Node Name.
Register Hard Address (RHA_ID)	The RHA_ID Name Server request is used to associate a Hard Address with a given Port Identifier.

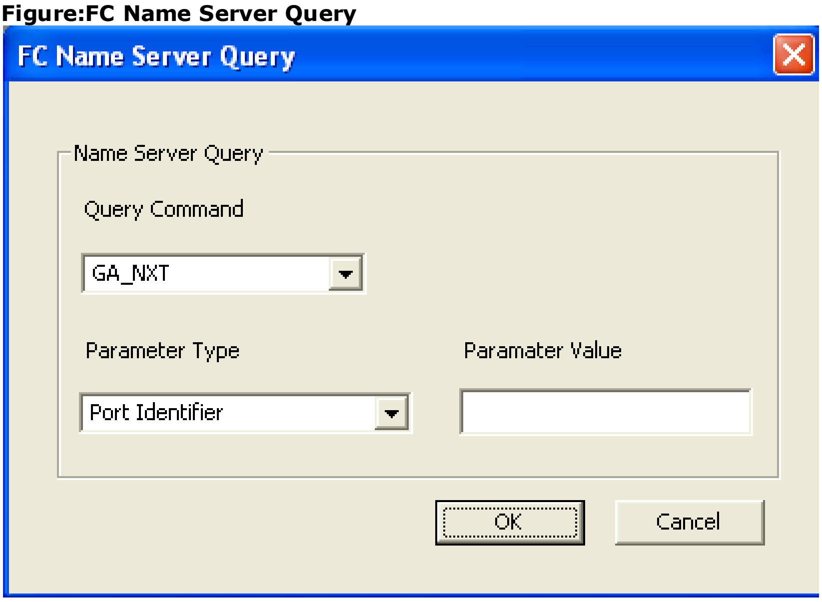
FC Name Server Query

The FC Name Server Query sends name server queries to the Fibre Channel module.

To access the *FC Name Server Query* dialog, select the *Name Server Query Enable* check box. The *Name Server Query parameters* field becomes active and the *Edit* button is available. Click *Edit* button to open the *FC Name Server Query* dialog to configure FC name server options.

The *Name Server Query* dialog is shown in *Figure:FC Name Server Query*.

Figure:FC Name Server Query



The fields and options in this dialog are described in *Table:FC Name Server Query*.

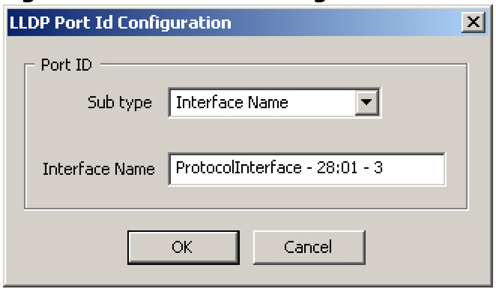
Table:FC Name Server Query

Section	Field/Options	Description
Query Command	GA_NXT	The GA_NXT is used by a requestor to obtain Name Server objects associated with a specific Port.
	GID_A	When the Name Server receives a GID_A request, it returns identifiers for the specified scope.
	GID_PN	When the Name Server receives a GID_PN request, it returns the Port Identifier associated with the specified Port Name.
	GID_PT	When the Name Server receives a GID_PT request, it returns all Port Identifiers having registered support for the specified Port Type. If the specified Port Type is equal to 'Nx_Port', then the Name Server returns all Port Identifiers that have registered Port Types with an unsigned value of less than 80h.
	GNN_ID	When the Name Server receives a GNN_ID request, it returns the registered Node Name object for the specified Port Identifier.
	GPN_ID	When the Name Server receives a GPN_ID request, it returns the registered Port Name object for the specified Port Identifier.
Parameter Type		The parameter type depends on the Query Command code. The types in the list are as follows: • Port Identifier • None • Port Name • Port Type
Parameter Value		The value depending on the parameter type.

DCBX Port Id

Click **Edit** to configure.

Figure:LLDP Port ID Configuration

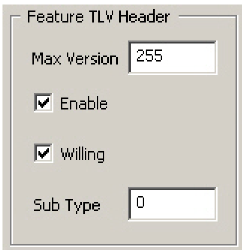


Sub type: select MAC Address or Interface Name. The second field is editable, although default values will display at first.

DCBX Feature Value

For each DCBS Subtype and Feature Type, there is a configuration dialog that allows setting the values.

Table:DCBX Feature Values

DCBX Subtype	DCBX Feature Type	DCBX Feature Value
Both	All	All the DCBX Feature Value configuration dialogs have these common elements.  **Max Version** - 255, in all cases **Enable** - selected, to enable the TLV **Willing** - indicates whether this feature accepts its configuration from the peer or not. **Subtype** - For Logical Link, 0 = FCoE, 1 = LAN. For negative testing or other purposes, any value is OK. Default = 0.
1 - Intel 1.0	2 - Priority Group	*DCBX Priority Group Configuration, Intel 1.0*.
	3 - PFC	*DCBX PFC Configuration, Intel 1.0*.
	4 - Custom (BCN)	(BCN is not yet implemented, as of IxOS 5.50)
	5 - FCoE	*DCBX FCoE Configuration, Intel 1.0*.
	6 - Logical Link	*DCBX Logical Link Configuration, Intel 1.0*.
	7, 8, and so on	*DCBX Custom Configuration, Intel 1.0 or IEEE 1.01*.

DCBX Sub-type	DCBX Feature Type	DCBX Feature Value
	(customizable)	
2 - IEEE 1.01	2 - Priority Group	*DCBX Priority Group Configuration, IEEE 1.01*
	3 - PFC	*DCBX PFC Configuration, IEEE 1.01*
	4 - FCoE	*DCBX FCoE Configuration, IEEE 1.01*.
	5, 6, etc. (customizable)	*DCBX Custom Configuration, Intel 1.0 or IEEE 1.01*.

DCBX Priority Group Configuration, Intel 1.0

For DCBX Subtype *Intel 1.0*, Feature Type *2 - Priority Group*, the following configuration dialog opens when **Edit** is clicked.

(For DCBX Subtype *IEEE 1.01*, *DCBX Priority Group Configuration, IEEE 1.01*.)

Figure:DCBX Priority Group Configuration, Intel 1.0

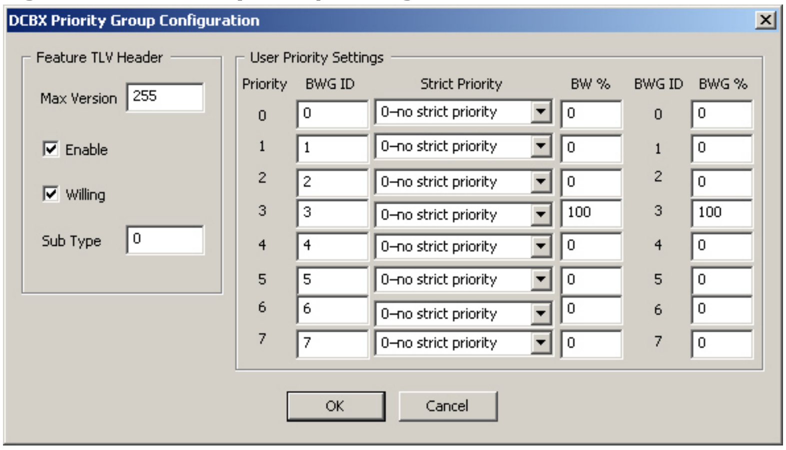


Table:DCBX Priority Group Configuration, Intel

Field	Description
Priority	User priority
BWG ID	Queue bandwidth group
Strict Priority	Strict priority settings: 0 - no strict priority 1 - Group Strict Priority (GSP) 2 - Link Strict Priority (LSP)
BW%	Percentage of BWG bandwidth
BWG ID	BWG to which the priority belongs
BWG%	Percentage of link bandwidth

DCBX PFC Configuration, Intel 1.0

For DCBX Subtype *Intel 1.0*, Feature Type *3 - PFC*, the following configuration dialog opens when **Edit** is clicked.

(For DCBX Subtype *IEEE 1.01*, *DCBX PFC Configuration, IEEE 1.01*.)

Figure:DCBX PFC Configuration, Intel

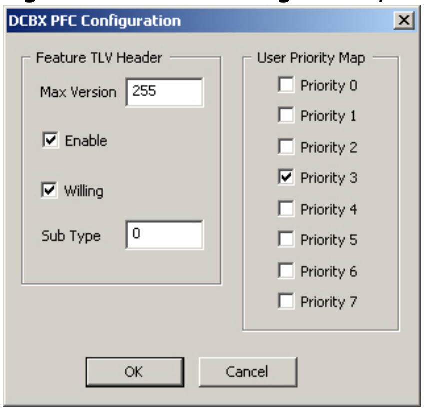


Table:DCBX PFC Configuration, Intel

Field	Description
User Priority Map	For this TLV, select a priority.

DCBX FCoE Configuration, Intel 1.0

For DCBX Subtype *Intel 1.0*, Feature Type *5 - FCoE*, the following configuration dialog opens when **Edit** is clicked.

(For DCBX Subtype *IEEE 1.01*, *DCBX FCoE Configuration, IEEE 1.01*.)

Figure:DCBX FCoE Configuration

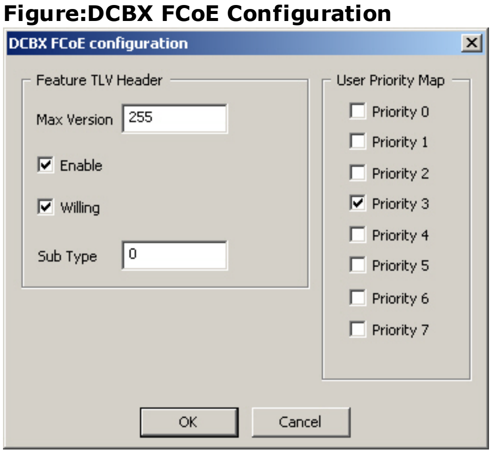


Table:DCBX FCoE Configuration, Intel

Field	Description
User Priority Map	For this TLV, select a priority (that is associated with FCoE traffic).

DCBX Logical Link Configuration, Intel 1.0

For DCBX Subtype *Intel 1.0*, Feature Type *6 - Logical Link*, the following configuration dialog opens when **Edit** is clicked.

Figure:DCBX Logical Link Configuration

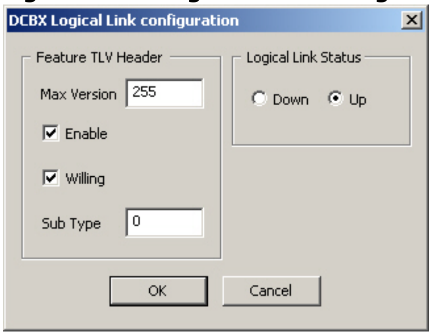


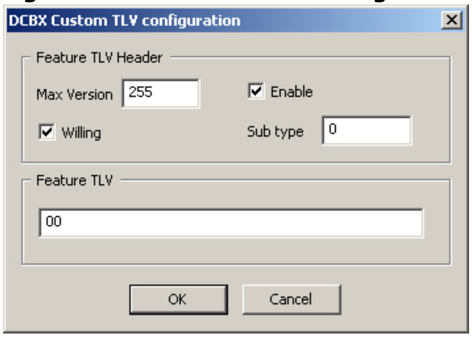
Table:DCBX Logical Link Configuration, Intel

Field	Description
Logical Link Status	Up or Down Signifies whether the Logical Link Status of this type of network (FCoE or LAN) is up or not.

DCBX Custom Configuration, Intel 1.0 or IEEE 1.01

For TLVs added after the known types, under either DCBX Subtype, this customization dialog will display.

Figure:DCBX Custom TLV Configuration



Enter the 16-bit header field definition into the Feature TLV field. The elements of the header field are described in *Table:Feature TLV Header*.

Table:Feature TLV Header

Position	Type	Description
Type (of TLV)	Integer	Type code of the DCB Feature. Following is a list of defined types: 1 - PROTOCOL Control (not a feature) 2 - Priority Groups 3 - Priority Flow Control 4 - BCN 5 - Application 6 - Logical Link Down
Length	Integer	Length of the DCB Feature sub-TLV payload (not including the Type and Length fields).

Position	Type	Description
Oper Version	Integer 0-255	Operating version of the feature. The system adjusts to operate at the highest version supported by both link partners.
Max Version	Integer 0-255	Highest feature version supported by the system.
Enable	Boolean	Locally administered parameter that indicates whether the DCB feature is enabled or not.
Willing	Boolean	Locally administered parameter that indicates whether this feature accepts its configuration from the peer or not.
Error	Boolean	Indicates that an error has occurred during the configuration exchange with the peer.
Subtype	Integer	For Logical Link, 0 = FCoE, 1 = LAN. For negative testing or other purposes, any value is OK. Default = 0.

DCBX Priority Group Configuration, IEEE 1.01

For DCBX Subtype *IEEE 1.01*, Feature Type *2 - Priority Group*, the following configuration dialog opens when **Edit** is clicked.

Figure:DCBX Priority Group Configuration, IEEE 1.01

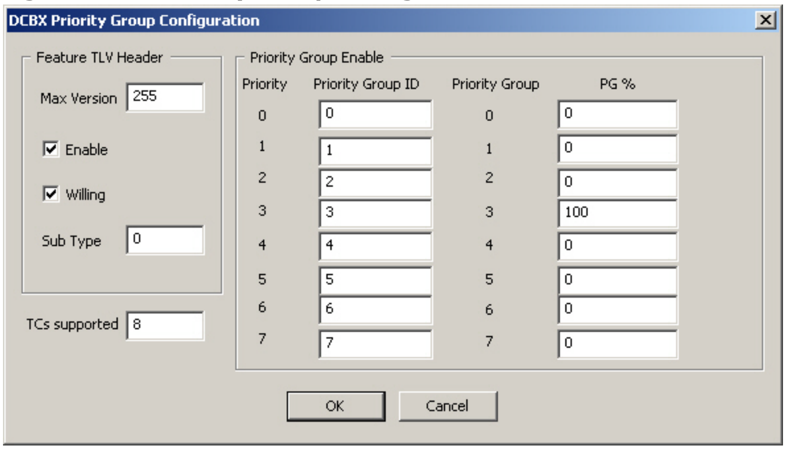


Table:DCBX Priority Group Configuration, IEEE

Field	Description
Priority	User priority
Priority Group ID	PG to which the priority belongs
Priority Group	Queue bandwidth group
PG%	Percentage of link bandwidth
TCs supported	Number of Traffic Classes supported by device.

DCBX PFC Configuration, IEEE 1.01

For DCBX Subtype *IEEE 1.01*, Feature Type *3 - PFC*, the following configuration dialog opens when **Edit** is clicked.

Figure:DCBX PFC Configuration, IEEE 1.01

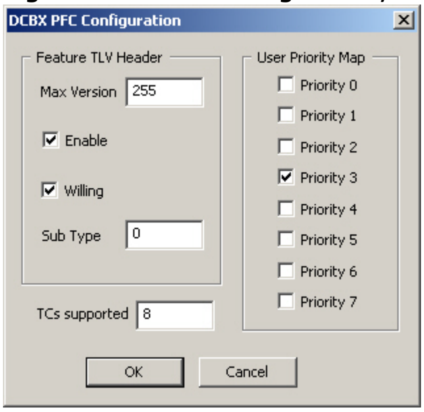


Table:DCBX PFC Configuration, IEEE

Field	Description
User Priority Map	For this TLV, select a priority.
TCs supported	Number of Traffic Classes that can simultaneously support PFC.

DCBX FCoE Configuration, IEEE 1.01

For DCBX Subtype *IEEE 1.01*, Feature Type *4 - FCoE*, the following configuration dialog opens when **Edit** is clicked.

Figure:DCBX FCoE Configuration

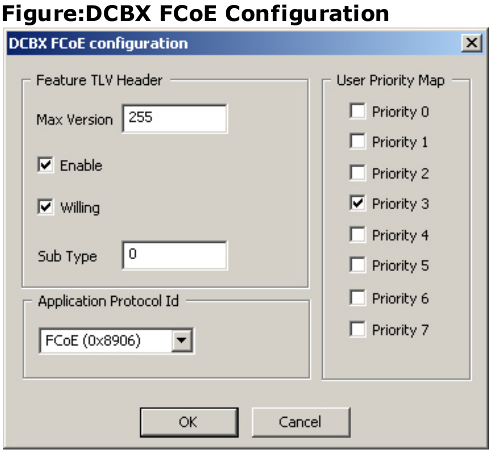
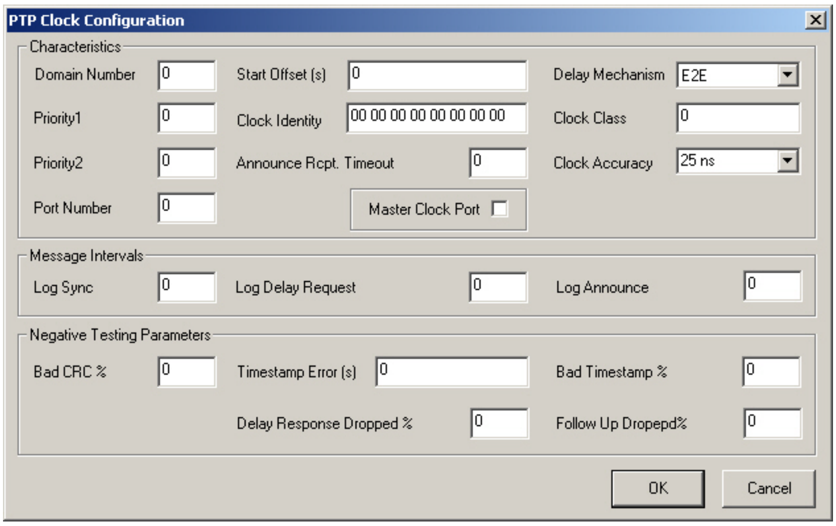


Table:DCBX FCoE Configuration, IEEE

Field	Description
User Priority Map	For this TLV, select a priority (that is associated with FCoE traffic).
Application Protocol Id	Identifies protocol supported by DCB node. Select: FCoE (0x8906) FIP (0x8914) Other = any 2-byte number (in Hex)

PTP Clock Configuration

Figure:PTP Clock Configuration



The field definitions for this screen appear in *Table:PTP Clock Configuration*, below.

Table:PTP Clock Configuration

Area	Field	Description
Characteristics	Domain Number	The domain is identified by an integer in the range of 0 to 255.
	Priority 1	A user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected.
	Priority 2	A user configurable designation that provides finer grained ordering among otherwise equivalent clocks.
	Port Number	A specific PTP port on a PTP node
	Start Offset(s)	Defines the clock offset in nanoseconds. Master sends PTP messages with Start Offset added to the clock.
	Clock Identity	Identifies a clock
	Announce Receipt Timeout	Number of *announceInterval* that must pass without receipt of an Announce message before the Announce Receipt Timeout event occurs The value range of this field depends on the value of Log Announce interval (below).
	Delay Mechanism	Either (1) 'end-to-end' or (254) 'disabled'
	Clock Class	Defines a clock's TAI traceability. The clockClass attribute of an ordinary or boundary clock denotes the traceability of the time or frequency distributed by the grandmaster clock.
	Clock Accuracy	Defines the accuracy of a clock. See *Table:Clock Accuracy*.
	Master Clock Port	If selected, configures the port in master mode.

Area	Field	Description
Message Intervals	Log Sync	The mean time interval between successive Sync messages Range -5 to 26 NOTE Instead of Message Interval values, the logarithm to base 2 of the Message Interval values are specified. So, for instance, 'Log Sync' is the logarithm to base 2 of the Sync Interval. Range of -5 to 26 would translate to 2^(-5) to 2^26 ---> 1/32 to 64M.
	Log Delay Request	The minimum permitted mean time interval between successive Delay_Req messages, sent by a to a specific port on the master. Range -5 to 22 See Note under Log Sync.
	Log Announce	Mean time interval between successive Announce messages Range -5 to 26 See Note under Log Sync.
Negative Testing Parameters	Bad CRC %	Percent of follow-up messages sent with bad CRC
	Timestamp Errors	The time error between a and a master ordinary or boundary clock
	Bad Timestamp %	Percent of follow-up messages sent with bad timestamp
	Delay Response Dropped %	Defines how many delay response messages to be dropped. Drop delay response messages exclicked as percentage of received delay request messages. Normally, delay response is sent by the master corresponding to each delay request massage received. For negative testing, you can configure Ixia port to drop the delay response message to see how the DUT behaves.
	Follow-up Dropped %	Defines how many follow-up messages to be dropped. Drop follow-up messages exclicked as percent of sync messages. Normally, a follow-up message is sent out corresponding to each sync message. For negative testing, you can configure Ixia port to drop the follow-up message to see how the DUT behaves.

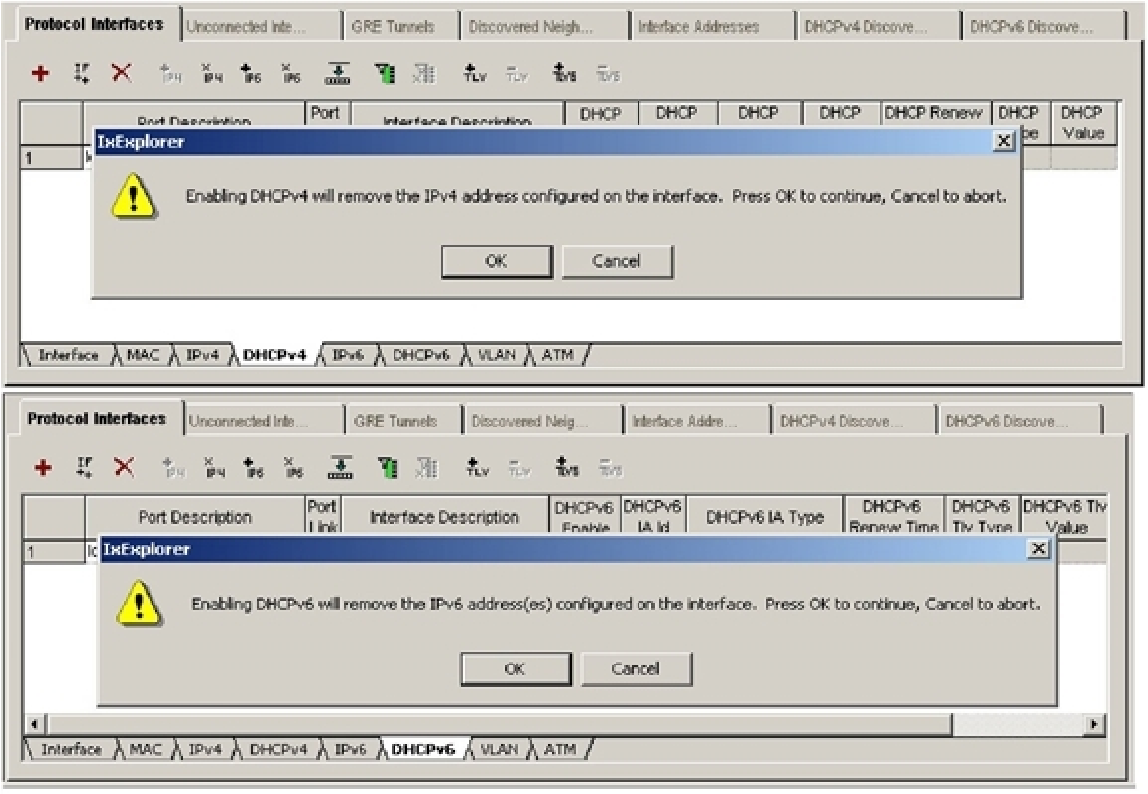
Table:Clock Accuracy

Value	Usage
32	accuracy 25 nanoseconds
33	accuracy 100 ns
34	accuracy 250 ns
35	accuracy 1 microsecond
36	accuracy 2.5 microseconds
37	accuracy 10 microseconds
38	accuracy 25 microseconds
39	accuracy 100 microseconds
40	accuracy 250 microseconds
41	accuracy 1 millisecond
42	accuracy 2.5 milliseconds
43	accuracy 10 milliseconds
44	accuracy 25 milliseconds
45	accuracy 100 milliseconds
46	accuracy 250 milliseconds
47	accuracy 1 second
48	accuracy 10 seconds
49	accuracy greater than 10 seconds
254	accuracy unknown

Adding DHCP Addresses

If an IPv4 or IPv6 address has already been assigned to an Ethernet port or an ATM port using Bridged Ethernet encapsulation, selecting the 'DHCPv4 Enable' or 'DHCPv6 Enable' check box, respectively, will open the appropriate warning message box shown in *Figure:DHCPv4 and DHCPv6 Messages*. Click the *OK* button to delete the existing address and use DHCPv4 or DHCPv6 for address assignment, or click the *Cancel* button to close the message box and use the previously assigned IPv4 or IPv6 address.

Figure:DHCPv4 and DHCPv6 Messages

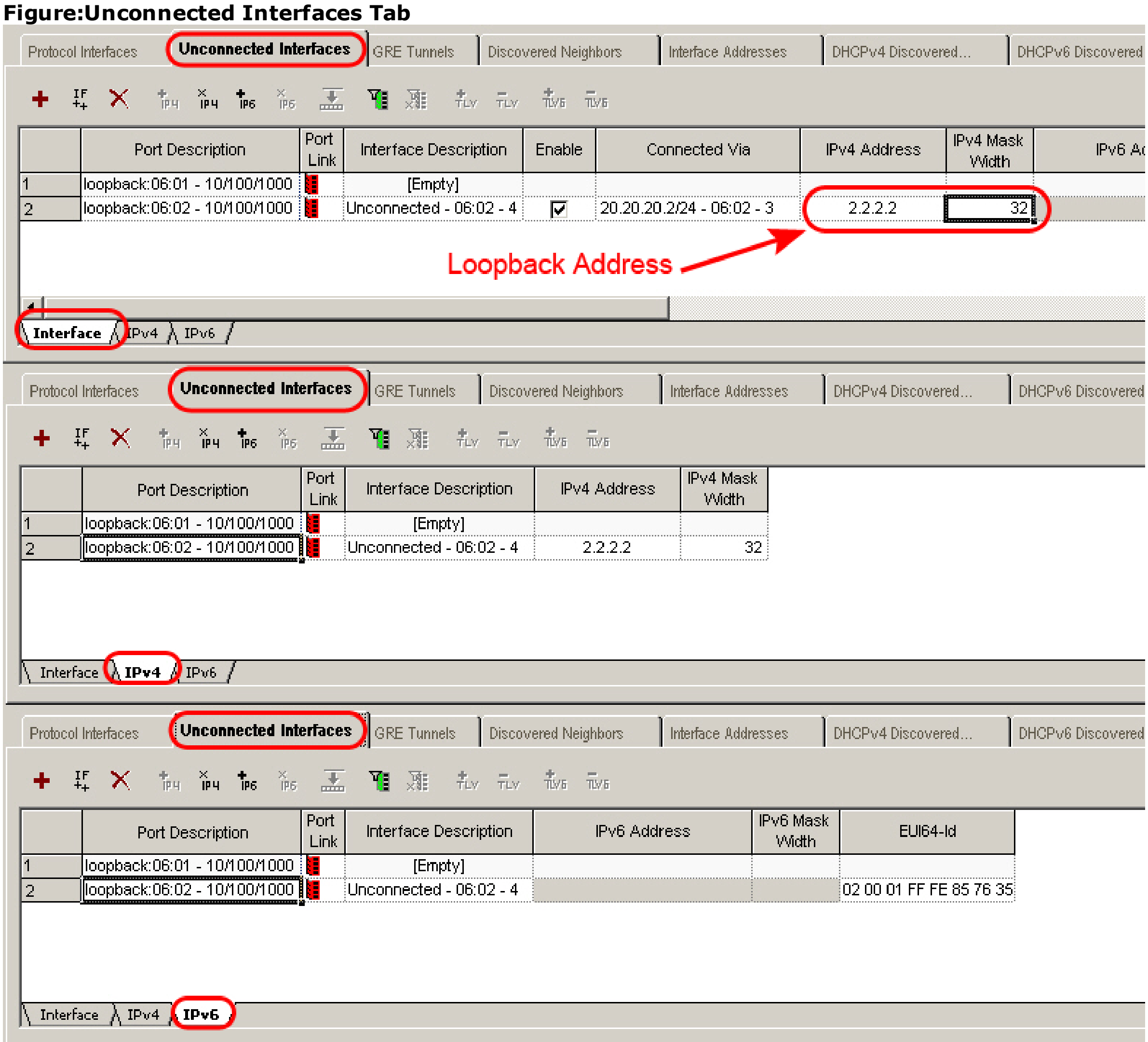


Unconnected Interfaces

The Unconnected Interfaces tab of the Protocol Interfaces window is shown in *Figure:Unconnected Interfaces Tab*. This window is provided so you can create virtual, 'unconnected' interfaces that are not connected by any links to the SUT or to other Ixia ports. The unconnected interfaces can be set up to link the Ixia-emulated router to virtual networks 'behind' the router, such as emulated OSPF network ranges.

Also, when L2 VPNs or L3 VPNs are being set up, the loopback IP addresses that identify the tunnel endpoints on the Ixia-emulated routers are created using unconnected interfaces—automatically, if the configuration and/or protocol interface wizards are used, or manually in the individual protocol windows.

Figure:Unconnected Interfaces Tab



The fields in the Unconnected Interfaces tab are described in *Table:Unconnected Interfaces Tab*.

Table:Unconnected Interfaces Tab

View	Field	Description
Interfaces	Port Description	The identification of the port, including the card number, port number, and type of port.
	Port Link	The status of the physical link for the Ixia port.
	Interface Description	A description for this unconnected protocol interface. The format will vary, depending on whether it is a loopback address configured for the Ixia port, or it is a virtual connection to a network range ‘behind’ the Ixia-emulated router. For example, interface description format when created with MVPN wizard: ‘Un-2.2.2.2/32 - 10:02 - 4’

View	Field	Description
		(Un-Address/Mask - Card No.:Port No. - Protocol Interface number for this port)
	Enable	If selected, this unconnected interface is enabled.
	Connected Via	The name of a specified ‘connected’ protocol interface on the link that is directly connected to the DUT.
	IPv4 Address	The 32-bit IPv4 address assigned to this unconnected interface.
	IPv4 Mask Width	The number of bits in the mask used with the IPv4 address. The default is 24 bits.
	IPv6 Address	The 128-bit IPv6 address assigned to this unconnected interface.
	IPv6 Mask Width	The number of bits in the mask used with the IPv6 address. The default is 64 bits.
	EUI-64 Id	This is the 64-bit IEEE Modified EUI Id value for the Interface Identifier portion of the IPv6 address. For **Ethernet** modules, this field is not editable by you. The value is automatically calculated, based on the 48-bit MAC address. For more information on how this value is calculated, refer to the IPv6 Interface Identifiers (IIDs) section in the ‘Theory of Operation: General’ chapter of the *Ixia Platform Reference Manual*. For OC48 and OC192 POS modules, you can edit the value.
IPv4	Interface Description	A user-defined description for this unconnected interface.
	IPv4 Address	The 32-bit IPv4 address assigned to this unconnected interface.
	IPv4 Mask Width	The number of bits in the mask used with the IPv4 address. The default is 24 bits.
IPv6	Interface Description	A user-defined description for this unconnected interface.
	IPv6 Address	The 128-bit IPv6 address assigned to this unconnected interface.
	IPv6 Mask Width	The number of bits in the mask used with the IPv6 address. The default is 64 bits.
	EUI-64 Id	This is the 64-bit IEEE Modified EUI Id value for the Interface Identifier portion of the IPv6 address. For **Ethernet** modules, this field is not editable by you. The value is automatically calculated,

View	Field	Description
		based on the 48-bit MAC address. For more information on how this value is calculated, refer to the IPv6 Interface Identifiers (IIDs) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*. For OC48 and OC192 POS modules, you can edit the value.

GRE Tunnels

NOTE The GRE Tunnels tab is available ONLY for modules that support GRE over IP. Refer to the *Ixia Platform Reference Manual* for information on modules that support this feature.

The Generic Routing Encapsulation (GRE) Tunnels tab is shown in *Figure:GRE Tunnels Tab* and *Figure:GRE Tunnels Tab (Continued)*. This window allows to set up GRE tunnels from the Ixia port to the DUT port. The GRE protocol can be used to encapsulate packets of many different protocol types and tunnel them across a network of a different protocol type. This basic encapsulation method indicates the Ethertype of the payload packet, and depends on a delivery header with both Layer 2 and Layer 3 information to forward the packet across the network. For additional information on GRE, refer to the *Ixia Platform Reference Manual*.

NOTE Creating multiple GRE tunnels that have the same Source IP address and same Destination IP address is an illegal configuration.
Each GRE tunnel must have a **unique** combination of:

Source IP, and
Destination IP, and
In-key.

Figure:GRE Tunnels Tab

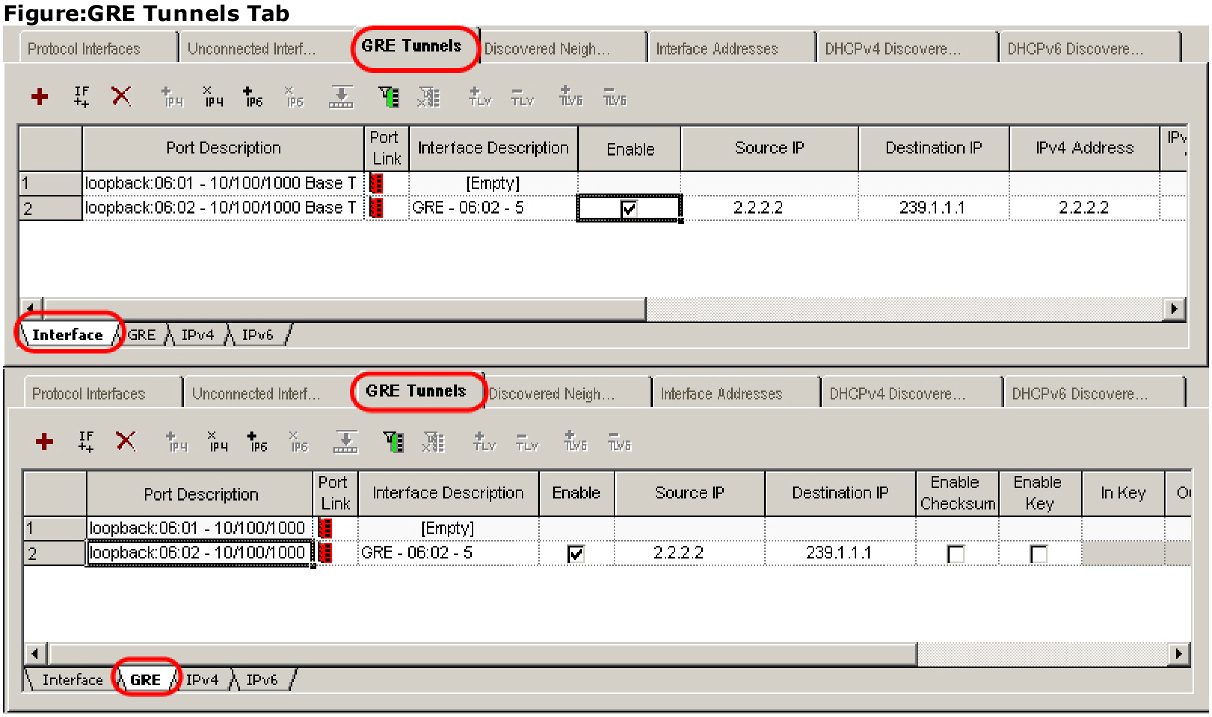
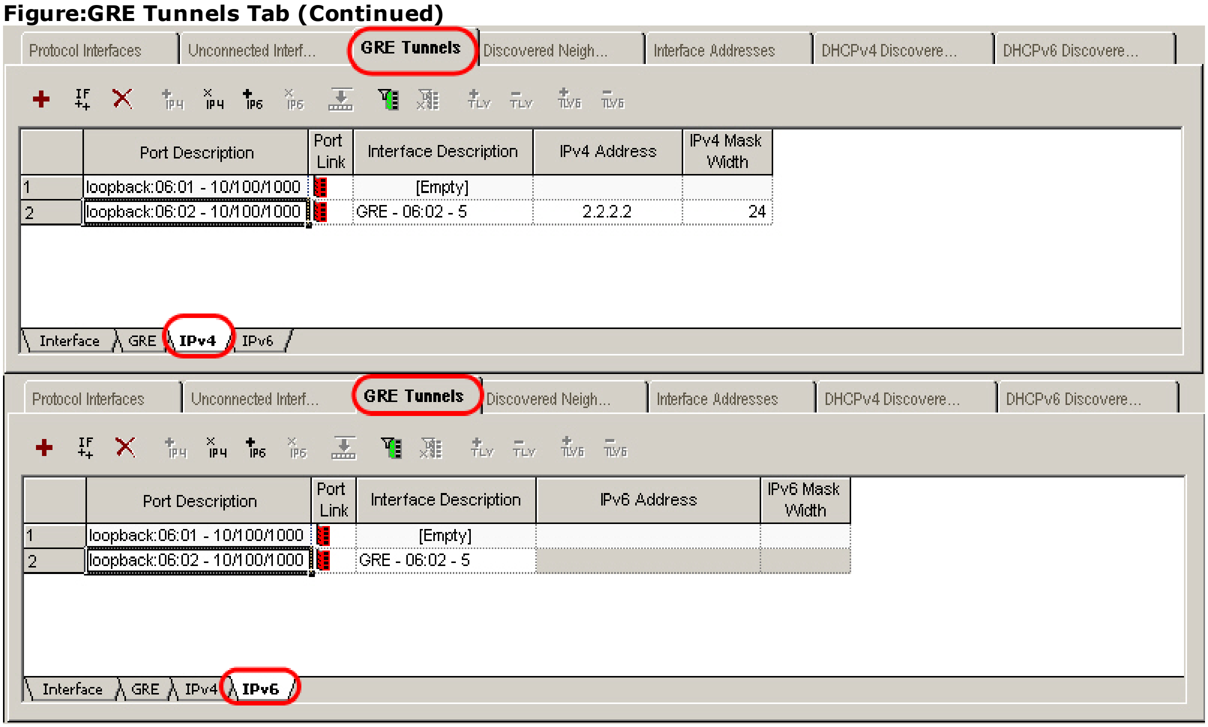


Figure:GRE Tunnels Tab (Continued)



The fields in the GRE Tunnels tab are described in *Table:GRE Tunnels Tab*.

Table:GRE Tunnels Tab

View	Field	Description
Interface	Port Description	The identifier for the port including card and port numbers, and the port type.
	Port Link	The color of this icon indicates the state of the link: • **Green**—Link is Up.

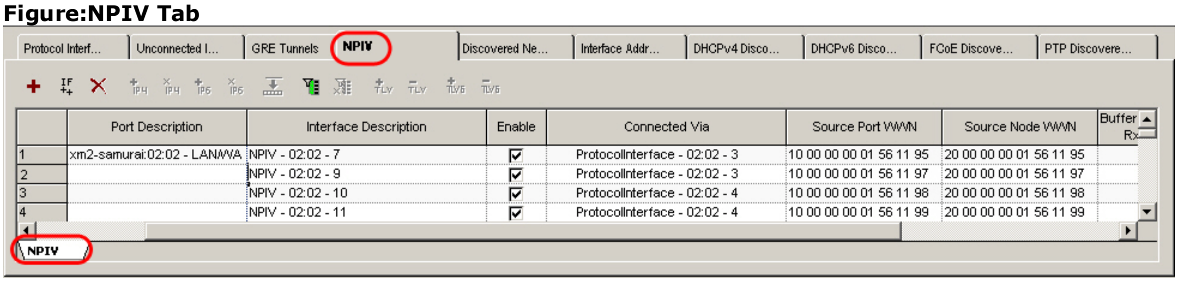
View	Field	Description
		• **Red**—Link is Down. • **Yellow—**Link is in loopback mode. • **Gray—**Link is unavailable because it is busy or it is an unsupported link type.
	Interface Description	A description for this GRE Tunnel Interface.
	Source IP	Part of the GRE Delivery Header: The IP address of the connected interface associated with the source of this GRE tunnel.
	Destination IP	Part of the GRE Delivery Header: The IP address of the Destination router at the remote end of the GRE tunnel.
	IPv4 Address	The 32-bit IPv4 address assigned to this unconnected interface.
	IPv4 Mask Width	The number of bits in the mask used with the IPv4 address. The default is 24 bits.
	IPv6 Address	The 128-bit IPv6 address assigned to this unconnected interface.
	IPv6 Mask Width	The number of bits in the mask used with the IPv6 address. The default is 64 bits.
	Enable Checksum	If selected, enables the use of the optional GRE Checksum.
	Enable Key	If selected, the optional authentication key feature will be added to the GRE header, per RFC 2890.
	In Key	This is the user-assigned GRE header authentication key value that the receiving router will check for to validate GRE packets being sent through the tunnel. All packets sent through a specific tunnel should contain the same key value (one key per GRE tunnel). In most cases, the In Key and Out Key will be the same.
	Out Key	This is the user-assigned GRE header authentication key value that will be included in the GRE packets being sent through the tunnel. All packets sent through a specific tunnel should contain the same key value (one key per GRE tunnel). In most cases, the In Key and Out Key will be the same.
GRE	Enable	If selected, this emulated GRE tunnel interface is enabled.
	Source IP	Part of the GRE Delivery Header: The IP address of the interface associated with the

View	Field	Description
		source of this GRE tunnel.
	Destination IP	Part of the GRE Delivery Header: The IP address of the Destination router.
	Enable Checksum	If selected, enables the use of the optional GRE Checksum.
	Enable Key	If selected, enables the use of the optional GRE header Key field.
	In Key	This is the user-assigned GRE header authentication key value that the receiving router will check for to validate GRE packets being sent through the tunnel. All packets sent through a specific tunnel should contain the same key value (one key per GRE tunnel). In most cases, the In Key and Out Key will be the same.
	Out Key	This is the user-assigned GRE header authentication key value that will be included in the GRE packets being sent through the tunnel. All packets sent through a specific tunnel should contain the same key value (one key per GRE tunnel). In most cases, the In Key and Out Key will be the same.
IPv4	Interface Description	A user-defined description for this unconnected interface.
	IPv4 Address	The 32-bit IPv4 address assigned to this unconnected interface.
	IPv4 Mask Width	The number of bits in the mask used with the IPv4 address. The default is 24 bits.
IPv6	Interface Description	A user-defined description for this unconnected interface.
	IPv6 Address	The 128-bit IPv6 address assigned to this unconnected interface.
	IPv6 Mask Width	The number of bits in the mask used with the IPv6 address. The default is 64 bits.

NPIV Protocol Interface

The NPIV tab is used to configure N_Port_ID Virtualization (NPIV), which provides a Fibre Channel facility for assigning multiple N_Port_IDs to a single N_Port, thereby allowing multiple distinguishable entities.

Figure:NPIV Tab



The fields and controls shown in the NPIV tab are described in *Table:Discovered Neighbors Tab*.

Table:NPIV Tab

Field/Control	Description
Interface Description	A description for this NPIV Interface.
Enable	Enables the NPIV interface
Connected Via	Specifies the FCoE interface that has to be used
Source Port WWN	Source port Worldwide Name - a Name_identifier that is worldwide unique, represented by a 64-bit value
Source Node WWN	Source node Worldwide Name - a Name_identifier that is worldwide unique, represented by a 64-bit value
Buffer to Buffer Rx Size	Maximum buffer-to-buffer Receive_Data_Field specified by the Fabric
SCR Enable	If enabled, the ENode will register for any changes with the Fabric by sending a State Change Registration packet.
NS Enable	Enables registration to Name Server
PLOGI Enable	Enables Port login to specified Destination ID
PLOGI Destination	Destination Identifier

NPIV interfaces can be configured using the Protocol Interface Wizard.

Discovered Neighbors

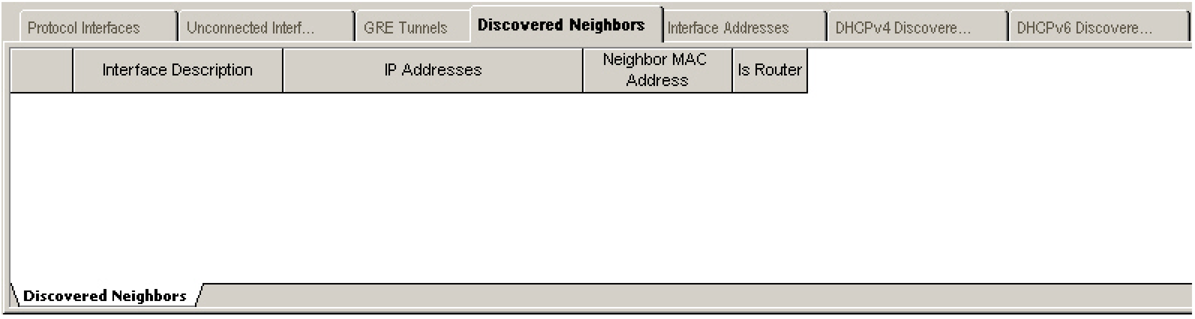
Learned IPV4 and IPv6 information for Discovered Neighbors is displayed in the window shown in *Figure:Discovered Neighbors Tab*. This tab contains a list of discovered IPv4 and IPv6 neighbors, including a MAC address (for Ethernet) and a list of interfaces for each neighbor. This list has one entry for each neighbor on attached links. For IPv6, it contains information received in an Advertisement Message.

An IPv4 node discovers its neighbor on an Ethernet link by sending an ARP request, which returns a MAC address for that neighbor.

When a protocol interface is created or enabled on an IPv6 node, or when the first IPv6 address is added, a Router Solicitation is sent from that interface. If the DUT responds to the Router Solicitation by sending a Router Advertisement, the DUT is 'discovered' (learned). A Neighbor Solicitation is also sent from the interface for Duplicate Address Detection (DAD), to confirm that no other node on the link has the same address.

Subsequently, when an upper layer (routing) protocol configured for the interface needs to find the MAC address for a link local address learned through other means, the discovery process is handled by sending Neighbor Solicitations and receiving Neighbor Advertisements.

Figure:Discovered Neighbors Tab



The fields and controls shown in the Discovered Neighbors tab are described in *Table:Discovered Neighbors Tab*.

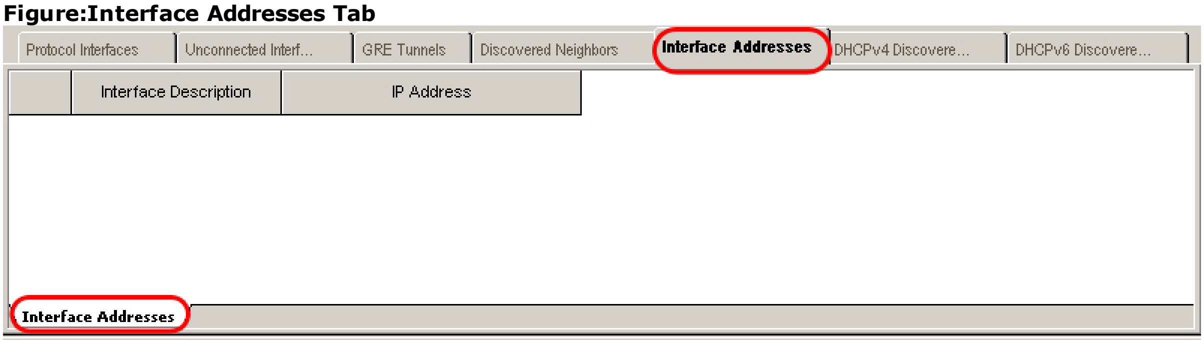
Table:Discovered Neighbors Tab

Field/Control	Description
Interface Description	The description of the interface which has learned the neighbor.
IP Addresses	The IP addresses for the discovered interface.
Neighbor MAC Address	The link layer (Layer 2) MAC address of the discovered interface on a neighbor.
IsRouter	For IPv6, the status of the router flag (R-bit) in the Neighbor Advertisement Message. If the bit is set, it Informs the local IPv6 node that the sender is a router.

Interface Addresses

The Interface Addresses tab in the Protocol Interfaces window is shown in *Figure:Interface Addresses Tab*. This tab contains a list of IP addresses learned for each of the Protocol Interfaces.

Figure:Interface Addresses Tab



The fields and controls shown in the Interface Addresses tab are described in *Table:Interface Addresses Tabs*.

Table:Interface Addresses Tabs

Field/Control	Description
Interface Description	The description of the interface which has learned the address.

Field/Control	Description
IP Address	A learned IP address for this interface.

DHCPv4 Discovered Information

The Dynamic Host Configuration Protocol (DHCP) Discovered Information, based on RFC 2131, is supported in the Protocol Interfaces window, as shown in *Figure:DHCPv4 Discovered Information*. When the protocol interface is set for DHCP and enabled, DHCP negotiations will be started. Configuration parameters, such as IPv4 network addresses, masks, and associated Gateway addresses learned from the DHCP server will be viewable in this read-only window.

NOTE

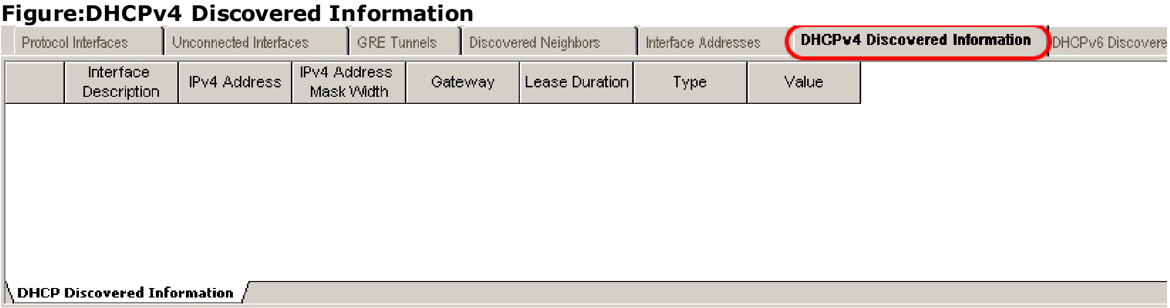
You will not be able to select DHCPv4-enabled interfaces for use with protocol emulations, with the exception of IGMP.

DHCP is applicable only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.

NOTE

When DHCP is enabled on a Protocol Interface, you will not be able to enter the IPv4 address, mask, or gateway address, as these values will be automatically assigned.

Figure:DHCPv4 Discovered Information



The fields and controls shown in this tab are described in *Table:DHCPv4 Discovered Information Tab*.

Table:DHCPv4 Discovered Information Tab

	Field/Control	Description
	Interface Description	The Interface Description for the Ixia protocol interface that is negotiating with the DHCP Server.
	IPv4 Address	A learned/allocated IPv4 address for this interface.
	IPv4 Address Mask Width	A learned/allocated IPv4 address prefix length (mask) for this interface.
	Gateway	A learned/allocated IPv4 Gateway address for this interface.
	Lease Duration	(in seconds) The lease timer value specified from the

	Field/Control	Description
		DHCP Server.
(DHCP Options)		Options advertised by the DHCP Server, presented as a list of Type/Length/Value tuples (TLVs).
	Type	(integer) The identifier or 'tag' for this DHCP option.
	Value	The DHCP option value field may contain data for configuration information such as time server information, and so forth.

DHCPv6 Discovered Information

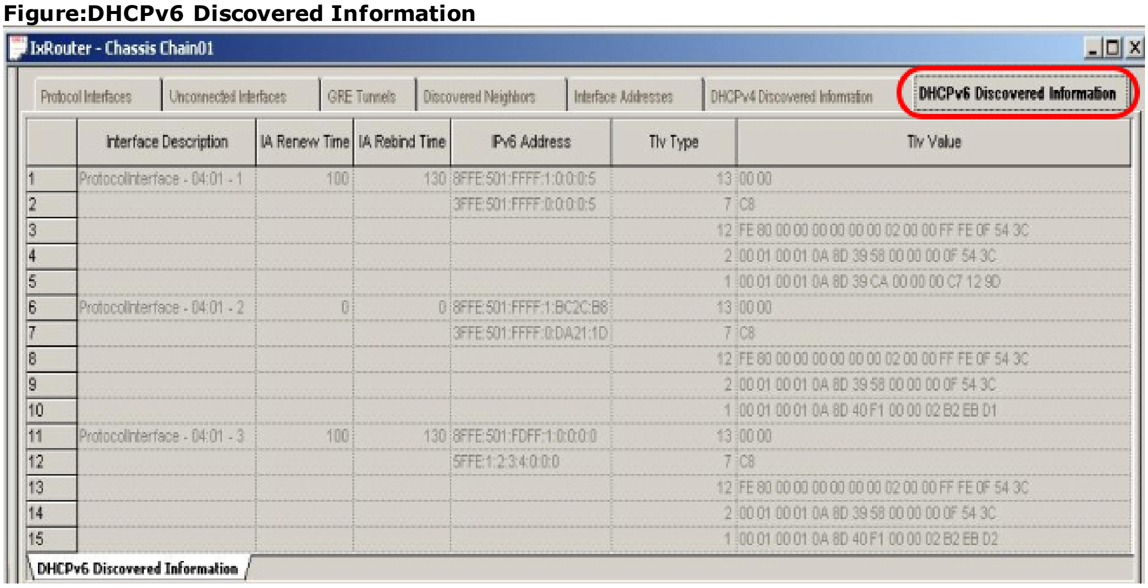
The Dynamic Host Configuration Protocol Version 6 (DHCPv6) Discovered Information, based on RFC 3315, is supported in the Protocol Interfaces window, as shown in *Figure:DHCPv6 Discovered Information*. When the protocol interface is set for DHCPv6 and enabled, DHCPv6 negotiations will be started. Configuration parameters, such as IPv6 network addresses learned from the DHCPv6 server will be viewable in this read-only window.

NOTE You will not be able to select DHCPv6-enabled interfaces for use with protocol emulations.

DHCP is applicable only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.

NOTE When DHCPv6 is enabled on a Protocol Interface, you will not be able to enter the IPv6 addresses, as these values will be automatically assigned.

Figure:DHCPv6 Discovered Information



The fields and controls shown in this tab are described in *Table:DHCPv4 Discovered Information Tab*.

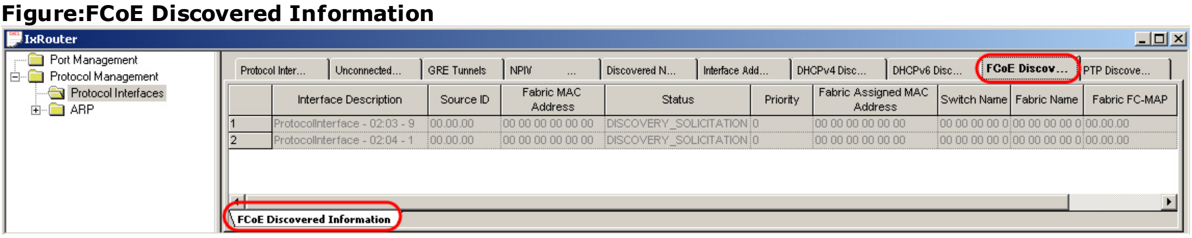
Table:DHCPv6 Discovered Information Tab

Field/Control	Description
Interface Description	The Interface Description for the Ixia protocol interface that is negotiating with the DHCPv6 Server.
IA Renew Time	(in seconds) The renew timer value specified by the DHCPv6 Server.
IA Rebind Time	(in seconds) The rebind timer value specified by the DHCPv6 Server.
IPv6 Address	A learned/allocated IPv6 address for this interface.
(DHCPv6 Options)	Options advertised by the DHCPv6 Server, presented as a list of Type/Length/Value tuples (TLVs).
Tlv Type	(integer) The identifier or 'tag' for this DHCPv6 option.
Tlv Value	The DHCPv6 option value field may contain data for configuration parameter information.

FCoE Discovered Information

The FCOE Discovered Information tab lists the obtained source FCID and status for each FCoE/NPIV interface.

Figure:FCoE Discovered Information



The read-only fields shown in this tab are described in *Table:DHCPv6 Discovered Information Tab*.

Table:FCoE Discovered Information Tab

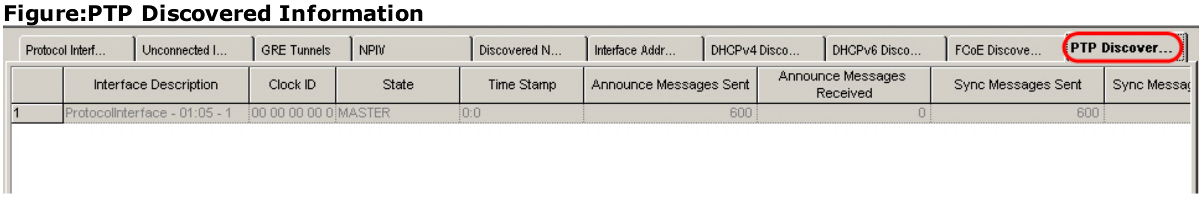
Field	Description
Interface Description	The Interface Description for the Ixia protocol interface that is negotiating with the FCoE Server.
Source ID	Source ID assigned by the Fabric
Fabric MAC Address	MAC address of the Fabric
Status	Textual description of the status of the interface
Priority	(Only if FIP is enabled) The priority of the Fabric we are logged into.
Fabric Assigned MAC Address	(Only if FIP is enabled) The MAC address assigned by the Fabric.
Switch Name	(Only if FIP is enabled) The switch name obtained from the Discovery Advertisement.

Field	Description
Fabric Name	(Only if FIP is enabled) The Fabric name obtained from the Discovery Advertisement.
Fabric FC-MAP	(Only if FIP is enabled) Obtained from the Discovery Advertisement.
Discovered VLAN ID	The list of IDs discovered from the VLAN Discovery notification

PTP Discovered Information

PTP ports discover other ports within a communication path through the receipt of multicast Announce messages.

Figure:PTP Discovered Information



The fields and controls shown in this tab are described in *Table:DHCPv6 Discovered Information Tab*.

Table:PTP Discovered Information Tab

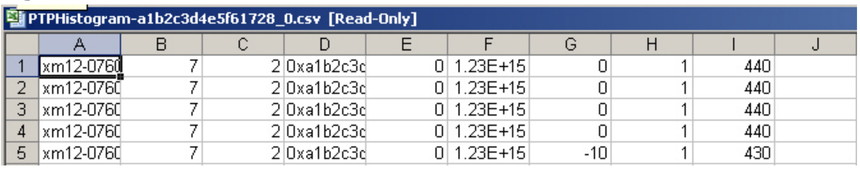
Field/Control	Description
Interface Description	The Interface Description for the Ixia protocol interface that is negotiating with the PTP Server.
Clock ID	
State	Defines the state of the clock: master or , unknown or uncalibrated
Time Stamp	Timestamp of statistics.
Announce Messages Sent	Number of announce messages sent by the interface.
Announce Messages Received	Number of announce messages received by the interface.
Sync Messages Sent	Number of sync messages sent by the interface.
Sync Messages Received	Number of sync messages received by the interface.
Follow-up Messages Sent	Number of follow-up messages sent by the interface.
Follow-up Messages Received	Number of follow-up messages received by the interface.
Delay Request Messages Sent	Number of delay request messages sent by the interface.
Delay Request Messages Received	Number of delay request messages received by the interface.
Delay Response Messages Sent	Number of delay response messages sent by the interface.
Delay Response Messages Received	Number of delay response messages received by the interface.

Field/Control	Description
Clock Offset	The offset of the clock in nanoseconds with reference to its master, as calculated by the per 1588 protocol. It is a measure of time transfer.
Time Slope	The ratio of the clock frequency to its master clock frequency. It is a measure of frequency transfer.
Mean Path Delay	The mean propagation time between master and clock.
Record Histogram Data	Click Start to start (or resume) recording. Click Stop to stop recording. Clicking Stop does not clear the accumulated data.
Clear Histogram Data	Click Clear to clear the accumulated data.
Save Histogram Data to Disk	Click Save to save all accumulated data. A typical Save As dialog will appear. **Note**: To avoid overwriting previously saved data, modify the suggested filename.

Saved PTP Discovered Info Data

When PTP histogram data is saved to disk, a comma-separated-values (.csv) file is created. The .csv file can be opened as-is, or can be opened in MS Excel, as shown in the following example (*Figure:PTP Discovered Information*).

Figure:PTP Discovered Information


PTPHistogram-a1b2c3d4e5f61728_0.csv [Read-Only]

	A	B	C	D	E	F	G	H	I	J
1	xm12-0760	7	2	0xa1b2c3c	0	1.23E+15	0	1	440	
2	xm12-0760	7	2	0xa1b2c3c	0	1.23E+15	0	1	440	
3	xm12-0760	7	2	0xa1b2c3c	0	1.23E+15	0	1	440	
4	xm12-0760	7	2	0xa1b2c3c	0	1.23E+15	0	1	440	
5	xm12-0760	7	2	0xa1b2c3c	0	1.23E+15	-10	1	430	

The columns in the spreadsheet contain the types of information described in *Table:PTP Discovered Information Saved Data*.

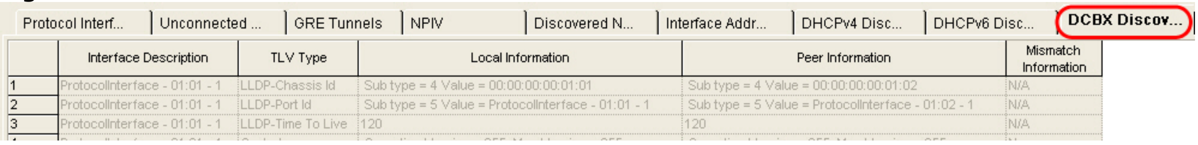
Table:PTP Discovered Information Saved Data

Column	Description
A	Chassis name
B	Card number
C	Port number
D	PTP Clock ID
E	PTP Port Identity
F	PTP Time Stamp
G	PTP Clock Offset from master
H	Time Slope
I	Mean Path Delay

DCBX Discovered Information

The Data Center Bridging (DCB) Capability Exchange Protocol (DCBX) Discovered Information is supported in the Protocol Interfaces window, as shown in *Figure:DCBX Discovered Information*. When the protocol interface is set for DCBX and enabled, DCBX negotiations will be started. Configuration information learned from peers will be viewable in this read-only window.

Figure:DCBX Discovered Information



The fields and controls shown in this tab are described in *Table:DHCPv6 Discovered Information Tab*.

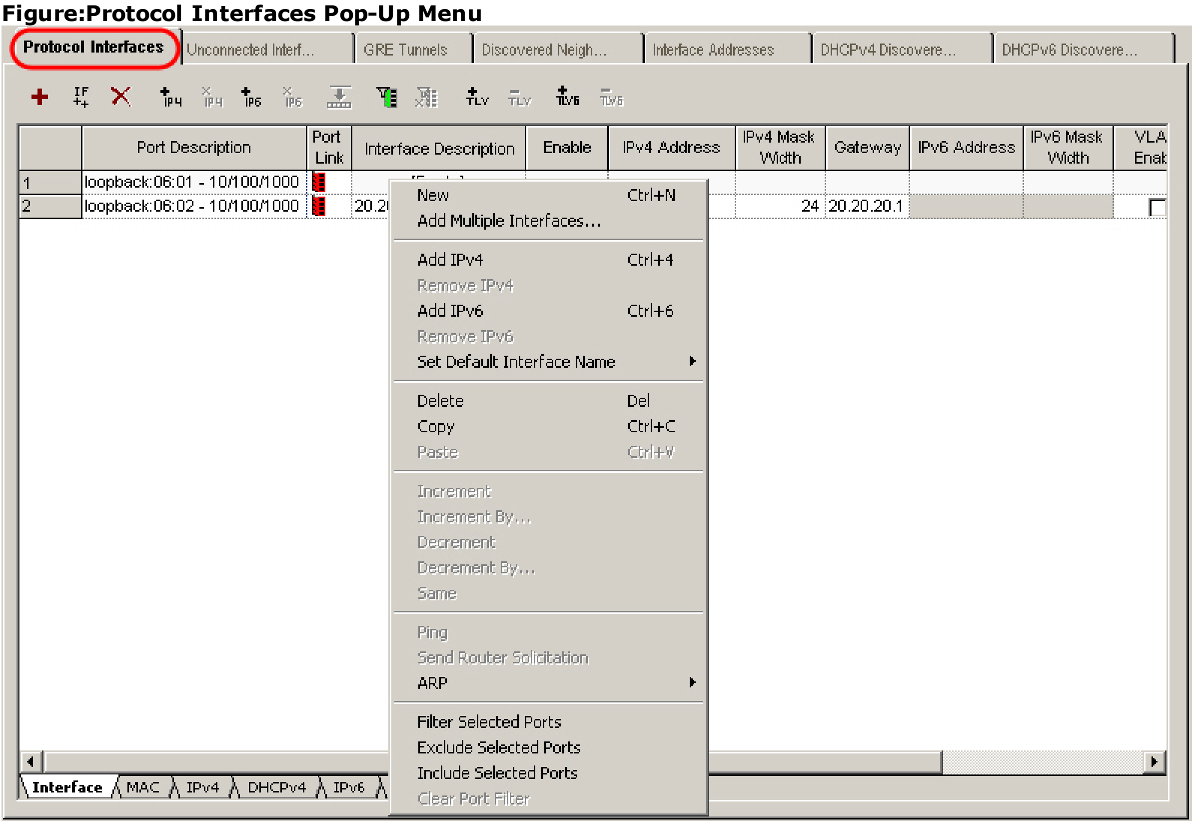
Table:DCBX Discovered Information Tab

Field/Control	Description
Interface Description	The Interface Description for the Ixia protocol interface
TLV Type	The name of the TLV (example: LLDP Chassis ID)
Local Information	The operating information of all TLVs on the local port
Peer Information	The peer TLV information
Mismatch Information	Indicates any mismatch in the TLVs . This applies only for DCBX TLVs and the algorithm to determine mismatches is different for each TLV.

Protocol Interfaces Pop-Up Menu

There is a pop-up menu that is displayed by right-clicking a row in any of the Protocol Interface views. The available menu options differ depending on the view selected. The pop-up menu for the Protocol Interfaces window is shown in *Figure:Protocol Interfaces Pop-Up Menu*.

Figure:Protocol Interfaces Pop-Up Menu



The options available in this menu depend on the type of view currently displayed. All of the possible options are described in *Table:Interfaces—Pop-Up Menu*.

Table:Interfaces—Pop-Up Menu

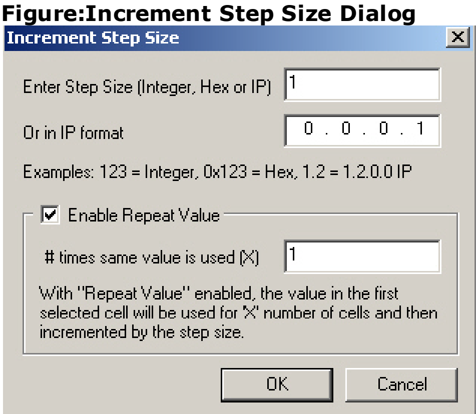
Menu Options	Description
New	Add one protocol interface to the selected port.
Add Multiple Interfaces...	Displays the Protocol Interfaces wizard. *Protocol Interface Wizard* for additional information.
Add IPv4	Add one IPv4 address entry to the selected interface. A maximum of one IPv4 address entry may be added to each interface.
Remove IPv4	Remove an IPv4 address from the selected interface.
Add IPv6	Add one IPv6 address entry to the selected interface. Multiple IPv6 addresses may be added to one interface.
Remove IPv6	Removes one or more IPv6 addresses from the selected interface.
Set Default Interface Name	Automatically renames the protocol interface with the IP addresses, to create unique names for the interfaces.
Delete	Permanently removes one or more selected interface(s) from the view.
Copy	Copy is used with the Paste operation. Selected fields for an interface may be copied and pasted into the fields for a different interface.
Paste	Paste is used with the Copy operation. Selected fields for an interface may be copied and pasted into the fields for a different interface.
Increment	For use with multiple, consecutive, and numerical items in a column. When the items are selected, and 'Increment' is chosen, all of the items will be numbered in increasing order—starting with the value for the topmost item in the column. The value for each consecutive selected item in the column will be one greater than the previous item.
Increment By...	For use with multiple, consecutive, numerical items in a column. When the items are selected, and 'Increment By...' is chosen, all of the items will be numbered in increasing order—starting with the value for the topmost item in the column. The value for each consecutive selected item in the column will be increased by the amount specified in the 'Increment Step Size' dialog. *Increment Step Size Dialog* for additional information.
Decrement	For use with multiple, consecutive, numerical items in a column. When the items are selected, and 'Decrement' is chosen, all of the items will be assigned values in decreasing order—starting with the value for the topmost item in the column. The value for each consecutive selected item in the column will be one less than the previous item.

Menu Options	Description
Decrement By...	For use with multiple, consecutive numerical items in a column. When the items are selected, and 'Decrement By...' is chosen, all of the items will be assigned values in decreasing order—starting with the value for the topmost item in the column. The value for each consecutive selected item in the column will be decreased by the amount specified in the 'Increment Step Size' dialog. *Increment Step Size Dialog* for additional information.
Same	For use with multiple, consecutive numerical items in a column. When the items are selected, and 'Same' is chosen, all of the items will be assigned the same value—the value for the topmost item in the column.
Ping	(for Ethernet type modules only) Displays the Ping dialog for the Interface views.
Send Router Solicitation	Sends a Router Solicitation Message for IPv6 Neighbor Discovery (RFC 2461). After an IPv6 interface is enabled on a host, an ICMPv6 Router Solicitation packet is sent by the host to request that routers **immediately** send Router Advertisements containing link-layer addresses in reply. This request temporarily overrides the timed cycle for sending Router Advertisements.
ARP	Displays a sub-pop-up list for the types of ARP operations. Choose one of: • Send ARP for selected • Refresh ARP for selected • Clear ARP for selected
Filter Selected Ports	Use the Filter Ports feature.
Exclude Selected Ports	Ports in the 'Include' list in the Port Filter dialog are disabled and removed from the list of ports in the Protocol Interfaces window.
Include Selected Ports	Ports in the 'Include' list in the Port Filter dialog are enabled and displayed in the list of ports in the Protocol Interfaces window.
Clear Port Filter	Clears the Port Filter feature—all owned ports are displayed in the table of the Protocol Interface window.

Increment Step Size Dialog

When the 'Increment By' or 'Decrement By' options are selected, the Increment Step Size dialog opens so you can define an increment/decrement step other than '1' (the default setting). This dialog applies ONLY for incrementing or decrementing selected, contiguous values in a column. The Increment Step Size dialog box is shown in *Figure:Increment Step Size Dialog*.

Figure:Increment Step Size Dialog



The fields and controls in this dialog are described in *Table:Increment Step Size Dialog*.

Table:Increment Step Size Dialog

Field/Control	Description
Enter Step Size (Integer, Hex or IP)	Enter an integer, a hex value, or an 'IP' value that will be used as the increment step value. Entry examples: • 123 = Integer • 0x123 = Hex • 1.2 = 1.2.0.0 IP
Or in IP format	Enter a 4-octet IP address that will be used as the increment step value.
Enable Repeat Value	With 'Repeat Value' enabled, the value in the first selected cell will be used for 'X' number of cells and then incremented by the increment step size.
# times same value is used (X) (Repeat Value)	Enter the number of times that a value will be used before this value will be incremented by the amount of the 'Step Size'. For example: If the initial value is 10.0.0.1, the Step Size is '0.0.0.1,' and the Repeat Value is '2': • 10.10.10.1 • 10.10.10.1 • 10.10.10.2 • 10.10.10.2 • 10.10.10.3 • 10.10.10.3 • etc.

Protocol Interface Wizard

The Protocol Interface Wizard is described in the following sections:

- *Accessing the Protocol Interface Wizard*
- *Protocol Interface Wizard Types*
  - *Protocol Interface Wizard–Connected Interfaces*
  - *Protocol Interface Wizard–Unconnected Interfaces*
  - *Protocol Interface Wizard—GRE Tunnels*
  - *Protocol Interface Wizard–FCoE and NPIV*

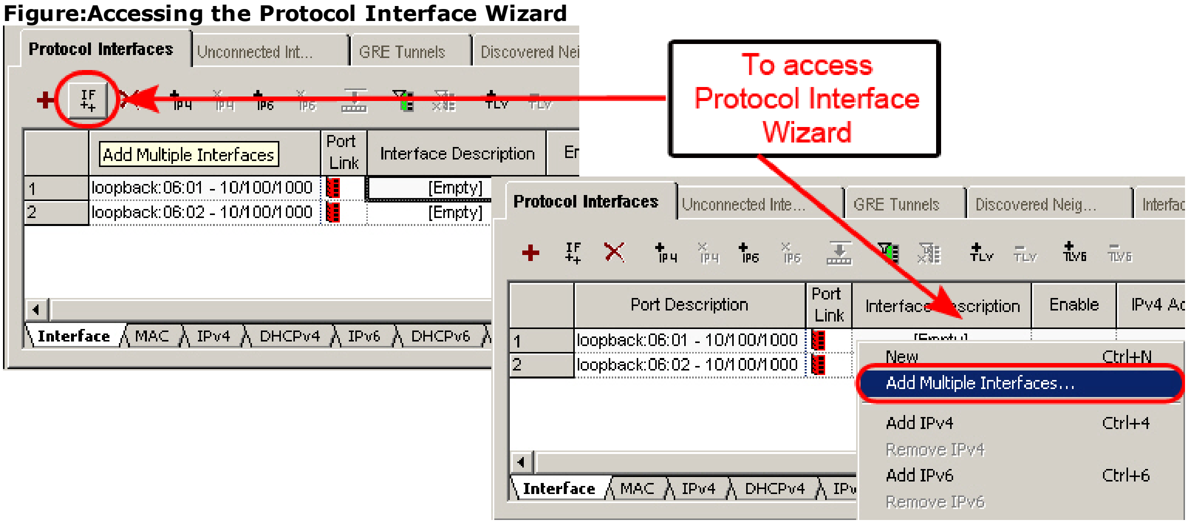
NOTE The GRE Tunnels wizard is available ONLY for modules that support GRE over IP.

Refer to the *Ixia Platform Reference Manual* for information on modules that support this feature.

Accessing the Protocol Interface Wizard

The Protocol Interface wizard can be accessed using the methods shown in *Figure:Accessing the Protocol Interface Wizard*. Information on the use of this wizard is found in *Protocol Interface Wizard Types*.

Figure:Accessing the Protocol Interface Wizard



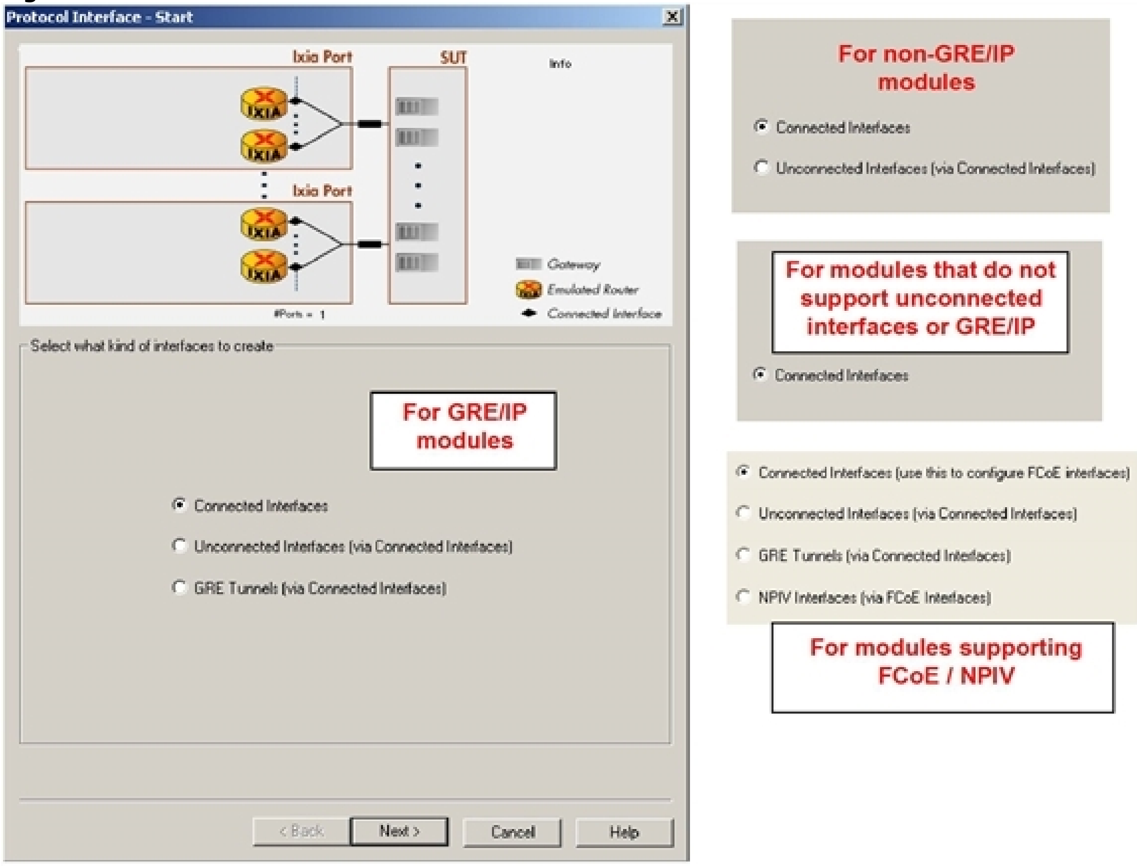
Protocol Interface Wizard Types

The Protocol Interface Wizard is shown in *Figure:Protocol Interface Wizard—Start Dialog (for Connected Interfaces)*. It allows to configure three different types of protocol interfaces, with customized dialogs and diagrams for each type, as described in the following sections:

- *Protocol Interface Wizard–Connected Interfaces*
- *Protocol Interface Wizard–Unconnected Interfaces*
- *Protocol Interface Wizard—GRE Tunnels*
- *Protocol Interface Wizard–FCoE and NPIV*

NOTE The GRE Tunnels wizard is available ONLY for modules that support GRE over IP.
Refer to the *Ixia Platform Reference Manual* for information on modules that support this feature.

Figure:Protocol Interface Wizard



Protocol Interface Wizard–Connected Interfaces

The GUI screens in the Protocol Interface Wizard for Connected Interfaces, and their use, are described in the following sections:

- *Protocol Interface Wizard—Start Dialog (for Connected Interfaces)*
- *Protocol Interface Wizard—Connected Interfaces Dialog (for Connected Interfaces)*
- *Protocol Interface Wizard—ATM Dialog (for Connected Interfaces)*
- *Protocol Interface Wizard—Finish Dialog (for Connected Interfaces)*

NOTE

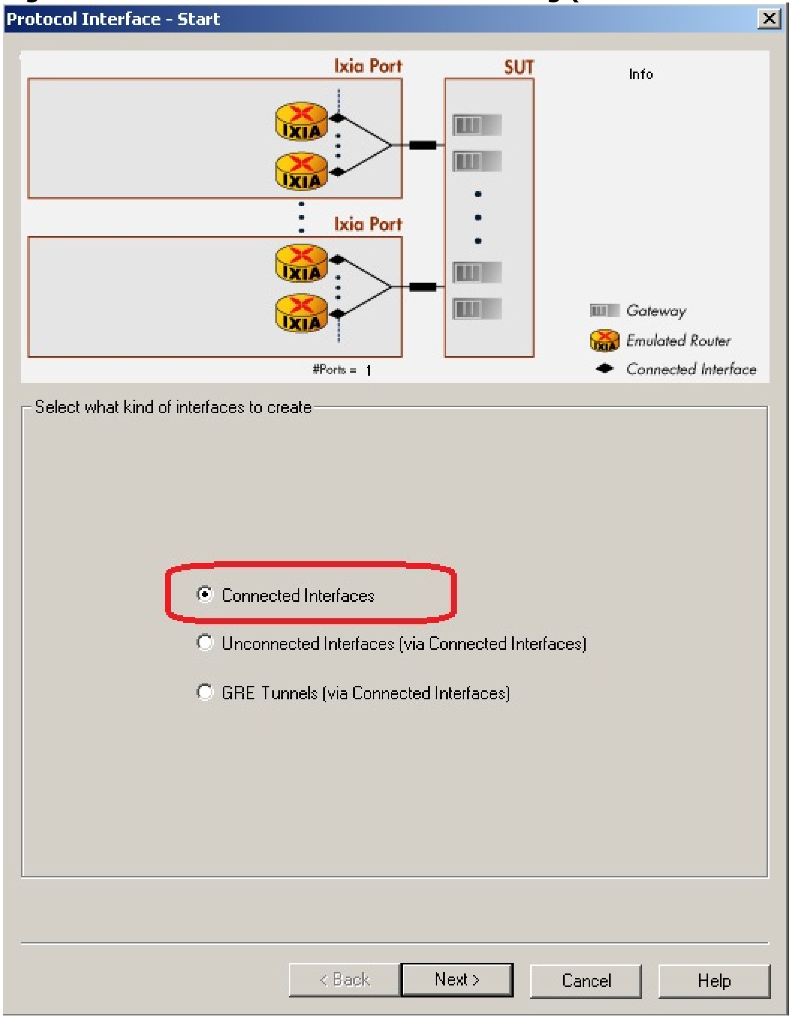
Protocol interfaces should not be created in the same subnet as the IxRemoteIP (the IxRemoteIP subnet default is 10.0.0.0). Creating protocol interfaces in this subnet will cause problems and odd behavior.

Chassis Properties—IxRemoteIp for more information on the IxRemoteIP, and how to change the default subnet.

Protocol Interface Wizard—Start Dialog (for Connected Interfaces)

The Protocol Interface Wizard—Start dialog, with 'Connected Interfaces' selected, is shown in *Figure:Protocol Interface Wizard—Start Dialog (for Connected Interfaces)*. Connected Interfaces are created on directly-connected links between the Ixia port and a DUT port.

Figure:Protocol Interface Wizard—Start Dialog (for Connected Interfaces)



The fields and controls in this dialog are described in *Table:Start Dialog (for Connected Interfaces)*.

Table:Start Dialog (for Connected Interfaces)

Section	Field/Control	Description
Select what kind of interfaces to create	Connected Interfaces	Select this option to create one or more 'Connected Interfaces'—Ixia-emulated protocol interfaces that are on the directly-connected physical link between an Ixia port and a DUT/SUT port.
	Unconnected Interfaces (via Connected Interfaces)	Select this option to create one or more 'Unconnected Interfaces'—Ixia-emulated protocol interfaces that are NOT on the directly-connected physical link between an Ixia port and a DUT/SUT port. The Unconnected Interfaces are 'virtual interfaces' that connect to 'virtual routers'—to create a virtual topology 'behind' the Ixia-emulated router.

Section	Field/Control	Description
		In order for the virtual routers 'behind' the Ixia-emulated router to 'communicate' with the DUT/SUT, each Unconnected Interface must be associated with a Connected Interface.
	GRE Tunnels (via Connected Interfaces)	Select this option to create one or more Ixia-emulated 'GRE Tunnels.' Each GRE tunnel is emulated over the directly-connected physical link between an Ixia port and a DUT/SUT port and beyond (to the GRE tunnel destination end point). Each GRE Tunnel must be associated with a Connected Interface—to be used as the Source IP address, for the local end of the tunnel.

Protocol Interface Wizard—Connected Interfaces Dialog (for Connected Interfaces)

The dialog for creating connected interfaces is shown in *Figure:Connected Interfaces Dialog (for Connected Interfaces)*. This dialog can be used to streamline the process of configuring multiple connected (connected to the DUT/SUT) interfaces on one or more Ixia ports. The diagram at the top of the dialog displays the configuration values that you are entering into the fields in the dialog.

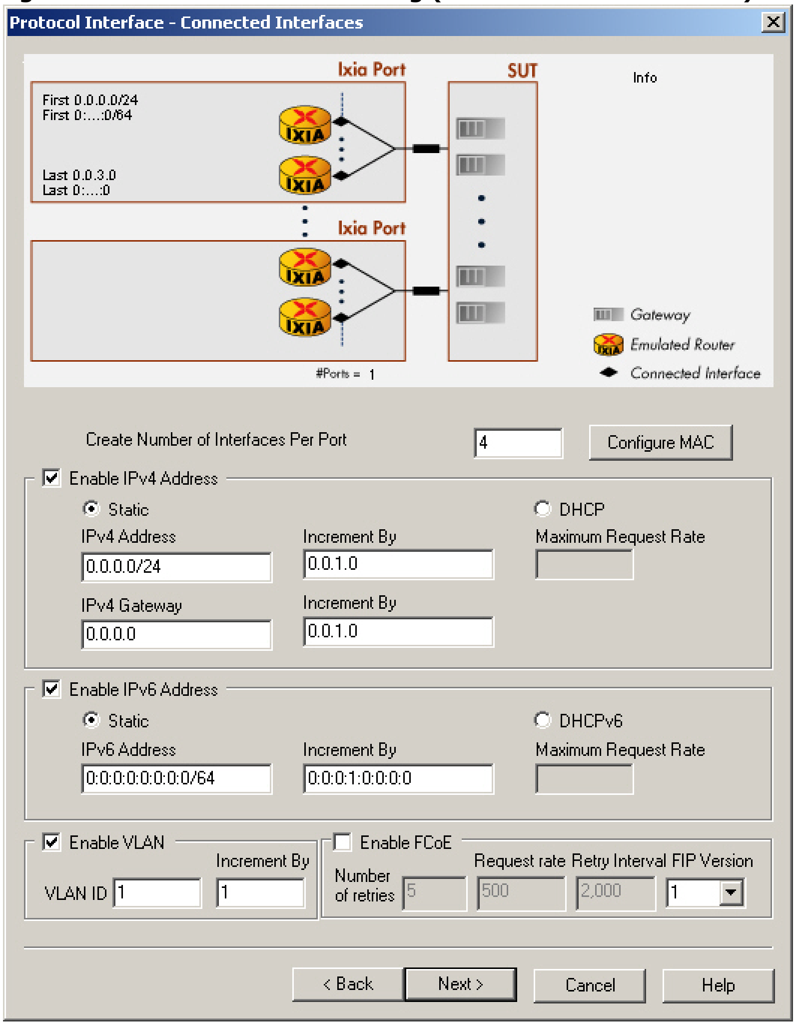
NOTE

You will not be able to select DHCPv4-enabled interfaces for use with protocol emulations, with the exception of IGMP.

You will not be able to select DHCPv6-enabled interfaces for use with protocol emulations.

DHCP is applicable only to Ethernet ports and to ATM ports using Bridged Ethernet encapsulation.

Figure:Connected Interfaces Dialog (for Connected Interfaces)



The fields and controls in this dialog are described in *Table:Connected Interfaces Dialog (for Connected Interfaces)*.

Table:Connected Interfaces Dialog (for Connected Interfaces)

Section	Field/Control	Description
Header	Create number of interfaces per port	Enter the number of interfaces to be added to the current port. The default is 1 interface. NOTE The number of protocol interfaces that can be added depends on the amount of memory available.
Enable IPv4 Address	Enable IPv4 Address	If selected, one or more IPv4 interface address(es) can be configured for this port.
(Address assign-ment mode)	Static	(Default) If selected, you may manually configure IPv4 addresses for this protocol interface.
(Address Assign-ment mode)	DHCP	**Available for Ethernet ports and ATM ports in Bridged Ethernet mode only.**

Section	Field/Control	Description
		If selected, the IPv4 address configuration fields will be dimmed and unavailable for configuration. IPv4 addresses and additional network configuration information will be allotted to this protocol interface through the DHCPv4 protocol. NOTE This option is available for connected interfaces only (interfaces directly connected to a DUT).
	Maximum Request Rate	The maximum number of request messages that will be sent by this interface.
	IPv4 Address	A 32-bit IPv4 Address (with mask) for this particular interface.
	Increment IPv4 By	A 32-bit value to be applied to the IPv4 Gateway address as an increment step for creating a range of consecutive IPv4 addresses, starting with the least significant bit of the IPv4 address.
	IPv4 Gateway	A 32-bit IPv4 Address for the network gateway (typically the DUT) connected to this particular interface.
	Increment GW By	A 32-bit value to be applied to the IPv4 Gateway address as an increment step for creating a range of consecutive IPv4 addresses, starting with the least significant bit of the IPv4 address.
Enable IPv6 Address	Enable IPv6 Address	If selected, one or more IPv6 interface address(es) can be configured for this port.
(Address assignment mode)	Static	(Default) If selected, you may manually configure IPv6 addresses for this protocol interface.
(Address Assignment mode)	DHCPv6	**Available for Ethernet ports and ATM ports in Bridged Ethernet mode only.** If selected, the IPv6 address configuration fields will be dimmed and unavailable for configuration. IPv4 addresses and additional network configuration information will be allotted to this protocol interface through the DHCPv6 protocol. NOTE This option is available for connected interfaces only (interfaces directly connected to a DUT).

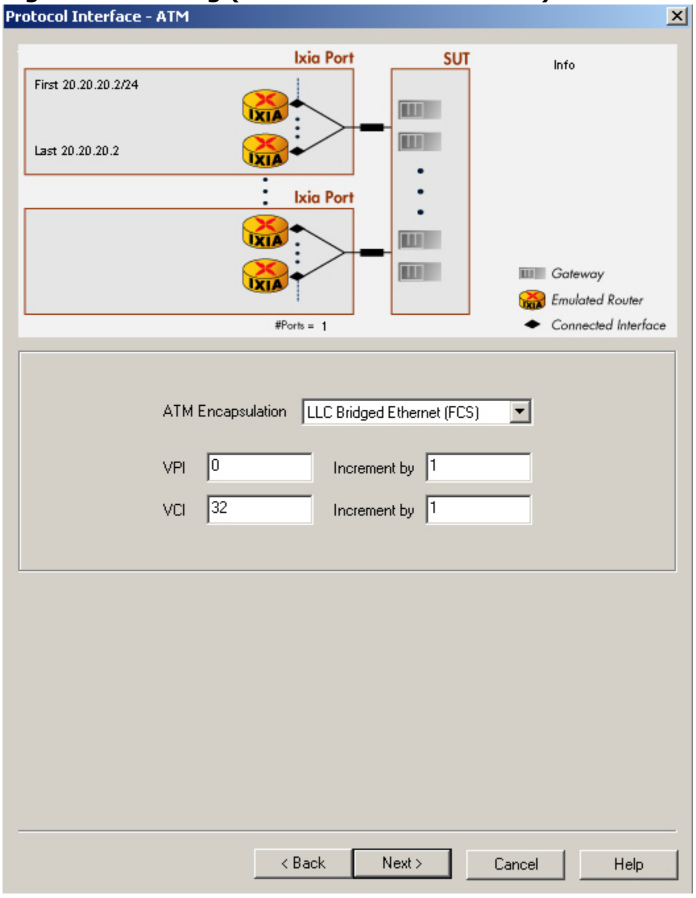
Section	Field/Control	Description
	Maximum Request Rate	The maximum number of request messages that will be sent by this interface.
	IPv6 Address	A 128-bit IPv6 Address (with mask) for this particular interface.
	Increment IPv6 By	A 128-bit value to be used with the IPv6 address as an increment step for creating a range of consecutive IPv6 addresses, starting with the least significant bit of the host part of the IPv6 address.
Enable VLAN		If selected, a VLAN can be assigned for each of the interfaces being created in this dialog.
	VLAN ID	(integer) The identifier value for the VLAN.
	Increment By	(integer) The value of the increment step to be used in creating the range of VLAN IDs for the interfaces created in this dialog.
Enable FCoE		If selected, FCoE will be enabled for each of the interfaces being created in this dialog.
	Number of retries	FCoE number of retries before being marked as Failure. (default = 5)
	Request rate	FCoE maximum rate (packets/second). (default = 500)
	Retry Interval	Interval between retries, when a packet is sent and no response received. Enter a value. Default = 2000 (milliseconds).
	FIP Version	0, 1, or Auto (default = 1). Auto = it will detect the version.

Protocol Interface Wizard—ATM Dialog (for Connected Interfaces)

NOTE This dialog is available for ATM ports **ONLY**.

For ATM ports there is an additional dialog in the Protocol Interface Wizard, as shown in *Figure:ATM Dialog (for Connected Interfaces)*. This dialog can be used to streamline the process of configuring one or more ‘connected’ (connected to the SUT) interfaces on one or more Ixia ATM ports. The diagram at the top of the dialog displays the configuration values that you are entering into the fields in the dialog.

Figure:ATM Dialog (for Connected Interfaces)



The fields and controls in this dialog are described in *Table:ATM Dialog (for Connected Interfaces)*.

Table:ATM Dialog (for Connected Interfaces)

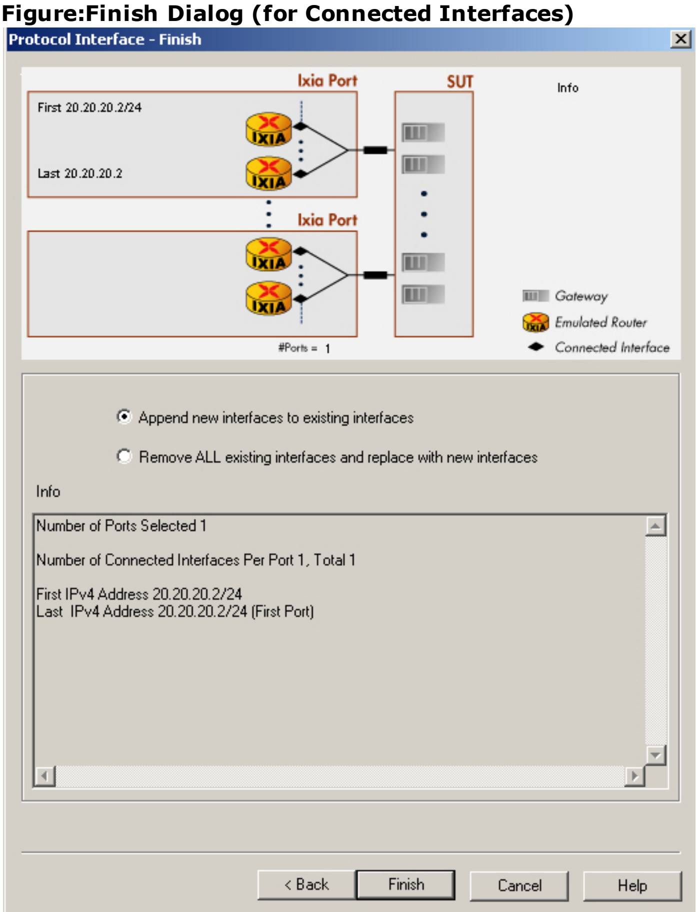
Field/Control	Description
ATM Encapsulation	The type of RFC 2684 ATM multiplexing encapsulation (routing) protocol to be used. Choose one of: • VC Mux IPv4 Routed • VC Mux IPv6 Routed • VC Mux Bridged Ethernet/802.3 (FCS) • VC Mux Bridged Ethernet/802.3 (no FCS) • LLC Routed AAL5 SNAP • LLC Bridged Ethernet (FCS) - (the Default) • LLC Bridged Ethernet (no FCS) NOTE See the information below regarding the two general types of ATM encapsulation. • **VC Mux**—VC MUX Protocols. For ATM Virtual Connection (VC) Multiplexing (‘Muxing’) encapsulation. Each ATM VC carries routed PDUs for only one protocol. Multiple VCs

Field/Control	Description
	are required for multiple protocols. Helps to reduce fragmentation overhead. • **LLC**—LLC Protocols. For ATM Logical Link Control (LLC) encapsulation. Each ATM VC carries routed PDUs for multiple types of protocols. Helps to reduce the number of separate VCs required when multiple protocols are used.
VPI	Virtual Path Identifier (VPI) for the ATM VC over which information is being transmitted. The valid minimum = 0.
Increment by	The increment step to add for creating each **additional** VPI.
VCI	Virtual Circuit/Connection Identifier (VCI) for the ATM VC over which information is being transmitted. The valid minimum = 32. (Values less than 32 are reserved.)
Increment by	The increment step to add for creating each **additional** VCI.

Protocol Interface Wizard—Finish Dialog (for Connected Interfaces)

The dialog for completing the configuration process for connected protocol interfaces is shown in *Figure:Finish Dialog (for Connected Interfaces)*. This dialog displays the configuration information in the 'Info' window, and allows to choose the way that interfaces will be applied to the ports. The diagram at the top of the dialog displays the configuration values that you have entered into the fields of the previous dialog.

Figure:Finish Dialog (for Connected Interfaces)



The fields and controls in this dialog are described in *Table:Finish Dialog (for Connected Interfaces)*.

Table:Finish Dialog (for Connected Interfaces)

Section	Field/Control	Description
Header	Append new interfaces to existing interfaces	Choose this option to add the newly created protocol interfaces to the list of existing protocol interfaces (in the Protocol Interface window).
	Remove ALL existing interfaces and replace with new interfaces	Choose this option if you want to delete the list of existing protocol interfaces (in the Protocol Interface window) and replace it with a list of the newly created protocol interfaces.
Info		This section of the dialog contains the current information regarding the newly created protocol interfaces, including: • Number of Ports selected • Number of Connected Interfaces for each port, and total number of Connected Interfaces • First and Last IPv4 Addresses of the range of IPv4 Addresses—for each port (if configured for IPv4) • First and Last IPv6 Addresses of the range of IPv6 Addresses—for each port (if configured for IPv6)

Protocol Interface Wizard–Unconnected Interfaces

The GUI screens in the Protocol Interface Wizard for Unconnected Interfaces, and their use, are described in the following sections:

- *Protocol Interface Wizard—Start Dialog (for Unconnected Interfaces)*
- *Protocol Interface Wizard—Connected Interface Dialog (for Unconnected Interfaces)*
- *Protocol Interface Wizard—Unconnected Interface Dialog*
- *Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)*
- *Protocol Interface Wizard—Finish Dialog (for Unconnected Interfaces)*

NOTE

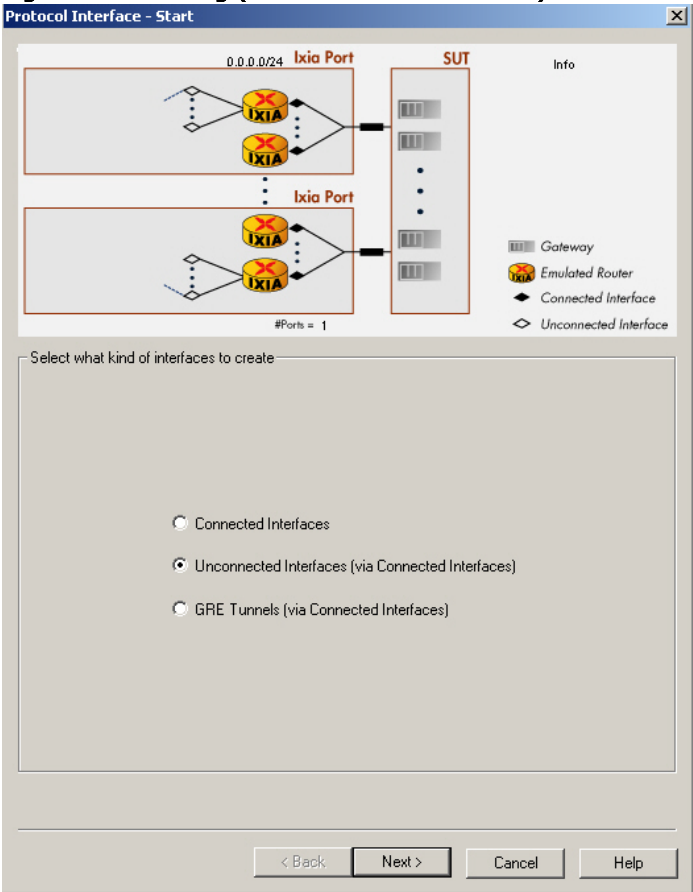
Protocol interfaces should not be created in the same subnet as the IxRemoteIP (the IxRemoteIP subnet default is 10.0.0.0). Creating protocol interfaces in this subnet will cause problems and odd behavior.

Chassis Properties—IxRemoteIp for more information on the IxRemoteIP, and how to change the default subnet.

Protocol Interface Wizard—Start Dialog (for Unconnected Interfaces)

The Protocol Interface Wizard—Start dialog, with 'Unconnected Interfaces' selected, is shown in *Figure:Start Dialog (Unconnected Interfaces)*. Unconnected Interfaces can be created as Loopback addresses for Ixia-emulated routers, or as virtual interfaces connecting to a virtual topology 'behind' the Ixia-emulated routers.

Figure:Start Dialog (Unconnected Interfaces)



The fields and controls in this dialog are described in *Table:Start Dialog (for Connected Interfaces)*.

Table:Start Dialog (for Connected Interfaces)

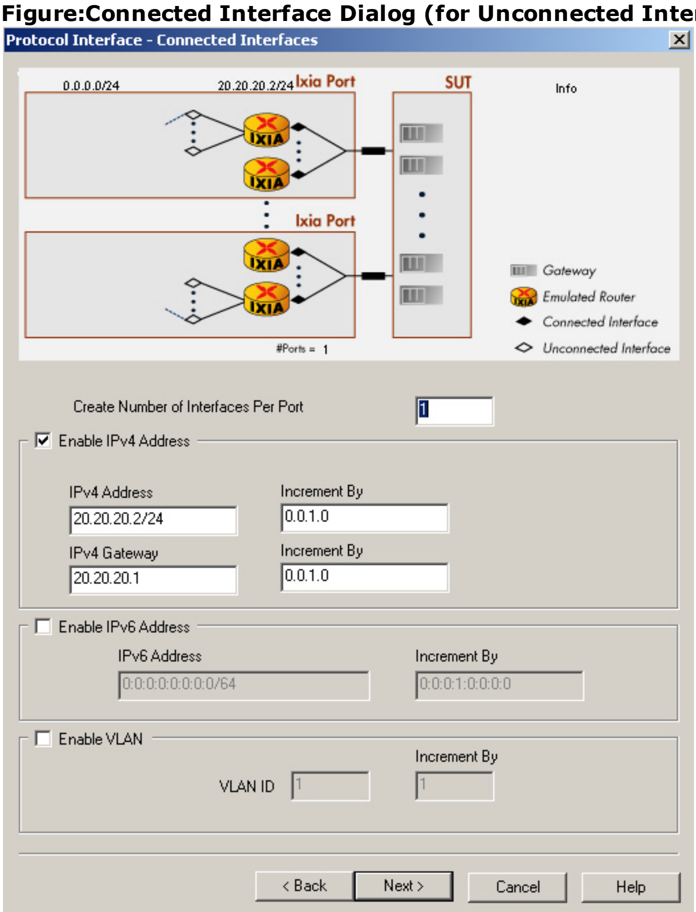
Section	Field/Control	Description
Select what kind of interfaces to create	Connected Interfaces	See *Table:Start Dialog (for Connected Interfaces)*.
	Unconnected Interfaces (via Connected Interfaces)	Select this option to create one or more 'Unconnected Interfaces'— Ixia-emulated protocol interfaces that are NOT on the directly-connected physical link between an Ixia port and a DUT/SUT port. The Unconnected Interfaces are 'virtual interfaces' that connect to 'virtual routers'—to create a virtual topology 'behind' the Ixia-emulated router.

Section	Field/Control	Description
		In order for the virtual routers 'behind' the Ixia-emulated router to 'communicate' with the DUT/SUT, each Unconnected Interface must be associated with a Connected Interface.
	GRE Tunnels (via Connected Interfaces)	See *Table:Start Dialog (for Connected Interfaces)*.

Protocol Interface Wizard—Connected Interface Dialog (for Unconnected Interfaces)

The Protocol Interface Wizard—Connected Interface dialog for Unconnected Interfaces is shown in *Figure:Connected Interface Dialog (for Unconnected Interfaces)*. The *Enable IPv4 Address* check box or *Enable IPv6 Address* check box must be selected, or the *Next* button will not be active and configuration cannot continue.

Figure:Connected Interface Dialog (for Unconnected Interfaces)



The fields and controls in this dialog are described in *Table:Connected Interfaces Dialog (for Unconnected Interfaces)*.

Table:Connected Interfaces Dialog (for Unconnected Interfaces)

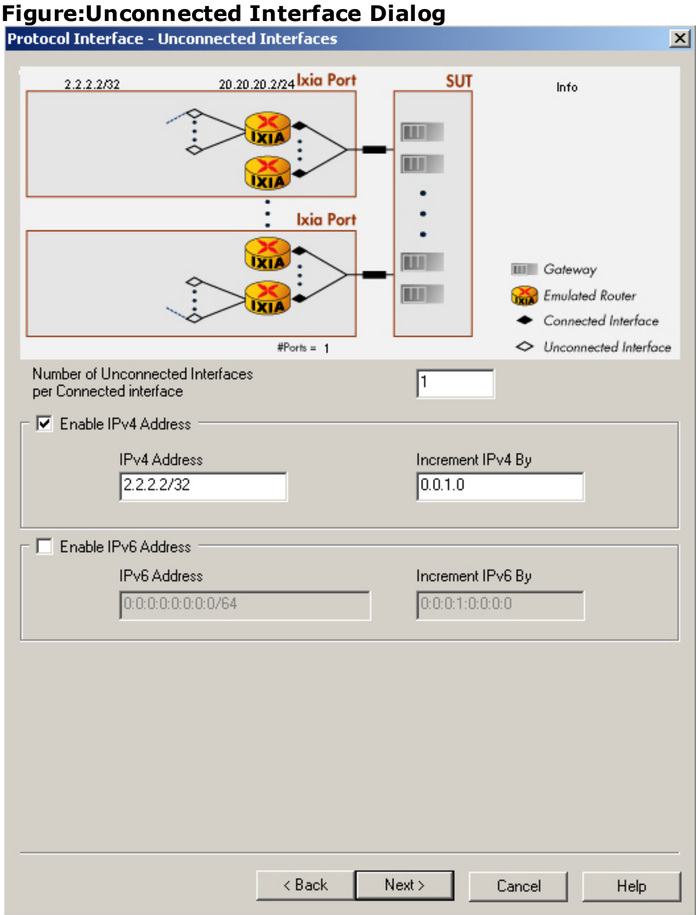
Section	Field/Control	Description
Header	Create number of interfaces per port	Enter the number of **connected** interfaces to be added to the current port. The default is 1 interface.

Section	Field/Control	Description
		NOTE The number of protocol interfaces that can be added depends on the amount of memory available.
Enable IPv4 Address	Enable IPv4 Address	If selected, one or more IPv4 interface address(es) can be configured for this port.
	IPv4 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv4 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	IPv4 Gateway	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment GW By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable IPv6 Address	Enable IPv6 Address	If selected, one or more IPv6 interface address(es) can be configured for this port.
	IPv6 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv6 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable VLAN	Enable VLAN	If selected, a VLAN can be assigned for each of the interfaces being created in this dialog.
	VLAN ID	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.

Protocol Interface Wizard—Unconnected Interface Dialog

The Protocol Interface Wizard—Unconnected Interface dialog is shown in *Figure:Unconnected Interface Dialog*.

Figure:Unconnected Interface Dialog



The fields and controls in this dialog are described in *Table:Unconnected Interface Dialog*.

Table:Unconnected Interface Dialog

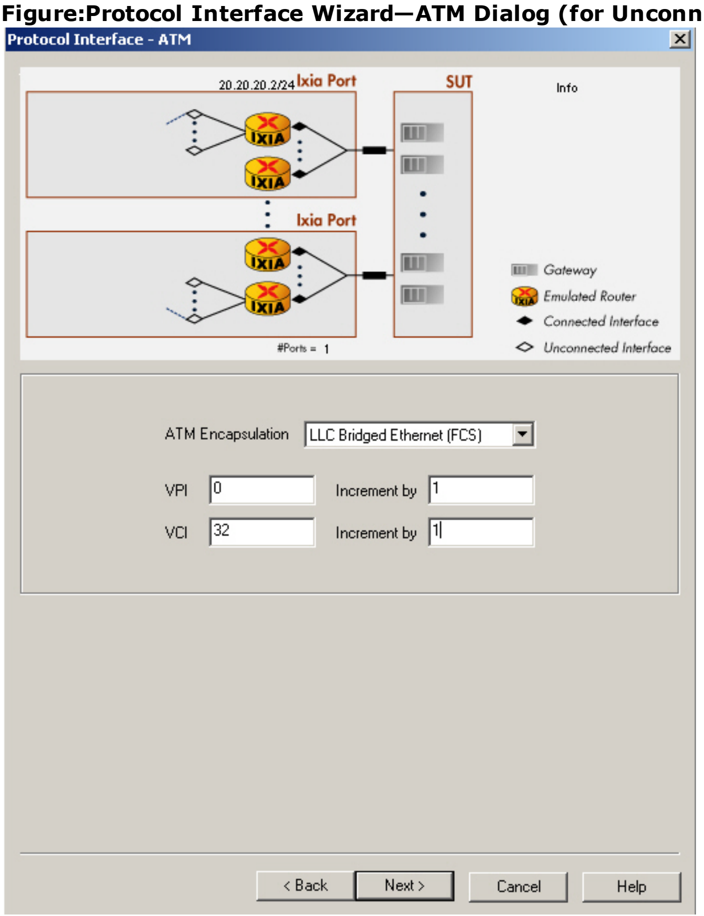
Section	Field/Control	Description
Header	Number of Unconnected Interfaces per Connected Interface	Enter the number of **Unconnected** interfaces to be created for each connected interface. The default is 1 unconnected interface. **NOTE** The number of protocol interfaces that can be added depends on the amount of memory available.
Enable IPv4 Address	Enable IPv4 Address	If selected, one or more IPv4 interface address(es) can be configured for this port.
	IPv4 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv4 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable IPv6 Address	Enable IPv6 Address	If selected, one or more IPv6 interface address(es) can be configured for this port.
	IPv6 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv6 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.

Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)

NOTE This dialog is available for ATM ports **ONLY**.

For ATM ports there is an additional dialog in the Protocol Interface Wizard for unconnected interfaces, as shown in *Figure:Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)*. This dialog can be used to streamline the process of configuring one or more Unconnected Interfaces (through Connected Interfaces) on one or more Ixia ATM ports. The diagram at the top of the dialog displays the configuration values that you are entering into the fields in the dialog.

Figure:Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)



The fields and controls in this dialog are described in *Table:Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)*.

Table:Protocol Interface Wizard—ATM Dialog (for Unconnected Interfaces)

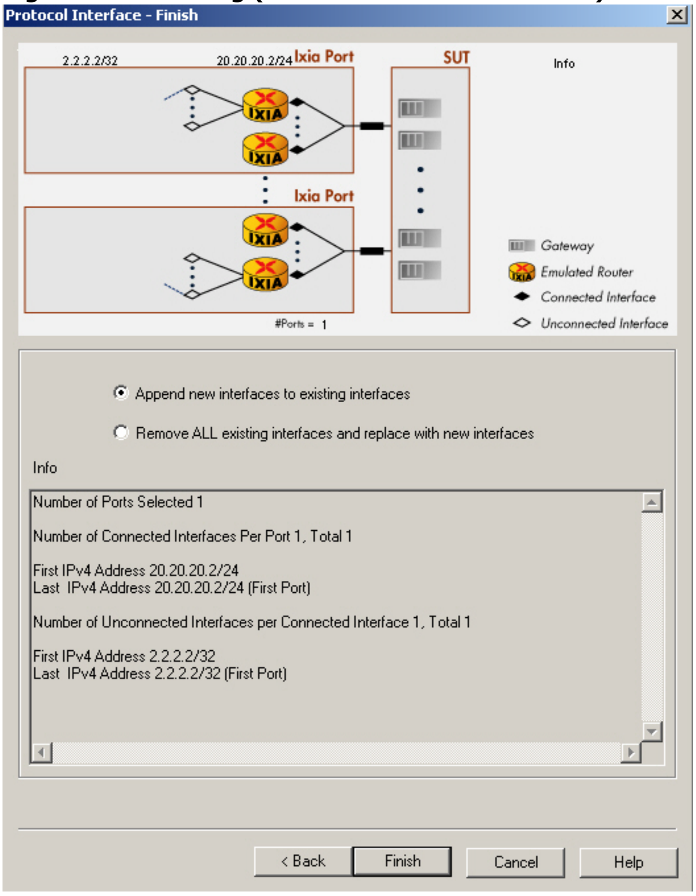
Field/Control	Description
ATM Encapsulation	The type of RFC 2684 ATM multiplexing encapsulation (routing) protocol to be used. See *Table:ATM Dialog (for Connected Interfaces)*.
VPI	See *Table:ATM Dialog (for Connected Interfaces)*.
Increment by	See *Table:ATM Dialog (for Connected Interfaces)*.

Field/Control	Description
VCI	See *Table:ATM Dialog (for Connected Interfaces)*.
Increment by	See *Table:ATM Dialog (for Connected Interfaces)*.

Protocol Interface Wizard—Finish Dialog (for Unconnected Interfaces)

The dialog for completing the configuration process for unconnected protocol interfaces is shown in *Figure:Finish Dialog (for Unconnected Interfaces)*. This dialog displays the configuration information in the 'Info' window, and allows to choose the way that interfaces will be applied to the ports. The diagram at the top of the dialog displays the configuration values that you have entered into the fields of the previous dialog.

Figure:Finish Dialog (for Unconnected Interfaces)



The fields and controls in this dialog are described in *Table:Finish Dialog (for Unconnected Interfaces)*.

Table:Finish Dialog (for Unconnected Interfaces)

Section	Field/Control	Description
Header	Append New Interfaces to existing interfaces	See *Table:Finish Dialog (for Connected Interfaces)*.
	Remove ALL existing Interfaces and replace with new inter-	See *Table:Finish Dialog (for Connected Interfaces)*.

Section	Field/Control	Description
	faces	
Info		This section of the dialog contains the current information regarding the newly created protocol interfaces, including: • Number of Ports Selected (Total) • Number of Connected Interfaces Per Port, and the Total number of connected interfaces • First and Last IPv4 Addresses of the range of IPv4 Addresses for connected interfaces—for each port (if configured for IPv4). • First and Last IPv6 Addresses of the range of IPv6 Addresses for connected interfaces—for each port (if configured for IPv6). • Number of Unconnected Interfaces per Connected Interface, and the Total number of unconnected interfaces. • First and Last IPv4 Addresses of the range of IPv4 Addresses for unconnected interfaces—for each port (if configured for IPv4). • First and Last IPv6 Addresses of the range of IPv6 Addresses for unconnected interfaces—for each port (if configured for IPv6).

Protocol Interface Wizard—GRE Tunnels

NOTE The GRE Tunnels wizard is available ONLY for modules that support GRE over IP. Refer to the *Ixia Platform Reference Manual* for information on modules that support this feature.

The GUI screens in the Protocol Interface Wizard for GRE Tunnels, and their use, are described in the following sections:

- *Protocol Interface Wizard—Start Dialog (for GRE Tunnels)*
- *Protocol Interface Wizard—Connected Interfaces Dialog (for GRE Tunnels)*
- *Protocol Interface Wizard—GRE Tunnels Dialog*
- *Protocol Interface Wizard—Finish Dialog (for GRE Tunnels)*

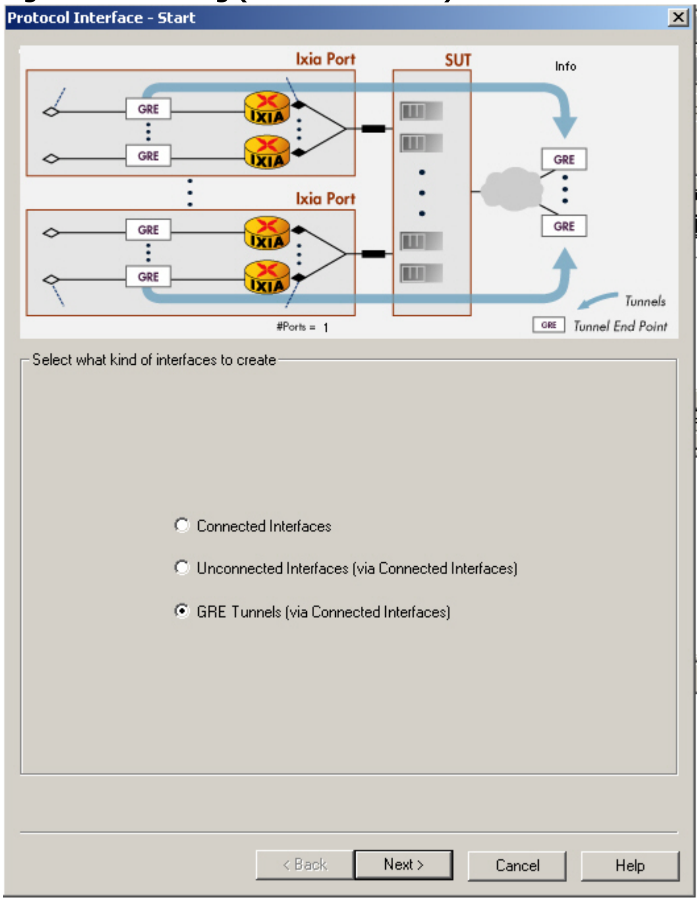
NOTE Protocol interfaces should not be created in the same subnet as the IxRemoteIP (the IxRemoteIP subnet default is 10.0.0.0). Creating protocol interfaces in this subnet will cause problems and odd behavior.

Chassis Properties—IxRemoteIp for more information on the IxRemoteIP, and how to change the default subnet.

Protocol Interface Wizard—Start Dialog (for GRE Tunnels)

The Protocol Interface Wizard—Start dialog, with 'GRE Tunnels' selected, is shown in *Figure:Start Dialog (for GRE Tunnels)*.

Figure:Start Dialog (for GRE Tunnels)



The fields and controls in this dialog are described in *Table:Protocol Interface Wizard—Start Dialog (for GRE Tunnels)*.

Table:Protocol Interface Wizard—Start Dialog (for GRE Tunnels)

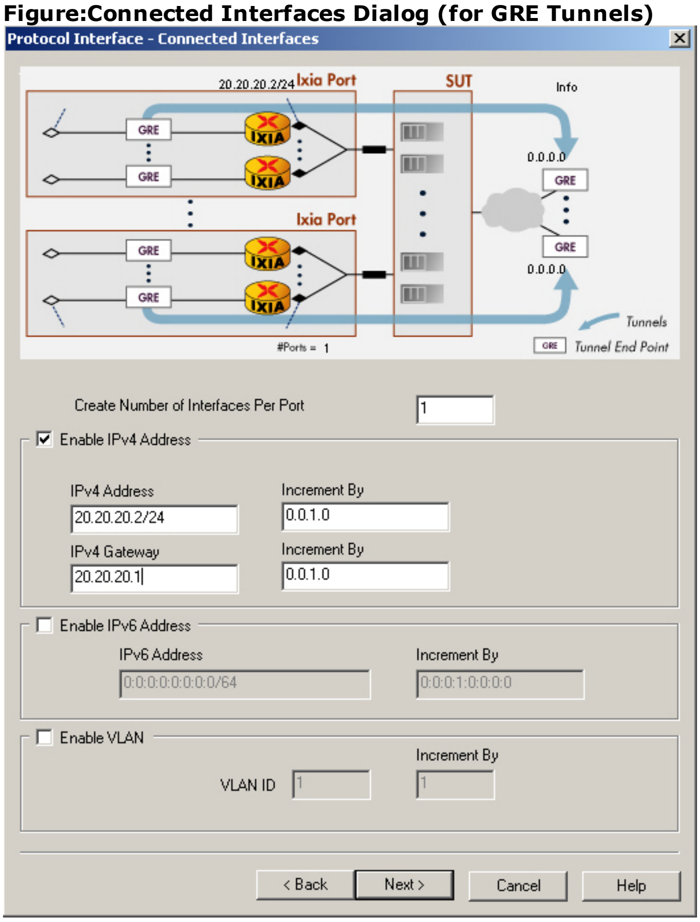
Section	Field/Control	Description
Select what kind of interfaces to create	Connected Interfaces	See *Table:Start Dialog (for Connected Interfaces)*.
	Unconnected Interfaces (via Connected Interfaces)	See *Table:Start Dialog (for Connected Interfaces)*.
	GRE Tunnels (via Connected Interfaces)	Select this option to create one or more Ixia-emulated 'GRE Tunnels.' Each GRE tunnel is emulated over the directly-connected physical link between an Ixia port and a DUT/SUT port and beyond (to the GRE tunnel destination end point). Each GRE Tunnel must be associated with a Connected Interface—to be used as the Source IP address, for the local end of the

Section	Field/Control	Description
		tunnel.

Protocol Interface Wizard—Connected Interfaces Dialog (for GRE Tunnels)

The Protocol Interface Wizard—Connected Interfaces dialog for GRE Tunnels is shown in *Figure:Connected Interfaces Dialog (for GRE Tunnels)*.

Figure:Connected Interfaces Dialog (for GRE Tunnels)



The fields and controls in this dialog are described in *Table:Connected Interfaces Dialog (for GRE Tunnels)*.

Table:Connected Interfaces Dialog (for GRE Tunnels)

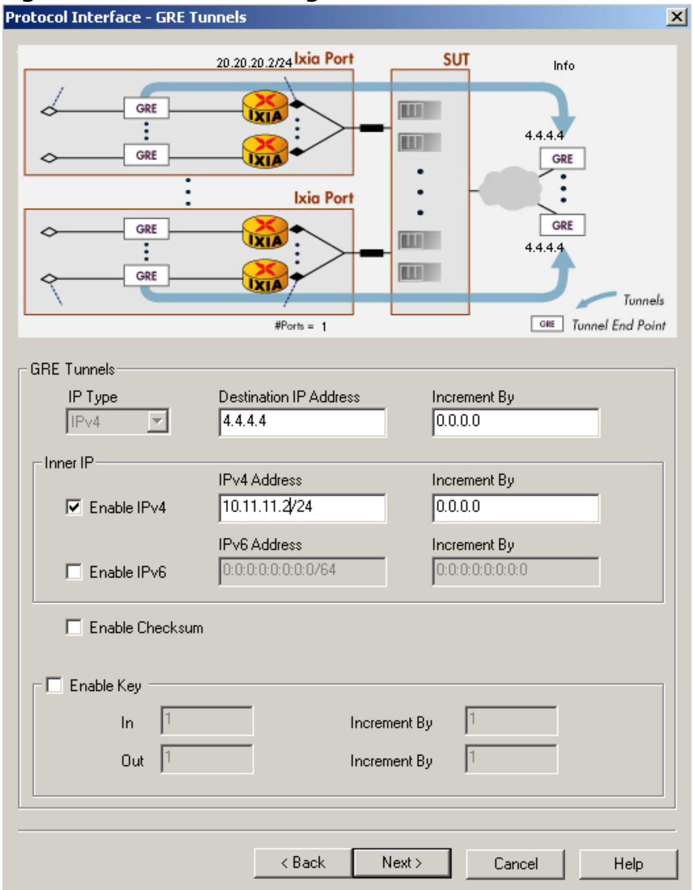
Section	Field/Control	Description
Header	Create number of interfaces per port	Enter the number of **connected** interfaces to be added to the current port. The default is 1 interface. NOTE: The number of protocol interfaces that can be added depends on the amount of memory available.
Enable IPv4	Enable IPv4 Address	If selected, one or more IPv4 interface

Section	Field/Control	Description
Address		address(es) can be configured for this port.
	IPv4 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv4 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	IPv4 Gateway	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment GW By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable IPv6 Address	Enable IPv6 Address	If selected, one or more IPv6 interface address(es) can be configured for this port.
	IPv6 Address	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment IPv6 By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable VLAN	Enable VLAN	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	VLAN ID	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
	Increment By	See *Table:Connected Interfaces Dialog (for Connected Interfaces)*.

Protocol Interface Wizard—GRE Tunnels Dialog

The Protocol Interface Wizard—GRE Tunnels dialog is shown in *Figure:GRE Tunnels Dialog*.

Figure:GRE Tunnels Dialog



The fields and controls in this dialog are described in *Table:GRE Tunnels Dialog*.

Table:GRE Tunnels Dialog

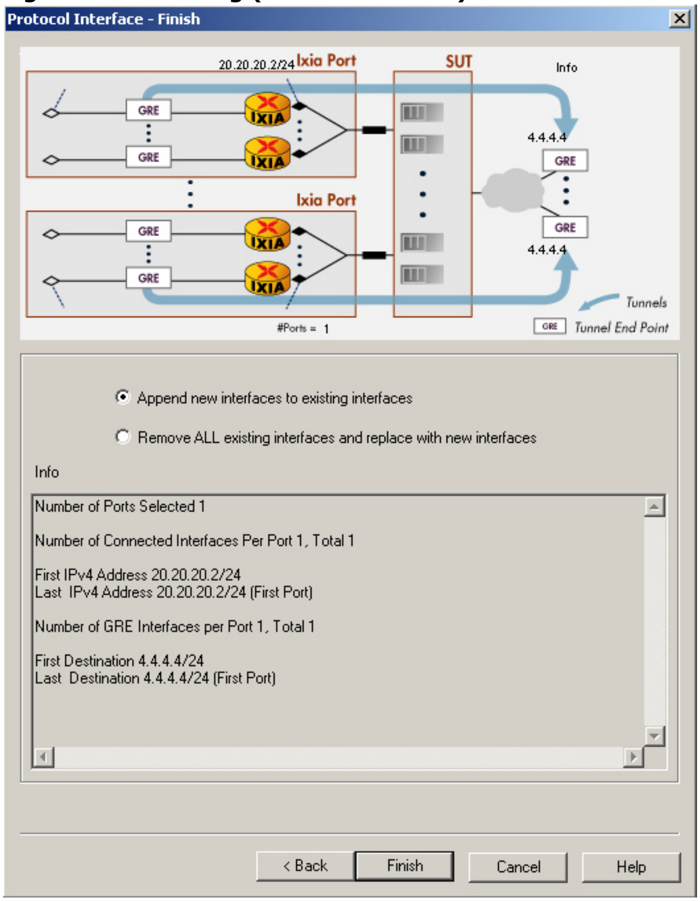
Section	Field/Control	Description
GRE Tunnels	IP Type	The type of IP address used in the Delivery Header of the GRE-encapsulated packet. Choose one of: • IPv4 • IPv6
	Destination IP Address	The IP address of the first GRE tunnel destination—part of the GRE Delivery Header.
	Increment By	If more than one Destination IP Address will be used, this is the amount that will be added to create each additional destination address.
Inner IP		The following fields are used to configure the destination IP (IP DA) addresses for the GRE-encapsulated payload IP packet.
	Enable IPv4	If selected, the payload IP packet will be assigned an IPv4 destination address.
	IPv4 Address	The IPv4 destination address for the first payload IP packet.
	Increment By	If more than one payload IPv4 address will be

Section	Field/Control	Description
		used, then this is the value that will be added to create each additional destination address.
	Enable IPv6	If selected, the payload IP packet will be assigned an IPv6 destination address.
	IPv6 Address	The IPv6 destination address for the first payload IP packet.
	Increment By	If more than one payload IPv6 address will be used, this is the value that will be added to create each additional destination address.
(GRE Header Fields)		The following fields are used to configure the optional information for the GRE header.
Enable Checksum		If selected, the optional Checksum will be added to the GRE header, per RFC 2890.
Enable Key		If selected, the optional authentication key feature will be added to the GRE header, per RFC 2890.
	In	A user-assigned integer value for the optional GRE header authentication key that will be expected in packets received through the first GRE tunnel that is created. This is the value that the receiving router will be expecting in the GRE packets being received through the tunnel. All packets arriving through a specific tunnel should contain the same key value (one key per GRE tunnel).
	Increment By	If more than one GRE tunnel will be used, this is the amount that will be added to create each additional authentication key value to look for in received GRE packets (one key per GRE tunnel).
	Out	A user-assigned integer value for the optional GRE header authentication key to be placed in packets for the first GRE tunnel that is created. This is the value that the sending router will be placed in the GRE packets being sent through the tunnel. All packets sent through a specific tunnel should contain the same key value (one key per GRE tunnel).
	Increment By	If more than one GRE tunnel will be used, this is the amount that will be added to create each additional authentication key value to be sent in the GRE packets (one key per GRE tunnel).

Protocol Interface Wizard—Finish Dialog (for GRE Tunnels)

The dialog for completing the configuration process for GRE Tunnel protocol interfaces is shown in *Figure:Finish Dialog (for GRE Tunnels)*. This dialog displays the configuration information in the 'Info' window, and allows to choose the way that interfaces will be applied to the ports. The diagram at the top of the dialog displays the configuration values that you have entered into the fields of the previous dialog.

Figure:Finish Dialog (for GRE Tunnels)



The fields and controls in this dialog are described in *Table:Finish Dialog (for GRE Tunnels)*.

Table:Finish Dialog (for GRE Tunnels)

Section	Field/Control	Description
Header	Append New Interfaces to existing interfaces	See *Table:Finish Dialog (for Connected Interfaces)*.
	Remove ALL existing Interfaces and replace with new interfaces	See *Table:Finish Dialog (for Connected Interfaces)*.
Info		This section of the dialog contains the current information regarding the newly created protocol interfaces, including: • Number of Ports Selected (Total)

Section	Field/Control	Description
		• Number of Connected Interfaces Per Port, and the Total number of connected interfaces • First and Last IPv4 Addresses of the range of IPv4 Addresses for connected interfaces—for each port (if configured for IPv4) • First and Last IPv6 Addresses of the range of IPv6 Addresses for connected interfaces—for each port (if configured for IPv6) • Number of GRE Interfaces per Connected Interface, and the Total number of GRE Tunnels • First and Last IPv4 Addresses of the range of IPv4 Addresses for GRE Tunnel Destinations—for each port (if configured for IPv4) • First and Last IPv6 Addresses of the range of IPv6 Addresses for GRE Tunnel Destinations—for each port (if configured for IPv6)

Protocol Interface Wizard–FCoE and NPIV

NOTE The FCoE / NPIV wizard is available ONLY for modules that support Fibre Channel over Ethernet.
Refer to the *Ixia Platform Reference Manual* for information on modules that support this feature.

The GUI screens in the Protocol Interface Wizard for NPIV through FCoE, and their use, are described in the following sections:

- *Protocol Interface Wizard–Start Dialog (for FCoE and NPIV)*
- *Protocol Interface Wizard–Connected Interfaces Dialog (for FCoE/NPIV)*
- *Protocol Interface Wizard–FCoE Dialog*
- *Protocol Interface Wizard—FIP Configuration*
- *Protocol Interface Wizard–NPIV Dialog*
- *Protocol Interface Wizard–Finish Dialog (for FCoE/NPIV)*

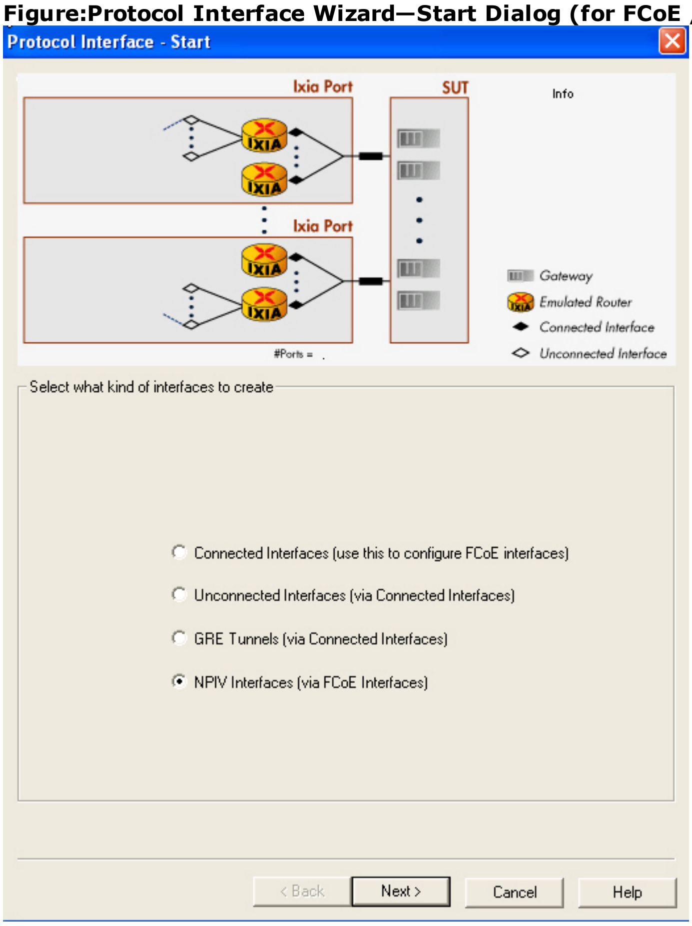
NOTE Protocol interfaces should not be created in the same subnet as the IxRemoteIP (the IxRemoteIP subnet default is 10.0.0.0). Creating protocol interfaces in this subnet will cause problems and odd behavior.

Chassis Properties—IxRemoteIp for more information on the IxRemoteIP, and how to change the default subnet.

Protocol Interface Wizard–Start Dialog (for FCoE and NPIV)

The Protocol Interface Wizard - Start dialog is shown in *Figure:Protocol Interface Wizard—Start Dialog (for FCoE / NPIV)*.

Figure:Protocol Interface Wizard—Start Dialog (for FCoE / NPIV)



The fields and controls in this dialog are described in *Table:Protocol Interface Wizard—Start Dialog (for GRE Tunnels)*.

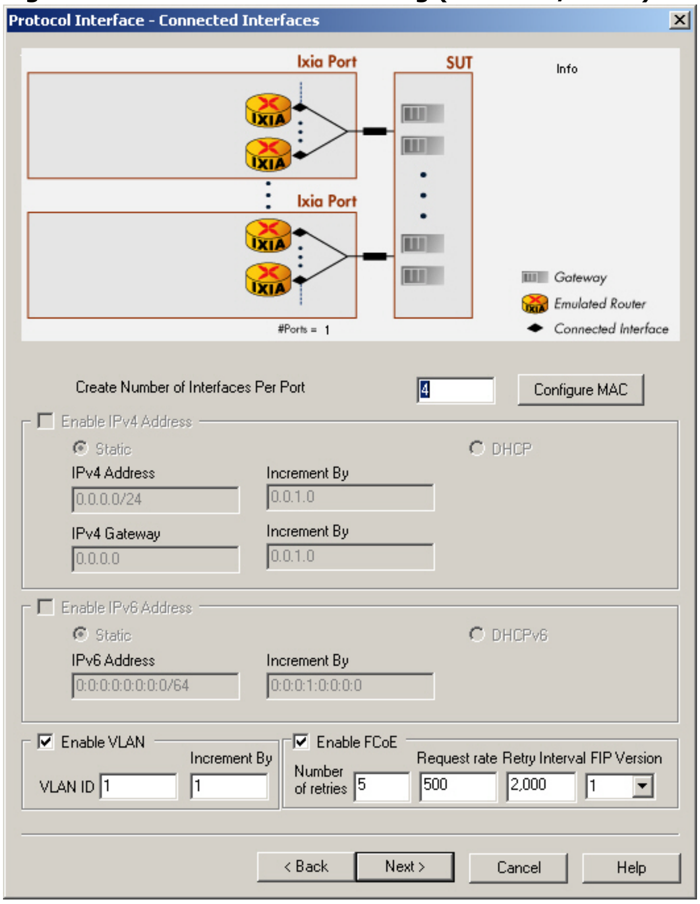
Table:Start Dialog (for NPIV/FCoE)

Section	Field/Control	Description
Select what kind of interfaces to create	Connected Interfaces	Select this option to create one or more FCoE 'Connected Interfaces'— Ixia-emulated protocol interfaces that are on the directly-connected physical link between an Ixia port and a DUT/SUT port.
	Unconnected Inter-faces (via Connected Interfaces)	See *Table:Start Dialog (for Connected Inter-faces)*.
	GRE Tunnels (via Con-nected Interfaces)	See *Table:Start Dialog (for Connected Inter-faces)*.
	NPIV Interfaces (via FCoE Interfaces)	Select this option to create one or more NPIV interfaces on each of one or more FCoE interfaces.

Protocol Interface Wizard–Connected Interfaces Dialog (for FCoE/NPIV)

The Protocol Interface Wizard - Connected Interfaces dialog for FCoE or NPIV interfaces (through FCoE) is shown in *Figure:Connected Interfaces Dialog (for FCoE / NPIV)*.

Figure:Connected Interfaces Dialog (for FCoE / NPIV)



The fields and controls in this dialog are described in *Table:Connected Interfaces Dialog (for NPIV/FCoE)*.

Table:Connected Interfaces Dialog (for NPIV/FCoE)

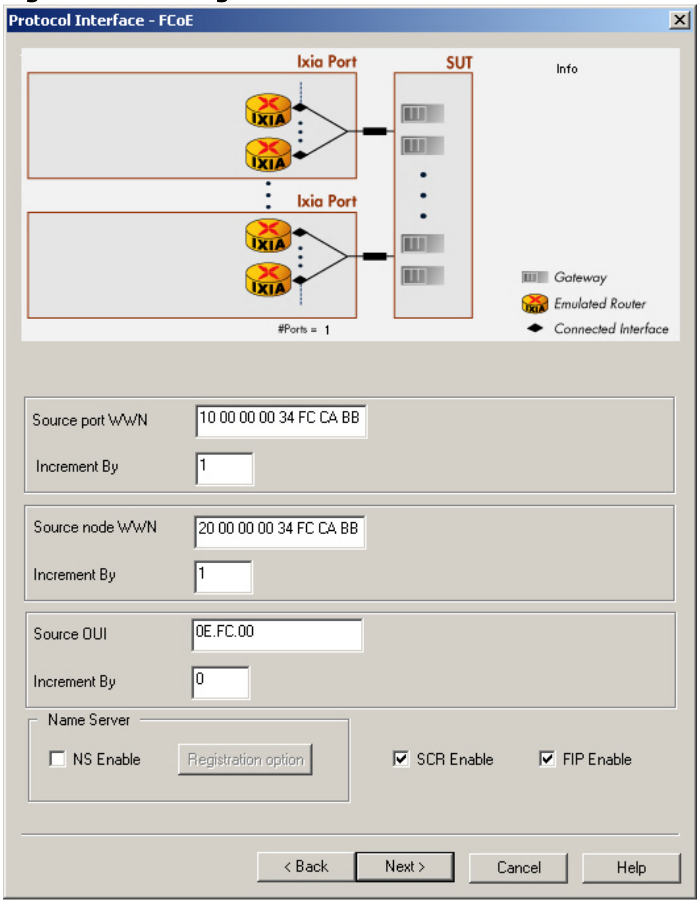
Section	Field/Control	Description
Header	Create number of interfaces per port	Enter the number of **NPIV** interfaces to be added to the current port. The default is 1 interface. NOTE The number of protocol interfaces that can be added depends on the amount of memory available.
Enable IPv4 Address	IPv4 Address Increment IPv4 By IPv4 Gateway Increment GW By	Grayed-out (not available). For definition, see *Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable IPv6	IPv6 Address	Grayed-out (not available). For definition, see

Section	Field/Control	Description
Address	Increment IPv6 By	*Table:Connected Interfaces Dialog (for Connected Interfaces)*.
Enable VLAN		If selected, a VLAN can be assigned for each of the interfaces being created in this dialog.
	VLAN ID	(integer) The identifier value for the VLAN.
	Increment By	(integer) The value of the increment step to be used in creating the range of VLAN IDs for the interfaces created in this dialog.
Enable FCoE		If selected, FCoE will be enabled for each of the interfaces being created in this dialog.
	Number of Retries	FCoE number of retries before being marked as Failure. (default = 5)
	Request Rate	FCoE maximum rate (packets/second). (default = 500)
	Retry Interval	Interval between retries, when a packet is sent and no response received. Enter a value. Default = 2000 (milliseconds).
	FIP Version	0, 1, or Auto (default = 1). Auto = it will detect the version.

Protocol Interface Wizard–FCoE Dialog

The Protocol Interface Wizard - FCoE dialog is shown in *Figure:FCoE Dialog*.

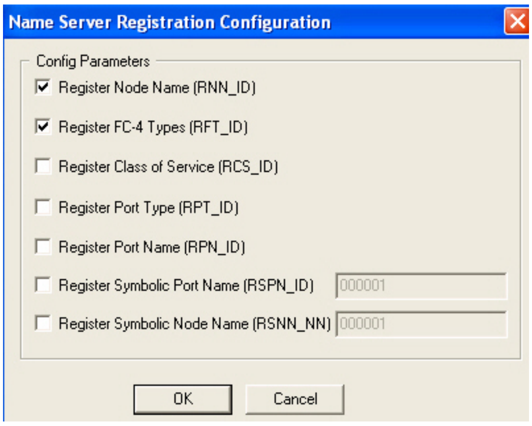
Figure:FCoE Dialog



The fields and controls in this dialog are described in *Table:FCoE Dialog*.

Table:FCoE Dialog

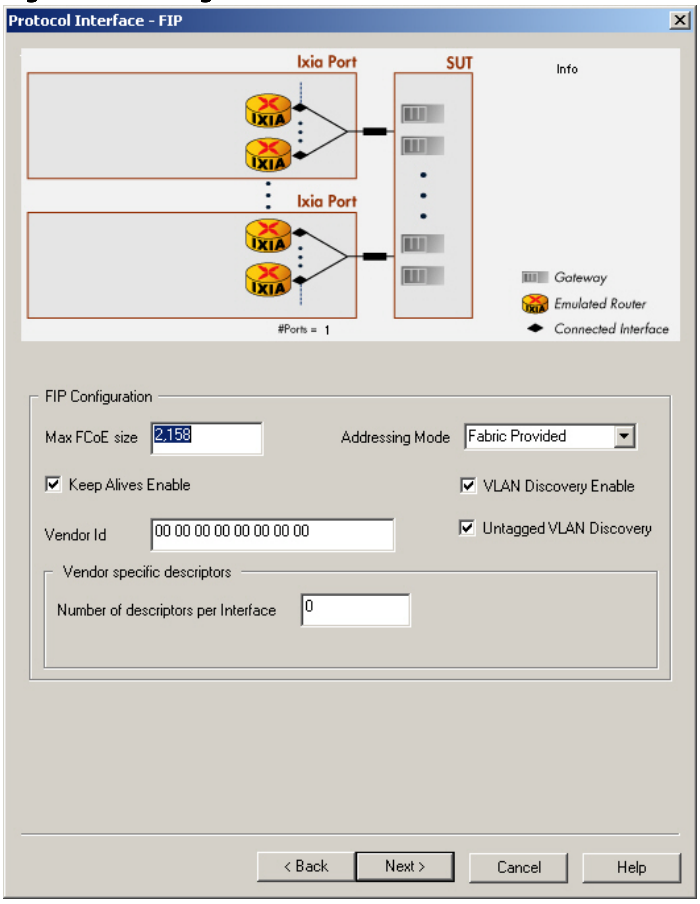
Section	Field/Control	Description
Source port WWN	Source port WWN	Source port Worldwide Name - a Name_identifier that is worldwide unique, represented by a 64-bit value
	Increment By	If more than one Source port WWN will be used, this is the amount that will be added to create each additional value to be sent in the FCoE packets.
Source node WWN	Source node WWN	Source node Worldwide Name - a Name_identifier that is worldwide unique, represented by a 64-bit value
	Increment By	If more than one Source node WWN will be used, this is the amount that will be added to create each additional value to be sent in the FCoE packets.
Source OUI	Source OUI	Use to configure the source Organization Unique Identifier. (*default = 0e.fc.00*)
	Increment By	If more than one Source OUI will be used, this is the amount that will be added to create each additional value to be sent in the FCoE

Section	Field/Control	Description
		packets. (*default* = *0*)
Name Server	NS Enable	Enables registration to Name Server
	Registration option	Click to open NS Registration Configuration page (shown here).
		
SCR Enable		If enabled, the ENode will register for any changes with the Fabric by sending a State Change Registration packet.
FIP Enable		Enables FIP (FCoE Initialization Protocol) If enabled, the interface will use FIP for its initialization. Otherwise, it will use Cisco adhoc standard.

Protocol Interface Wizard—FIP Configuration

If FIP is enabled in the FCoE dialog, the FIP dialog will display next. The Protocol Interface Wizard - FIP dialog is shown in *Figure:FIP Dialog*.

Figure:FIP Dialog



The fields and controls in this dialog are described in *Table:FIP Dialog*.

Table:FIP Dialog

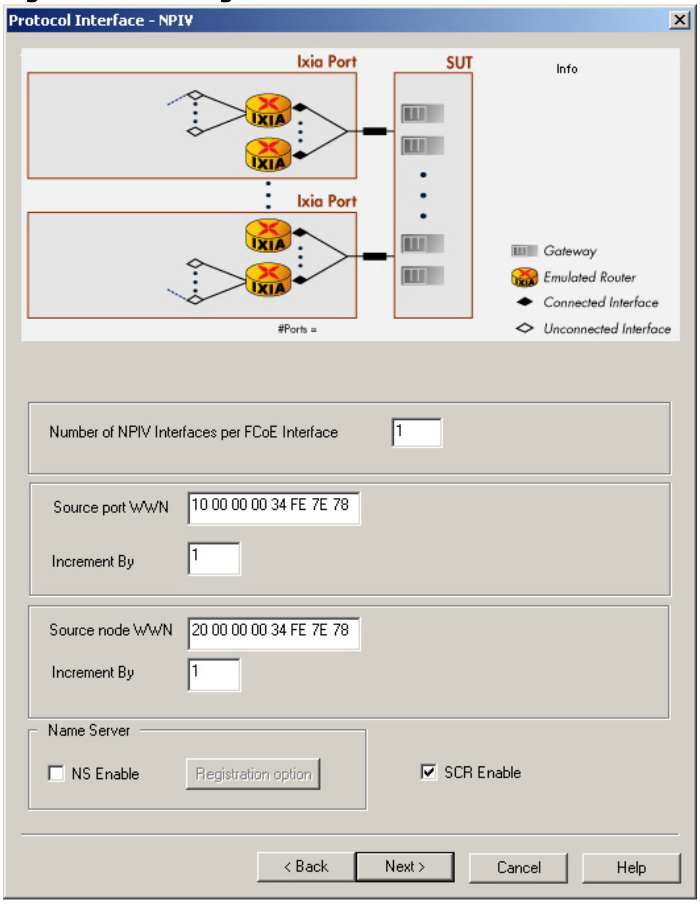
Section	Field/Control	Description
FIP Configuration	Max FCoE size	Enter the maximum FCoE size (default - 2,158)
	Addressing Mode	Specifies the addressing mode to be used by the FLOGI requests. Select from pulldown: Fabric Provided Server Provided Both
	Keep Alives Enable	If enabled, ENode will send periodic keep alives.
	VLAN Discovery Enable	If selected, specifies that VLAN Discovery is to be performed.
	Untagged VLAN Discovery	If VLAN Enable is selected, this check box becomes accessible (and is selected by default). Enables untagged FIP VLAN discovery. If this option is cleared, the VLAN discovery packet is tagged with whatever VLAN the user configures.
	Vendor ID	This value is used in the vendor specific descriptor (default = all zeroes)
Vendor specific	Number of	When enabled, this number of descriptors will be

Section	Field/Control	Description
descriptors	descriptors per interface	part of every FIP message.

Protocol Interface Wizard–NPIV Dialog

The Protocol Interface Wizard - NPIV dialog is shown in *Figure:NPIV Dialog*.

Figure:NPIV Dialog



The fields and controls in this dialog are described in *Table:NPIV Dialog*.

Table:NPIV Dialog

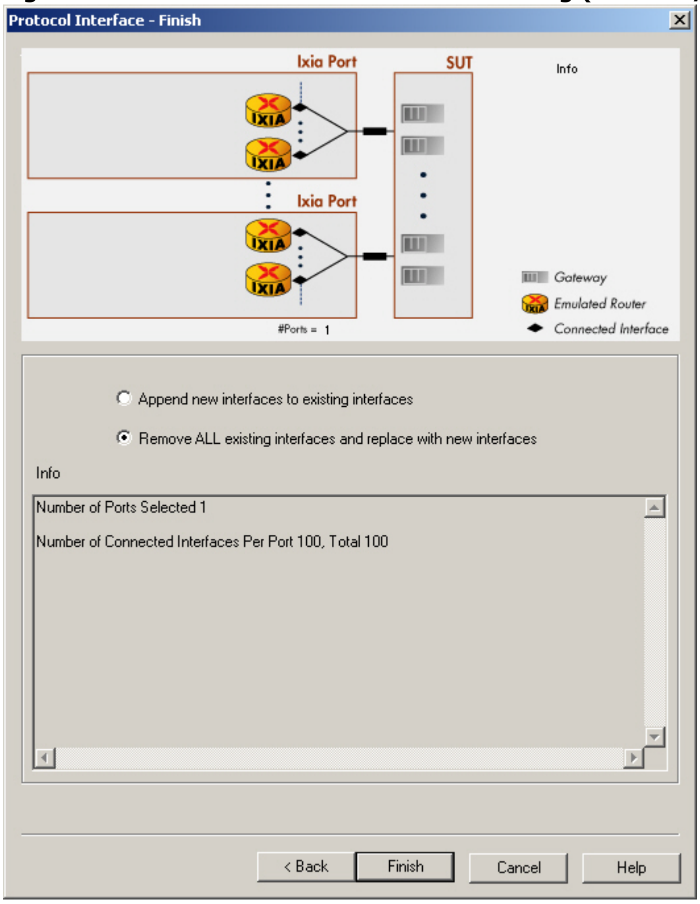
Section	Field/Control	Description
Number of NPIV Interfaces per FCoE Interface		Number of NPIV interfaces to be created per FCoE interface. Max. 256.
Source port WWN	Source port WWN	Source port Worldwide Name - a Name_identifier that is worldwide unique, represented by a 64-bit value
	Increment By	If more than one Source port WWN will be used, this is the amount that will be added to create each additional value to be sent in the NPIV packets.
Source node WWN	Source node WWN	Source node Worldwide Name - a Name_identifier that is worldwide unique, represented by a

Section	Field/Control	Description
		64-bit value
	Increment By	If more than one Source node WWN will be used, this is the amount that will be added to create each additional value to be sent in the NPIV packets.
NS Enable		Enables registration to Name Server
	Registration option	Click to open NS Registration Configuration page (shown in *Table:FCoE Dialog*).
SCR Enable		If enabled, the ENode will register for any changes with the Fabric by sending a State Change Registration packet.

Protocol Interface Wizard–Finish Dialog (for FCoE/NPIV)

The dialog for completing the configuration process for NPIV/FCoE protocol interfaces is shown in *Figure:Protocol Interface Wizard—Finish Dialog (for FCoE/NPIV)*. This dialog displays the configuration information in the 'Info' window, and allows to choose the way that interfaces will be applied to the ports. The diagram at the top of the dialog displays the configuration values that you have entered into the fields of the previous dialog.

Figure:Protocol Interface Wizard—Finish Dialog (for FCoE/NPIV)



The fields and controls in this dialog are described in *Table:Finish Dialog (for NPIV/FCoE)*.

Table:Finish Dialog (for NPIV/FCoE)

Section	Field/Control	Description
Header	Append New Interfaces to existing interfaces	See *Table:Finish Dialog (for Connected Interfaces)*.
	Remove ALL existing Interfaces and replace with new interfaces	See *Table:Finish Dialog (for Connected Interfaces)*.
Info		This section of the dialog contains the current information regarding the newly created protocol interfaces, including: • Number of Ports Selected (Total) • Number of Connected Interfaces Per Port, and the Total number of connected interfaces

Chapter 11 - Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) window controls the manner in which ARP requests are sent from the port. This option is only available on Ethernet-based cards. The resulting responses from ARP requests are held in the ARP Table, which is used to set MAC addresses for transmitted data. ARP'ing the Device Under Test (DUT) allows tests and generated frames to be configured with a specific IP address, which at run time is associated with the MAC address of that particular DUT.

NOTE ARP/Ping is not supported on XDM10G32S load module in IxRouter window through IxExplorer.

This chapter includes information on the use of the ARP window and the IP window, in the following sections:

- *ARP Window*
- *IP Window*

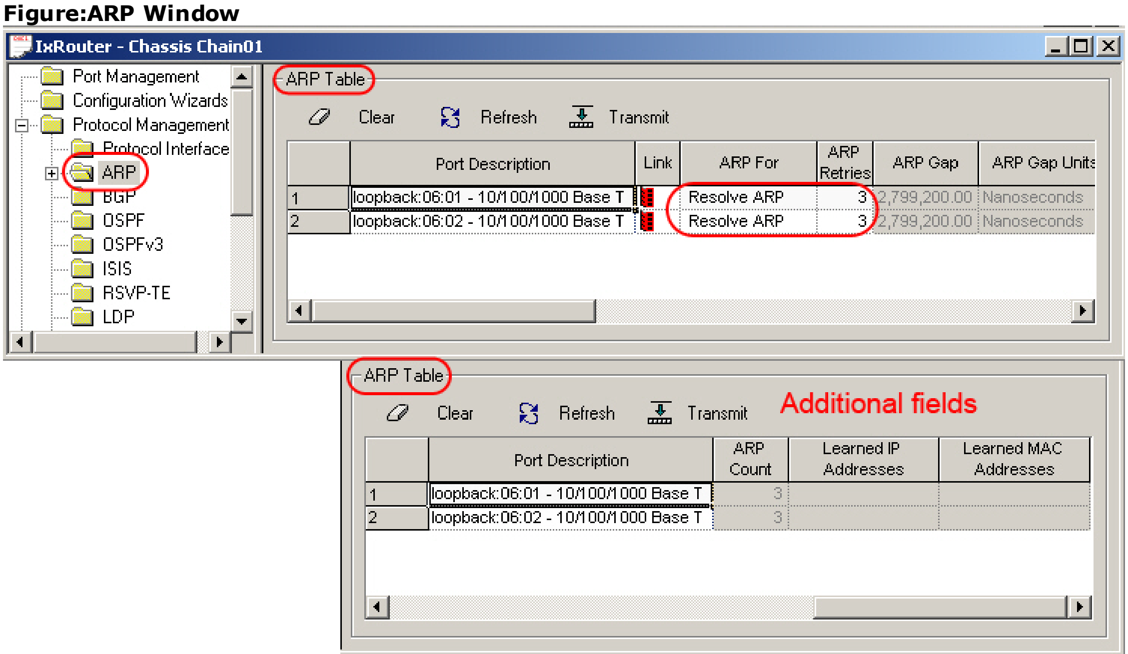
ARP Window

NOTE For information on the IP Window, go to *IP Window*.

ARP requests are generated from this window, from the main IxExplorer window, or when a Destination Address type of 'ARP Table' is used in the Frame Data dialog. Entries in the ARP table are not aged; they are always considered valid. The ARP window is shown in *Figure:ARP Window*.

NOTE On per-port Linux CPU-based cards with the ARP mode set to 'Resolve ARP' (only), the 'Send ARP' command from a client will result in the transmission of an ARP request ONLY if the ARP table does not have an updated entry.

Figure:ARP Window



The ARP table holds the local addresses used, as well as the learned addresses from the Gateway/DUT port on the link. The learned entries are automatically added to the table following discovery. The fields and controls in this window are shown in *Table:ARP Window*.

Table:ARP Window

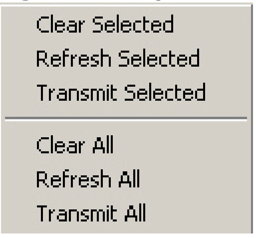
Field/Control	Description
	Press this button to clear the learned information for the selected ARP entries.
	Press this button to refresh the selected ARP entries with values from the Ixia server software, without sending any new ARP requests.
	Press this button to transmit ARP requests for the selected entries.
Port Description	The name/number of the local port and the port type.
Link	The color of this icon indicates the state of the link for this port: • **Green**—Link is up. • **Red**—Link is down. • **Yellow—**Link is in loopback mode. • **Gray—**Link is unavailable because it is busy or it is an unsupported link type.
ARP For:	Transmit ARP request for one of the following: • **Resolve ARP**—(get MAC address) a single ARP request is sent to each Gateway IP address, using the first IP address found in the IP table entry for the port as the source address. The result of the ARP request is saved in the ARP table. • **Learn ARP**—(for learning) sends ARP requests using all of the addresses found in the IP Address Table for this port as source addresses. The Ixia hardware does not listen for or record the responses. This is used to allow switches to learn the addresses of the Ixia-simulated devices that they will be seeing during the test. • **Both (Resolve + Learn)—**performs both of the operations (Resolve/get MAC Address + Learning).
ARP Retries	(Used for Resolve and Resolve + Learn requests) When transmitted ARP requests do not yield a result, this is the number of retries to execute before giving up. Used only with the 'First' and 'Both' options.
ARP Gap	(Used for Learn and Resolve + Learn requests) (Used **with** the ARP Gap Unit) A value that is the length of the gap inserted between the ARP packets when ARP Requests are sent for multiple addresses.
ARP Gap Units:	(Used **with** the ARP Gap value)

Field/Control	Description
• Nanoseconds • Microseconds • Milliseconds • Seconds • Clock Ticks	The gap units available are: • Nanoseconds • Microseconds • Milliseconds • Seconds • Clock ticks—this is dependent on the load module used. It is the minimum packet gap found in *Ixia Platform Reference Manual*.
ARP Count	(Used for Learn and Resolve + Learn requests) Each ARP request is repeated this number of times, with gaps between the requests.
Learned IP Addresses	For each row entry, the IP address learned from the Gateway/DUT port on the link.
Learned MAC Addresses	For each row entry, the MAC address learned from the Gateway/DUT port on the link.

ARP Options Pop-Up Menu

The ARP options pop-up menu is shown in *Figure:ARP Options Pop-Up Menu*.

Figure:ARP Options Pop-Up Menu



The options in this menu are described in *Table:ARP Options Pop-Up Menu*.

Table:ARP Options Pop-Up Menu

Menu Options	Description
Clear Selected	Clear the learned information for the selected entries.
Refresh Selected	Refresh the learned information for the selected entries with values from the Ixia server software, without sending any new ARP requests.
Transmit Selected	Transmit ARP requests for the selected entries.
Clear All	Clear the learned information for ALL entries.
Refresh All	Refresh the learned information for ALL entries with values from the Ixia server software, without sending any new ARP requests.
Transmit All	Transmit ARP requests for ALL entries.

IP Window

The IP Table window allows IPv4 addresses to be assigned on a per-port basis. This window differs from the Protocol Interfaces window since the IP Table allows to create a very large range of IPv4 addresses, while the Protocol Interface table allows only one IPv4 address per interface. But, the IP Table addresses do not support routing protocol configuration in IxExplorer. This table is used if you want ARP and PING responses, or ARP learning frames, for a very large range of addresses.

In most cases, you should be using the Protocol Interfaces window. See *Protocol Interfaces* for additional information.

The correspondence between source IP addresses and MAC addresses (for Ethernet ports only) can be specified, and the Gateway IP address is also specified here. The IP Table for POS cards is similar except for the omission of the Mapping Option and MAC Address columns. IP addresses may be exclicked as individual addresses or as a range of addresses.

All ARP requests (for Ethernet) are sent to the Gateway address. In most cases, the default Gateway Address is the address of the DUT. When a gateway separates the Ixia port from the DUT, the IP address of that gateway is used as the default.

The IP Table window, shown in *Figure:IP Table Window*, consists of a header and a grid with fields that control IP to MAC address and Gateway correspondence information. In this example, three IPv4 addresses have been added to the first port and are shown with the automatically-generated default addresses. (See *IP Table–Default IP Addressing Method* for additional information.)

NOTE

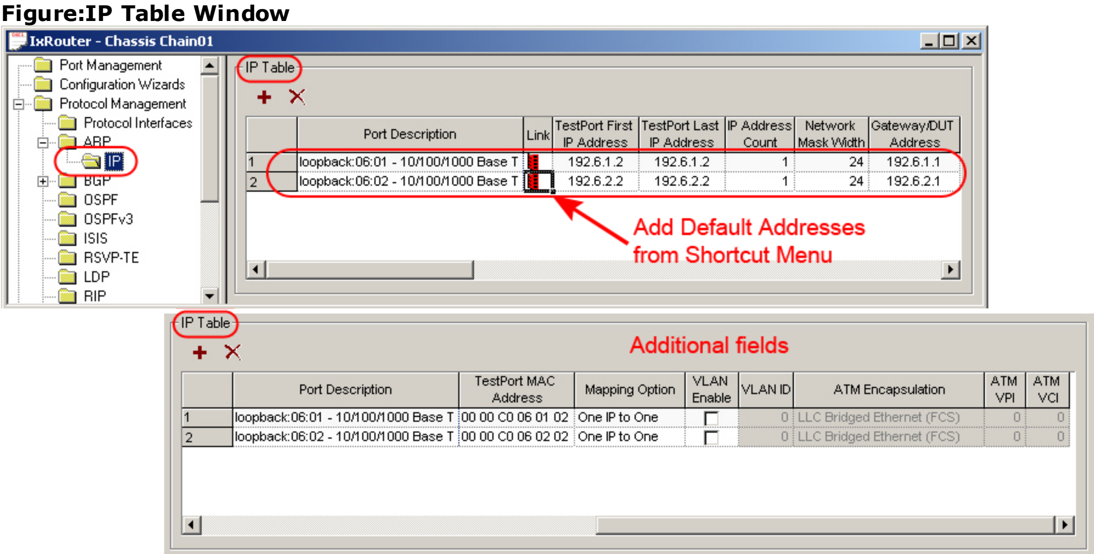
Port identifiers are displayed in the Protocol Window using the following format:

Chassis Name: Card Number: Port Number

Example:

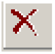
Your Chassis:01:01

Figure:IP Table Window



The fields and controls for the IP Table window are described in *Table:IP Table Window*. For information on the Shortcut Menu,See *IP Table Shortcut Menu*. The values in the fields may be added or edited manually. Press ‘F2’ to insert the cursor in the field.

Table:IP Table Window

Field/Control	Description
	Press this button to add an IPv4 address to the IP table for the selected port.
	Press this button to delete selected IP address(es) from the IP table for the selected port.
Port Description	The name/number of the port, and port type.
Link	The color of this icon indicates the state of the link for this port: • **Green**—Link is up. • **Red**—Link is down. • **Yellow**—Link is in loopback mode. • **Gray**—Link is unavailable because it is busy or it is an unsupported link type.
TestPort First IP Address	Sets the starting IP address of an IP address range for the Ixia Test Port. *IP Table–Default IP Addressing Method* for information on default addresses.
TestPort Last IP Address	Sets the last IP address of an IP address range for the Test Port.
IP Address Count	Sets the number of addresses to be created for this IP address range for the Test Port.
Network Mask Width	The number of digits in the network mask, to be used to create a range of network addresses.
Gateway/DUT Address	The gateway address for the current entry. If multiple DUTs are to be tested, this should be set to the IP address of the DUT that corresponds to this address range. The default Gateway IP Address. *Gateway/DUT Address for additional information.*
TestPort MAC Address	(For Ethernet only) Sets the MAC address associated with the Ixia port IP address(es). *IP Table—Default MAC Addressing* for additional information.
Mapping Option	Choose one of the following mapping options: • **One IP to One MAC**—Sets up a one-to-one mapping of IP addresses to MAC addresses. For each of the IP addresses configured for the port, a different MAC address will be created. The rightmost octet in the initial MAC address will be incremented by ‘1’ for each additional MAC address. • **Many IPs to One MAC**—For each of the IP addresses in this range of IP addresses, the same MAC address will be used. *MAC Mapping* for additional information.

Field/Control	Description
VLAN Enable	If selected, enables the use of VLANs.
VLAN ID	
ATM Encapsulation	The type of RFC 2684 ATM multiplexing encapsulation (routing) protocol to be used. Each of these ATM encapsulation modes is described in the *Ixia Platform Reference Guide*. Choose one of: • VC Mux IPv4 Routed • VC Mux IPv6 Routed • VC Mux Bridged Ethernet/802.3 (FCS) • VC Mux Bridged Ethernet/802.3 (no FCS) • LLC Routed AAL5 Snap • LLC Bridged Ethernet (FCS) • LLC Bridged Ethernet (no FCS) NOTE See the information below regarding the general types of ATM encapsulation. • **VC Mux**—VC MUX Routed Protocol. For ATM Virtual Connection (VC) Multiplexing. Each ATM VC carries routed PDUs for only one protocol. Multiple VCs are required for multiple protocols. Helps to reduce fragmentation overhead. • **LLC Snap**— LLC/SNAP Routed Protocol. For ATM LLC Encapsulation. Each ATM VC carries routed PDUs for multiple protocols. Helps to reduce the number of separate VCs required if multiple protocols are used.
ATM VPI	Virtual Path Identifier (VPI) for the VC over which information is being transmitted.
ATM VCI	Virtual Circuit/Channel Identifier (VCI) for the VC over which information is being transmitted.

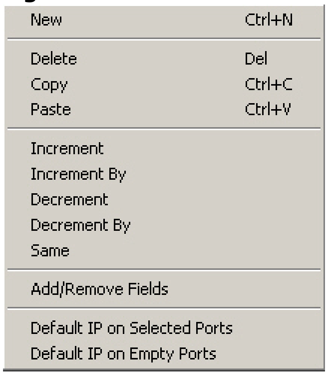
Gateway/DUT Address

Unless otherwise specified for a specific range of addresses, all ARP requests are sent to the Default Gateway IP address. In most cases, the Default Gateway Address is the address of the DUT. Where a gateway separates the Ixia port from the DUT, this should be set to the IP address of the gateway.

IP Table Shortcut Menu

Right-clicking anywhere in the IP table displays the shortcut menu shown in *Figure:IP Table Shortcut Menu*.

Figure:IP Table Shortcut Menu



The options in this menu are described in *Table:IP Table Shortcut Menu*.

Table:IP Table Shortcut Menu

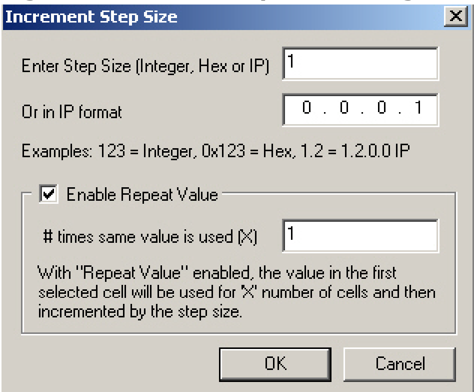
Menu Options	Description
New	Right-click a port listed in the IP Table, and select 'New' to add an IPv4 address set (one row entry) to the port.
Delete	Right-click an address set (one row entry) for a port listed in the IP Table, and select 'Delete' to delete that row entry.
Copy	Right-click a row entry, and select 'Copy' to copy the addressing information in that row to a row entry for another port. (Use with the 'Paste' option.)
Paste	Right-click a row entry, and select 'Paste' to paste the copied addressing information to the selected row entry. (Use with the 'Copy' option.)
Increment	For use when multiple, contiguous row entries in a column are selected. The top selected entry will be used as the base value. Each additional entry will be increased in value by 1 (hex, integer, or as an IP value, depending on the type).
Increment By	For use when multiple, contiguous row entries in a column are selected. Displays the IP address Step Size dialog for creating customized incrementing values in the column. *Increment Step Size Dialog* for additional information.
Decrement	For use when multiple, contiguous row entries in a column are selected. The top selected entry will be used as the base value. Each additional entry will decreased in value by 1 (hex, integer, or as an IP value, depending on the type).
Decrement By	For use when multiple, contiguous row entries in the column are selected. Displays the IP address Step Size dialog for creating customized decrementing values in the column. *Increment Step Size Dialog* for additional information.
Same	For use when multiple row entries are selected. Forces all of the selected address fields to be identical, with all values matching those in the uppermost row entry.

Menu Options	Description
Add/Remove Fields	Opens the Add/Remove Fields dialog, so the selection of field-s/column headings displayed in a view can be customized.
Default IP on Selected Ports	Applies the default IP addressing method to the selected ports. *IP Table–Default IP Addressing Method* for additional information.
Default IP on Empty Ports	Applies the default IP addressing method to all of the ports which do not yet have IP addresses assigned. *IP Table–Default IP Addressing Method* for additional information.

Increment Step Size Dialog

When the 'Increment By' or 'Decrement By' options are selected, the Increment Step Size dialog opens so you can define an increment/decrement step other than '1' (the default setting). This dialog applies only for incrementing or decrementing selected, contiguous values in a column. The Increment Step Size box is shown in *Figure:Increment Step Size Dialog*.

Figure:Increment Step Size Dialog



The fields and controls in this dialog are described in *Table:Increment Step Size Dialog*.

Table:Increment Step Size Dialog

Field/Control	Description
Enter Step Size (Integer, Hex or IP)	Enter an integer, a hex value, or an 'IP' value that will be used as the step value. Entry examples: • 123 = Integer • 0x123 = Hex • 1.2 = 1.2.0.0 IP (a decimal value that will be translated into a 4-octet IP address)
Or in IP format	Enter a 4-octet IP address that will be used as the step value.
Enable Repeat Value	With 'Repeat Value' enabled, the value in the first selected cell will be used for 'X' number of cells, and then incremented by the step size.
# times same value is	Enter the number of times that a value will be used before this

Field/Control	Description
used (X) (Repeat Value)	value will be incremented by the amount of the 'Step Size'. For example—If the initial value is 10.0.0.1, the Step Size is '0.0.0.1', and the Repeat Value is '2': • 10.10.10.1 • 10.10.10.1 • 10.10.10.2 • 10.10.10.2 • 10.10.10.3 • 10.10.10.3 • etc.

IP Table–Default IP Addressing Method

To assist in speeding up the address configuration process for large numbers of ports in the IP table, a default addressing scheme is available for use. The two types of addressing are:

- *IP Table—Default IPv4 Addressing*
- *IP Table—Default MAC Addressing*

IP Table—Default IPv4 Addressing

The default IPv4 addresses consist of a network address (first 3 bytes) plus the one-byte host portion of the address, and are based on the following rules:

- The first byte is 192 (hex value = C0).
- The second byte is based on the number of the card slot in the chassis where the port is located. For example: If the load module is located in Slot 2, then the first 2 bytes of the IP address will be: 192.2.
- The third byte is based on the number of the port in the card. For example: If the port is the first port or only port on the card, the first 3 bytes of the IP address will be: 192.2.1.
- For the fourth byte (the host portion of the address) the IP address for the DUT/Gateway port on the link is assigned the first available host address on the subnet for that link, so its address would be: 192.2.1.1.
- The IP address for the Ixia port on that link is assigned the second available host address on the subnet for that link, so its address would be: 192.2.1.2.

IP Table—Default MAC Addressing

The default Test Port MAC addresses are automatically assigned according to the following rules:

- First 2 octets are zeros (00 00).
- Third octet is C0 (decimal value = 192).
- The last 3 bytes of the MAC address copy the values last 3 bytes of the IP address, but exclicked in hexadecimal notation.

See also *MAC Mapping*.

MAC Mapping

There are two types of mapping MAC addresses to IP addresses:

- *One IP to One MAC Mapping*
- *Many IPs to One MAC Mapping*

One IP to One MAC Mapping

- One MAC Address is created for each IP address in the range, according to the formatting described above.
- The last byte of the MAC Address is incremented by '1' for each additional address.
- The number of MAC Addresses is determined by the value in the IP Address Count column.
- Example (For Port 04:01, IP Address Count = 3):

TestPort IP Address	TestPort MAC Address
192.4.1.2	00 00 C0 04 01 02
192.4.1.3	00 00 C0 04 01 03
192.4.1.4	00 00 C0 04 01 04

Many IPs to One MAC Mapping

- The same MAC Address is used for every IP address in the range.
- Example (For Port 04:01, IP Address Count = 3):

TestPort IP Address	TestPort MAC Address
192.4.1.2	00 00 C0 04 01 02
192.4.1.3	00 00 C0 04 01 02
192.4.1.4	00 00 C0 04 01 02

Chapter 12 - ICMP/PINGv4

ICMP is the Internet Control Message Protocol. The Packet InterNet Groper (PING) utility, based on ICMP, is used to test for connectivity. PING messages are ICMP messages of type *Echo Request.* Responses are ICMP message of type *Echo Response*. This chapter describes the use of the PING utility in the IxExplorer and IxRouter GUI.

ICMP/PING Overview

PINGs can be sent for both IPv4 and IPv6 addresses:

- **For IPv4**—The PING messages are IPv4 ICMP messages of type *Echo Request.* Ping Responses are IPv4 ICMP message of type *Echo Response*.
- **For IPv6**—The PING protocol is available for modules which support IPv6, using ICMPv6.

!!! 'PING' REQUIRES AN ENABLED PROTOCOL INTERFACE!!!!
1) Add an interface to the port.
2) Add an IPv4 and/or IPv6 address to the interface.
3) Enable the interface.

The PING message is sent from the PING dialog (*Ping Dialog*) which can be accessed in two locations:

- **Protocol Interfaces Window**—From the pop-up menu in the Protocol Interfaces table. *PING from Protocol Interfaces Window*.
- **Network Resources Window**—From the port level pop-up menu. The 'Send Ping...' option is available in this menu IF a protocol interface has been created and enabled for that port. *PING from Network Resources Window*.

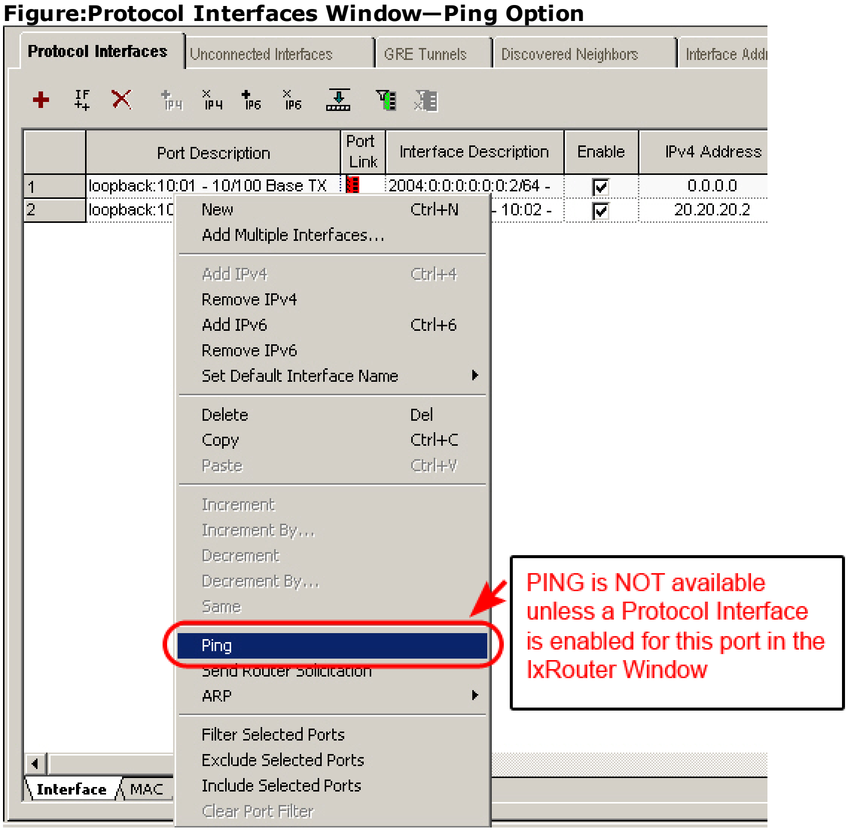
When a PING is sent to an IPv4 address, the check boxes for 'Enable PING for IPv4' and 'Enable ARP' will be enabled automatically in the Protocol Management window. To disable the PING function:

- **For IPv4**—Clear the check box for 'Enable PING for IPv4,' or disable the protocol interface.
- **For IPv6**—Disable the protocol interface.

PING from Protocol Interfaces Window

The Protocol Interfaces Window is shown in *Figure:Protocol Interfaces Window—Ping Option*. The Right-Click menu for a port is shown, with the 'Ping' option available.

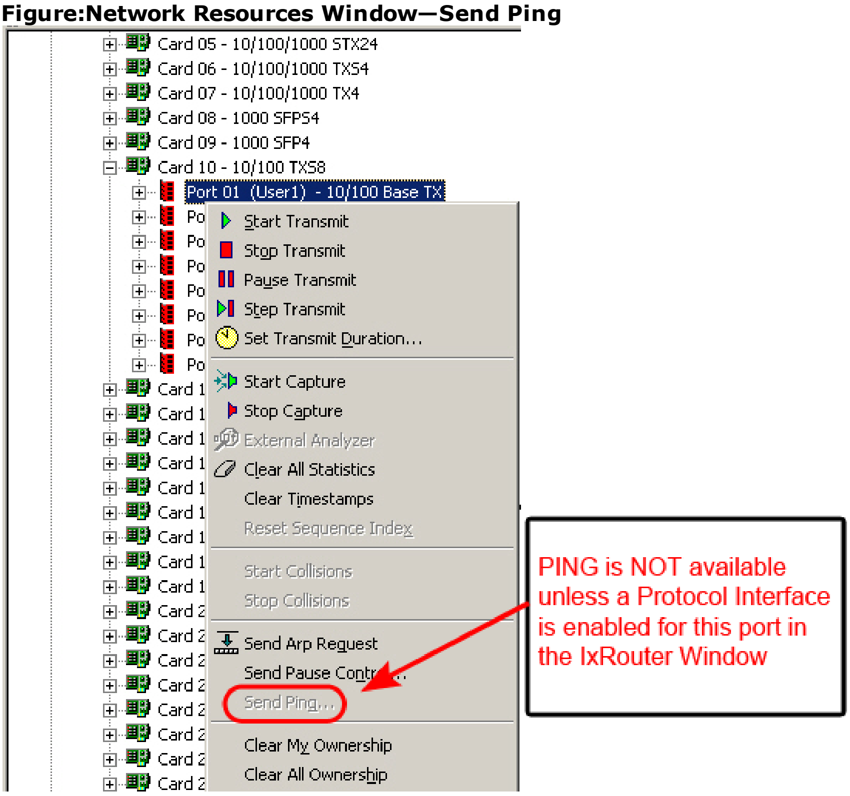
Figure:Protocol Interfaces Window—Ping Option



PING from Network Resources Window

The 'Send Ping...' option in the Network Resources window port pop-up menu is shown in *Figure:Network Resources Window—Send Ping*.

Figure:Network Resources Window—Send Ping

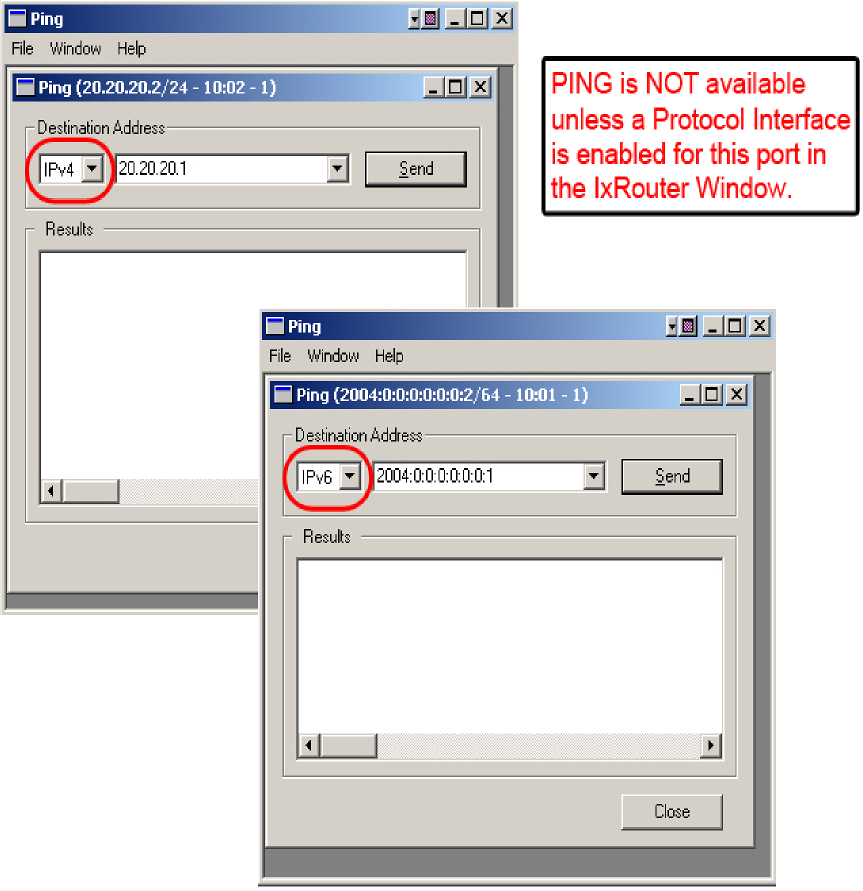


Ping Dialog

The Ping dialog, which can be accessed from the Protocol Interfaces window, or from the Network Resources port level, is shown in *Figure:Ping Dialog for IPv4 and IPv6*.

MANDATORY for Using PING:
1) In the Protocol Interfaces Window, a named Protocol Interface**MUST**first be added to the port.
2) An IPv4 and/or IPv6 address **MUST** be assigned to that interface.
3) The named interface **MUST**be enabled.

Figure:Ping Dialog for IPv4 and IPv6



The fields and controls in this dialog are described in *Table:Ping Dialog for IPv4 and IPv6*.

Table:Ping Dialog for IPv4 and IPv6

Section	Field/Control	Description
Protocol Interface	(Named Protocol Interfaces)	Select from the dropdown list of named, **enabled**, interfaces for the port.
Destination Address	(IP Version) Choose one of: • IPv4 • IPv6	The options displayed in this list depend on the type of IP addresses that have been added to the interface. **IPv4 (only)**—For an interface that has an IPv4 address only.

Section	Field/Control	Description
		IPv6 (only)—For an interface that has an IPv6 address only. (Also available for each of multiple IPv6 addresses assigned to the interface.) **IPv4 and IPv6**—For an interface that has both IPv4 and IPv6 addresses.
	(Address)	Displays the IPv4 or IPv6 address to which the Ping message will be sent. For a 32-bit IPv4 address, the format will be: x.x.x.x For a 128-bit IPv6 address, the format will be: x:x:x:x:x:x:x:x (or any of the other standard IPv6 address formats)
	Send	Press the *Send* button after the IP version and Destination address have been set.
Results		The status and results of the Ping will be displayed in the Results window.

Chapter 13 - Filter Properties

The Filters selection for a port allows for a number of settings related to capturing, filtering, and statistics. There are three tabs for the Filters, Statistics, Receive Mode dialog, described in the following sections:

Filter Properties Tab	Controls the settings for the capture trigger and filter as well as the setting of the user defined-statistics.
Statistics Tab	Controls the selection of alternative statistics to be displayed.
Receive Mode Tab	Controls the options related to data capture and latency operations.

Filter Properties Tab

The *Filter Properties* tab sets trigger and filter parameters that are used in three different areas within the Ixia system:

User Defined Statistics	Sets up the conditions for the accumulation of up to four user-definable statistics.
Capture Trigger and *Capture Filter*	Sets up the conditions under which a port will start capturing data, and a filter for the data it will retain in its capture buffer.

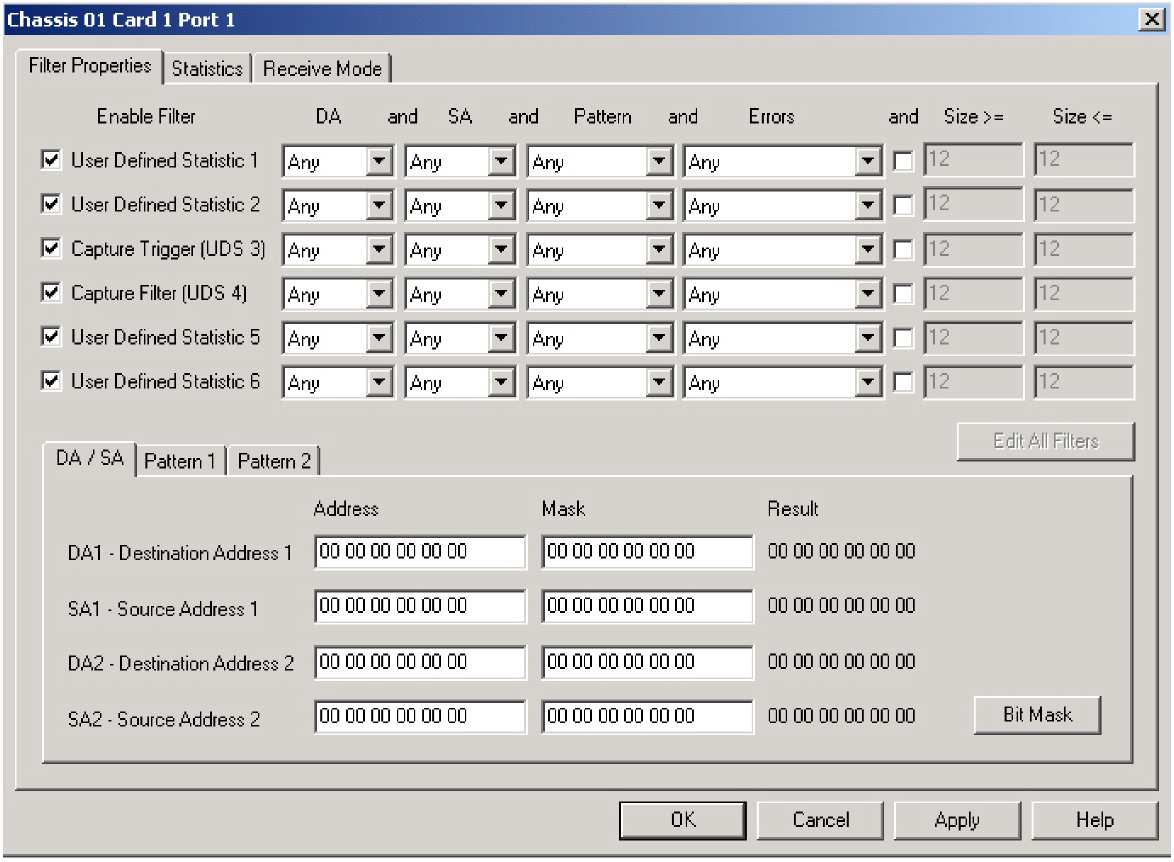
The parameters used to construct these values are based on:

- Masked MAC DA/SA addresses. MAC DA/SA addresses are not applicable to Packet over SONET modules.
- Type of packet or masked data patterns within the packet.
- Any error condition, including a good packet.
- The size of the received packet.

The *Filter Properties* tab for a 10/100 module—with the optional User-Defined Statistics 5 & 6 enabled—is shown in *Figure:Filter Properties—Overview*. The dialogs for Packet over SONET modules do not display the DA and SA columns. The dialogs for OC-48 channelized port mode display the Circuit column.

NOTE Incase user changes any parameters under Filter Properties or Receive mode, the traffic related to capture will not stop and the latency will also not be affected.

Figure:Filter Properties—Overview



The upper part of the dialog contains rows for the following major elements:

User Defined Statistics	Set the conditions that will cause the four user defined statistics to accumulate data.
Capture Trigger	Set the conditions under which capture will commence.
Capture Filter	Set the filtering conditions for captured data.

The lower part of the tab has property sheets that allow the parameters used in defining the elements above to be set:

DA/SA Values	Allows masked values for Destination and Source MAC addresses to be set for Ethernet modules.
Pattern Match Tabs	Allows either a type of packet or masked data patterns to be defined.
VCAT Circuit Filter Properties	For OC-48 channelized port mode (only). Allows filtering on circuit.

Capture Trigger

The Capture Trigger settings control the conditions that cause a port to start capturing data after a 'Start Capture' command has been given. The elements of the *Filter Properties* tab related to Capture Triggers are shown in 1. *Table:Capture Trigger Condition Fields*.

Figure:Filter Properties—Capture Trigger

In order for the Capture Trigger to take effect, the box must be selected (enabled), and all of the visible basic categories (DA, SA, Pattern, Errors, and the optional Size Range, if enabled) must be matched for the same packet at the same time. The *DA* and *SA* fields are not shown for Packet over SONET modules.

By default, the Capture Trigger is enabled for every port with the 'Any' condition set for all of the fields and with no size requirements. This will result in immediate data capture after a 'Start Capture' command has been given.

The fields and controls are described in Table:Capture Trigger Condition Fields.

Table:Capture Trigger Condition Fields

Field/Control	Choice	Description
check box		This box must be selected to activate the row and enable the remaining fields. If this box is cleared, the port will not capture any data.
DA	Any	Any destination address is matched.
	DA1/DA2	The (possibly masked) value for Destination Address 1 or 2 is matched. *DA/SA Values*
	Not DA1/DA2	Anything but the (possibly masked) value for Destination Address 1 or 2 is matched. *DA/SA Values.*
SA	Any	Any source address is matched.
	SA1/SA2	The (possibly masked) value for Source Address 1 or 2 is matched. *DA/SA Values*
	Not SA1/SA2	Anything but the (possibly masked) value for Source Address 1 or 2 is matched. *DA/SA Values*
Pattern	Any	Any data pattern is matched.
	Pattern 1/2	The (possibly masked) data pattern for Data Pattern 1 or 2 is matched. *Pattern Match Tabs*
	Not Pattern 1/2	Anything but the (possibly masked) data pattern for Data Pattern 1 or 2 is matched. *Pattern Match Tabs*
	Pattern 1& 2	The (possibly masked) values for both Patterns 1 and 2, are matched.
Error		*Table:Error Condition Filters.* This contains a description of the error conditions available, depending on type of module.
and	Check or Unselected	Enable this box if the condition should depend on the size range of the received

Field/Control	Choice	Description
		packet.
Size >=	Decimal number	The minimum packet size to match.
Size <=	Decimal number	The maximum packet size to match.

Error Condition Filters

Several error condition filters are available depending on the module as listed in .

Table:Error Condition Filters

Error Filter	Description
Any	Any good or bad packet.
Good Packet	A good packet is matched.
Bad CRC	A packet with a bad CRC.
Bad Packet	A frame with one or more of the following defects: • Bad CRC • Alignment Error - Ethernet only • Dribble Error - Ethernet only • Fragment - Ethernet only • Undersize - Ethernet only, less than 64 • Oversize - Ethernet only, if frame greater than 1588 (non-VLAN), or greater than 1522 (VLAN)
IPv4/TCP/UDP Checksum Error	Any IPv4, TCP, or UDP checksum error.
Alignment	A packet with an extra nibble, with bad CRC.
Dribble	A packet with an extra nibble, but with good CRC.
Bad CRC/Alignment/Dribble	Any packet with this combination of errors.
Line Error	A packet received with symbol errors with either a good or bad CRC.
Line Error & Bad CRC	A packet received with symbol errors and with a bad CRC.
Line Error & Good CRC	A packet received with symbol errors and with a good CRC.
Data Integrity Error	A packet received with a data integrity error. The *Data Integrity* check box must first be selected in the *Receive Mode* tab for this selection to become available. *Data Integrity* for additional information.
Any Sequence Error	A packet received with any type of sequence error: Small, Big, or Reverse error. The *Advanced Sequence Checking* option must first be enabled in the *Receive Mode* tab for this selection to become available. *Advanced Sequence Checking* for additional information.
Small Sequence Error	A packet received with a small sequence error—which is when the current sequence number minus the previous

Error Filter	Description
	sequence number is less than or equal to the error threshold (set by software) and not negative, **OR** when the current sequence number is equal to the previous sequence number. The *Advanced Sequence Checking* option must first be enabled in the *Receive Mode* tab for this selection to become available. *Advanced Sequence Checking* for additional information.
Big Sequence Error	A packet received with a big sequence error—which is when the current sequence number minus the previous sequence number is greater than the error threshold (set by software) and not negative. The *Advanced Sequence Checking* option must first be enabled in the *Receive Mode* tab for this selection to become available. *Advanced Sequence Checking* for additional information.
Reverse Sequence Error	When the current sequence number is less than the previous sequence number. *Table:Advanced Sequence Checking Error Conditions* for a full definition of Reverse Sequence Error. *Advanced Sequence Checking* option must first be enabled in the *Receive Mode* tab for this selection to become available.
For Cisco CDL only	
CDL Error	A packet received with a CDL checksum error.
For GFP only	
GFP Error	A packet received with a GFP checksum error.
For FCoE only	
Invalid FCoE Frame	A packet received with an invalid FCoE frame.

Capture Filter

The Capture Filter settings control which data is captured after a Start Capture command has been given and after the *Capture Trigger* *has been satisfied. The DA and SA fields are not shown for Packet over SONET (POS) modules. The Error fields are not shown for USB ports. The elements of the Filter Properties tab related to capture filter are shown in Figure:Filter Properties—Capture Filter.*

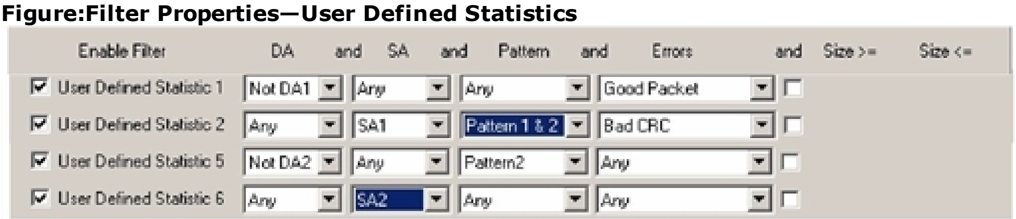
Figure:Filter Properties—Capture Filter

In order for the Capture Filter to take effect, the check box must be selected and all of the basic categories (DA, SA, Pattern, Error and optional Size Ranges) matched for the same packet at the same time. By default, the Capture Filter is enabled for every port with *Any* conditions for all of the fields and with no size requirements. This will result in complete data capture after a *Start Capture* command has been given and the *Capture Trigger function has taken effect, following receipt of the first packet. The fields and their usage are described in Table:Capture Trigger Condition Fields.*

User Defined Statistics

The User Defined Statistics 1/2/5/6 fields are used to define conditions that cause the four user-defined statistics to accumulate. These figures appear in the Statistic View. The elements of the *Filter Properties* tab related to the user defined statistics are shown in *Figure:Filter Properties—User Defined Statistics.*

Figure:Filter Properties—User Defined Statistics



In order for a User Defined Statistic to be counted, the check box must be selected and all of the basic categories (DA, SA, Pattern, Error, and optional Size Range) will be matched for the packet simultaneously.

In most cases, the filtering for UDS 1 is monitored, and packets received on the port that satisfy the conditions of that UDS cause a pulse signal to be generated on the corresponding Trigger Out pin located in the load module faceplate. The Trig LED on the face plate follows the state of the Trigger Out pin. It displays green when the pulse signal is being sent to the pin. Refer to the *Ixia Platform Reference Manual* for information about the functions of the individual load modules.

The fields and their usage are shown in *Figure:Filter Properties—Overview*.

NOTE

To get the rate count for a User Defined Statistic (UDS) into a StatisticView created to display multiple ports, do the following:

Create a statistic view.

The UDS rate will not be shown. You will have to add additional statistics to the view.

Tile the main IxExplorer view and the statistic view so you can see them together.

In IxExplorer, select the statistic that you want to see the rate for by left-clicking the name field. Then left click the mouse on the selected statistics and hold it down as you drag the stat to the statistics view.

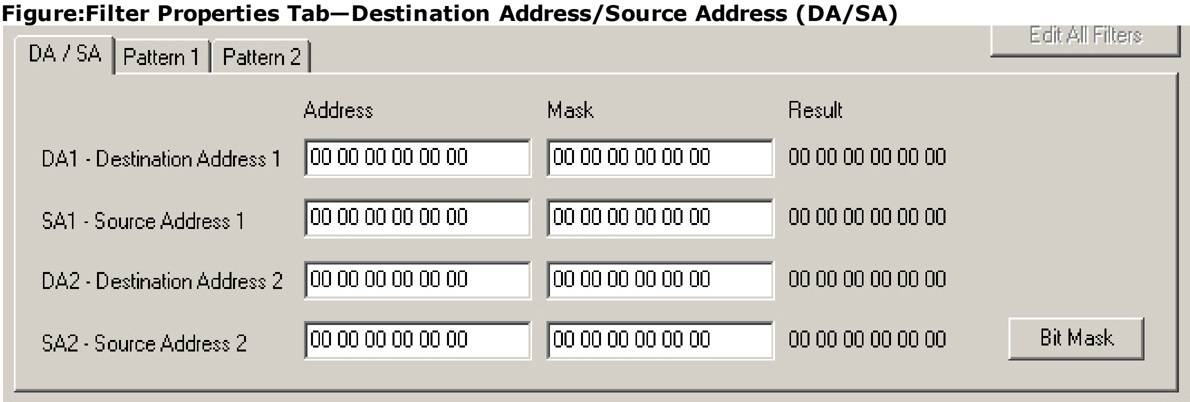
Right-click the mouse and hold it down to drag the stat to the statistics view to add the rate of the stat to the statistics view.

DA/SA Values

(For Ethernet modules) The DA/SA property sheet allows the specification of two Destination MAC Addresses and two Source MAC Addresses which may be used in any combination of *Capture Trigger*, *Capture Filter*, *User Defined Statistics*, and *DA/SA Values settings. This property sheet does not appear for Packet over SONET modules. The DA/SA property sheet is shown in Figure:Filter Properties Tab—Destination Address/Source Address (DA/SA)*

The DA1 value and mask may be used to filter for packets to retransmit when the port is set to Echo Mode. *Echo* for additional information.

Figure:Filter Properties Tab—Destination Address/Source Address (DA/SA)



These four rows define values for two Destination Addresses (DA1 and DA2) and two Source Addresses (SA1 and SA2). Each of the four values is formatted as a 48-bit MAC address in hex notation. The fields for each row are described in *Table:DA/SA Fields*.

Table:DA/SA Fields

Field	Description
Address	The hex value for the MAC address to be matched on incoming packets.
Mask	The hex mask value to be applied to the address. Each '0' bit in the mask indicates that the corresponding incoming port data and DA/SA address bit are compared. Each '1' bit in the mask indicates that no comparison should be made.
Result	The result of applying the mask against the address. The possible values are shown below.

The possible values displayed in the Results column are shown in *Table:Result Values*.

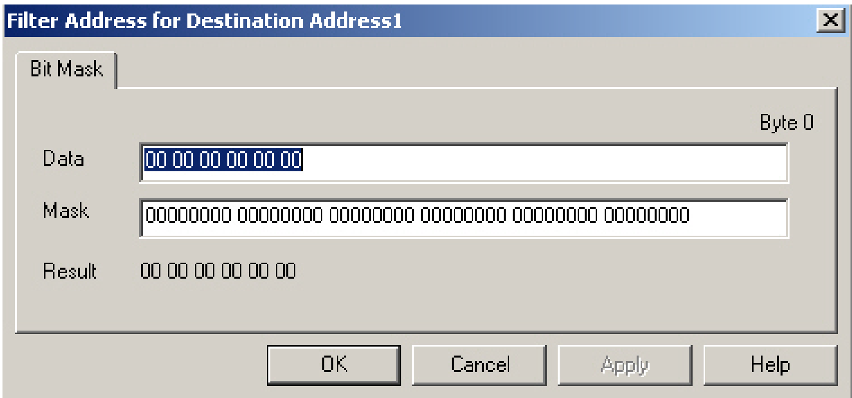
Table:Result Values

Mask Value	Description
0 through F	The corresponding four bits of the MAC address are matched against this value.
X	The corresponding four bits of the MAC address are ignored during matching.
?	This indicates that the mask nibble value is a combination of '0's', '1's',

Mask Value	Description
	and 'X' bit values. The *Bit Mask* dialog must be used to view and edit this value.

When the *Bit Mask* button is used, the *Bit Mask* dialog presents the values for the currently selected DA or SA row, as shown in *Figure:Filter Properties—Bit Mask for DA/SA*.

Figure:Filter Properties—Bit Mask for DA/SA



The fields in this dialog are described in *Table:Bit Mask Dialog*.

Table:Bit Mask Dialog

Field	Description
Data	The hexadecimal data value (MAC address) to be masked. Its value may be set using any hexadecimal character (0 through 9, a through f, and A through F). Characters entered as lowercase are displayed in uppercase, by default. Each character corresponds to a 4-bit nibble, and two nibbles make up a byte/octet. Spacing between bytes is provided automatically.
Mask	The bit mask consists of 8 bits per byte of the data value. Each bit can be set to '0' or '1.' Spacing between each group of 8 bits (= one byte) is provided automatically. Each '0' in the mask lets the corresponding bit in the data field be used for matching. Each '1' in the mask causes the corresponding data bit to be ignored.
Result	(Read-only) See the Result Values in *Table:Result Values* for information on the masked results displayed in this field.

Pattern Match Tabs

The *Pattern Match* sub-tabs of the *Filter Properties* tab allow for the specification of two data patterns to be matched against the contents of incoming packets for the purpose of filtering packets. Each pattern may be up to 16 bytes in length. The *Pattern Match* sub-tabs for Patterns 1 & 2 is shown in *Figure:Filter Properties - Patterns 1 and 2 (shown for Gigabit module).*

NOTE For information on the ATM Pattern 3 sub-tabs, *ATM Filter Properties*. For information on the GFP Pattern 3,*GFP Filter Properties*. For information on the VCAT Circuit, *VCAT Circuit Filter Properties*.

Figure:Filter Properties - Patterns 1 and 2 (shown for Gigabit module)

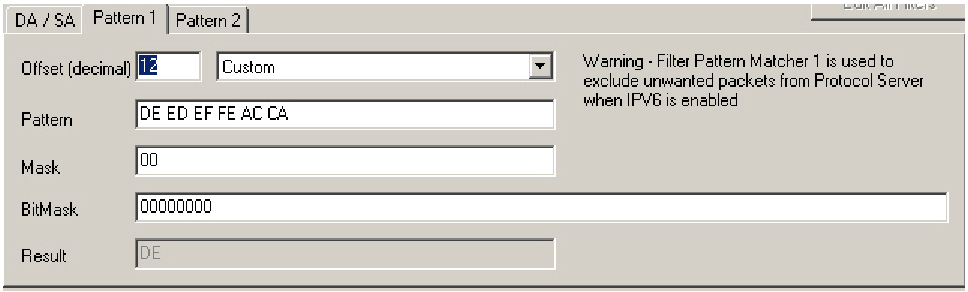
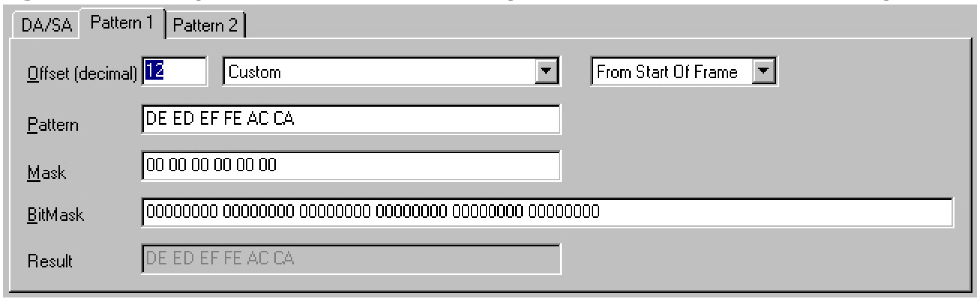


Figure:Filter Properties–Patterns 1 and 2 (shown for a 10GE LSM module)



The fields and controls in this sub-tab are described in *Table:Filter Properties—Patterns 1 and 2*.

Table:Filter Properties—Patterns 1 and 2

Field/Control	Description
Offset (decimal)	(in bytes) The offset from the beginning of the packet.
(Pattern Selection List)	Refer to *Table:Pattern Match Choices—Ethernet-Type Modules* for a list of all the available types of patterns.
Pattern	(in hex) The value of the pattern
Mask	(in hex) The mask value to be applied against the pattern.
Bit Mask	The bit mask value to be applied against the pattern. Each *0* bit in the mask indicates that the corresponding are compared. Each *1* bit in the mask indicates that no comparison should be made for that bit.
Result	The result of applying the mask against the pattern.
Flexible Offset	A pull-down menu that allows to specify where the data pattern (including the offset) should start. Options are: • From Start of Frame • From Start of IP • From Start of Protocol
(Warning)	Filter Pattern Matcher 1 is may be used to exclude unwanted packets from IxNetwork when IPv6 is enabled. For more information on adding IPv6 addresses to Protocol Interfaces, see the *IxNetwork User Guide*.

The basic choices available in the dropdown list for Ethernet-type modules are shown in *Table:Pattern Match Choices—Ethernet-Type Modules*.

The number and types of fields in the sub-tab change, based on the choice of pattern.

Table:Pattern Match Choices—Ethernet-Type Modules

Pattern Type	Configurable Fields	Description
IP/Ethernet II	None	Match any packet that is an IP packet formatted according to Ethernet II conventions.
IP SA/Ethernet II	IP SA Submask Bit Mask	Match a specific IP source address, under a mask for Ethernet II packets.
IP DA/Ethernet II	IP DA Submask Bit Mask	Match a specific IP destination address, under a mask for Ethernet II packets.
IP DA, SA/Ethernet II	IP SA Submask Bit Mask	Match a specific IP source and destination addresses, under masks for Ethernet II packets.
TCP Source Port/Ethernet II	Pattern	Match a specific TCP source port for Ethernet II IP packets. Two bytes should be specified.
TCP Dest Port/Ethernet II	Pattern	Match a specific TCP destination port for Ethernet II IP packets. Two bytes should be specified.
UDP Source Port/Ethernet II	Pattern	Match a specific UDP source port for Ethernet II IP packets. Two bytes should be specified.
UDP Dest Port/Ethernet II	Pattern	Match a specific UDP destination port for Ethernet II IP packets. Two bytes should be specified.
IP/Ethernet SNAP	None	Match any packet that is an IP packet formatted according to Ethernet SNAP conventions.
IP SA/Ethernet SNAP	IP SA Submask Bit Mask	Match a specific IP source address, under a mask for Ethernet SNAP packets.
IP DA/Ethernet SNAP	IP SA Submask Bit Mask	Match a specific IP destination address, under a mask for Ethernet SNAP packets.
IP SA, DA/Ethernet SNAP	IP SA Submask Bit Mask	Match a specific IP source and destination addresses, under masks for Ethernet SNAP packets.
TCP Source Port/Ethernet SNAP	Pattern	Match a specific TCP source port for Ethernet SNAP IP packets. Two bytes should be specified.
TCP Dest Port/Ethernet SNAP	Pattern	Match a specific TCP destination port for Ethernet SNAP IP packets. Two bytes should be specified.
UDP Source Port/Ethernet SNAP	Pattern	Match a specific UDP source port for Ethernet SNAP IP packets. Two bytes

Pattern Type	Configurable Fields	Description
		should be specified.
UDP Dest Port/Ethernet SNAP	Pattern	Match a specific UDP destination port for Ethernet SNAP IP packets. Two bytes should be specified.
VLAN	None	Match any packet that is a recognizable VLAN packet.
IPv6 SA/Ethernet II	IPv6 Address BitMask	Match the IPv6 Source Address for an Ethernet II packet.
IPv6 DA/Ethernet II	IPv6 Address BitMask	Match the IPv6 Destination Address for an Ethernet II packet.
IPv6 SA/8023Snap	IPv6 Address BitMask	Match the IPv6 Source Address for an 802.3 SNAP packet.
IPv6 DA/8023Snap	IPv6 Address BitMask	Match the IPv6 Destination Address for an 802.3 SNAP packet.
IPv6 TCP Source Port Ethernet II	Pattern	Match the IPv6 TCP source port number for an Ethernet II packet.
IPv6 TCP Dest Port Ethernet II	Pattern	Match the IPv6 TCP destination port number for an Ethernet II packet.
IPv6 UDP Source Port Ethernet II	Pattern	Match the IPv6 UDP source port number for an Ethernet II packet.
IPv6 UDP Dest Port Ethernet II	Pattern	Match the IPv6 UDP destination port number for an Ethernet II packet.
IPv6 TCP Source Port 8023 SNAP	Pattern	Match the IPv6 TCP source port number for an 802.3 SNAP packet.
IPv6 TCP Dest Port 8023 SNAP	Pattern	Match the IPv6 TCP destination port number for an 802.3 SNAP packet.
IPv6 UDP Source Port 8023 SNAP	Pattern	Match the IPv6 UDP source port number for an 802.3 SNAP packet.
IPv6 UDP Dest Port 8023 SNAP	Pattern	Match the IPv6 UDP destination port number for an 802.3 SNAP packet.
IPv6 IP TCP Source Port Eth-ernet II	Pattern	Match the TCP source port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an Ethernet II frame.
IPv6 IP TCP Dest Port Ethernet II	Pattern	Match the TCP destination port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an Ethernet II frame.
IPv6 IP UDP Source Port Eth-ernet II	Pattern	Match the UDP source port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an Ethernet II frame.

Pattern Type	Configurable Fields	Description
IPv6 IP UDP Dest Port Ethernet II	Pattern	Match the UDP destination port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an Ethernet II frame.
IPv6 IP TCP Source Port 8023 Snap	Pattern	Match the TCP source port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an 802.3 SNAP frame.
IPv6 IP TCP Dest Port 8023 Snap	Pattern	Match the TCP destination port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an 802.3 SNAP frame.
IPv6 IP UDP Source Port 8023 Snap	Pattern	Match the UDP source port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an 802.3 SNAP frame.
IPv6 IP UDP Dest Port 8023 Snap	Pattern	Match the UDP destination port number for an IPv4 over IPv6 or IPv6 over IPv4 packet in an 802.3 SNAP frame.
IP/IPv6 IP SA/Ethernet II	IP SA Submask BitMask	Match the IPv4 source address in an IPv4 packet encapsulated in an IPv6 packet in an Ethernet II frame.
IP/IPv6 IP DA/Ethernet II	IP SA Submask BitMask	Match the IPv4 destination address in an IPv4 packet encapsulated in an IPv6 packet in an Ethernet II frame.
IP/IPv6 IP SA/8023Snap	IP SA Submask BitMask	Match the IPv4 source address in an IPv4 packet encapsulated in an IPv6 packet in an 802.3 SNAP frame.
IP/IPv6 IP DA/8023Snap	IP SA Submask BitMask	Match the IPv4 destination address in an IPv4 packet encapsulated in an IPv6 packet in an 802.3 SNAP frame.
IPv6/IP IPv6 SA/Ethernet II	IPv6 Address BitMask	Match the IPv6 source address in an IPv6 packet encapsulated in an IPv4 packet in an Ethernet II frame.
IPv6/IP IPv6 DA/Ethernet II	IPv6 Address BitMask	Match the IPv6 destination address in an IPv6 packet encapsulated in an IPv4 packet in an Ethernet II frame.
IPv6/IP IPv6 SA/8023Snap	IPv6 Address BitMask	Match the IPv6 source address in an IPv6 packet encapsulated in an IPv4 packet in an 802.3 SNAP frame.
IPv6/IP IPv6 DA/8023Snap	IPv6 Address BitMask	Match the IPv6 destination address in an IPv6 packet encapsulated in an IPv4 packet in an 802.3 SNAP frame.
Custom	Offset Pattern Mask	Match particular data items within a packet. The remaining fields in the sub-tab are used to specify how the match occurs.

The basic choices available for POS modules are shown in *Table:Pattern Match Choices—POS modules*. The options for IP/PPP, IP/Cisco HDLC, SRP, or RPR appear only if a POS packet with a header of that type is being configured. POS packets with headers of types other than those mentioned here, can be matched only for the choices from IP/SA onward.

Pattern Match Choices—POS modules

Pattern Type	Description
IP/PPP	(For use with PPP only) Match any packet that is an IP packet formatted according to PPP conventions.
IP/Cisco HDLC	(For use with IP/HDLC only) Match any packet that is an IP packet formatted according to Cisco HDLC conventions.
For SRP only:	
SRP Mode Reserved (000, 001, 010)	Match any SRP-formatted packet that has this mode set in the SRP generic header.
SRP Mode ATM Cell (011)	Match any SRP-formatted packet that has this mode set in the SRP generic header. The binary value 011 indicates an SRP/ATM cell.
SRP Mode Control Message Pass to Host (100)	Match any SRP-formatted packet that has this mode set in the SRP generic header.
SRP Mode Control Message Buffer For Host (101)	Match any SRP-formatted packet that has this mode set in the SRP generic header.
SRP Mode Usage Message (110)	Match any SRP-formatted packet that has this mode set in the SRP generic header.
SRP Mode Packet Data (111)	Match any SRP-formatted packet that has this mode set in the SRP generic header.
SRP Mode All Control Messages (10x)	Match any SRP-formatted packet that has this mode set in the SRP generic header, where ‘x’ can be a ‘0’ or ‘1.’ The binary value 10x indicates a control message.
SRP Mode Usage Message Or Packet Data (11x)	Match any SRP-formatted packet that has this mode set in the SRP generic header, where ‘x’ can be a ‘0’ or ‘1.’ The binary value 11x indicates a Usage Message or Packet Data.
SRP Mode Control Usage Or Packet Data (1xx)	Match any SRP-formatted packet that has this mode set in the SRP generic header where ‘x’ can be a ‘0’ or ‘1.’ The binary value 1xx indicates a Control or Usage message.
SRP Inner Ring (1)	Match any SRP-formatted packet that has the ring identifier set to inner ring (1).
SRP Outer Ring (0)	Match any SRP-formatted packet that has the ring identifier set to outer ring (0).
SRP Priority 0-7 (000-111)	Match any SRP-formatted packet according to this user-assigned priority.

Pattern Type	Description
SRP Parity Bit Odd (xx1)	Match any SRP-formatted packet that has odd parity.
SRP Parity Bit Even (xx0)	Match any SRP-formatted packet that has even parity.
SRP Discovery Frame	Match any SRP Discovery Frame. See **Note** below.
SRP IPS Frame	Match any SRP IPS Frame. See **Note** below.
For RPR only	
RPR Ringlet 0	Match any RPR packet which specifies Ringlet 0. (Originally transmitted on Ringlet 0 by the Source.)
RPR Ringlet 1	Match any RPR packet which specifies Ringlet 1. (Originally transmitted on Ringlet 1 by the Source.)
RPR Fairness Eligibility 0	Match any RPR packet which specifies Fairness Eligibility 0. (0 = Not eligible for Fairness algorithm.)
RPR Fairness Eligibility 1	Match any RPR packet which specifies Fairness Eligibility 1. (1 = Eligible for Fairness algorithm.)
RPR Reserved Packet	Match any RPR packet with Packet Type = 00 (Reserved).
RPR Control Packet	Match any RPR Control Packet (Control message). (Packet Type = 01)
RPR Fairness Packet	Match any RPR Fairness Packet (RPR Fairness Control Message/FCM). (Packet Type = 10)
RPR Data Packet	Match any RPR Data Packet. (Packet Type = 11)
RPR Service Class C	Match any RPR packet which specifies service Class C. Class C is the lowest level of MAC service ‘best-effort’ traffic that is subject to the RPR fairness algorithm.
RPR Service Class B	Match any RPR packet which specifies MAC service Class B. ClassB actually has two types of service: 1) some traffic is allocated, with guaranteed data rate and bounded delay and jitter, not subject to the RPR fairness algorithm. 2) remainder is best-effort traffic and subject to the RPR fairness algorithm.
RPR Service Class A1	Match any RPR packet which specifies service Class A1. ClassA service has an allocated, guaranteed data rate, with bounded (low) end-to-end delay and jitter. The RPR fairness algorithm does not apply to allocated bandwidth. The MAC subclassA1 is for **reclaimable** bandwidth.
RPR Service Class A0	Match any RPR packet which specifies service Class A0. ClassA service has an allocated, guaranteed data rate, with bounded (low) end-to-end delay and jitter. The RPR fairness algorithm does not apply to allocated bandwidth. The MAC subclassA0 is for **reserved** bandwidth.
RPR Wrap Eligibility 0	Match any RPR packet which specifies Wrap Eligibility 0. (0 = Steerable only)
RPR Wrap Eligibility 1	Match any RPR packet which specifies Wrap Eligibility 1. (1 = Wrap Eligible)

Pattern Type	Description
RPR Reserved Bit 0	Match any RPR packet which specifies Reserved Bit 0. (Parity Bit = 0 is reserved for future use, applies to data frames and control frames. Parity Bit = 1 for fairness and idle frames.)
RPR Reserved Bit 0	Match any RPR packet which specifies Reserved Bit 0. (Parity Bit = 0 is reserved for future use, applies to data frames and control frames. Parity Bit = 1 for fairness and idle frames.)
For GFP only	
Data Fcs Null Extension Ethernet	Match for GFP Payload type emulating Data information, with a Frame Check Sequence, with no extension indicated, using Ethernet.
Data NoFcs Null Extension Ethernet	Match for GFP Payload type emulating Data information, with no Frame Check Sequence, with no extension indicated, using Ethernet.
Data Fcs Linear Extension Ethernet	Match for GFP Payload type emulating Data information, with a Frame Check Sequence, with Linear extension indicated, using Ethernet.
Data NoFcs Linear Extension Ethernet	Match for GFP Payload type emulating Data information, with no Frame Check Sequence, with Linear extension indicated, using Ethernet.
Data Fcs Null Extension PPP	Match for GFP Payload type emulating Data information, with a Frame Check Sequence, with no extension indicated, using Point-to-Point Protocol.
Data NoFcs Null Extension PPP	Match for GFP Payload type emulating Data information, with no Frame Check Sequence, with no extension indicated, using Point-to-Point Protocol.
Data Fcs Linear Extension PPP	Match for GFP Payload type emulating Data information, with a Frame Check Sequence, with Linear extension indicated, using Point-to-Point Protocol.
Data NoFcs Linear Extension PPP	Match for GFP Payload type emulating Data information, with no Frame Check Sequence, with Linear extension indicated, using Point-to-Point Protocol.
Mgmt Fcs Null Extension Ethernet	Match for GFP Payload type emulating Management information, with a Frame Check Sequence, with no extension indicated, using Ethernet.
Mgmt NoFcs Null Extension Ethernet	Match for GFP Payload type emulating Management information, with no Frame Check Sequence, with no extension indicated, using Ethernet.
Mgmt Fcs Linear Extension Ethernet	Match for GFP Payload type emulating Management information, with a Frame Check Sequence, with Linear extension indicated, using Ethernet.
Mgmt NoFcs Linear Extension Ethernet	Match for GFP Payload type emulating Management information, with no Frame Check Sequence, with Linear extension indicated, using Ethernet.

Pattern Type	Description
Mgmt Fcs Null Extension PPP	Match for GFP Payload type emulating Management information, with a Frame Check Sequence, with no extension indicated, using Point-to-Point Protocol.
Mgmt NoFcs Null Extension PPP	Match for GFP Payload type emulating Management information, with no Frame Check Sequence, with no extension indicated, using Point-to-Point Protocol.
Mgmt Fcs Linear Extension PPP	Match for GFP Payload type emulating Management information, with a Frame Check Sequence, with Linear extension indicated, using Point-to-Point Protocol.
Mgmt NoFcs Linear Extension PPP	Match for GFP Payload type emulating Management information, with no Frame Check Sequence, with Linear extension indicated, using Point-to-Point Protocol.
General	
IP SA	Match a specific IP source address.
IP DA	Match a specific IP destination address.
IP DA, SA	Match specific IP source and destination addresses.
TCP Source Port/IP	Match a specific TCP source port for IP packets. Two bytes should be specified.
TCP Dest Port/IP	Match a specific TCP destination port for IP packets. Two bytes should be specified.
UDP Source Port/IP	Match a specific UDP source port for IP packets. Two bytes should be specified.
UDP Dest Port/IP	Match a specific UDP destination port for IP packets. Two bytes should be specified.
IPv6 SA/Pos	Match the IPv6 Source Address for a POS frame.
IPv6 DA/Pos	Match the IPv6 Destination Address for a POS frame.
IPv6 TCP Source Port	Match the IPv6 TCP source port number for a POS frame.
IPv6 TCP Dest Port	Match the IPv6 TCP destination port number for a POS frame.
IPv6 UDP Source Port	Match the IPv6 UDP source port number for a POS frame.
IPv6 UDP Dest Port	Match the IPv6 UDP destination port number for a POS frame.
IPv6 IP TCP Source Port	Match the TCP source port for an IPv4 over IPv6 or IPv6 over IPv4 packet in a POS frame.
IPv6 IP TCP Dest Port	Match the TCP destination port for an IPv4 over IPv6 or IPv6 over IPv4 packet in a POS frame.
IPv6 IP UDP Source Port	Match the UDP source port for an IPv4 over IPv6 or IPv6 over IPv4 packet in a POS frame.
IPv6 IP UDP Dest Port	Match the UDP destination port for an IPv4 over IPv6 or IPv6 over IPv4 packet in a POS frame.
IP/IPv6 IP SA/Pos	Match the IPv4 Source Address in an IPv4 packet encapsulated in an IPv6 packet in a POS frame.
IP/IPv6 IP DA/Pos	Match the IPv4 Destination Address in an IPv4 packet encapsulated in an IPv6 packet in a POS frame.
IPv6/IP IPv6 SA/Pos	Match the IPv6 Source Address in an IPv6 packet encapsulated in an IPv4 packet in a POS frame.

Pattern Type	Description
IPv6/IP IPv6 DA/Pos	Match the IPv6 Destination Address in an IPv6 packet encapsulated in an IPv4 packet in a POS frame.
Custom	Match particular data items within a packet. The remaining fields in the sub-tab are used to specify how the match occurs.

NOTE To match an SRP IPS or a Topology Discovery Frame, set Pattern 1 = Control and Pattern 2 to IPS/Discovery.
Pattern 1 filters MODE bits, and Pattern 2 checks for Protocol type.

The additional fields for each of the data patterns are shown in *Table:Pattern Match Fields*.

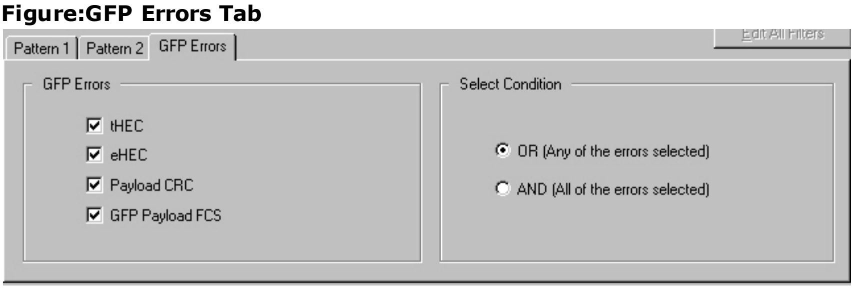
Table:Pattern Match Fields

Field	Description
Offset	The offset within the packet. Any value within the maximum packet length size may be specified. An offset from 0 through 11 may intentionally be used to overlap the DA/SA fields.
Pattern	Up to 16 bytes of data may be exclicked in hexadecimal. The data value that is being masked is shown in this field. Its value may be set using any hexadecimal character (0 through 9, a through f and A through F); lowercase characters are displayed in uppercase. Each character corresponds to a 4-bit nibble; spacing between bytes is automatically provided.
Mask	The mask value to be applied against the incoming data and pattern exclicked in hex. Each *0* bit in the mask indicates that the corresponding incoming port data and pattern are compared. Each *1* bit in the mask indicates that no comparison should be made.
Bit Mask	The mask value to be applied against the incoming data and pattern exclicked in bits. Each permitted byte of the mask consists of 8 characters, each character corresponding to one bit. Values of *0* or *1* are permitted. Spacing between each byte is automatically provided. The first 8 bits of mask operate on the first byte (2 nibbles) of the data value. Each *0* in the mask causes the corresponding bit in the data field to be used for matching; each *1* in the mask causes the bit to be ignored.
Result	The value resulting from the masking process.

GFP Filter Properties

On OC-48c load modules that employ GFP, it is possible to use GFP parameters as a matching pattern. When GFP is selected, a *GFP Errors* sub-tab appears, as shown in *Figure:GFP Errors Tab*.

Figure:GFP Errors Tab



The options in this sub-tab are described in *Table:GFP Errors Tab Usage*.

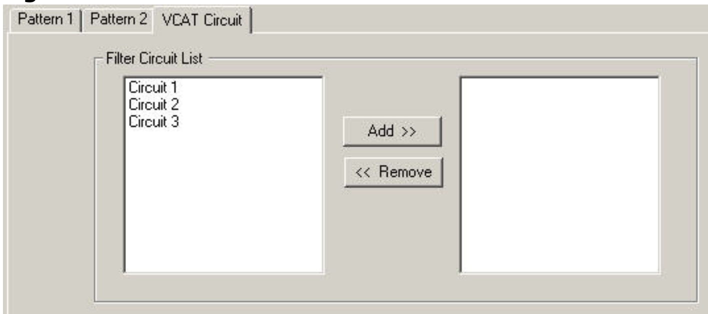
Table:GFP Errors Tab Usage

Field	Usage
tHEC	A packet received with a bad Type Header Error Check, which means the CRC-16 error control code will not match the expected code.
eHEC	A packet received with a bad Extension Header Error Check, which means the CRC-16 error control code will not match the expected code.
Payload CRC	A packet received with a bad Cyclical Redundancy Check sequence, which means the CRC-32 sequence does not match the expected sequence.
GFP Payload FCS	A packet received with a bad Payload Frame Check Sequence.
OR	Selecting this option button means that any of the selected errors can be used as a match.
AND	Selecting this option button means that all of the selected errors must be used as a match.

VCAT Circuit Filter Properties

On OC-48c load modules that employ channelization, it is possible to use VCAT parameters as a matching pattern. A *VCAT Circuit* sub-tab appears, as shown in *Figure:VCAT Circuit Tab*.

Figure:VCAT Circuit Tab

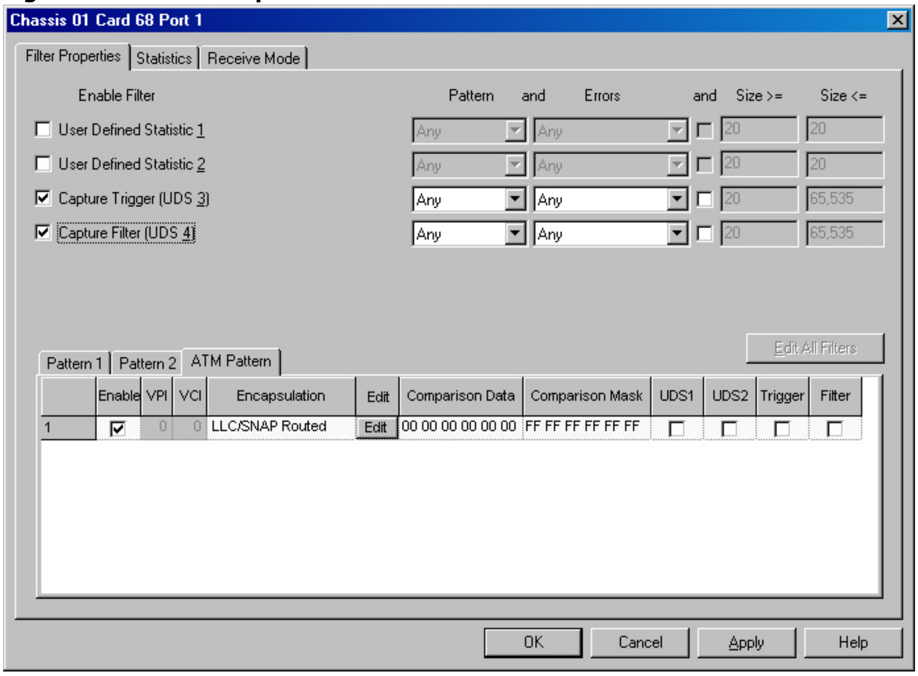


Use the Add >> and Remove << buttons to add or remove circuits to the list of filter patterns. For informaton about VCAT channelized port mode, *VCAT Circuit Properties*.

ATM Filter Properties

The *Filter Properties* tab provides the *ATM Pattern* sub-tab specific to ATM, as shown in *Figure:ATM Filter Properties—Pattern 3*. This dialog is activated by selecting *ATM Pattern Matching* in the *ATM* tab of the *Port Properties* dialog, as described in *ATM Tab*.

Figure:ATM Filter Properties—Pattern 3



This sub-tab allows to configure various filtering patterns to be matched against incoming ATM traffic on the port. The filtering is done at the ATM AAL5 level and includes the 5-byte ATM cell header. The UDF, filter, and trigger options change depending upon what selections are made on the *Receive Mode* tab. Table shows what UDF, trigger, and filter options are available for each Receive Mode selection.

Table:Enable Filter Options

Receive Mode	Available UDF, Trigger, and Filter Options
Capture Mode	UDS 1, Capture Trigger (UDS 3), Capture Filter (UDS 4)
Packet Groups	UDS 1
Sequence Checking (with Capture Mode)	UDS 1, Capture Trigger (UDS 3), Capture Filter (UDS 4)
Sequence Checking (Packet Groups)	UDS 1
Data Integrity	UDS 1, UDS 2, Capture Trigger (UDS 3), Capture Filter (UDS 4)

For more information on the Receive Mode tab, *Receive Mode Tab*.

The fields and controls in this sub-tab are described in *Table:ATM Filter Properties—Pattern 3*. (Note that if Packet Group mode is selected in the *Receive Mode* tab, the *Pattern 2* sub-tab will not be available.)

Table:ATM Filter Properties—Pattern 3

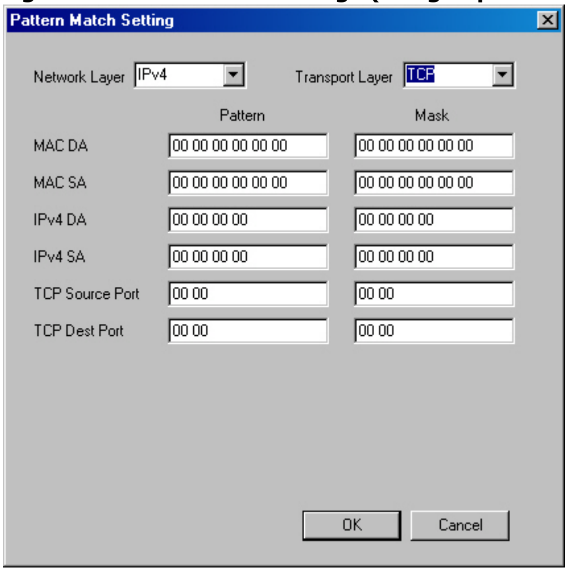
Field/Control	Description
Enable	If this option is selected, Pattern 3 can be configured for use in filter pattern matching.
VPI	(Read-only) Virtual Path Identifier. You can set this value

Field/Control	Description
	when registering the VPI/VCI in the VPI/VCI Statistic View—when a VPI/VCI is added to the *Receive Stats* list.
VCI	(Read-only) Virtual Circuit/Connection Identifier. You can set this value when registering the VPI/VCI in the VPI/VCI Statistic View—when a VPI/VCI is added to the *Receive Stats* list.
Encapsulation	Select the encapsulation type for the ATM filter, from a pull-down list of types. Select from the following list: • LLC SNAP Routed Protocol • LLC Bridged Ethernet/802.3 • LLC Bridged Ethernet/802.3 no FCS • LLC Encapsulated PPP • VC Multiplexed PPP • VC MUX Routed Protocol • VC MUX Bridged Ethernet • VC MUX Bridged Ethernet with No FCS
Edit	Selecting this button opens the *Pattern Match Settings* dialog box, which allows to edit layer 3 and layer 4 filter matching information (in Hex). This dialog is discussed in *ATM Pattern Match Settings Dialog*.
Comparison Data	(in Hex) The data pattern to be used for pattern matching on this VC. This is only user-editable when the 'Custom' encapsulation type is selected.
Comparison Data Mask	(in Hex) The Mask to be used with the Comparison Data pattern on this VC. This is only user-editable when the 'Custom' encapsulation type is selected.
UDS1	If selected, this pattern will be used as User-Defined Statistic 1 for this VC.
UDS2	If selected, this pattern will be used as User-Defined Statistic 2 for this VC.
Trigger	If selected, this pattern will be used as the Capture Trigger (UDS3) for this VC.
Filter	If selected, this pattern will be used as the Capture Filter (UDS4) for this VC.

ATM Pattern Match Settings Dialog

The ATM *Pattern Match Settings* dialog allows to specify a Layer 3/Layer 4 data pattern and mask that can be used for trigger or filter cases. The *Pattern Match Settings* dialog is shown in *Figure:Pattern Match Settings (bridged protocol using IPv4 and TCP)*.

Figure:Pattern Match Settings (bridged protocol using IPv4 and TCP)



The options shown in this dialog are described in *Table:Pattern Match Settings Configuration*. The configurable fields change depending upon the settings selected.

Table:Pattern Match Settings Configuration

Field	Usage
Network Layer	Select a Layer 3 protocol from the options in the pull-down list: • None • IPv4 • IPv6 Once a protocol is selected, you can specify a pattern for the Source and Destination Address.
Transport Layer	Select a Layer 4 protocol from the options in the pull-down list: • None • TCP • UDP Once a protocol (or protocols) are selected, you can specify a pattern for the Source and Destination Port.
MAC DA	(In Hex) Specify a pattern and mask match for the MAC Destination Address. NOTE This field only appear if a a bridged encapsulation option is option is selected. *ATM Filter Properties* for information.
MAC SA	(In Hex) Specify a pattern and mask match for the MAC Source Address. NOTE This field only appear if a a bridged encapsulation

Field	Usage
	NOTE option is option is selected. *ATM Filter Properties* for information.
IP4/IPv6 DA Pattern and Mask	(In Hex) Specify a pattern and mask match for the IPv4 or IPv6 Destination Address. The name of this field changes to reflect the protocol or protocols selected from the Network Layer pull down list. NOTE Only IPv4 DA/SA has mask. IPv6 DA/SA does not have mask.
IP4/IPv6 SA Pattern and Mask	(In Hex) Specify a pattern and mask match for the IPv4 or IPv6 Source Address. The name of this field changes to reflect the protocol or protocols selected from the Network Layer pull down list. NOTE Only IPv4 DA/SA has mask. IPv6 DA/SA does not have mask.
TCP/UDP Source Port Pattern	(In Hex) Specify a pattern match for the TCP or UDP Source Port. The name of this field changes to reflect the protocol or protocols selected from the Transport Layer pull down list. A Layer 3 protocol must be selected to make these fields active.
TCP/UDP Dest Port Pattern	(In Hex) Specify a pattern match for the TCP or UDP Destination Port. The name of this field changes to reflect the protocol or protocols selected from the Transport Layer pull down list. A Layer 3 protocol must be selected to make these fields active.

Stream Extraction Module Filter Properties

The Stream Extraction module allows for capturing and filtering many types of stream data from Ethernet/IP traffic (video, voice, e-mail, web, and so on) from ports 2→3 and 3←2. AFM hardware supports two sets of eight filters. There are eight tabs each on two pages for configuring the filters. A logic control setup is present to configure logic combinations of these filters. Each filter works independently from others. The filters are described in the following paragraphs. The Logic Control setup is described in *Logic Control*.

Filter Offset is set to a default value by selecting a filter type, but you can change it manually, in some cases. A pattern can be used to match any data at any offset. For example, Filter 1 can be used to match data 0xABCD at offset 32 while Filter 2 is used to match MAC DA data at offset 0.

The elements that combine to configure a filter vary with the type of filter.

- Custom, IP Version, or L4 Protocol: *Custom, IP Version, or L4 Protocol Filter Type*.
- MAC DA or MAC SA: *MAC DA or SA Filter Type*.
- DA/IPv4 or SA/IPv4: *DA/IPv4 or SA/IPv4 Filter Type*.
- DA/IPv6 or SA/IPv6: *DA/IPv6 or SA/IPv6 Filter Type*.
- Dest Port or Source Port /TCP or UDP /IPv4 or v6: *Port Filter Type*.

Modifiers are enabled when at least one filter is enabled. A Modifier will have its own offset GUI input. The three Modifiers (Destination MAC Address, IPv4 Destination IP Address, and UDP Destination Address) are described in *Address Modifiers*.

Figure:AFM Module Filter Properties (Custom Filter Type) shows the Port 2->3 filter properties page for the Stream Extraction module with filter type *Custom* selected.

Figure:AFM Module Filter Properties (Custom Filter Type)

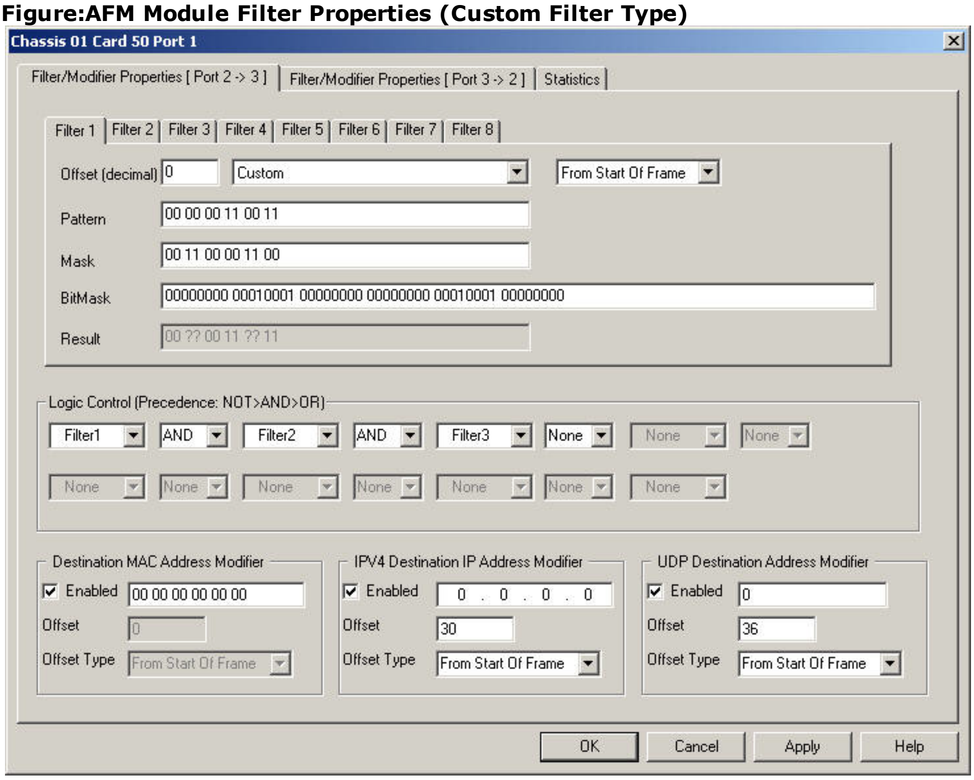


Table:AFM Module Configuration Options (Overview) gives an overview of configuration options of the AFM module Filter Properties page (using filter type *Custom)*..

Table:AFM Module Configuration Options (Overview)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type, but in some cases can be edited.
	(Filter type)	List of filter types: • MAC DA • MAC SA • IP Version • DA / IPV4 • SA / IPV4 • DA / IPV6 • SA / IPV6 • L4 Protocol Type • Dest Port / TCP / IPV4

Section	Field/Control	Description
		• Source Port / TCP / IPV4 • Dest Port / TCP / IPV6 • Source Port / TCP / IPV6 • Dest Port / UDP / IpV4 • Source Port / UDP / IPV4 • Dest Port / UDP / IpV6 • Source Port / UDP / IPV6 • Custom Each type gives a default **Offset** based on its description. NOTE ‘DA / IPV4’ only sets the filter for ‘DA’, another filter must be set to filter ‘IPV4’ packets. The same rule applies to all these combo filter types such as ‘ SA/IPV6’ or ‘Dest Port / TCP / IPV4’
	(Offset mode)	From start of frame, or From start of IP The ‘start of IP’ is based on a default format of IP packet.
	Pattern	The data to be compared by the filters. The length of pattern is pre-defined by filter types. MAC DA and MAC SA have 6-byte pattern, ‘DA/IPV4’ has 4-byte pattern, ‘Custom’ has maximum 16 byte pattern. Pattern data are in Hex format.
	Mask	Default = 00 (0 to 16 bytes) Hex format.
	Bitmask	Default = 00000000 binary format. Auto-generated from the **Mask**
	Result	Auto-generated from **Pattern** + **Mask**
Logic Control		*Logic Control*.
Destination MAC Address Modifier		*Address Modifiers*
IPv4 Destination IP Address Modifier		*Address Modifiers*
UDP Destination Address Modifier		*Address Modifiers*

Custom, IP Version, or L4 Protocol Filter Type

Figure:AFM Module Filter Properties (Custom, IP Version, or L4 Protocol Type) shows the filter properties page for filter types Custom, IP Version, and L4 Protocol.

Figure:AFM Module Filter Properties (Custom, IP Version, or L4 Protocol Type)

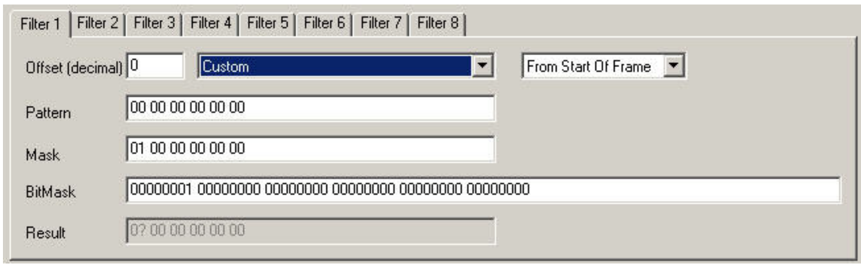


Table:AFM Module Filter Properties (Custom, IP Version, or L4 ProtocolType) provides definitions for the fields to configure the Custom, IP Version, or L4 Protocol filter type..

Table:AFM Module Filter Properties (Custom, IP Version, or L4 Protocol Type)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type, but can be edited. • Custom, default = 0 • IP Version, default = 14 • L4 Protocol, default = 23
	(Filter type)	Custom or IP Version or L4 Protocol
	(Offset mode)	Two options: • From start of frame • From start of IP The 'start of IP' is based on a default format of IP packet.
	Pattern	The data to be compared by the filters. The length of pattern is pre-defined by filter types. 'Custom' has maximum 16 byte pattern.
	Mask	Default = 00 (0 to 16 bytes)
	Bitmask	Default = 00000000 Auto-generated from the **Mask**
	Result	Auto-generated from **Pattern** + **Mask**

MAC DA or SA Filter Type

Figure:AFM Module Filter Properties (MAC DA /SA Type) shows the filter properties page for filter types MAC DA and MAC SA.

Figure:AFM Module Filter Properties (MAC DA /SA Type)

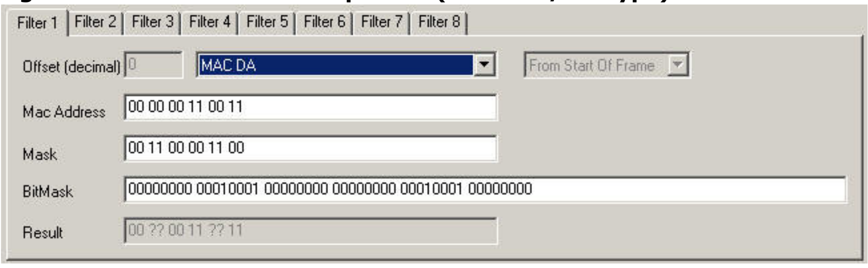


Table:AFM Module Filter Properties (MAC DA/SA Filter Type) provides definitions for the fields to configure the MAC DA or MAC SA filter type..

Table:AFM Module Filter Properties (MAC DA/SA Filter Type)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type. MAC DA default = 0 MAC SA default = 6
	(Filter type)	MAC DA or MAC SA
	(Offset mode)	*Read-only, fixed*. From start of frame
	MAC Address	The data to be compared by the filters. The length is pre-defined by filter types. MAC DA and MAC SA have 6-byte length.
	Mask	Default = 00 (0 to 16 bytes)
	Bitmask	Default = 00000000 Auto-generated from the **Mask**
	Result	Auto-generated from **MAC Address** + **Mask**

DA/IPv4 or SA/IPv4 Filter Type

Figure:AFM Module Filter Properties (DA/IPv4 or SA/IPv4 Type) shows the filter properties page for filter types DA/IPv4 or SA/IPv4.

Figure:AFM Module Filter Properties (DA/IPv4 or SA/IPv4 Type)

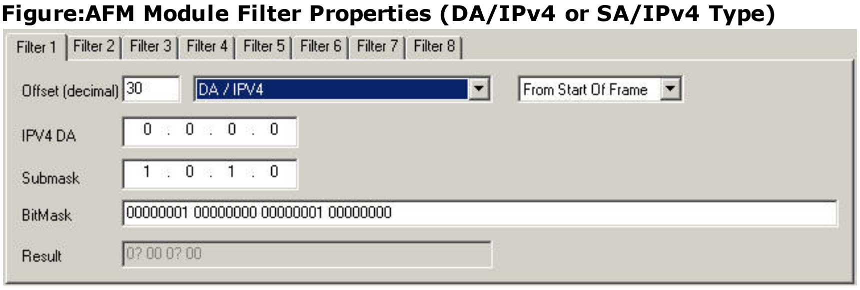


Table:AFM Module Filter Properties (DA/IPv4 or SA/IPv4 Filter Type) provides definitions for the fields to configure the DA/IPv4 or SA/IPv4 filter type..

Table:AFM Module Filter Properties (DA/IPv4 or SA/IPv4 Filter Type)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type. DA/IPv4 default = 30 SA/IPv4 default = 26
	(Filter type)	DA/IPv4 or SA/IPv4
	(Offset mode)	From start of frame (default) or From start of IP
	IPv4 DA or IPv4 SA	The data to be compared by the filters. The length is pre-defined by filter types. 'DA/IPv4' and 'SA/IPv4' have 4-byte pattern 0.0.0.0 in IP address format.
	Submask	Default =0.0.0.0 in IP address format.
	Bitmask	Auto-generated from the **Mask**
	Result	Auto-generated from **IPv4 DA or IPv4 SA** + **Mask**

DA/IPv6 or SA/IPv6 Filter Type

Figure:AFM Module Filter Properties (DA/IPv6 or SA/IPv6 Type) shows the filter properties page for filter types DA/IPv6 or SA/IPv6.

Figure:AFM Module Filter Properties (DA/IPv6 or SA/IPv6 Type)

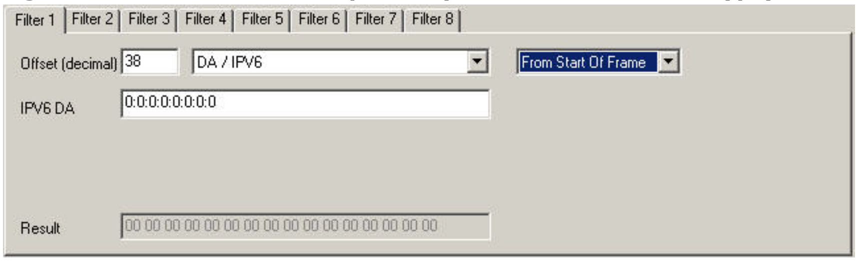


Table:AFM Module Filter Properties (DA/IPv6 or SA/IPv6 Filter Type) provides definitions for the fields to configure the DA/IPv6 or SA/IPv6 filter type..

Table:AFM Module Filter Properties (DA/IPv6 or SA/IPv6 Filter Type)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type. DA/IPv6 default = 38 SA/IPv6 default = 22
	(Filter type)	DA/IPv6 or SA/IPv6

Section	Field/Control	Description
	(Offset mode)	From start of frame (default) or From start of IP
	IPv6 DA or IPv6 SA	The data to be compared by the filters. The length is pre-defined by filter types. 'DA/IPv6' and 'SA/IPv6' have 8-byte pattern 0.0.0.0.0.0.0.0
	Result	Auto-generated from **IPv6 DA or IPv6 SA**

Port Filter Type

The following filter types share the same basic filter configuration elements:

- Dest Port / TCP / IPv4
- Source Port / TCP / IPv4
- Dest Port / TCP / IPv6
- Source Port / TCP / IPv6
- Dest Port / UDP / IPv4
- Source Port / UDP / IPv4
- Dest Port / UDP / IPv6
- Source Port / UDP / IPv6

Figure:AFM Module Filter Properties (Port Type) shows the filter properties page for the filter types listed above.

Figure:AFM Module Filter Properties (Port Type)

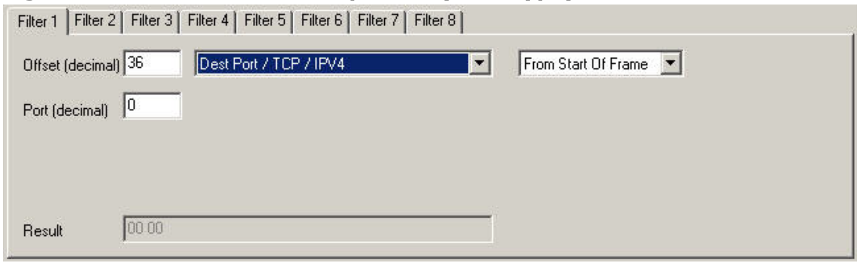


Table:AFM Module Filter Properties (Port Filter Type) provides definitions for the fields to configure the Port filter type..

Table:AFM Module Filter Properties (Port Filter Type)

Section	Field/Control	Description
Filter (1 to 8)	Offset (decimal)	The length of the offset, in bytes. The default setting is determined by the selected Filter type. Dest Port / TCP / IPv4 default = 36 Source Port / TCP / IPv4 default = 34 Dest Port / TCP / IPv6 default = 56 Source Port / TCP / IPv6 default = 54

Section	Field/Control	Description
		Dest Port / UDP / IPv4 default = 36 Source Port / UDP / IPv4 default = 34 Dest Port / UDP / IPv6 default = 56 Source Port / UDP / IPv6 default = 54
	(Filter type)	One of these: • Dest Port / TCP / IPv4 • Source Port / TCP / IPv4 • Dest Port / TCP / IPv6 • Source Port / TCP / IPv6 • Dest Port / UDP / IPv4 • Source Port / UDP / IPv4 • Dest Port / UDP / IPv6 • Source Port / UDP / IPv6
	(Offset mode)	From start of frame (default) or From start of IP
	Port (decimal)	default = 0 (range = 0 to 65535)
	Result	Auto-generated from Filter type and Port

Logic Control

Figure:AFM Module Filter Properties (Logic Control) shows the Logic Control section of the filter properties page.

NOTE

Be careful to set the correct equation based the pre-defined precedence. NOT has precedence over AND, which has precedence over OR (NOT>AND>OR). All equations must end in NONE.

Figure:AFM Module Filter Properties (Logic Control)

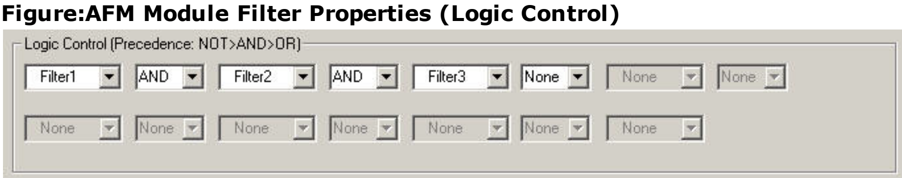


Table:AFM Module Filter Properties Logic Control provides definitions for the fields to configure the Logic Control.

Table:AFM Module Filter Properties Logic Control

Section	Field/Control	Description
Logic Control		Precedence: NOT>AND>OR Use the sequence of lists to construct the logic sequence. Example: F1 AND F2 OR F3 AND !F4 '!Filter ' = NOT Filter
	(First list)	Select a filter (1 through 8) or

Section	Field/Control	Description
		!Filter (NOT Filter)
	(Next list)	Select AND, OR, or None 'None' is used to end the logic sequence.
	(Next list)	Select the next filter or (!Filter) in the logic sequence.

Address Modifiers

All three modifiers will be forced disabled if there is no filter enabled, which means no traffic can pass filters. Any modifier can be enabled if there is at least one filter enabled. When enabling an IPv4 or UDP Destination modifier, set the modifier's offset and offset type.

NOTE The IPV4 DA modifier can be used to modify any packet at any offset, depending on user's setting.

Figure:AFM Module Filter Properties (Address Modifiers shows the Address Modifiers section of the filter properties page.

Figure:AFM Module Filter Properties (Address Modifiers

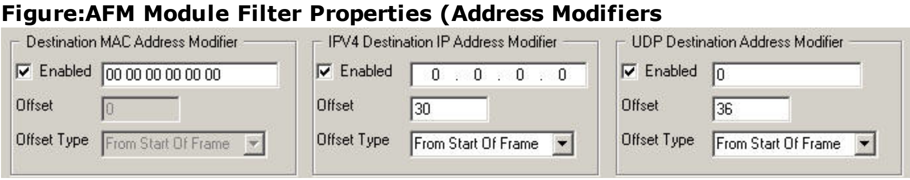


Table:AFM Module Filter Properties (Address Modifiers) provides definitions for the fields to configure the Address Modifiers..

Table:AFM Module Filter Properties (Address Modifiers)

Section	Field/Control	Description
Destination MAC Address Modifier	Enabled	Selecting this check box enables the AFM to modify the Destination MAC Address of the packet. *AFM Packet Modification Feature*. **NOTE** To enable this modifier, any one of the the filters must be enabled (MAC address, IP address, or TCP/UDP).
	Modifier	Enter the new address that will replace the original contents of the Destination MAC address field.
	Offset	Default = 0. The length of the offset, in bytes
	Offset Type	From start of frame (default)
IPv4 Destination IP Address Modifier	Enabled	Selecting this check box enables the AFM to modify the IPv4 Destination IP Address of the packet. *AFM Packet Modification Feature*

Section	Field/Control	Description
		NOTE To enable this modifier any one of the filters must be enabled (MAC address, IP address, or TCP/UDP).
	Modifier	Enter the new address that will replace the original contents of the IPv4 Destination IP address field.
	Offset	Default = 30. The length of the offset, in bytes.
	Offset Type	From start of frame From start of IP
UDP Destination Address Modifier	Enabled	Selecting this check box enables the AFM to modify the UDP Destination Address of the packet. *AFM Packet Modification Feature*. NOTE To enable this modifier any one of the filters must be enabled (MAC address, IP address, or TCP/UDP).
	Modifier	Enter the new address that will replace the original contents of the UDP Destination address field.
	Offset	Default = 36. The length of the offset, in bytes
	Offset Type	From start of frame From start of IP

AFM Packet Modification Feature

The packet modification feature for AFM1000SP-01 enables external monitoring of unicast UDP video streams by replacing, in real time, UDP Video Client addresses in a monitored flow with the addresses of a monitoring device. The packet modification performed by AFM will allow the video monitor to view many different streams, without ever having to change its addresses.

Statistics Tab

The *Statistics* tab allows the selection of which sets of statistics are displayed for the port. The selections available depend on the type of module. For example, the *Statistics* tab for a 10/100/1000 STXS4 (CPU per port) module is shown in *Figure:Statistics Tab (for 10/100/1000 STXS4 module)*. The *Statistics* tab for a 10GE LAN module is shown in *Figure:Statistics Tab (for 10GE LSM module)*. The *Statistics* tab for an ALM1000T8 module is shown in *Figure:Statistics Tab (for ALM1000T8)*.

Figure:Statistics Tab (for 10/100/1000 STXS4 module)

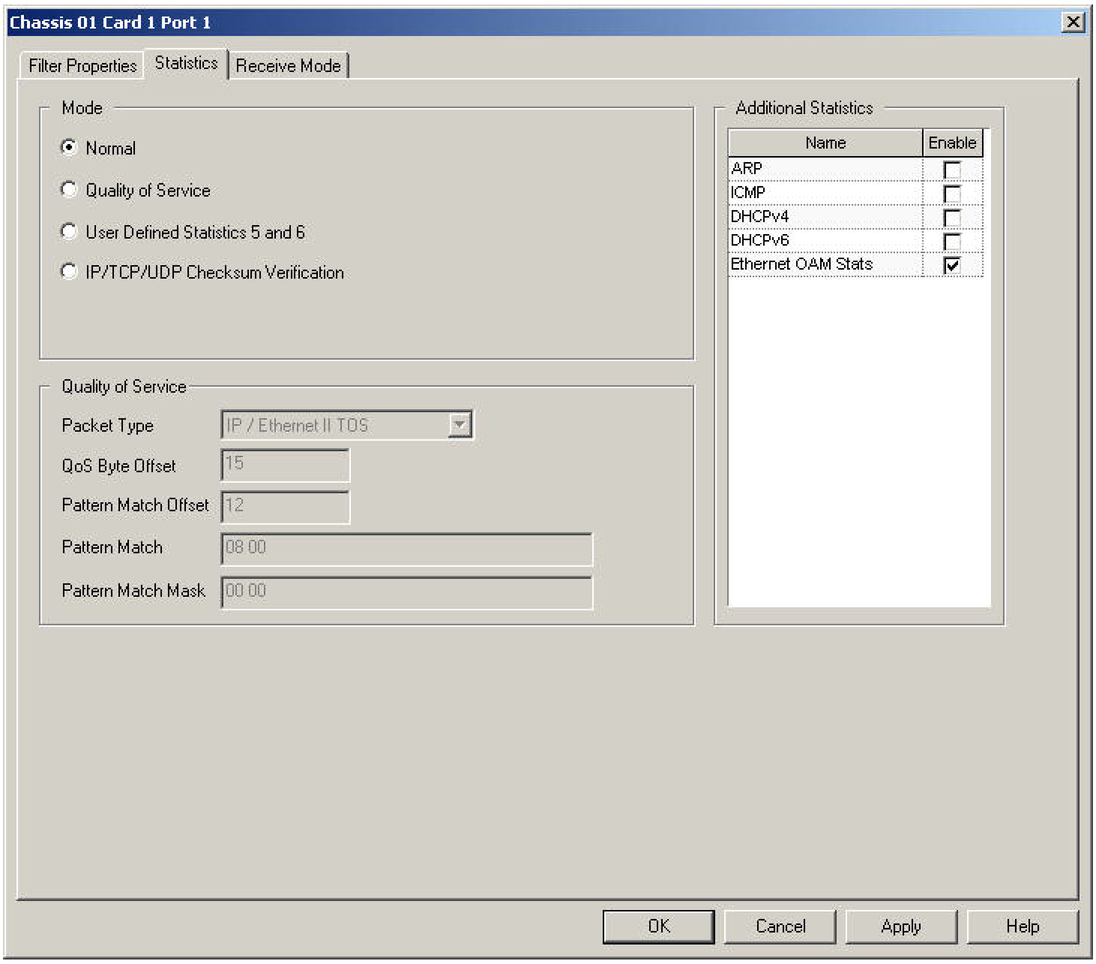


Figure:Statistics Tab (for 10GE LSM module)

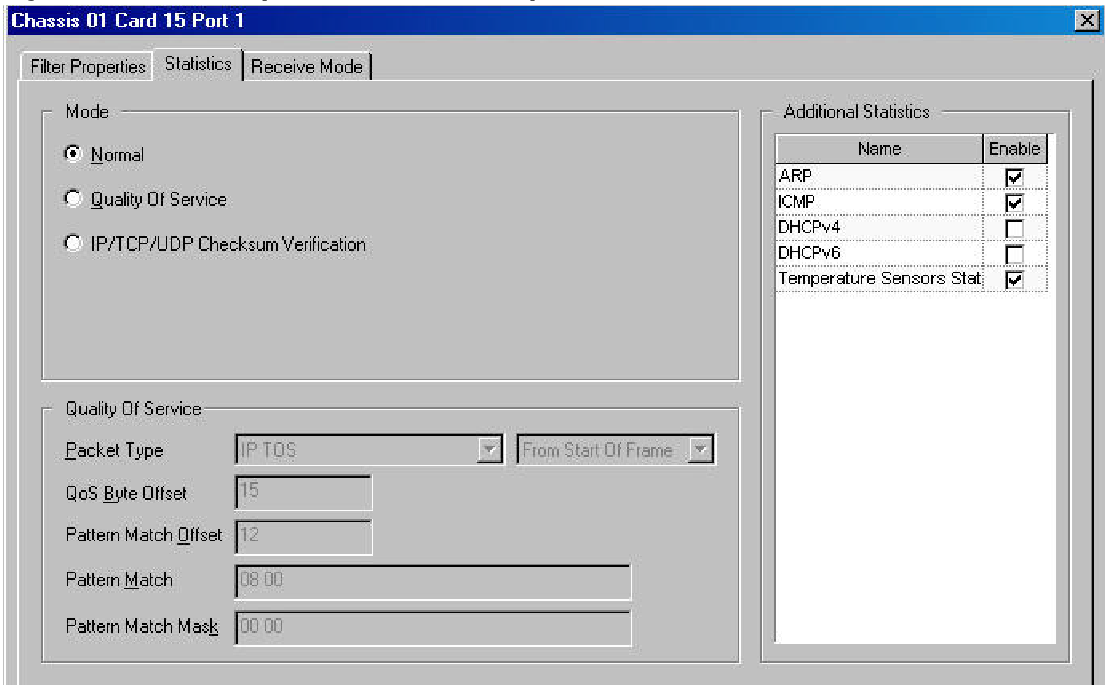


Figure:Statistics Tab (for ALM1000T8)

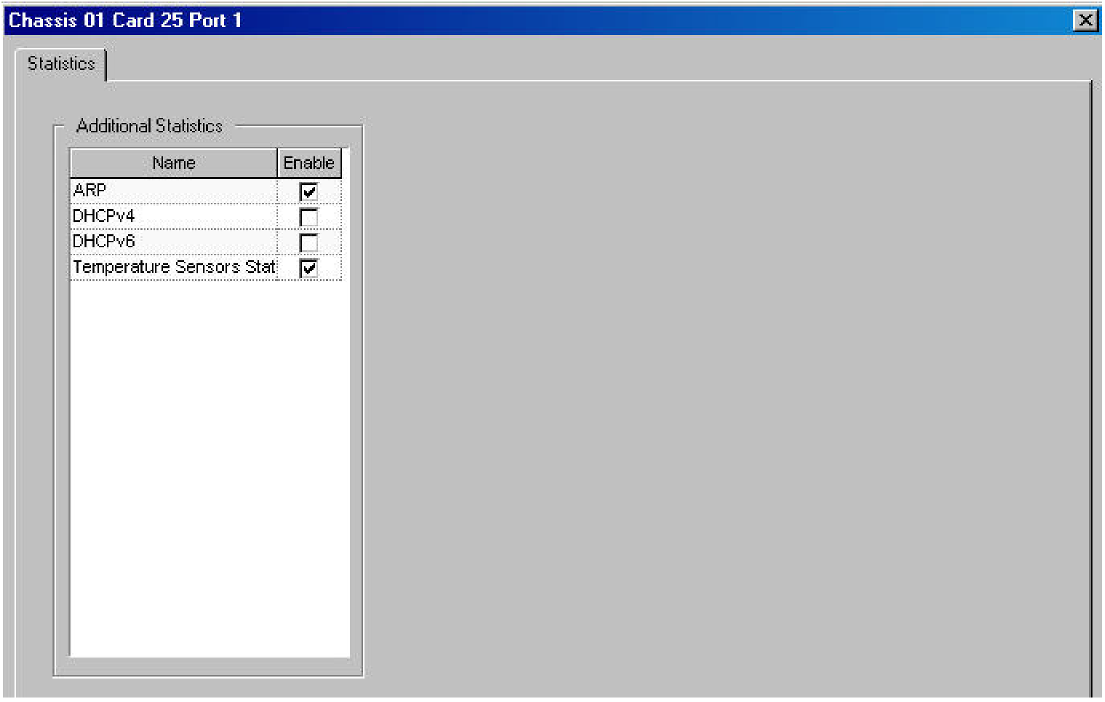
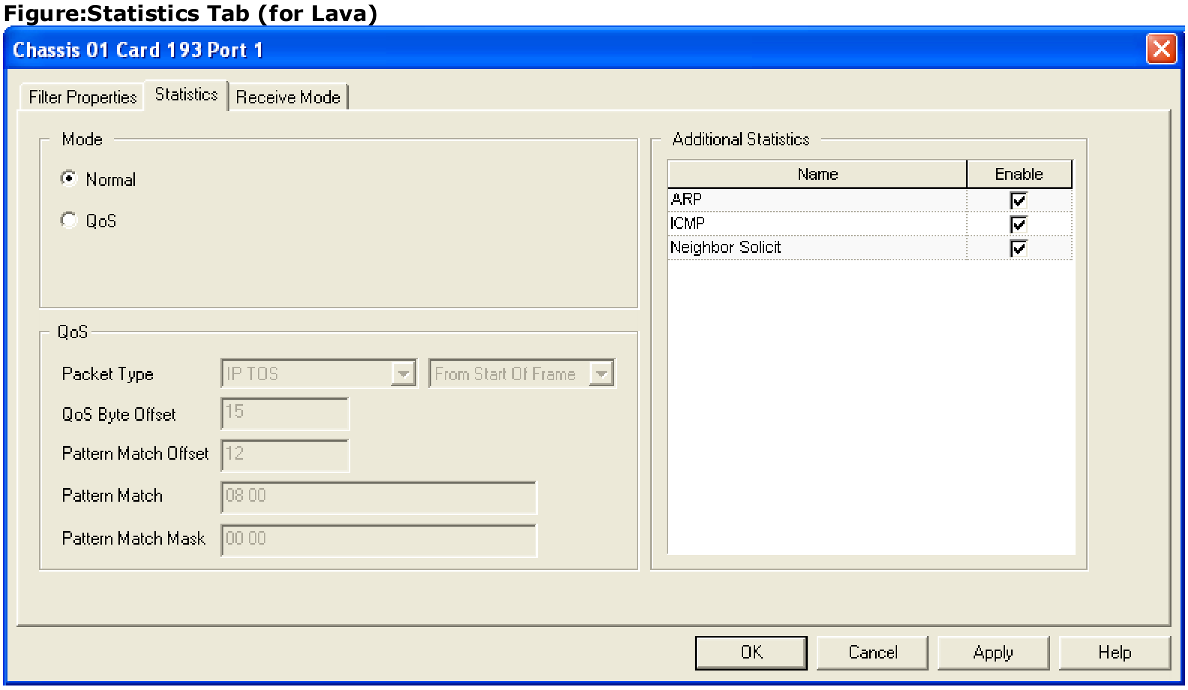


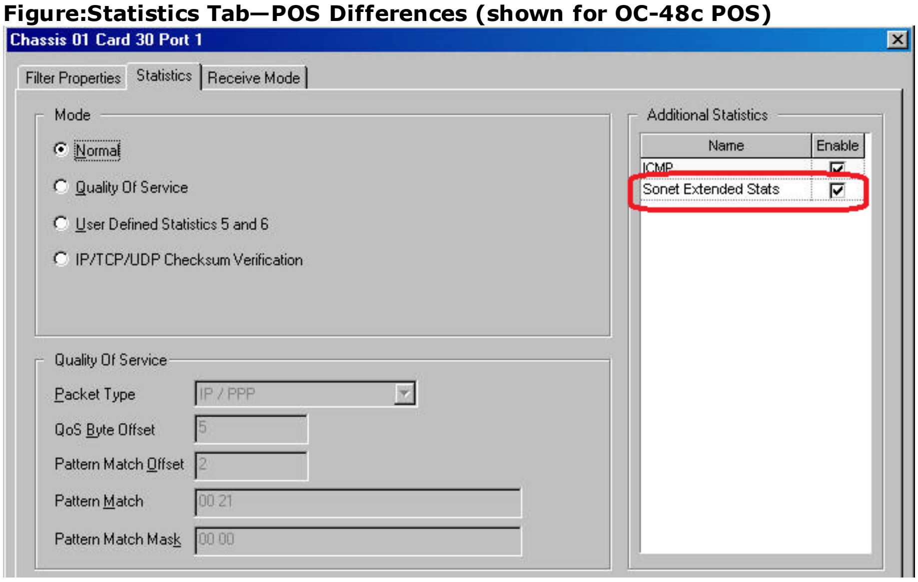
Figure:Statistics Tab (for Lava)



SONET Extended Statistics

The *Statistics* tab for POS and ATM modules includes a *SONET Extended Stats* check box, as shown in *Figure:Statistics Tab—POS Differences (shown for OC-48c POS)*.

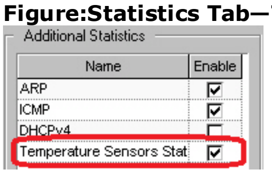
Figure:Statistics Tab—POS Differences (shown for OC-48c POS)



Temperature Sensor Statistics

The *Statistics* tab for OC-192, 10 GE (including LSM and MSM), 2.5G MSM POS, and ALM1000T8 modules includes an additional *Temperature Sensor Stats* check box, as shown in *Figure:Statistics Tab—Temperature Sensor Stats*. This option is enabled by default, so these statistics also appear in Statistic View for the 10GE XAUI/BERT or 10GE XENPAK/BERT modules when set to BERT mode (which makes this *Statistics* tab unavailable).

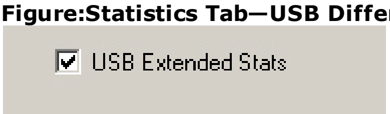
Figure:Statistics Tab—Temperature Sensor Stats



USB Extended Statistics

The *Statistics* tab for USB modules includes an additional *USB Extended Stats* check box, as shown in *Figure:Statistics Tab—USB Differences*.

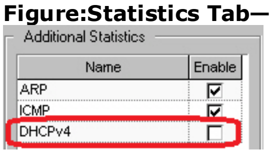
Figure:Statistics Tab—USB Differences



DHCPv4 Statistics

All TXS, 10GE (including LSM and MSM), and ATM POS modules have optional DHCPv4 statistics available in the *Statistics* tab, as shown in *Figure:Statistics Tab—DHCPv4 Stats*.

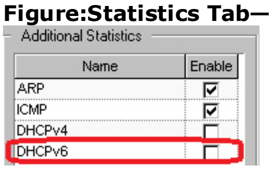
Figure:Statistics Tab—DHCPv4 Stats



DHCPv6 Statistics

All TXS, 10GE LSM, and ATM POS modules have optional DHCPv6 statistics available in the *Statistics* tab, as shown in *Figure:Statistics Tab—DHCPv6 Stats*.

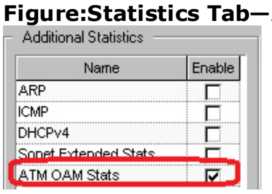
Figure:Statistics Tab—DHCPv6 Stats



ATM OAM Statistics

The ATM POS module has optional ATM OAM statistics available in the *Statistics* tab, as shown in *Figure:Statistics Tab—ATM OAM Stats*.

Figure:Statistics Tab—ATM OAM Stats

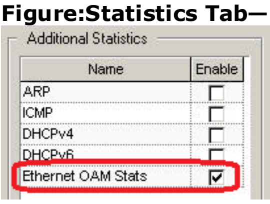


Ethernet OAM Statistics

The following Ethernet load modules have optional OAM statistics available in the *Statistics* tab, as shown in *Figure:Statistics Tab—Ethernet OAM Stats*.

10/100/1000 (S)TX(S)2, 4, 24
1000 SFP(S)4
10/100/1000 XMS(R)12
10/100/1000 LSM XMV(R)4, 16
10/100/1000 ASM XMV12
10GE LSM (XM3, XMR3, XL6) in LAN mode
10G MSM in LAN mode

Figure:Statistics Tab—Ethernet OAM Stats



Statistics Tab Fields

The fields and controls in the *Statistics* tab are described in *Table:Statistics Tab Options*.

Table:Statistics Tab Options

Section	Field/Control	Description
Mode		A set of mutually exclusive choices related to which statistics to accumulate and display.
	Normal	A 'normal' set of statistics.
	Quality of Ser-	Quality of Service statistics are displayed at the expense

Section	Field/Control	Description
	vice (QoS)	of all the User Defined Statistics, Capture Trigger and Filter and several 'normal' statistics.
	User Defined Statistics 5 and 6	UDS 5 and 6 are displayed at the expense of Quality of Service statistics and several 'normal' statistics (this limitation is not true for LSM and MSM modules).
	IP/UDP/TCP Checksum Verification	IP, UDP, and TCP checksums are displayed at the expense of assorted other statistics.
	Data Integrity	Sequence and data integrity errors are selected at the expense of assorted other statistics. Refer to the Sequence Checking Operation and Data Integrity Checking Operation sections in the 'Theory of Operation: Chapter' of the *Ixia Platform Reference Manual* for more information.
Additional Stats	Protocol Server Stats	Statistics related to Protocol Server Transmit and Receive are displayed.
	ARP Stats	Statistics related to sending and receiving ARP requests and replies are displayed.
	ICMP Stats	Statistics related to sending and receiving PING requests and replies are displayed.
	Neighbor Solicit	
	BGP Stats	Statistics related to configuration and establishment of BGP sessions are displayed (only seen if IxRouter is installed).
	OSPF Stats	Statistics related to configuration and establishment of OSPF(v2) sessions are displayed (only seen if IxRouter is installed).
	OSPFv3 Stats	Statistics related to configuration and establishment of OSPFv3 sessions are displayed (only seen if IxRouter is installed).
	ISIS Stats	Statistics related to configuration and establishment of ISIS sessions are displayed (only seen if IxRouter is installed).
	RSVP-TE Stats	Statistics related to configuration and establishment of RSVP-TE sessions are displayed (only seen if IxRouter is installed).
	LDP Stats	Statistics related to the configuration and establishment of LDP sessions are displayed (only seen if IxRouter is installed).
	PIM-SM Stats	Statistics related to the configuration and establishment of PIM-SM sessions are displayed (only seen if IxRouter is installed).
	ATM OAM Stats	Statistics related to the use of ATM OAM cells.
	DHCPv4 Stats	Statistics related to the use of DHCPv4 with protocol interfaces.

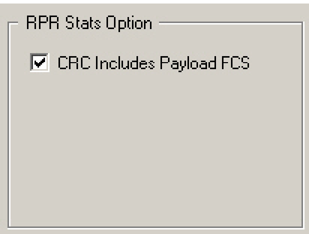
Section	Field/Control	Description
	DHCPv6 Stats	Statistics related to the use of DHCPv4 with protocol interfaces.
	IGMP Stats	Statistics related to the configuration and establishment of protocol server IGMP sessions are displayed.
	SONET Extended Stats	(POS cards only) Statistics related specifically to Packet over SONET are displayed.
	Temperature Sensor Stats	Statistics related specifically to temperature readings on high-powered cards are displayed.
	USB Extended Stats	(USB/Ethernet ports in USB mode only) Statistics related specifically to USB are displayed.
	RPR Stats	*RPR Statistics Option (below).*
	Ethernet OAM Stats	Statistics related specifically to Ethernet OAM are displayed.
Quality of Service Statistics		Settings related to the display of Quality of Service statistics. These are described in *Table:Quality of Service*.

The particular statistics shown for each of the choices is detailed in the 'Available Statistics' appendix of the *Ixia Platform Reference Manual*.

RPR Statistics Option

When Resilient Packet Ring (RPR) is selected for the SONET header, the *Statistics* tab displays an area with an option for enabling RPR Statistics, as shown in *Figure:Enable RPR Statistics*. The check box specifically notes that the RPR frame CRC calculation will include the FCS field of the encapsulated packet in the payload of the RPR frame.

Figure:Enable RPR Statistics

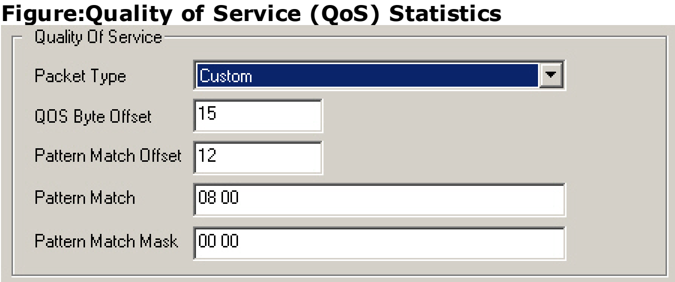


The particular statistics shown for RPR are detailed in 'Available Statistics' appendix of the *Ixia Platform Reference Manual*.

Quality of Service Statistics

The Quality of Service (QoS) fields within the *Statistics* tab are shown in . The *Packet Type* and other parameters in the tab differ, depending on the type of load module.

Figure:Quality of Service (QoS) Statistics



The fields and controls in this tab are described in *Table:Quality of Service.*

Table:Quality of Service

Field/Control	Description
Packet Type (for non-POS modules, except 10 Gigabit modules)	The type of packet is specified. The choices for non-POS modules are: • IP/Ethernet II TOS • IP/IEEE 802.3 SNAP TOS • VLAN User Priority These choices automatically set the values of the remaining tab items to the correct settings for those types of protocols. The final setting is: • Custom This allows for the complete specification of the location of QoS information in a packet. Selecting Custom makes the other fields active, so values can be entered.
Packet Type (for some POS modules) NOTE QoS is not available for OC-192c POS.	The choices for POS modules are: • IP/PPP • IP/CISCO HDLC These choices automatically set the values of the remaining tab items to the correct settings for those types of protocols. The final setting is: • Custom This allows for the complete specification of the location of QoS information in a packet. Selecting Custom makes the other fields active, so values can be entered.
Packet Type (for 10 Gigabit modules)	The choices for 10 Gigabit modules are: • IP TOS—for IP Type of Service (TOS). (Settings for the 8-bit TOS field in the IP packet header.) • VLAN User Priority These choices automatically set the values of the remaining tab items to the correct settings for those types of protocols. The final setting is: • Custom This allows for the complete specification of the location of QoS information in a packet. Selecting Custom makes the other fields active, so values can be entered.
Packet Type (for ATM modules)	The choices for ATM modules are: • IP/ATM This choice automatically sets the values of the remaining tab

Field/Control	Description
	items to the correct settings for those types of protocols. • Custom This allows for the complete specification of the location of QoS information in a packet. Selecting Custom makes the other fields active, so values can be entered.
QOS Byte Offset	The byte offset from the beginning of the packet for the byte which contains the QoS level for the packet.
Pattern Match Offset	The byte offset from the beginning of the packet for the byte (s) that contains a value to be matched. If the pattern is matched, then the packet is deemed to contain a QoS level.
Pattern Match	The value to be matched for at the Pattern Match Offset, subject to the Pattern Match Mask.
Pattern Match Mask	The mask to be applied to the pattern match. '1' values indicate that the corresponding bit is **not** to be matched.

Receive Mode Tab

The *Receive Mode* tab controls the port's receive mode configuration. The format of the dialog changes based on the receive mode(s) selected.

NOTE

The following features are not supported in XDM10G32S load module through IxExplorer:

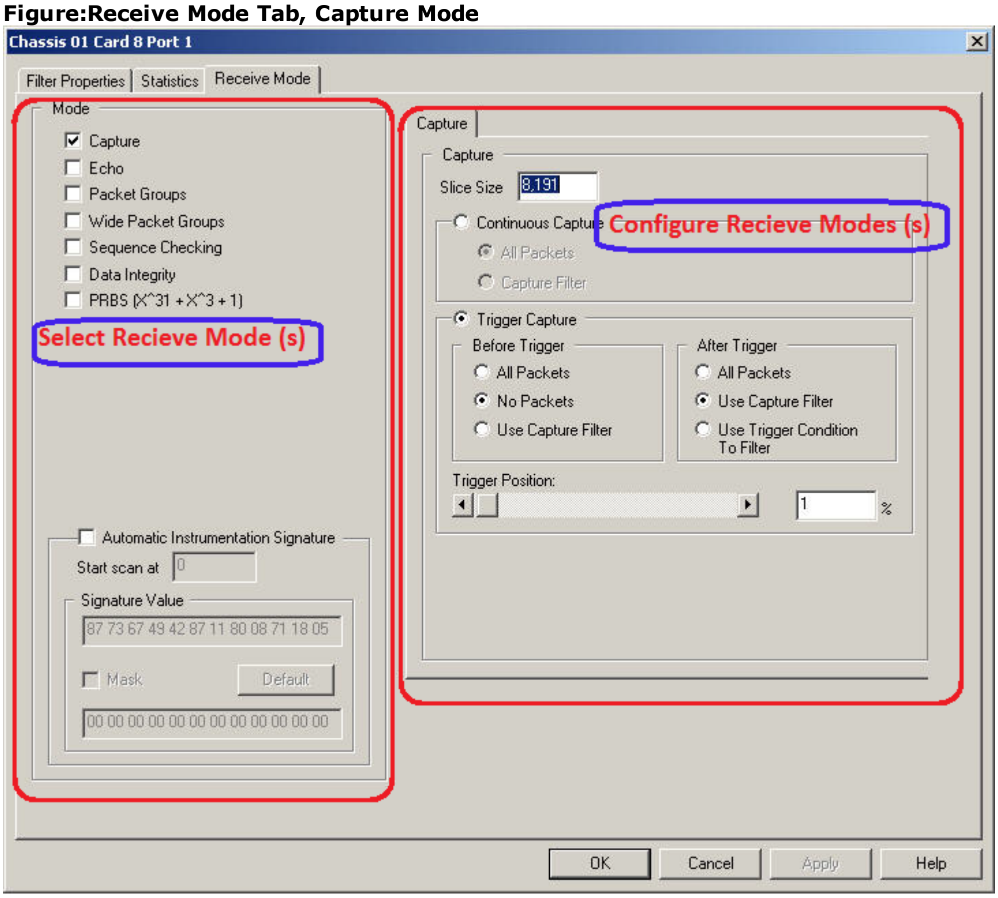
Latency testing

Packet Capture functionality on receive side

PRBS Mode

An example of the *Receive Mode* tab is shown for a port on the 1000 SFPS4 load module in *Figure:Receive Mode Tab, Capture Mode.*

Figure:Receive Mode Tab, Capture Mode



NOTE The Apply changes to all Ports for this chassis check box causes the settings on the Receive Mode tab to be copied to all ports on the current chassis, where applicable.

As shown in *Figure:Receive Mode Tab, Capture Mode*, receive mode configuration consists of two main tasks:

- **STEP 1**—*Select Receive Mode(s)*
- **STEP 2**—*Configure Receive Mode(s)*

Select Receive Mode(s)

The subset of receive mode types displayed in the *Receive Modes* tab is based on the type of port in use. The various types of Receive Modes are listed below:

- *Capture Mode*
- *Echo*
- *Packet Groups*
- *Wide Packet Groups*
- *Sequence Checking*
- *Latency/Jitter (for Lava)*
- *Data Integrity*
- *PRBS Mode*
- *Round Trip TCP Flows*

- *First Time Stamp*
- *ISL Encapsulation*
- *DCC*
- *Automatic Instrumentation Signature*
- *Rate Monitoring*
- *Per PGID Checksum Error Stats*

Refer to the *Ixia Platform Reference Manual* for additional information on card/port capabilities. The receive modes are described in *Table:Receive Modes*.

Table:Receive Modes

Mode	Description
Capture	If selected, the port is set to Capture Mode, in which the buffer memory is used to hold recorded data. For some modules the following options are available on the right side of the screen. • Continuous capture • Trigger Capture *Capture Mode* for additional information.
Packet Groups	If selected, the port is set to Packet Group/Latency/Jitter mode, in which packets are matched according to a signature and then classified in buckets according to Packet Group IDs. *Packet Groups for additional information.*
Sequence Checking	If selected, the port is set to Sequence Checking mode, in which the proper sequencing of packets is selected. Packets are matched according to a signature and then an embedded sequence number is used. For some modules the following options are available on the right side of the screen. • Standard sequence checking • Advanced threshold sequence checking *Sequence Checking* for additional information.
Data Integrity	If selected, the port is set to Data Integrity mode, where a signature must be matched and a CRC is selected. Data Integrity can only be used with Wide Packet Groups on a limited number of load modules (that is, OC-192c load modules). *Data Integrity for additional information.*
Wide Packet Groups	If selected, the port is set to Wide Packet Group mode, in which packets are matched according to a signature, and then classified in bins (buckets) according to Packet Group IDs. NOTE Novus 100GE/25GE supports dual PGID stat mode.

Mode	Description
	NOTE For 100GE the available stats are: • 8k stat • 32K stat For 25GE the available stats are: • 4k stat • 8k stat In the **Novus** module, if **4k stat** is selected in the **Wide Packet Group tab**, the **Switched-Path Duplicate/Gap Checking** and Advance Sequence Tracking options are available. *Wide Packet Groups for additional information.* NOTE When Rate Monitoring mode is selected, Wide Packet Groups is also automatically selected.
Round Trip TCP Flows	If selected, the port is set to Round Trip TCP Flows. *Round Trip TCP Flows* for additional information.
First Time Stamp	If selected, it reflects a port setting made in the IxAutomate (previously IxScriptmate) program. It may be disabled here. *First Time Stamp for additional information.*
ISL Encapsulation	If selected, the port is set for checking ISL encapsulation on the received packets. *ISL Encapsulation* for additional information.
Echo	Before selecting the *Echo* check box in the *Receive Mode* tab, read the following warning: WARNING The following warning message is issued when Echo is selected in the Transmit Modes or Receive Mode tabs: **'Setting this mode on a live network may cause severe problems. All ethernet frames with a DA which matches the Receive Filter DA1 will be 'echoed' back onto the network. Setting this mode will IMMEDIATELY start echoing packets. Are you sure you want to set Echo Mode? Yes or No'** If selected, the receiving port is set for Echo mode. (Available on SFPS4, 10/100/1000 TXS4, Gigabit, GBIC, and Copper 10/100/1000 modules running Gigabit mode). *Echo* for additional information.
DCC	The SONET Data Communications Channel (DCC) option allows capture of DCC packets transmitted in DCC Packet Streams or DCC Advanced Streams.

Mode	Description
	NOTE In the case of two simultaneous channels being transmitted, where both DCC Packet flows and normal SPE packet streams are being transmitted, the user must choose between normal Capture (for the SPE packet streams) or DCC capture (for the flow packets in the DCC channel). *DCC* for additional information.
PRBS	In PRBS mode, both *Wide Packet Groups* and *Sequence Checking* are automatically enabled. In PRBS mode, all latency-related statistics are removed and the following per-PGID statistics are added: • PRBS Bits Received • PRBS Errored Bits • PRBS BER *PRBS Mode*.
Rate Monitoring	In Rate Monitoring mode, the Rate Monitoring tab will display. This tab contains two buttons: View Threshold List and Clear Threshold Timestamp. NOTE When this mode is selected, *Wide Packet Groups* is also automatically selected, and *Sequence Checking* is automatically deselected. Also, the latency mode Inter-Arrival Time is automatically selected (and other latency modes are grayed out).
Per PGID Checksum Error Stats	In Per PGID Checksum Error Stats mode, per-flow checksum error statistics will be provided for Tcp\Udp and IPV4 checksum errors. NOTE When this mode is selected, *Wide Packet Groups* is also automatically selected.

Configure Receive Mode(s)

Detailed explanations of the receive mode configuration for the different types of receive modes are provided in the following sections.

Capture Mode

If *Capture* is selected, the port is set to Capture Mode in which the buffer memory is used to hold received data. There are three main types of Capture mode:

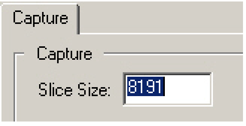
- *Capture Slice ONLY*
- *Small Packet Capture*
- *Continuous and Triggered Capture*

Capture Slice ONLY

When the *Capture Mode* check box is chosen for 10/100 and Gigabit modules, the right-hand side of the dialog is as pictured in *Figure:Capture Mode (shown for 10/100)—Capture*

*Slice **only***, with the *Capture* sub-tab.

Figure:Capture Mode (shown for 10/100)—Capture Slice only



The control available in this sub-tab is described in *Table:Capture Mode—Capture Slice **only***.

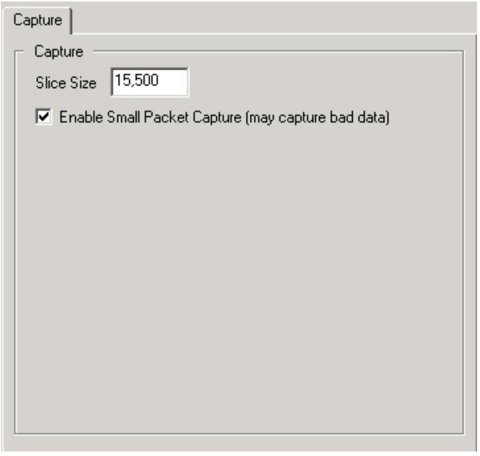
Table:Capture Mode—Capture Slice only

Field	Description
Slice Size	(in bytes) The amount of each packet to be saved in the memory buffer.

Small Packet Capture

The *Capture Mode* sub-tab for older OC-12c/OC-3c POS modules allows the selection of the Small Packet capture option, as shown in *Figure:Capture Mode (shown for Older OC-12c/OC-3c POS)*. When this option is selected, frames smaller than the 'legal' minimum size can be captured. As noted in the *Receive Mode* tab shown in *Figure:Capture Mode (shown for Older OC-12c/OC-3c POS)*, this may result in the capture of bad data.

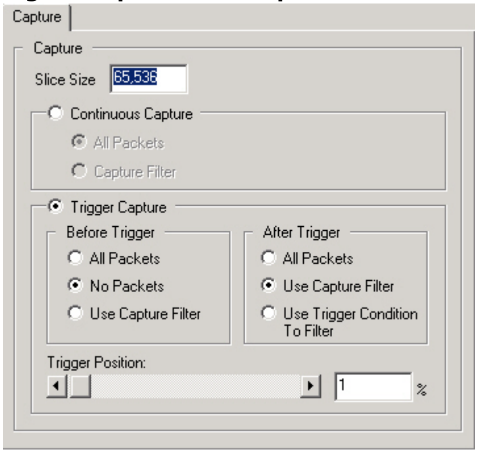
Figure:Capture Mode (shown for Older OC-12c/OC-3c POS)



Continuous and Triggered Capture

The *Capture Mode* sub-tab for a number of other modules, such as the ATM/POS 622 module, includes advanced capture options, as shown in *Figure:Capture Mode Options—Continuous and Triggered Capture*.

Figure:Capture Mode Options—Continuous and Triggered Capture



The fields and controls in this sub-tab are described in *Table:Capture Mode Options* .

Table:Capture Mode Options

Section	Field/Control	Sub-Field/Control	Description
Slice Size			The amount of each packet to be saved in the memory buffer.
Continuous Capture			Select this option button to enable the Continuous Capture option.
	All Packets		Select this option button for continuous capture of all received packets.
	Capture Filter		Select for continuous capture of received packets which match the filter conditions applied.
Trigger Capture			Select this option button to enable the Trigger Capture option. Prior to the Capture Trigger being activated, all received packets are retained in the capture buffer.
	Before Trigger	All Packets	Prior to the Capture Trigger being activated, **all** received packets are retained in the capture buffer.
		No Packets	Prior to the Capture Trigger being activated, **no** received packets are retained in the capture buffer.
		Use Capture Filter	Prior to the Capture Trigger being activated, applies the Capture Filter conditions to all received packets to select which packets will be retained in the capture buffer.
	After Trigger	All Packets	After the Capture Trigger is activated, all received packets are retained in the capture buffer.

Section	Field/Control	Sub-Field/Control	Description
		Use Capture Filter	After the Capture Trigger is activated, applies the Capture Filter conditions to all received packets to select which packets will be retained in the capture buffer.
		Use Trigger Condition to Filter	After the Capture Trigger is activated, applies the trigger conditions to all received packets to select which packets will be retained in the capture buffer.
	Trigger Position	Slider and Percentage (%) field	Used to set the position (% transmitted) in the data stream where the Capture Trigger will be first applied to incoming packets.

NOTE When Continuous Capture is enabled, the Capture Trigger and Capture Trigger statistics do not display. Capture Trigger for more information on the Capture Trigger.

Packet Groups

Packet Groups are created for use with Latency/Jitter testing. When Packet Groups mode is chosen, the right-hand side of the window displays the both the *Packet Groups* sub-tab and the related *Latency/Jitter* sub-tab, as shown in *Figure:Packet Groups/Latency (shown for 10/100 module)*. (Note that when *Packet Groups* check box is selected for many modules, the regular Capture Mode - Capture Slice mode is unavailable.)

The *Packet Groups* and *Latency/Jitter* sub-tabs differ depending on the load module. The sub-tabs for Packet Groups and Latency/Jitter for the varying load modules are described in the following sections:

- *10/100/1000, 10GE Ethernet, and POS modules*
- *OC-48c Packet Groups/Latency Dialogs*
- *Wide Packet Group Inter-Arrival Jitter*

Wide Packet Groups are also available, and are described in *Wide Packet Groups*

Table:Number of PGIDs per Load Module and Feature Use shows the maximum number of Packet Groups a port can process (by load module) for:

- Latency View
- Latency and Sequence View
- Sequence View

The maximum number of PGIDs supported on a port will vary depending on whether packet groups/wide packet groups, sequence checking, or both modes are enabled. Modifying packet group parameters may reduce the maximum number of PGIDs the port supports.

Table:Number of PGIDs per Load Module and Feature Use

Load Module	Packet Groups	Wide Packet Groups	Wide Packet Groups (Wide Bin Mode)	Packet Groups with Sequence Checking	Wide Packet Groups with Sequence Checking	Wide Packet Groups with Sequence Checking (Wide Bin Mode)	Sequence Checking
(S)TX(S)4/2/1 TXS8	65536	65536	131072	128	65536	131072	128
Legacy Ethernet (Gigabit, LM1000T, LM100TX)	57344	N/A	N/A	N/A	N/A	N/A	
LSM 10GE	N/A	65536	2097152	N/A	65536	524288	65536
MSM2.5G POS	N/A	65536	2097152	N/A	65536	524288	65536
MSM10G LAN/WAN	N/A	65536	2097152	N/A	65536	524288	65536
	N/A	65536	2097152	N/A	65536	524288	65536
LM622 ATM	65536	65536	131072	128	65536	131072	128
LM622 POS	65536	65536	131072	128	65536	131072	128
LM10G LAN/WAN	65536	65536	131072	8192	8192	8192	8192
OC192 POS/LM10G POS	1024	65536	131072	1024	8192	8192	1024
OC3/12 POS	57344	N/A	N/A	N/A	N/A	N/A	N/A
OC48 POS	65536	N/A	N/A	512	N/A	N/A	512

CAUTION For OC-192c POS legacy modules (in packet group mode)

When performing latency/jitter measurements, the following restrictions apply:

1,024 or fewer packet group IDs should be used if different frame sizes are used at full line rate.

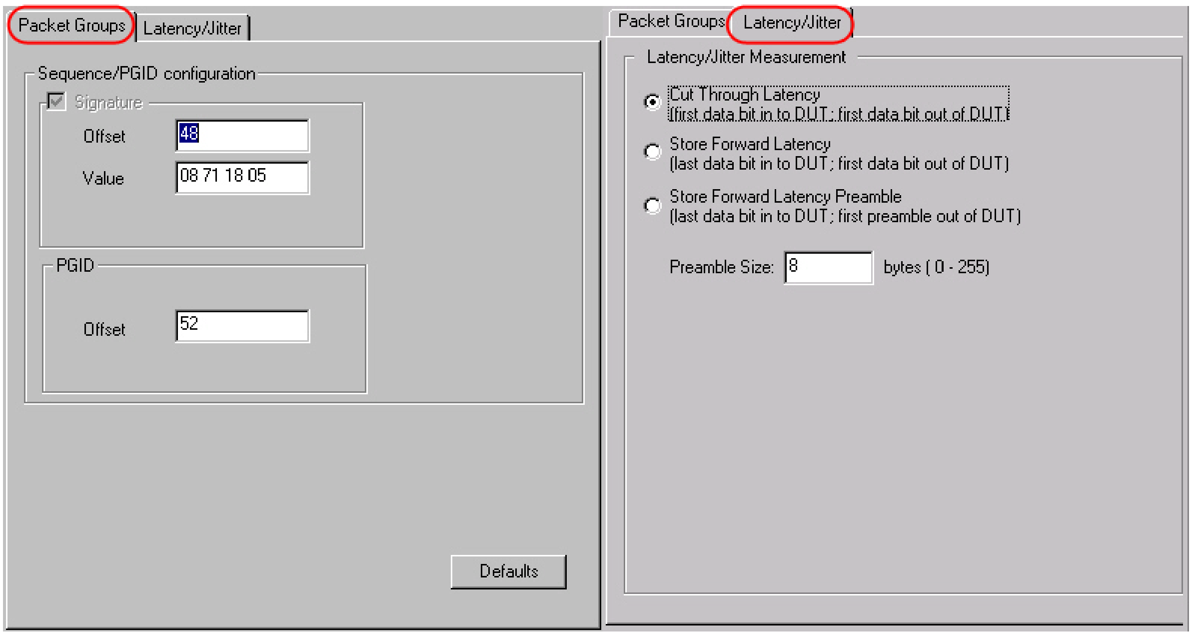
More than 1,024 packet group IDs may be used at line rate and varying frame sizes, so long as the frame sizes are between 256 and 1,024 bytes.

When performing sequence checking, no more than 1,024 packet group IDs should be used.

10/100/1000, 10GE Ethernet, and POS modules

Figure:Packet Groups/Latency (shown for 10/100 module) shows the *Packet Groups* and *Latency/Jitter* sub-tabs for 10/100, Gigabit Ethernet, and POS (including ATM/POS 622) modules.

Figure:Packet Groups/Latency (shown for 10/100 module)



The fields and controls for these sub-tabs are described in *Table:Packet Groups/Latency Configuration*.

Table:Packet Groups/Latency Configuration

Dialog	Field/Control	Description
Packet Group	Signature Offset	(in bytes) The offset within the packet where the 4-byte signature will be found.
	Signature Value	The actual 4-byte value matched against for a signature.
	Group ID Offset	(in bytes) The offset within the packet where the 2-byte packet group ID will be found.
	Defaults	Resets the signature offset, value, and group ID offset to default values.
Latency Measurement	Cut Through Latency (first data bit in to DUT; first data bit out of DUT)	First data bit in to first data bit out. If selected, the time interval between the first data bit out of the Ixia transmit port and the first data bit received by the Ixia receive port is measured.
	Store Forward Latency (last data bit in to DUT; first data bit out of DUT)	(Not available for some modules.) Last data bit out to first data bit in. If selected, the time interval between the last data bit out of the Ixia transmit port and the first data bit received by the Ixia receive port is measured. This option is available on 10/100/1000 and 10GE modules when using Wide Packet Groups, as described in *Wide Packet Groups*. NOTE Store and Forward latency mode is intended to test Store and Forward switching

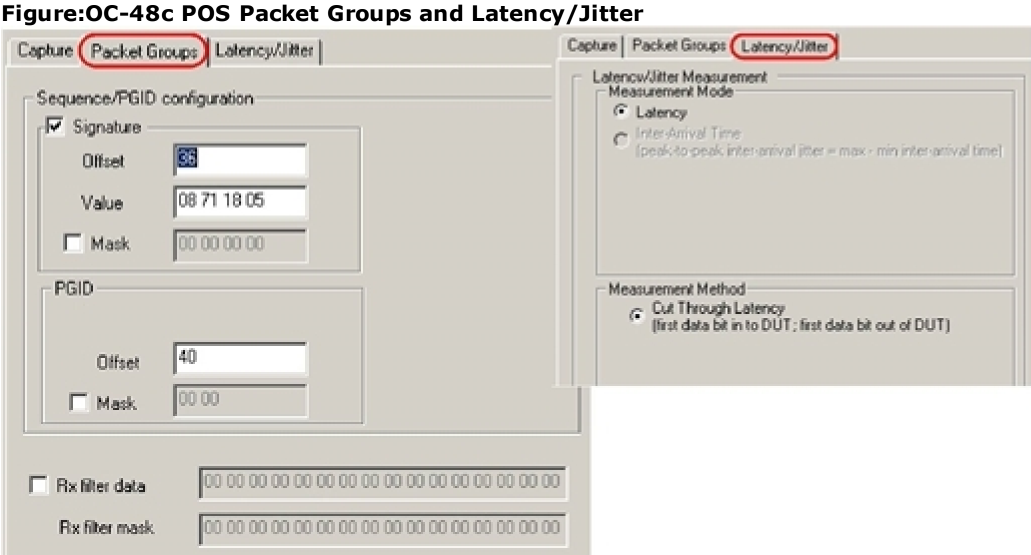
Dialog	Field/Control	Description
		NOTE devices, which receive the entire packet before transmitting it to its destination. If Store and Forward latency is used in loopback, back-to-back or without a Store and Forward switch, then either a zero latency or very high latency will be reported.
	Store and Forward Preamble	(Not available for some modules.) If selected, the time interval between the last data bit out of the Ixia transmit port and the first preamble data bit received by the Ixia receive port is measured
	Inter-Arrival Time (peak-to-peak inter-arrival jitter = max - min inter-arrival time)	(Not available for some modules, only available when using Wide Packet Groups. *Wide Packet Groups* and *Wide Packet Group Inter-Arrival Jitter* for more information.) If selected the time interval between packets in the same PGID is measured.
	Preamble Size	(in bytes) When Store and Forward Preamble is selected, this is the expected size of the preamble. (Displays the value of the Preamble Size set in the *Frame Data* tab of the *Stream Properties* dialog.) Valid range is 0 to 255 bytes.

OC-48c Packet Groups/Latency Dialogs

The *Packet Groups* and *Latency/Jitter* tabs for the OC-48c POS load module ports have some special Receive Mode options available—*Figure:OC-48c POS Packet Groups and Latency/Jitter*.

A user-defined 128-bit data pattern filter can be inserted at the start of the frame, which can filter addresses in the frame header. This filter, as well as the Signature and Group ID, may be masked. (These additional options support the IxProfile feature.)

Figure:OC-48c POS Packet Groups and Latency/Jitter



The fields and controls in these sub-tabs are described in *Table:Packet Group/Latency*.

Table:Packet Group/Latency

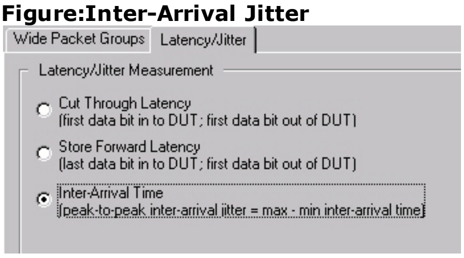
Dialog	Field/Control	Description
Packet Groups Sequence/PGID Configuration	Signature (check box)	When this check box is cleared, the signature fields are disabled (dimmed). This allows all packets to be measured for real-time latency, not just those which contain a specified signature.
	Signature Offset	The offset within the packet where the 4-byte signature will be found.
	Signature Value	The actual 4-byte value matched against for a signature.
	Signature Mask (check box)	When selected, the bit mask used for masking the value in the *Signature* field.
	PGID Offset	The offset within the packet where the 2-byte packet group ID will be found.
	PGID Mask (check box)	When selected, the bit mask used for masking the value in the *Packet Group ID* (PGID) field.
	Rx Filter Data (check box)	When selected, the 128-bit field for filtering packets on the receive side. The Offset for this field is fixed at 0, the beginning of the packet.
	Rx Filter Mask	128-bit mask to be used with the filter data field.
	Defaults	The button resets the signature offset, value and group ID offset to default values, and disables the *Signature Mask*, *Group ID Mask*, the *Rx Filter Data* and *Mask* fields, and leaves *Ignore Signature* check box empty.
Latency/Jitter Measurement Measurement Mode	Latency	Automatically selected when Packet Groups is selected Receive mode.
Latency Measurement Method	Cut Through	Automatically selected when Packet Groups is selected Receive mode. The time interval between the first data bit in to DUT and the first data bit out of DUT.

Wide Packet Group Inter-Arrival Jitter

Some modules have another Latency option when using Wide Packet Groups (*Wide Packet Groups* for more information on Wide Packet Groups), called Inter-Arrival Jitter. It measures the time between arrival of packets in the same PGID.

The Inter-Arrival Jitter option is shown in *Figure:Inter-Arrival Jitter*.

Figure:Inter-Arrival Jitter



This option is only available when using Wide Packet Groups. For more information on Inter-Arrival Jitter, refer to the Latency/Jitter Measurements section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

Sequence Checking

There are three types of Sequence Checking—Standard, Advanced with Threshold Error, and Advanced Sequence Tracking. Availability of the options depends on the type of load module. Refer to the *Ixia Platform Reference Manual* for additional information.

- *Advanced Sequence Checking (for TXS Ethernet, 10 GE, OC-192c, OC-48c, POS 622 (OC-12c/OC-3c POS) load modules)*
- *Standard Sequence Checking (for Copper 10/100/100, older OC-12c/OC-3c modules)*
- *Advanced Sequence Tracking (for LSM XMVDC16, ASM XMV 10/100/1000, LSM XM 10/100/1000, FCM GXM, Xcellon-Flex-AP-10GE, and Xcellon-Flex-AP-Combo-10GE load modules)*

CAUTION For OC-192c POS legacy modules (in packet group mode)—

When performing latency measurements, the following restrictions apply:

1024 or fewer packet group IDs should be used if different frame sizes are used at full line rate.

More than 1024 packet group IDs may be used at line rate and varying frame sizes, so long as the frame sizes are between 256 and 1024 bytes.

When performing sequence checking, no more than 1024 packet group IDs should be used.

Advanced Sequence Checking

Advanced Sequence Checking with Error Threshold is available for some modules. The Sequence Checking sub-tab for Advanced Sequence Checking changes depending on whether Packet Groups or Wide Packet Groups is used.

The sub-tabs for Advanced Sequence Checking are shown in *Figure:Advanced Sequence Checking for Packet Groups* and figure.

Figure:Advanced Sequence Checking for Packet Groups

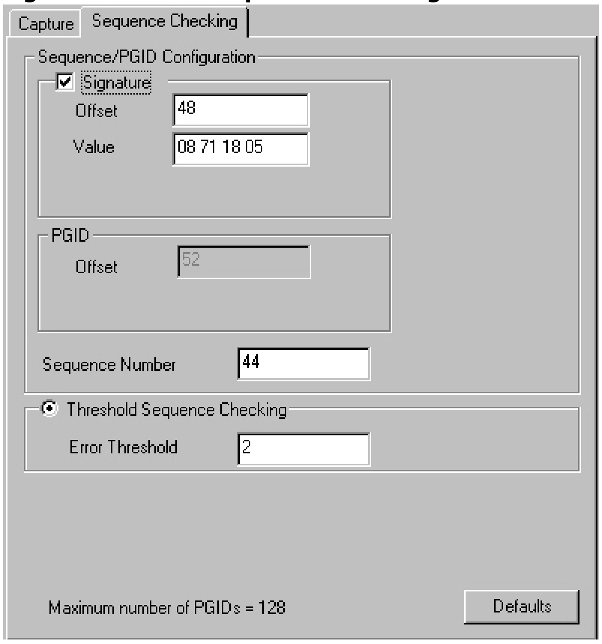
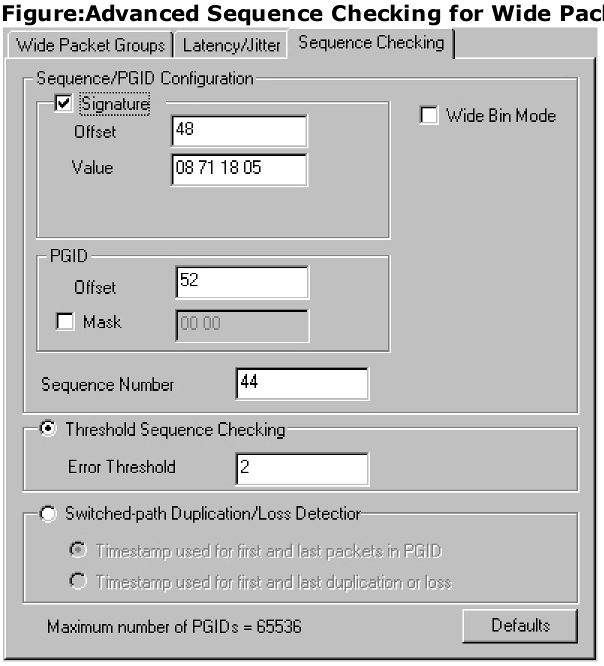


Figure:Advanced Sequence Checking for Wide Packet Groups



The fields and controls in this sub-tab are described in *Table:Advanced Sequence Checking*.

Table:Advanced Sequence Checking

Section	Field/Control	Description
Signature		If not selected, the *Signature Offset* and *Signature Value* fields will be disabled (dimmed). This allows ALL packets to be measured for real-time latency, not just those which contain a specified sig-

Section	Field/Control	Description
		nature.
	Signature Offset	The offset within the packet where the 4-byte signature will be found.
	Signature Value	The actual 4-byte value matched against for a signature.
PGID	Offset	The offset within the packet where the packet group ID (PGID) will be found. NOTE The maximum number of PGIDs for Advanced Sequence Checking is 256 (one-byte field).
	Mask	If selected, the packet Group ID will be masked. If the mask bit = 0, the corresponding bit in the PGID will be used. If the mask bit = 1, the corresponding bit in the PGID will be masked with a '0'.
Wide Bin Mode		(Not available on all modules.) If selected, the 128K Bin mode will be used, where up to 128K PGID bins (time buckets) can used for grouping PGIDs. The maximum length of the Group ID will be increased from 16 to 17 bits. NOTE • In the Novus 100GE module, if you select **8k Stat** the maximum number of PGID is 8192 and if you select **32k Stat** the maximum number of PGID is 32768. • In the Novus 25GE module, if you select **4k Stat** the maximum number of PGID is 4096 and if you select **8k Stat** the maximum number of PGID is 8192.
Sequence Number Offset		The offset within the packet where the 4-byte sequence number will be found.
Threshold Sequence Checking	Error Threshold	The user-configurable threshold value used to determine error levels for

Section	Field/Control	Description
		out-of-sequence, received packets. This option and *Switched-path Duplicate/Gap Checking* are mutually exclusive.
Switched-Path Duplicate/Gap Checking	Record First/Last Packet Arrival Time	Store the timestamp of the first and last packet received for each PGID (and each latency bin). This option and *Error Threshold* are mutually exclusive. Refer to the Switched Path Duplicate/Gap Checking Mode section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.
	Record First/Last Switched-Path Events Time.	Store the first and last timestamp when an error occurs for each PGID (and each latency bin). This option and *Error Threshold* are mutually exclusive.
	Defaults	Resets the signature offset, value and group ID offset to default values.

This sub-tab provides an additional Sequence Checking option, *Sequence Error Threshold*. When the sequence numbers show that the packets are being received in the correct order, it is a 'no error' condition. When the packets are received out of sequence or if packets are missing, sequence errors occur. These errors can be used as a trigger condition for capture, based on a user-configurable threshold value.

There are four sets of error statistic counters per Group ID: Small Errors, Big Errors, Reverse Errors, and Total Errors. These errors are listed in the Packet Group Statistic View for the port. *Packet Group Stats/Sequence Checking Data Display* for additional information. The definitions of the possible error conditions are listed in *Table:Advanced Sequence Checking Error Conditions*.

Table:Advanced Sequence Checking Error Conditions

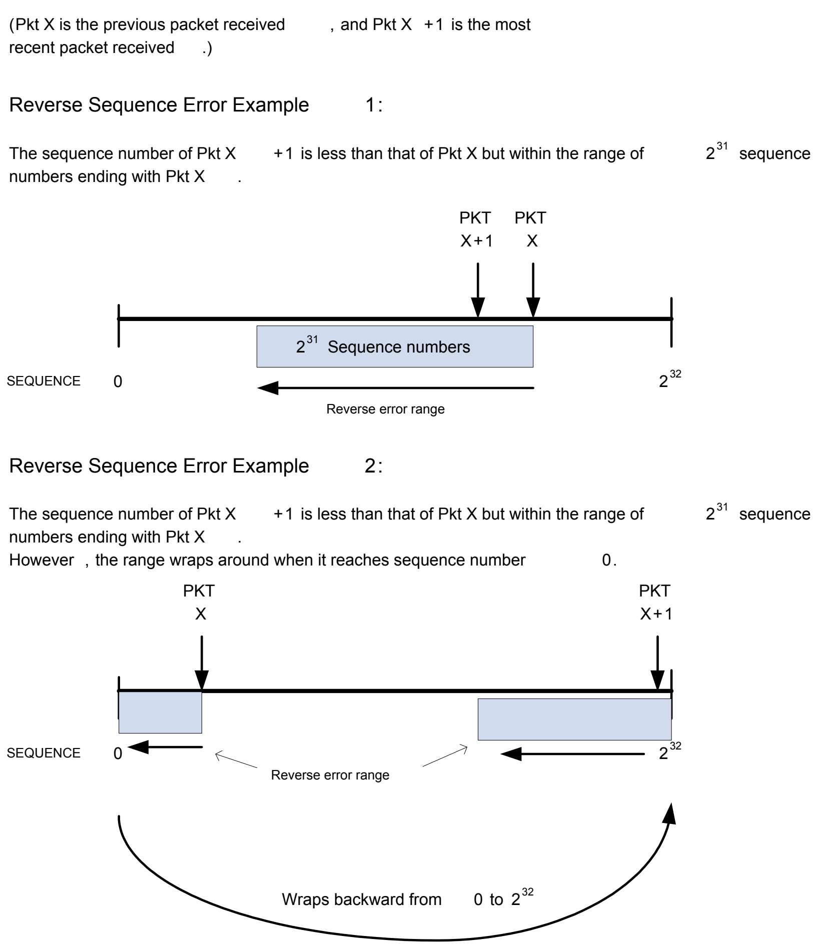
Error	Description
No Error	When the current sequence number is **one** greater than the previous sequence number.
Small Errors	When the current sequence number minus the previous sequence number is less than or equal to the error threshold (set by software) and not negative.
Big Errors	When the current sequence number minus the previous sequence number is greater than the error threshold (set by software) and not negative.
Reverse Errors	A packet received with a reverse sequence error — which is when the current sequence number is less than the previous sequence number, but is still within the 'slid-

Error	Description
	ing window' range of sequence numbers. (*Examples of Reverse Sequence Error* following this table.) **NOTE** The sequence counter can roll over without error — going from sequence number 0x FF FF FF FF to 0 is OK... this is a normal roll-over. Going from 0 to 0x FF FF FF FF (roll-back) is not OK. It is a reverse error.
Total Errors	The sum of all the errors: small, big, and reverse Sequence Checking errors.

Examples of Reverse Sequence Error

The total range of sequence numbers is 4 bytes, or 2^{32} (4,294,967,296). The 'sliding window' is the set of sequence numbers equal to one-half the total 4 byte range (2^{31} or 2,147,483,648), ending with the sequence number of the previous packet. Each time the current sequence number increments, the 'sliding window' moves incrementally. For example, the total range is 4,294,967,296 numbers, and if the current sequence number received is 3,800,000,000 then the 'sliding window' would have started with sequence number 1,652,516,352 (3,800,000,000 minus 1/2 of the total range). When the current sequence number is less than the value of the previous packet's sequence number, but lies within the 'sliding window' range of numbers, it is a Reverse Sequence Error.

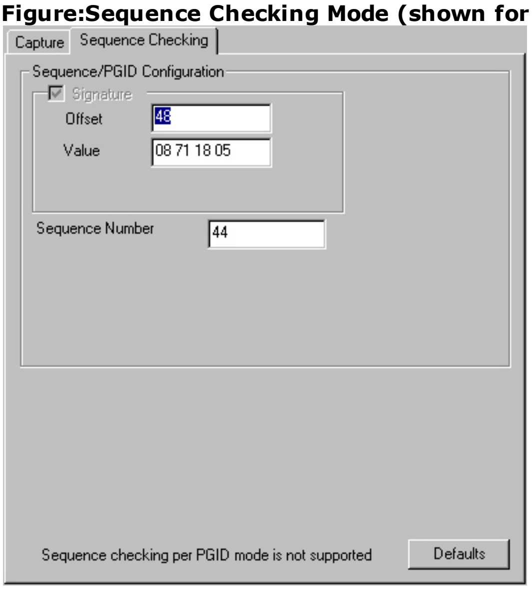
Figure:Reserve Sequence Error, Examples



Standard Sequence Checking

When standard Sequence Checking Mode is chosen, the right-hand side of the *Receive Mode* tab is shown in *Figure:Sequence Checking Mode (shown for a Gigabit module)*, with the *Sequence Checking* sub-tab.

Figure:Sequence Checking Mode (shown for a Gigabit module)



Sequence checking is used to verify that packets are received in the correct order. Refer to the Sequence Checking Operation section in the 'Theory of Operation: General' chapter in the *Ixia Platform Reference Manual* for additional information. The fields and controls in this sub-tab are described in *Table:Sequence Checking Configuration*.

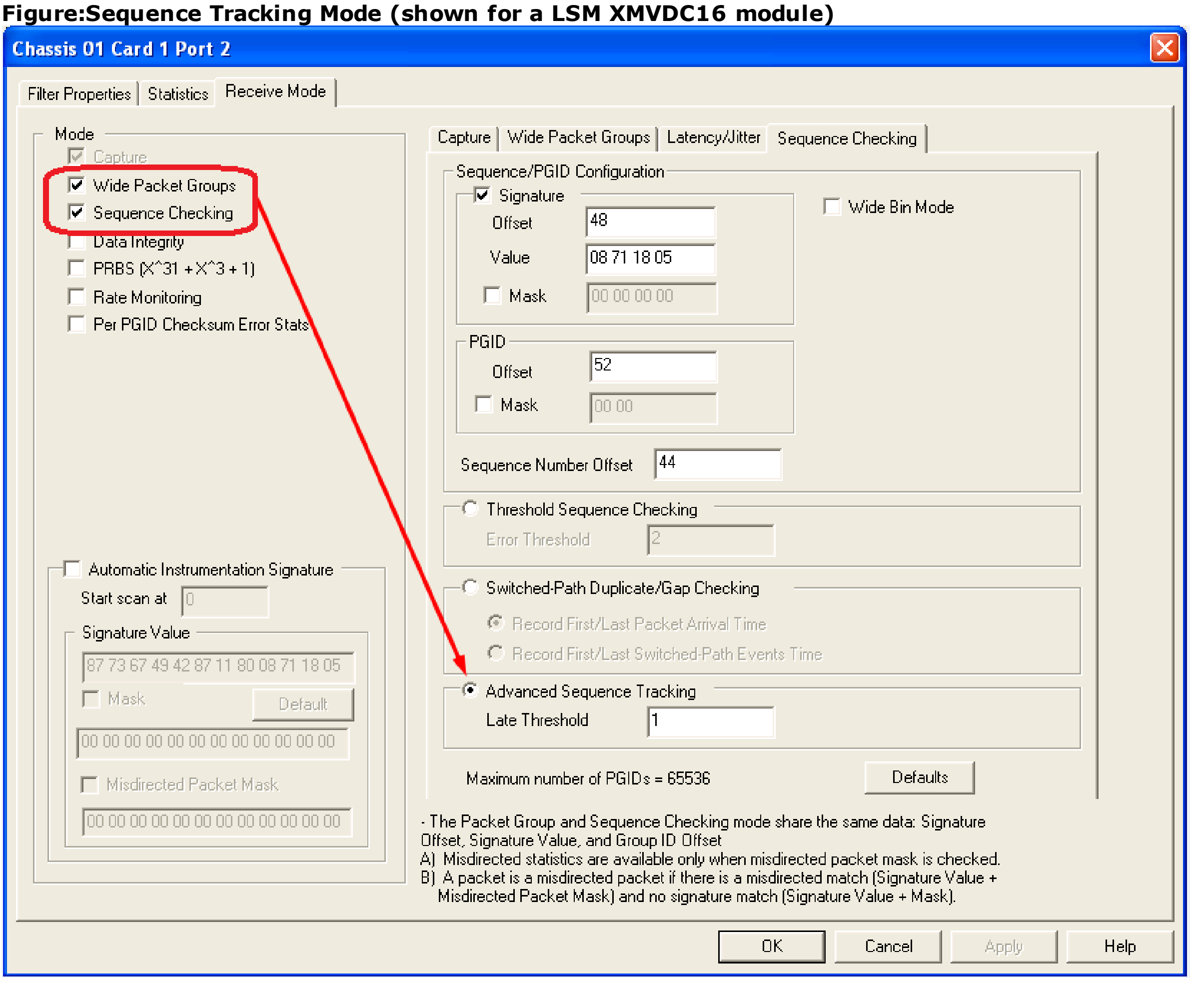
Table:Sequence Checking Configuration

Section	Field/Control	Description
Sequence/PGID Configuration	Signature Offset	The offset within the packet where the 4-byte signature will be found.
	Signature Value	The actual 4-byte value matched against for a signature.
	Group ID Offset	The offset within the packet where the 2-byte packet group ID will be found.
	Sequence Number Offset	The offset within the packet where the 4-byte sequence number will be found.
	Defaults	Resets the signature offset, value and group ID offset to default values.

Advanced Sequence Tracking

When **Wide Packet Groups** and **Sequence Checking** check boxes are selected in the **Receive Mode** port, the **Advanced Sequence Tracking** option is made available in the **Sequence Checking** tab. This mode allows to track a frame by five new statistics.

Figure:Sequence Tracking Mode (shown for a LSM XMVDC16 module)



The fields and controls are described in the following table.

Table:Advanced Sequence Tracking Configuration

Section	Field/Control	Description
Advanced Sequence Tracking	Late Threshold	A fixed value that sets a threshold to track the expected sequence value. The Late Threshold value is subtracted from the expected sequence number when the received sequence numbers are less than the late threshold value. Default value is 1. Maximum value is 19,555. **NOTE** For information on the additional statistic options to track a frame, *Wide Packet Groups/Sequence Checking—Advanced Sequence Tracking.*

Supported Load Modules

Advanced Sequence Tracking support is available for the load modules. The names of the load modules along with the sequence tracking statistics are provided in the following table.

Figure:Advanced Sequence Tracking Statistics

Counter	Normal Mode	Sequence Tracking Mode
10/100/1000 LSM XMVDC16		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
10/100/1000 LSM XMVDC12		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
10/100/1000 LSM XMVDC8		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
10/100/1000 LSM XMVDC4		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
10/100/1000 LSM XMVAE16		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
Xcellon-Ultra XP		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits

Counter	Normal Mode	Sequence Tracking Mode
		Late Packets, 32 bits
		Lost Packets, 32 bits
Xcellon-Ultra NP		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
FlexAP1040SQ		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
FlexAP10G16S		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
NGY-NP8		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4CXP		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4CXP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM40GE12QSFP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits

Counter	Normal Mode	Sequence Tracking Mode
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM10/40GE12QSFP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM10/40GE06QSFP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4CFP4		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4QSFP28		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4CFP4 + ENH		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM100GE4QSFP28 + ENH		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR10GE32SFP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits

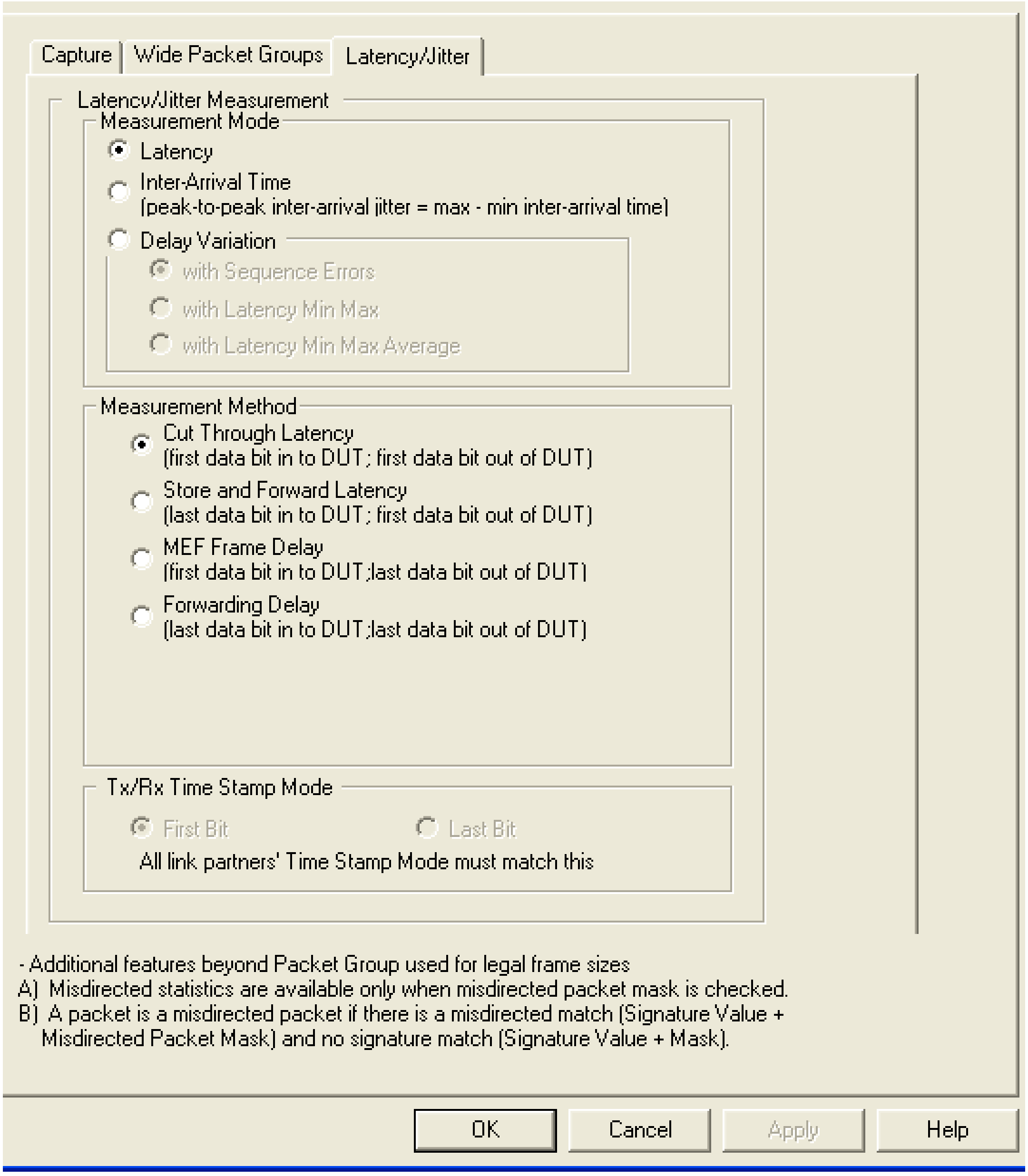
Counter	Normal Mode	Sequence Tracking Mode
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR10GE16SFP + FAN		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR10GE32SFP + FAN + 40G		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR10GE16SFP + FAN + 40G		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR40GE12QSFP+		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XMR40GE6QSFP+		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM10/40GE12QSFP + FAN +10G		
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits
XM10/40GE06QSFP + FAN +10G		

Counter	Normal Mode	Sequence Tracking Mode
	Small Error, 32 bits	In Order Packets, 32 bits
	Big Error, 32 bits	Reordered Packets, 32 bits
	Reverse Error, 32 bits	Duplicate Packets, 32 bits
		Late Packets, 32 bits
		Lost Packets, 32 bits

Latency/Jitter (for Lava)

When the Latency/Jitter mode for Lava is chosen, the right-hand side of the *Receive Mode* tab is as pictured in *Figure:Latency/Jitter (for Lava)*, with the *Data Integrity* sub-tab.

Figure:Latency/Jitter (for Lava)



The fields and controls in the *Latency/Jitter* sub-tab for Lava are described in *Table:Latency/Jitter Configuration for Lava*.

Table:Latency/Jitter Configuration for Lava

Section	Field/Control	Description
Measurement Mode	Latency	
	Inter-Arrival Time	
	Delay Variation	
Measurement Method	Cut Through Latency (first data bit in to DUT; first data bit out of DUT)	First data bit in to first data bit out. If selected, the interval between the first data bit out of the Ixia transmit port and the first data bit received by the Ixia receive port is measured.
	Store and Forward latency (last data bit in to DUT; first data bit out of DUT)	Last data bit out to first data bit in. If selected, the interval between the last data bit out of the Ixia transmit port and the first data bit received by the Ixia receive port is measured. Note: Store and Forward latency mode is intended to test Store and Forward switching devices, which receive the entire packet before transmitting it to its destination. If Store and Forward latency is used in loopback, back-to-back or without a Store and Forward switch, then either a zero latency or very high latency will be reported.
	MEF Frame Delay	
	Forwarding Delay	
Tx/Rx Time Stamp Mode	First Bit	
	Last Bit	

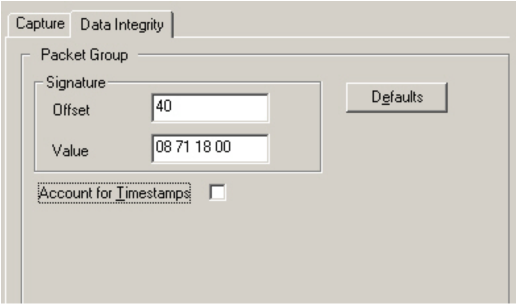
Data Integrity

If selected, the port is set to Data integrity mode, in which packets are matched according to a signature, and then an embedded CRC-16 checksum is selected against the data.

NOTE: Only a limited number of load modules support the use of Data Integrity and Wide Packet Mode simultaneously (that is, OC-192c load modules).

When the Data Integrity mode is chosen, the right-hand side of the *Receive Mode* tab is as pictured in *Figure:Data Integrity*, with the *Data Integrity* sub-tab.

Figure:Data Integrity



The fields and controls in the *Data Integrity* sub-tab are described in *Table:Data Integrity Configuration*.

Table:Data Integrity Configuration

Section	Field/Control	Description
Packet Group	Signature Offset	The offset from the beginning of the packet to the start of the data integrity signature value field.
	Signature Value	The 4-byte value to use as a signature value. Any value may be chosen, but it should be something that is unlikely to appear in 'normal' data, so it is easily recognized when viewing the captured data.
	Defaults	Restores the Data Integrity default settings.
	Account for Timestamps	When selected, the port does not look at the last two bytes of the payload for the data integrity checksum. Instead it looks for the checksum six bytes before the end of the payload to allow for the 48-bit timestamp at the end of the payload. NOTE For floating timestamps, the length of the timestamp is 4 bytes (32-bit) and it will be part of the Auto Instrumentation header, not at the end of the payload. *Auto Instrumentation Tab for Ethernet Modules*.

PRBS Mode

When the Receive Mode is set to Pseudo Random Binary Sequence (PRBS) mode, both *Wide Packet Groups* and *Sequence Checking* are automatically enabled. In PRBS mode, all latency-related statistics are removed and the following per-PGID statistics are added:

- PRBS Bits Received
- PRBS Errored Bits
- PRBS BER

For detailed information, see *PRBS Mode*.

Wide Packet Groups

The *Wide Packet Groups* sub-tab for modules is shown in *Figure:Wide Packet Groups—10/100/1000 Ethernet/ATM Modules*, and *Figure:Wide Packet Groups—10GE Modules for 10GE modules*. When Wide Packet Groups mode is enabled, Instantaneous Latency, Sequence Checking, and First and Last Timestamps, and Data Integrity are available, but not Latency over Time. A frame less than 64 bytes long is invalid in this mode.

NOTE Only a limited number of load modules support the use of Wide Packet Mode and Data Integrity simultaneously (that is, OC-192c load modules).

Certain modules have an additional *Inter-Arrival Jitter* option available on the *Latency/Jitter* sub-tab when using Wide Packet Groups. See *Wide Packet Group Inter-Arrival Jitter* for more information.

When the Wide Packet Groups feature is enabled, the Latency View for this port is modified to display the First Timestamp and Last Timestamp. See *Wide Packet Groups* for additional information on Wide Packet Groups implementation in the Latency View for the port.

The use of the PGID Mask is shown in *Figure:Wide Packet Groups—Group ID Mask*. Note that in this example, 17 bits are used for the Wide Packet Group Mask. However, not all modules are limited to only 17 bits.

Figure:Wide Packet Groups—Group ID Mask

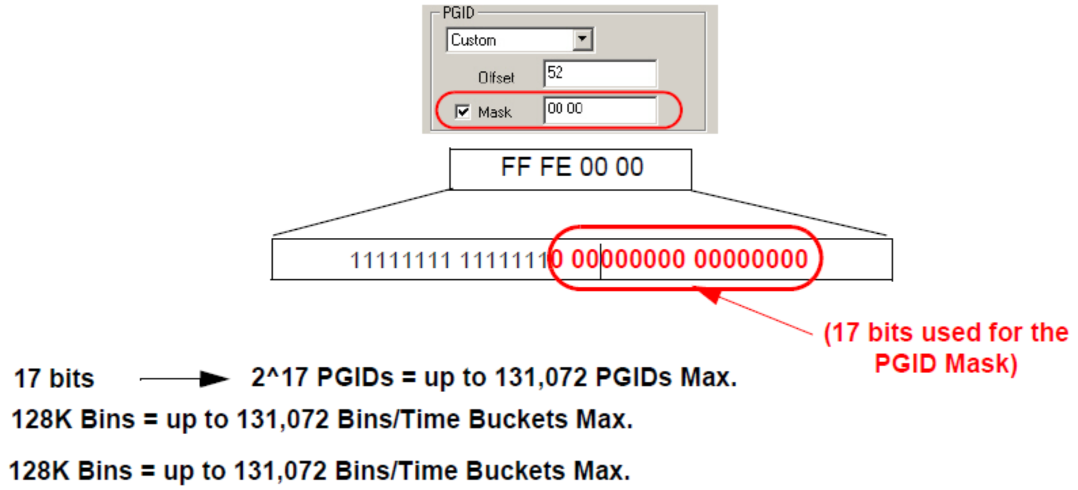
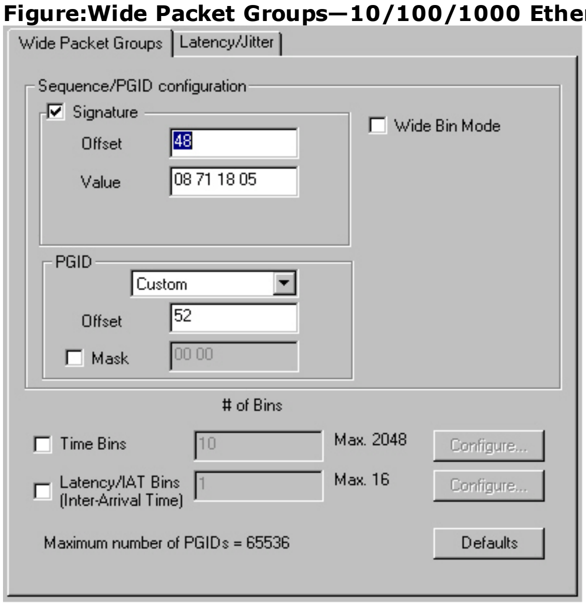


Figure:Wide Packet Groups—10/100/1000 Ethernet/ATM Modules



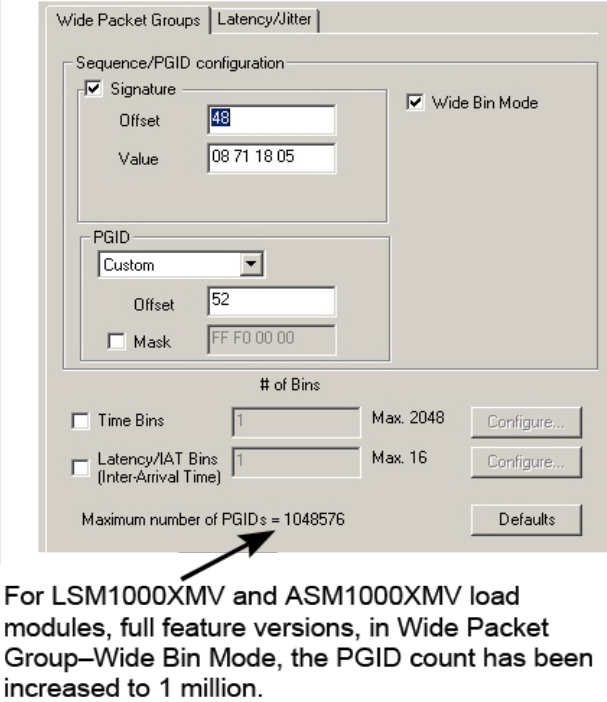
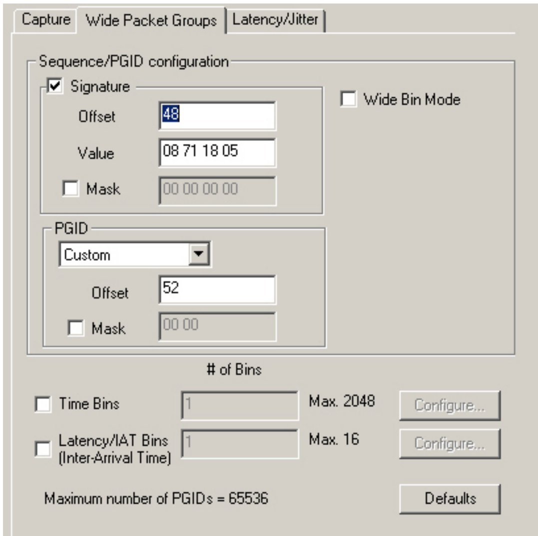


Figure:Wide Packet Groups—10GE Modules



The fields and controls in the *Wide Packet Groups* sub-tab are described in *Table:Wide Packet Groups Configuration*.

Table:Wide Packet Groups Configuration

Section	Field/Control	Description
Sequence/PGID Configuration Signature	Signature (check box)	If cleared, the *Signature Offset* and *Signature Value* fields will be disabled (dimmed). This allows ALL packets to be measured for real-time latency, not just those which contain a specified signature.
	Signature Offset	(in bytes) The offset from the beginning

Section	Field/Control	Description
		of the packet to the start of the data integrity signature value field.
	Signature Value	The 4-byte value to use as a signature value. Any value may be chosen, but it should be something that is unlikely to appear in 'normal' data, so it is easily recognized when viewing the captured data.
	Signature Mask (check box)	When selected, the bit mask used for masking the value in the *Signature* field.
PGID	(pull-down menu)	Select a PGID mode: • Custom • DSCP • IPv6 Traffic Class • MPLS Exp • Split If any option besides *Custom* is selected, the configurable fields are dimmed (they are pre-set to the selected protocol option). If Split is selected, then a Config button appears that allows to configure the split PGID. *Split PGIDs* for more information. NOTE If one of the preset options is selected, it assumes that there is no header information (such as MPLS, GRE, VLAN, and so forth) on the received packet. It looks for the PGID at the preset offset. If such headers are used in the received packet, the PGID offset must be manually adjusted to the correct setting using the *Custom* option.
	Offset	(in bytes) The offset, from the beginning of the packet, where the packet Group ID will be found.
	Mask	If selected, the packet Group ID will be masked. If the mask bit = 0, the corresponding bit in the PGID will be used. If the mask bit = 1, the corresponding bit in the PGID will be masked with a '0.'

Section	Field/Control	Description
Wide Bin Mode	(check box)	(Not available on all modules.) If selected, the 128K Bin mode will be used, where up to 128K PGID bins (time buckets) can used for grouping PGIDs. The maximum length of the Group ID will be increased from 16 to 17 bits. This 17 bit maximum does not apply for the LSM and MSM family of modules.
Time Bins	(check box)	(Not available on all modules.) Selecting this check box activates the Time Bins feature, which can be configured by selecting the *Configure* button. Time Bins are discussed in *Wide Packet Mode Latency/IAT Bins*. The field to the right of this check box allows to set the number of Time Bins to create.
Latency/IAT Bins (Inter-Arrival Time)	(check box)	(Not available on all modules.) Selecting this check box activates the Latency/IAT feature, which can be configured by selecting the *Configure* button. are discussed in *Wide Packet ModeLatency/IAT Bins on. The field to the* right of this check box allows to set the number of Latency/IAT Bins to create.
Defaults		Restores the default settings for this sub-tab.

Wide Packet Mode Latency/IAT Bins

All 10/100/1000, 10 Gigabit Ethernet, and ATM load modules have an added Latency/IAT Bin feature. This allows for greater granularity in collecting latency statistics. Latency/IAT Bin controls set the granularity of the latency or Inter-Arrival Time (IAT) to be monitored (called Latency/IAT Bins).

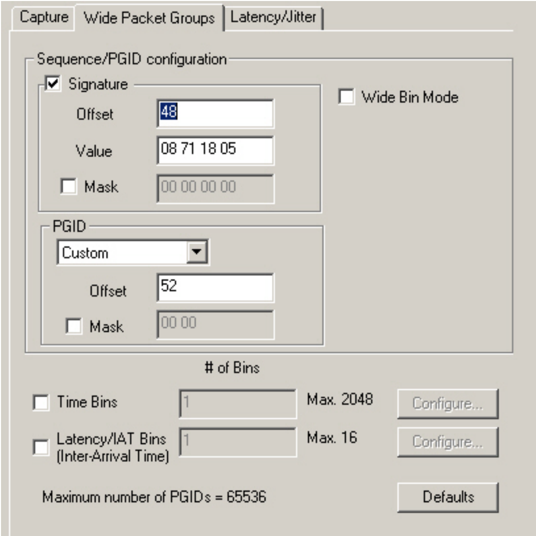
Additionally, the 10/100/1000 Ethernet, LSM, MSM, and LM622 ATM/POS modules have a Time Bin feature, which sets the number of time buckets (bins) and the durations of the buckets.

You can set up to 2048 Time Bins and up to 16 Latency/IAT Bins.

NOTE For a complete explanation of Time Bins, see the Time Buckets explanation in *Latency Type Tab*. The differences between Time Bins and Time Buckets are noted there.

Figure:Wide Packet Groups—10GE Modules shows the added Latency/IAT Bin controls for 10/100/1000 and 10 Gigabit Ethernet load modules.

Figure:Wide Packet Groups—10GE Modules



Over the set number of Time Bins configured, Latency ranges are specified and grouped into Latency/IAT Bins. All latency times recorded are separated into the Bin range in which the time falls.

Most of the controls on the *Wide Packet Groups* sub-tab are described in *Table:Wide Packet Groups Configuration*. The added Latency/IAT Bin configuration options are described in *Table :Latency Bin Configuration Controls below*.

Table:Latency Bin Configuration Controls

Field/Control	Description
Time Bins	Set the number of Time Bins for the latency test. The maximum number is 2048. The higher the number of Time Bins, the lower the number of Packet Group Identifications (PGIDs) that can be assigned to a single Time Bin.
Latency/IAT Bins	Set the number of latency bins for the latency test. The maximum number is 16.
Configure (Time Bins)	Opens the *Time Bins* dialog, which allows the configuration of time bins, as described in *Time Bins Configuration*.
Configure (Latency/IAT Bins)	Opens the *Latency Bins* dialog, which allows the configuration of latency bins, as described in *Latency/IAT Bins Configuration*.

For information on running a latency test using the Latency/IAT Bins, see *Packet Group Statistic View*.

Time Bins Configuration

Time Bins are used as time divisions in a latency test. Time Bins are given specific time values, each of which are added together to make up the entire test time. Each Time Bin can be assigned a set number of Packet Group identification (PGID) numbers, depending on the number of Time Bins. The greater the number of Time Bins, the less PGIDs can be assigned per Time Bin.

Time bins are available on all 10/100/1000 Ethernet, LSM, MSM, and LM622 ATM/POS modules.

NOTE For more detailed information on Time Bins, see *Latency/IAT Bins Configuration* . Time Bins are identical to Time Buckets in function.

The *Time Bins* dialog is shown in *Figure:Time Bins Dialog*.

Figure:Time Bins Dialog

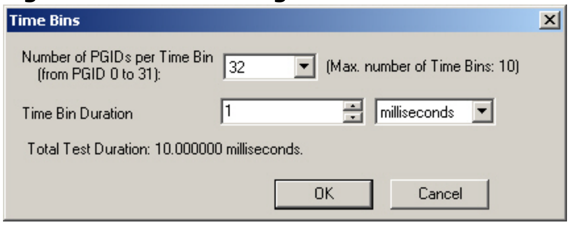


Table:Time Bin Configuration defines the Time Bin configuration controls.

Table:Time Bin Configuration

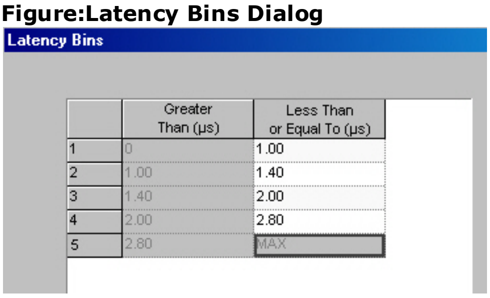
Field/Control	Usage
Number of PGIDs per Time Bin	Select the number of PGID's to be processed per time bin from the list.
Max. Number of Time Bin	The total number of time buckets to be used. (The maximum number of Time Bins available is indicated as a comment displayed next to the *Number of PGIDs per Time Bucket* field.)
Time Bin Duration	The time duration of each time bin. Units of time available are: • microseconds • milliseconds • seconds • minutes • hours

Latency/IAT Bins Configuration

Latency/IAT Bins allow for a more granular look at latency times in a test. Each bin is assigned a latency range in microseconds (for example, greater than 0 to less than or equal to 1). Each latency time recorded is put into a bin based on whether or not it falls into that bin's range.

The *Latency Bins* dialog is shown in *Figure:Latency Bins Dialog*.

Figure:Latency Bins Dialog



For example, using *Figure:Latency Bins Dialog* above, a latency time of 1.5 microseconds would be classified into Bin 3, and a latency time of 2.2 microseconds would be classified into Bin 4.

The controls in the *Latency Bins* dialog are described in *Table:Latency Bin Configuration*.

Table:Latency Bin Configuration

Field/Control	Usage
Greater Than (us)	The lower limit of the Latency/IAT Bin, in microseconds. The latency value must be greater than this number to be included in this Latency/IAT Bin. The Latency/IAT Bin number is shown on the far left.
Less Than or Equal To (us)	The upper limit of the Latency/IAT Bin, in microseconds. The latency value must be less than or equal to this number to be included in this Latency Bin. The Latency/IAT Bin number is shown on the far left. This number can be changed by clicking the field and manually typing in a new value. The new value automatically becomes the Greater Than limit for the next Latency/IAT Bin.

Split PGIDs

Splitting the PGID allows the 32-bit PGID field (used to identify and group packets) to be generated from a concatenation of three separate PGID fields. Instead of having one PGID offset value with one mask, you are allowed to enter up to three separate PGID offsets and masks.

This feature is accessed in the Wide Packet Group mode of the Receive Mode tab.*Figure:Split PGID Configuration* shows the New Split PGID Configuration dialog.

Figure:Split PGID Configuration

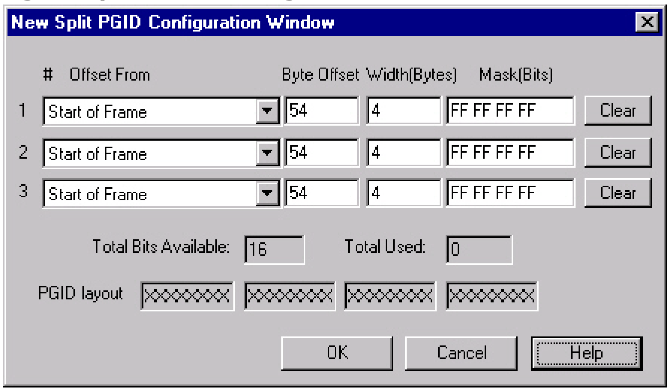


Table:Split PGID Configuration describes the configuration options of the New Split PGID Configuration dialog.

Table:Split PGID Configuration

Field/Control	Description
# Offset From	Where in the packet to start the offset for the PGID split section.
Byte Offset	The offset, in bytes, from the starting point set in # Offset

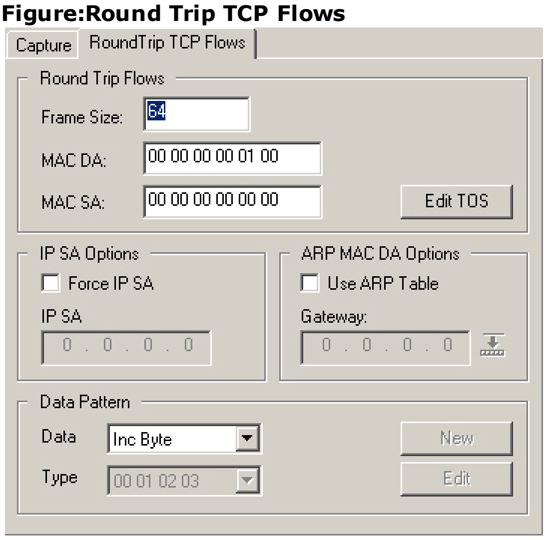
Field/Control	Description
	From.
Width (Bytes)	The number of bytes in the PGID split section.
Mask (Bits)	The PGID mask bits.
Clear	Sets the values of the PGID split section back to their defaults.
Total Bits Available	Remaining bits available for use in the configured split PGID. This number decreases as each split segment is configured.
Total Used	The number of bits used.
PGID Layout	The current configuration of the PGID.

Round Trip TCP Flows

If selected, a port is configured to reflect a received packet with modifications. Only cards supporting 10 or 100 Mbps can be configured for this option. Refer to the Round Trip TCP Flows section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

When Round Trip TCP Flows (RTF) mode is chosen, the right-hand side of the *Receive Mode* tab is as pictured in , with the *Round Trip TCP Flows* sub-tab.

Figure:Round Trip TCP Flows



The fields and controls in the *Round Trip TCP Flows* sub-tab are described in *Table:Round Trip TCP Configuration*.

Table:Round Trip TCP Configuration

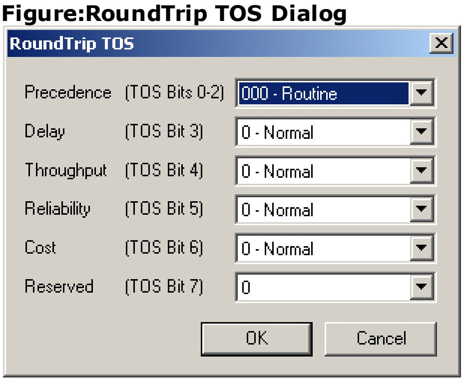
Section	Field/Control	Description
Round Trip Flows	Frame Size	The frame size for outbound reflected packets.
	MAC DA	The destination MAC address used for outbound reflected packets.
	MAC SA	The source MAC address used for outbound reflected packets. This may be overridden through the settings in the *ARP MAC DA Options* category.

Section	Field/Control	Description
	Edit TOS	By checking this box, the *RoundTrip TOS* dialog is displayed. This controls the TOS byte used for reflected packets.
IP SA Options	Force IP SA	By checking this box, the IP address within the packet may be forced for outbound reflected packets.
	IP SA	If the *Force IP SA* box is selected, this address is used in the outbound packet contents.
ARP MAC DA Options	Use ARP Table	Instead of using the constant value in the *MAC DA* field above, a value looked up in the ARP table may be used. Check this box to enable this feature.
	Gateway	The gateway IP address is ARP'd to set the MAC DA.
Data Pattern		Allows for the specification of the background data pattern. The selections and usage is identical to the *Frame Data* tab. Refer to *Data Pattern Box*.

RoundTrip TOS Dialog

When the *Edit TOS* button is clicked, the *RoundTrip TOS* dialog appears, as shown in *Figure:RoundTrip TOS Dialog*.

Figure:RoundTrip TOS Dialog



The fields and controls in this dialog, based on the Type of Service (TOS) bits in the IP header, are described in *Table:Round Trip TOS Dialog Fields*.

Table:Round Trip TOS Dialog Fields

Field/Control	Description
Precedence (TOS Bits 0-2)	Choose one of: • 000 - Routine • 001 - Priority • 010 - Immediate • 011 - Flash

Field/Control	Description
	• 100 - Flash Override • 101 - CRITIC/ECP • 110 - Internet Control • 111 - Network Control
Delay (TOS Bit 3)	Choose one of: • 0 - Normal • 1 - Low
Throughput (TOS Bit 4)	Choose one of: • 0 - Normal • 1 - High
Reliability (TOS Bit 5)	Choose one of: • 0 - Normal • 1 - High
Cost (TOS Bit 6)	Choose one of: • 0 - Normal • 1 - Low
Reserved (TOS Bit 7)	Choose one of: • 0 • 1

First Time Stamp

First Time Stamp is a timing option which is not used in this release of IxExplorer. It is provided in Ixia's IxAutomate (previously IxScriptmate) application. If the box is selected, it reflects a setting which was made in IxAutomate, and this option can be disabled by selecting the *First Time Stamp* check box in the *Receive Modes* tab.

This option is available on TX8 and TXS8 10/100 Ethernet Modules.

ISL Encapsulation

By enabling the ISL Encapsulation option, the receiving port is set to receive packets which are in the proprietary Cisco ISL encapsulation mode.

Echo

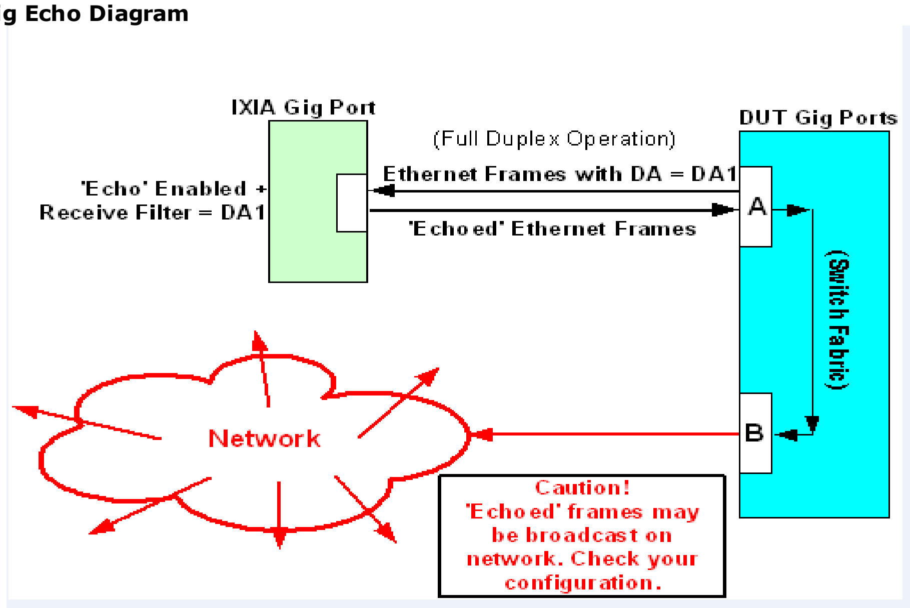
Before selecting the *Echo* check box in the *Receive Mode* tab for a gigabit module, read the following warning.

WARNING The following warning message is issued when Echo is selected in the Transmit Modes or Receive Mode tab:

'Setting this mode on a live network may cause severe problems. All ethernet frames with a DA which matches the Receive Filter DA1 will be 'echoed' back onto the network. Setting this mode will IMMEDIATELY start echoing packets. Are you sure you want to set Echo Mode? Yes or No.'

The gigabit TXS modules (10/100/1000 TXS4 and TX4, 1000 SFPS4 and SFP4, and 10/100/1000 STXS24 and STX24), Gigabit, GBIC, and Copper 10/100/1000 (running in Gigabit mode) load modules offer an additional feature—Layer 2 Echo. This feature operates in conjunction with gigabit rates in full duplex mode, for testing Ethernet loopback mode at up to wire speed. A diagram for the Echo feature is shown in *Figure:Gig Echo Diagram*.

Figure:Gig Echo Diagram



The transmitting side (the DUT) sends simple Ethernet frames. The minimum valid length of an incoming frame is 16 bytes, which includes the MAC DA, MAC SA, and CRC. A preamble of at least 8 bytes must precede the incoming Ethernet frame. The minimum length of a valid incoming frame is 16 bytes (for DA + SA + CRC).

When the frames are received, the MAC DA and MAC SA will be swapped, a standard 8-byte preamble will be inserted for each echoed frame (no matter how long the preamble is on the received frame), and the CRC will be recalculated before the frame is echoed (retransmitted) back. If an incoming frame has a bad CRC, the frame will be retransmitted with a bad CRC. To control the amount of traffic echoed back onto the network, the receiving port will echo ONLY received frames which match a specified DA1 (Destination Address) set to act as a receive filter. *DA/SA Values* for additional information.

The Echo feature will support VLAN-encapsulated Ethernet or SNAP Ethernet frames. *Transmit Modes for Gigabit Modules* for additional information on setting the Transmit Mode to Echo for retransmitting the filtered packets.

DCC

Data Communications Channel (DCC) network management uses the embedded SONET/SDH Operation and Maintenance (OAM&P) channel to manage SONET/SDH networks and devices. The OAM&P channels carry management commands and information, plus alarms, over the OH bytes of the SONET frame. The bytes that make up the DCC channel are:

- For the Section-level DCC (192 Kbps)—D1 to D3 bytes in the Section overhead.
- For the Line-level DCC (576 Kbps)—D4 to D12 bytes in the Line overhead.

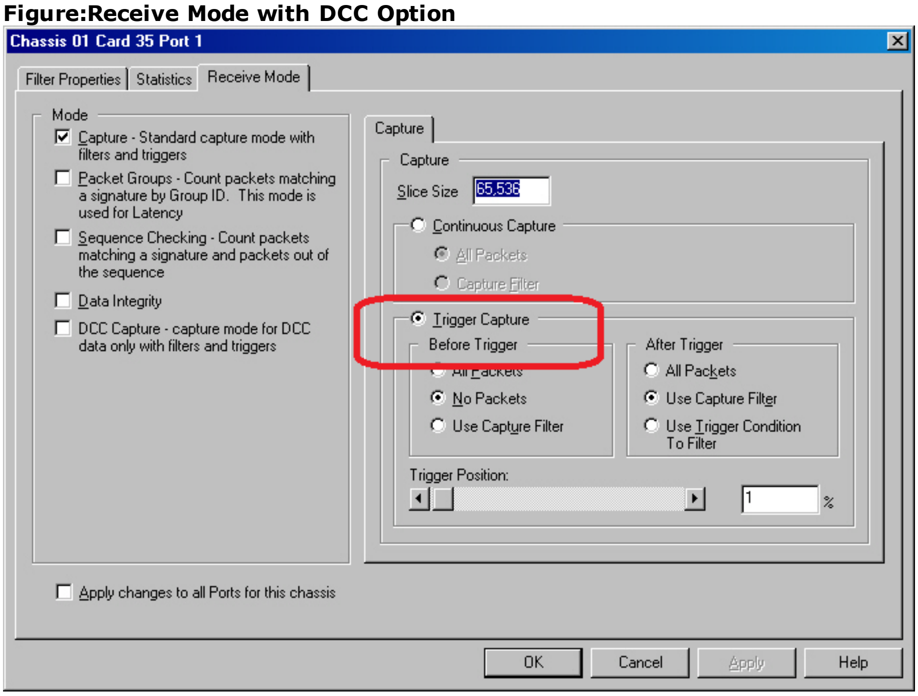
This feature provides access from a remote management workstation to network devices for uses such as:

- Collection of network management information, including alarms
- Remote configuration
- Remote troubleshooting

When control messages are sent from a workstation to a network device through an Ethernet link, it is called 'out-of-band.' When the control messages are sent through the overhead bytes of the SONET frames, it is called 'in-band.'

The *Receive Mode* tab for an OC-192c POS module, with the optional DCC feature, is shown in *Figure:Receive Mode with DCC Option*.

Figure:Receive Mode with DCC Option



If the Transmit Mode for the OC-192c POS port has been set to DCC Packet Streams or DCC Advanced Streams, enable the DCC option for capture of the DCC packets.

NOTE For protocols to work in DCC packet streams, this box MUST be selected. No protocols are supported in DCC flow modes.

If the Transmit Mode has been set to one of the dual-modes, transmitting DCC Packet Flows in addition to normal packet streams in the SPE payload, the packets in only one of the types of streams can be captured upon receipt. If the DCC receive mode is enabled, the normal (SPE) packets will not be captured. If the DCC receive mode is disabled, only the normal packets will be captured.

When the DCC receive mode is enabled, five DCC statistics will be displayed in the Statistic View. See the 'Available Statistics' appendix of the *Ixia Platform Reference Manual*. for additional information.

Automatic Instrumentation Signature

The *Automatic Instrumentation Signature* option of the *Receive Mode* tab allows the receive port to look for a signature at a variable offset from the start of frames. The instrumentation block supports Sequence Checking, Latency, Data Integrity functionality, with signature and Packet Group ID (when *Automatic Instrumentation Signature* is enabled, these receive port options are enabled as well, unless manually disabled).

For more information on Automatic Instrumentation Signature, Instrumentation Box, and see the chapter titled 'Theory of Operation: General' in the *Ixia Platform Reference Manual*.

Figure:Automatic Instrumentation Signature Sub-Tab displays the *Automatic Instrumentation Signature* sub-tab.

Figure:Automatic Instrumentation Signature Sub-Tab

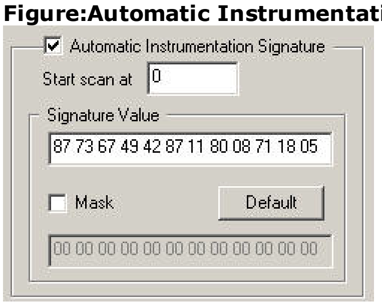


Table:Automatic Instrumentation Signature Configuration explains the configuration options of the *Automatic Instrumentation Signature* sub-tab.

Table:Automatic Instrumentation Signature Configuration

Field/Control	Description
Start scan at	Where to look in the packet for the instrumentation signature.
Signature Value	The data signature that is being matched (12 bytes).
Mask (check box and data field)	The data signature mask.
Defaults	Selecting this button resets the defaults.

Misdirected Packet Detection

All ports use the same signature to trigger the decision to analyze the packet for PGID information. For some load modules, the signature decision has been modified by using a subset of the signature to make the processing decision. If the packet should be processed, the remainder of the signature will be used to determine whether this packet is misdirectied and to increment a counter accordingly, or to proceed with PGID processing. Each Rx port has a separate counter for *Misdirected Packets Received*. See Appendix B *Available Statistics*, in the *Ixia Platform Reference Manual* for information about statistics for all load modules.

The following Ixia load modules can detect misdirected packets:

- LSM10GXM8 (all NGY family)
- LSM1000XMVx16
- ASM1000XMV12

The Automatic Instrumentation Signature block on the Receive Mode tab has added fields, as shown in Figure:Automatic Instrumentation Signature, Misdirected Packets.

Figure:Automatic Instrumentation Signature, Misdirected Packets

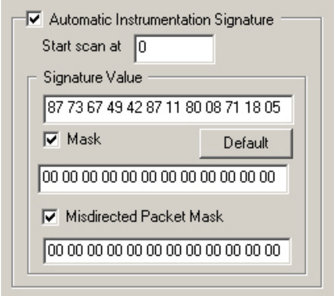


Table:Automatic Instrumentation Signature Configuration, Misdirected Packet explains the configuration options of the *Automatic Instrumentation Signature* sub-tab including the misdirected packet detection.

Table:Automatic Instrumentation Signature Configuration, Misdirected Packet

Field/Control	Description
Start scan at	Where to look in the packet for the instrumentation signature.
Signature Value	The data signature that is being matched (12 bytes).
Mask (check box and data field)	The data signature mask. Used to determine whether the packet is valid for PGID processing.
Defaults	Selecting this button resets the defaults.
Misdirected Packet Mask	check box and data field. Misdirected packet statistics are available only when this is selected. Used to compare the signature value to a valid port ID to identify a misdirected packet. A packet is a misdirected packet if there is a misdirected match (Signature Value + Misdirected Packet Mask) and no signature match (Signature Value + Mask).

Rate Monitoring

The Rate Monitoring *Receive Mode* enables testing convergence times and service interruption from the Ixia load modules.

Rate Monitoring mode is available in the following load modules:

- LSM10GXM family (NGY)
- LSM1000XMV family
- ASM1000XMV12X

When Rate Monitoring mode is selected, Wide Packet Groups is also automatically selected and Sequence Checking is automatically deselected. In Rate Monitoring mode, the only available Latency mode is Inter-Arrival Time.

The Rate Monitoring tab (*Figure:Rate Monitoring Receive Mode*) contains two buttons:

- **View Threshold List**: displays the Threshold Value List, a list of the threshold values with their PGID ranges
- **Clear Threshold Timestamp**: sends a message to the Server to clear threshold timestamps.

It also contains a grayed-out check box **Rate Jitter Filtering**. This check box indicates whether Jitter Filtering has been enabled. It is not enabled using IxExplorer; rather it is enabled using the IxTclHal interface (see *packetGroupThresholdList* command, *enableJitterFilter* option). If enabled, then the Threshold Value List display will be altered. The Threshold value will be shown in packets, and an additional column labeled Filter Window (ns) is added, which displays in nanoseconds.

Two new statistics 'Below Threshold Timestamp' and 'Above Threshold Timestamp' are available when in Rate Monitoring mode. *Rate Monitoring Mode*.

Figure:Rate Monitoring Receive Mode

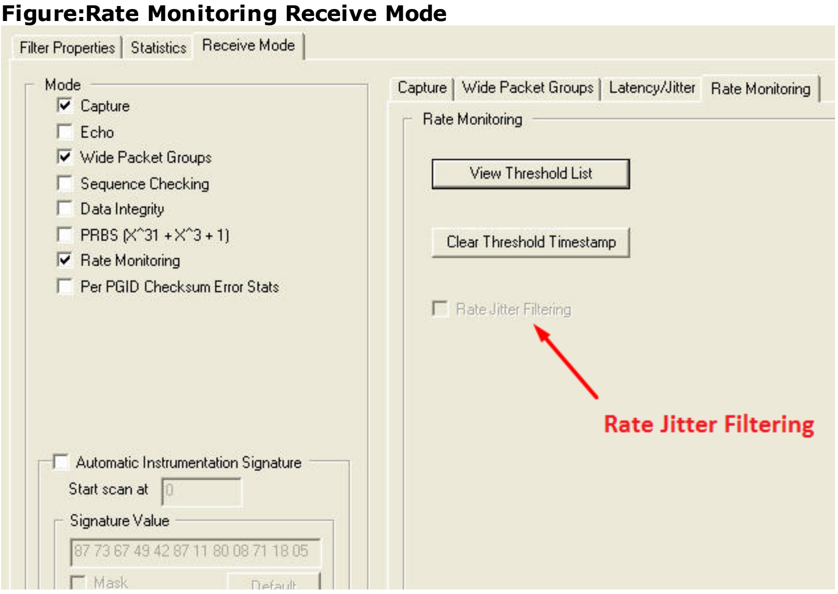


Table:Rate Monitoring Receive Mode

Field/Control	Description
View Threshold List	Displays a list of the threshold values with their PGID ranges
Clear Threshold Timestamp	Sends a message to the Server to clear threshold timestamps
Rate Jitter Filtering	(read-only) If enabled (using IxTclHal), the Threshold Value List will show Threshold in packets and Filter Window in nanoseconds.

Threshold Value List

Click the**View Threshold List** button to display the Threshold Value List.

Figure:Threshold Value List

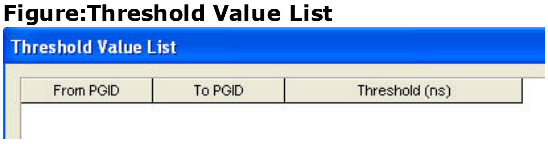


Table:Threshold Value List

Field/Control	Description
From PGID	the sequence number of the PGID at the start of the range
To PGID	the sequence number of the PGID at the end of the range
Threshold	if Rate Jitter Filtering is OFF, this number (in nanoseconds) is the threshold for the Inter-Arrival Time (latency) of a PGID or a range of PGIDs. If Rate Jitter Filtering is ON, its units become packets instead of nanoseconds.
Filter Window	(Only present if Rate Jitter Filtering is ON.) Specifies the filter window, in nanoseconds.

Per PGID Checksum Error Stats

The Per PGID Checksum Error Stats *Receive Mode* enables collection of per-flow checksum error statistics.

This mode is available in the following load modules:

- LSM10GXM family (NGY)
- LSM1000XMV family
- ASM1000XMV12X

If enabled, the following statistics will be included (in Packet Group Statistic View):

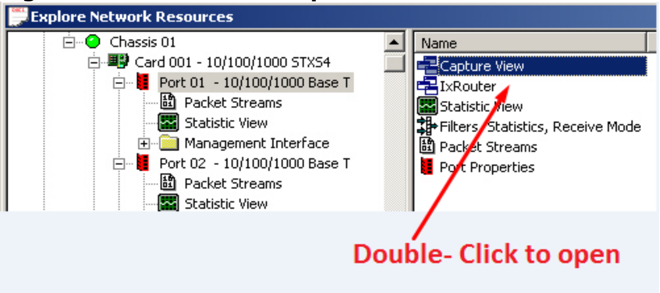
- IPv4 Checksum Errors
- UDP Checksum Errors
- TCP Checksum Errors

Chapter 14 - Capture View

Capture View Window

Capture View enables captured data to be viewed. Capture View is selectable from the Resource Details view when a port has been selected, as shown in *Figure:Port Resources Capture View*.

Figure:Port Resources –Capture View

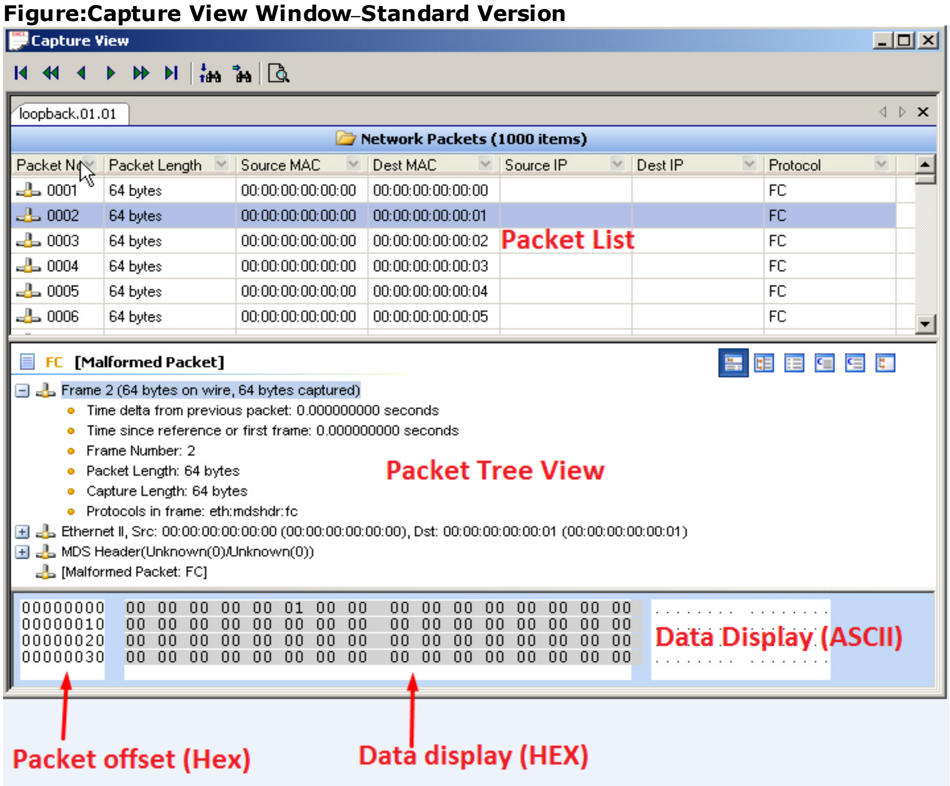


The Capture Trigger and Capture Filter (as described in *Capture Trigger and Capture Filter) for that port determine which packets are 'allowed' into the Capture View. The slice size of the port (see Configure Receive Mode(s)) sets the number of bytes captured and decoded for each packet. If the slice size is less than the packet length, not all of the packet will be available for review, analysis, and conversion. The timestamp, frame length, and status values for the packet are not affected by the slice size, however.*

Refer to the *Port Data Capture Capabilities* section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for additional information on captured data.

The *Capture View* window has two variations, one for standard capture view and one for PRBS capture mode. The standard variation is shown in *Figure:Capture View Window–Standard Version*. The PRBS capture mode is shown in *Figure:Capture View Dialog–PRBS Version*.

Figure:Capture View Window–Standard Version



The standard *Capture View* window is split into panels, from top to bottom. These are described in *Table:Capture View Dialog Windows*.

Table:Capture View Dialog Windows

Window	Contents
Packet List (upper)	Packet List: A list that contains columns for a packet number, packet length, the destination address, the source address, timestamp data, and the error status of the frame. These fields are described in *Table:Capture View– Packet List Fields*.
Packet Tree View (lower)	Packet Tree View, expandable to show the parameters of the selected packet..
Hex and ASCII Data	Hexadecimal and ASCII byte display of the contents of the selected packet

Packet List

The top portion of the *Capture View* contains a summary view of each frame captured. The fields shown in this display are described in *Table:Capture View– Packet List Fields*.

Table:Capture View– Packet List Fields

Heading	Contents
Packet No.	The sequential frame number captured. Depending on the *Capture Filter* *settings, these may not be sequentially received packets.*
Packet Length	The length of the packet, in bytes. Ethernet II packets use this for the *Type* field, while 802.3 SNAP packets use this for the Length

Heading	Contents
	field.
Source MAC	The Source MAC Address, exclicked in hexadecimal.
Dest MAC	The Destination MAC Address, exclicked in hexadecimal.
Source IP	The Source IP that is configured for traffic in transmit side.
Dest IP	The Destination IP that is configured for traffic in receive side.
Protocol	The protocol that is configured on the transmit side.
Status	The status of the received packet. The possible status conditions are shown in *Table:Capture View Status* (below).
Time Stamp - from last clear	Time stamp shows amount of time since last *clear* (when counter was reset to zero)
Time Stamp - relative to previous	Time stamp relative to the preceding packet (preceding row).
Time Stamp - relative to first	Time stamp relative to the first packet (first row).

The possible status conditions vary with module type. *Table:Capture View Status* describes the types of errors.

Table:Capture View Status

Error	Description
Any	Any good or bad packet.
Good Packet	A good packet is matched.
Bad CRC	A packet with a bad CRC.
Bad Packet	A frame with one or more of the following defects: • Bad CRC • Alignment Error–Ethernet only • Dribble Error–Ethernet only • Fragment–Ethernet only • Undersize–Ethernet only, less than 64 • Oversize–Ethernet only, if frame greater than 1588 (non-VLAN), or greater than 1522 (VLAN)
Alignment	A packet with an extra nibble, with bad CRC.
Dribble	A packet with an extra nibble, but with good CRC.
Bad CRC/Alignment/Dribble	Combination of: Bad CRC, Alignment, and Dribble errors.
Line Error	A packet received with symbol errors with either a good or bad CRC.
Line Error & Bad CRC	A packet received with symbol errors with a bad CRC.
Line Error & Good CRC	A packet received with symbol errors with a good CRC.
Core Header	**(GFP ONLY)** A GFP packet received with Core Header information.
Type Header	**(GFP ONLY)** A GFP packet received with Type Header information.

You can advance between all of the captured frames using various keys and the icons at the top of the screen that simulate tape transport controls, as described in *Table:Capture View Window Operations*.

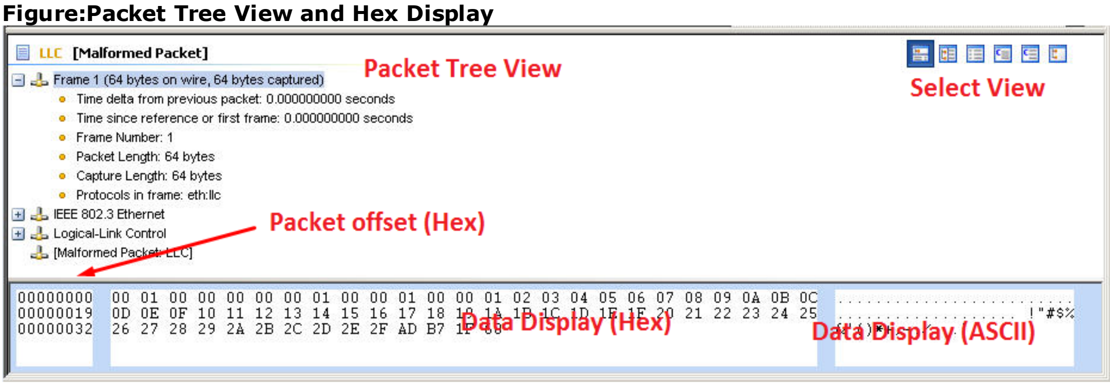
Table:Capture View Window Operations

Icon	Icon Label	Operation
	Home	Move to first item in list
	Page Up	Page up
	Move Up	Move up one item
	Move Down	Move down one item
	Page Down	Page down
	End	Move to last item
	Goto Item	Opens a prompt for the frame number.
	Go To Trigger	Goes to the capture trigger packet.
	Show or hide string filter	Show or hide string filter (*Filtering Captured Data*)

Packet Tree View and Hex Display

The lower half of the standard *Capture View* dialog shows the entire contents of the selected packet. The tree view summarizes the breakdown of the selected packet into its components. Then in the lower panel (shown in 3 parts horizontally) the left-hand column is the packet offset, exclicked in hexadecimal. This is followed by 16 bytes of data display, all in hexadecimal. Finally, the right-hand column contains a display of the data in ASCII, if the byte can be displayed as such; otherwise the byte is displayed as a dot (.).

Figure:Packet Tree View and Hex Display



The **Select View** buttons allow to select the desired view of packet data. As shown in *Figure:Select View Buttons*, from left to right, the view options are:

- Horizontal splitted packet tree and hex viewer (shown above)
- Vertical splitted packet tree and hex viewer
- Application data as ASCII
- Packet array

- Protocols arrays
- Packet tree view

Figure:Select View Buttons

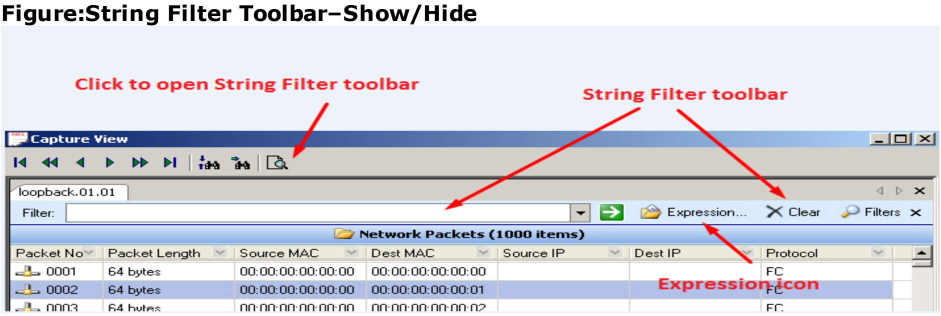
Filtering Captured Data

The Capture View display of data can be filtered to show only specified types of packets, using the string filter feature.

As mentioned previously, the Capture Trigger and Capture Filter (as described in *Capture Trigger and Capture Filter) for the selected port determine which packets are selected for display in Capture View. The slice size of the port (Configure Receive Mode(s)) sets the number of bytes captured and decoded for each packet. But the data that has been captured can be filtered further, to show only particular types of packets.*

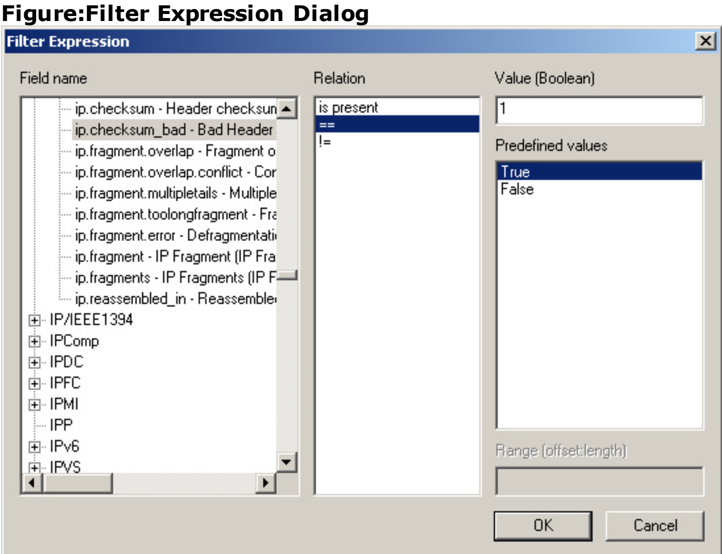
Click the the *Show or hide string filter* icon in the toolbar of the Capture View window to display the string filter toolbar (*Figure:String Filter Toolbar–Show/Hide*). This icon is a toggle, so clicking it again will hide the toolbar.

Figure:String Filter Toolbar–Show/Hide



Filtering of the Capture View data is performed by configuring an expression (string) that functions as the qualifying characteristic. Click the **Expression** icon in the string filter toolbar, shown above (*Figure:String Filter Toolbar–Show/Hide*). The **Filter Expression** dialog will appear.

Figure:Filter Expression Dialog

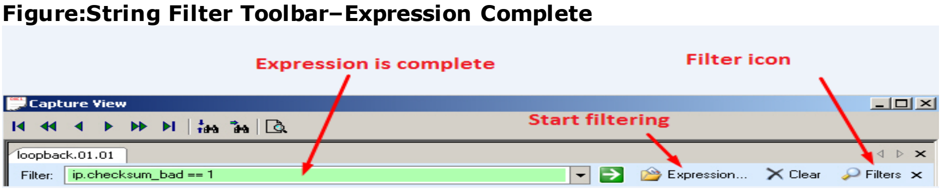


1. To build the filter expression, scroll down in left column (**Field name**) to locate and select the field you wish to focus on. Click the + to expand the listing under each heading. In the example above, ip.checksum_bad (under the expanded IP entry) has been selected.
2. In the center column (Relation) choose the relational operator for the expression. The choices are 'is present', (==) 'equal to' and (!=) 'not equal to'. In the example above, 'equal to' is selected.
3. In the right column (**Values** and **Predefined values**) column, select the value portion of the expression. In the example above, two values (True, False) are available and 'True' has been selected. In the Value (Boolean) field, the number 1 appeared when 'True' was selected. For other expressions, you may need to simply type an entry into the Value field..

   NOTE: Depending on the Field name selected, the Relation operator list and the two Value fields will be different.

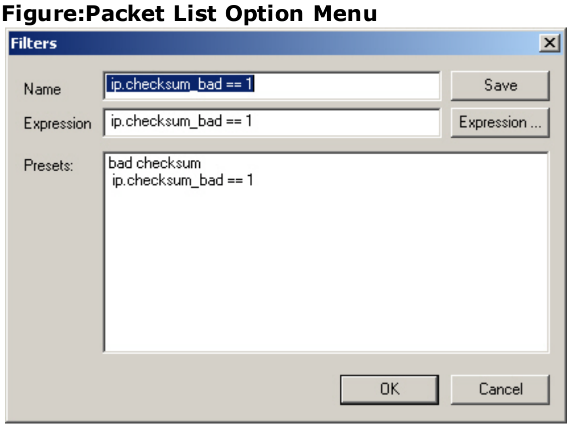
4. When all three parts of the expression are complete (two parts, if 'is present' is the relational operator), click OK. The expression will appear in the Filter fileld of the string filter toolbar (*Figure:String Filter Toolbar–Expression Complete*).

   Figure:String Filter Toolbar–Expression Complete

5. (Optional) If you want to save this string filter for use in the future, click the Filters icon (*Figure:Packet List Option Menu*). The Filters dialog will appear, offering the ability to save the string filter just configured.

   Figure:Packet List Option Menu

6. (Optional) Enter a name or accept the default name for this string filter (which is the same as the field name in the expression). Then click **OK**.

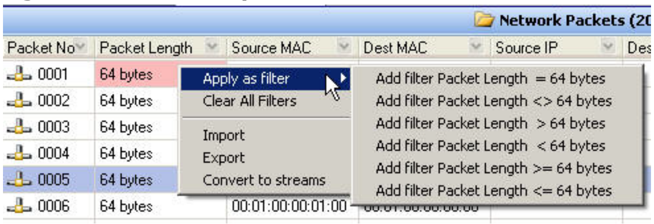
   In the future, you can click the **Filters** icon to open the list of saved strings, then select one and click **OK** to load it into the Capture View Filter field.

7. Finally, click the green 'start' arrow (*Figure:Packet List Option Menu*) to activate the string filter. The displayed list of captures will change according to the filter you have selected.

Capture View Option Menu

Right-click any packet within the Packet List (upper panel) and select an option from this menu.

Figure:Packet List Option Menu

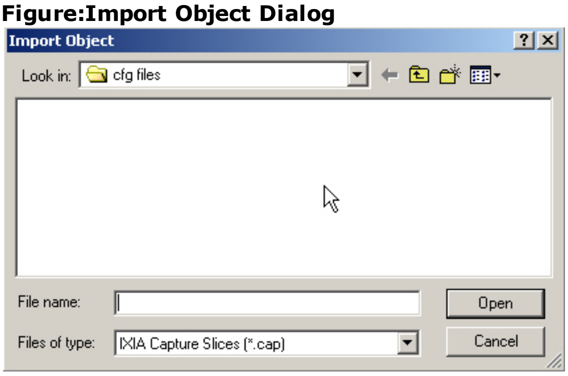


- Apply as filter–choose to filter on one of available values in the selected column (*Figure:Packet List Option Menu* shows Packet Length column is selected)
- Clear All Filters–undo filtering, restore unfiltered listing
- Import–imports captured data from a file; opens Import Object dialog (*Capture File Import*)
- Export–exports captured data to a file; opens Capture Export dialog (*Capture File Export*)
- Convert to streams–*Convert to Stream*.

Capture File Import

Captured data may be imported into the capture buffer. From there it may be converted to streams as desired. The *Import Object* dialog displays saved data files and is shown in *Figure:Import Object Dialog*.

Figure:Import Object Dialog



Two file formats are acceptable for import:

- Ixia capture slice (*.cap*)—a binary format created with IxExplorer File Export.
- Sniffer encoding (*.enc*)
  - Network General Sniffer Format enc file version 4.x (*.enc*)
  - Network General Sniffer Format enc file version 1.6 (*.enc*)

This dialog allows the selection of existing files. The *Files of Types* field only provides for *.cap* and *.enc* file types. Imported data replaces the port's capture buffer.

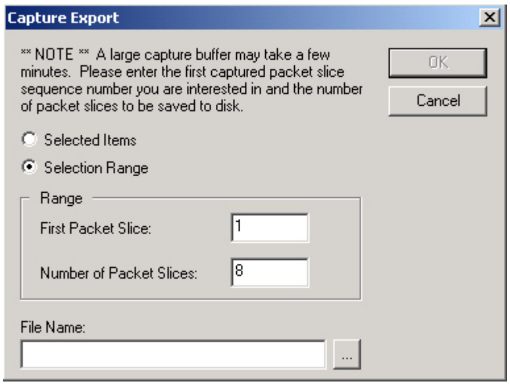
NOTE IxExplorer does not allow to import .cap file that is saved from wireshark. IxExplorer only supports Ixia .cap file format. The .cap file imported from wireshark uses a different format. If you want to import the .pcap file from wireshark, NOTE first save it as a Sniffer .enc file and then import it to IxExplorer.

The Sniffer encoding file format is compatible with Wireshark. When you import a .enc file, the CRC frame check sequence is preserved and no additional bytes are created.

Capture File Export

Data from the Capture View Frame Display can be saved to files, as shown in *Figure:Capture Export Dialog*.

Figure:Capture Export Dialog



Each slice starts at the beginning of a packet and contains all or part of that one packet only. Different types of encodings for the export file are available, *Export Object Dialog* for additional information.

If large amounts of captured data are being exported, a status bar appears showing time remaining until completion.

The fields and controls in this dialog are described in *Table:Capture Export Dialog*.

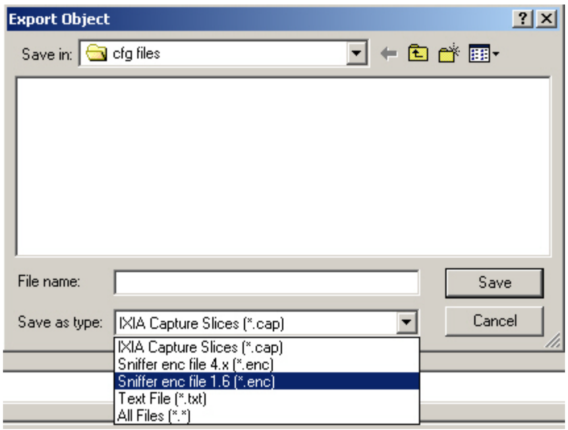
Table:Capture Export Dialog

Field/Control	Description
Selected Items	Highlights selected data in *Capture View* dialog and saves it to a file.
Selected Range	Enables fields in the *Range* box for data entry, which can then be saved in the selected range to a file.
Range - First Packet Slice	The sequence number of the first packet slice to save.
Range - Number of Packet Slices	The number of packet slices to be saved.
File Name	The name of the file to save to. *Export Object Dialog* for additional information on file formats.
...	Invokes a standard windows file dialog that allows directory navigation and file choice, as described in *Export Object Dialog*.
OK	Causes the data to be saved.
Cancel	Exits the dialog.

Export Object Dialog

The *Export Object* dialog is shown in *Figure:Export Object Dialog*.

Figure:Export Object Dialog

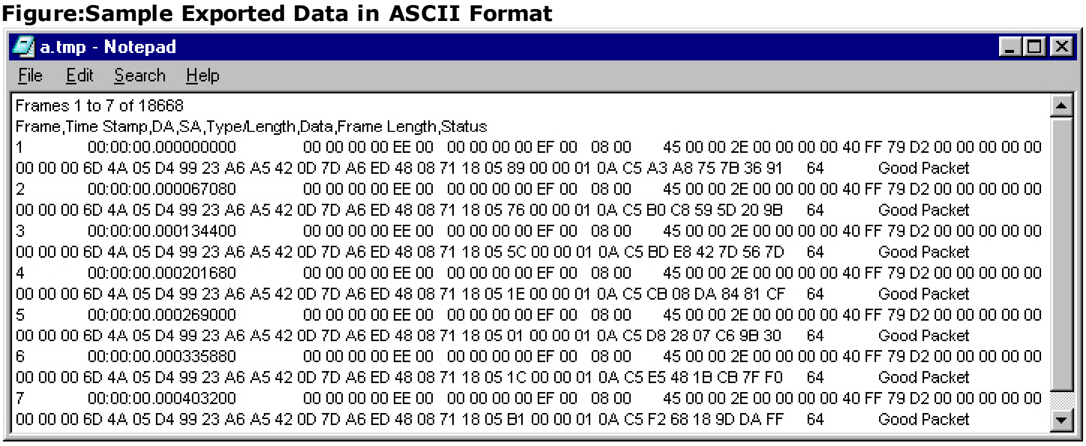


The types of captured data files that can be saved are:

- IXIA Capture Slices (*.cap*)—a binary format for use with IxExplorer File Import.
- Sniffer encoding (*.enc*):
  - Network General Sniffer Format enc file version 4.x (*.enc*)
  - Network General Sniffer Format enc file version 1.6 (*.enc*)
- Text File (*.txt*)—an ASCII text file suitable for import into a database. A sample of the ASCII file (*.txt*) format is shown in *Figure:ample Exported Data in ASCII Format*.

NOTE When a file is exported to .enc format, the CRC frame check sequence is preserved.

Figure:Sample Exported Data in ASCII Format



The saved data file contains the same information as the top window of the *Capture View* dialog, as shown in *Figure:Capture View Window–Standard Version*. This list has columns for a frame index number, a timestamp, the destination address, the source address, the type/length, the packet data, the frame length, and the error status of the frame.

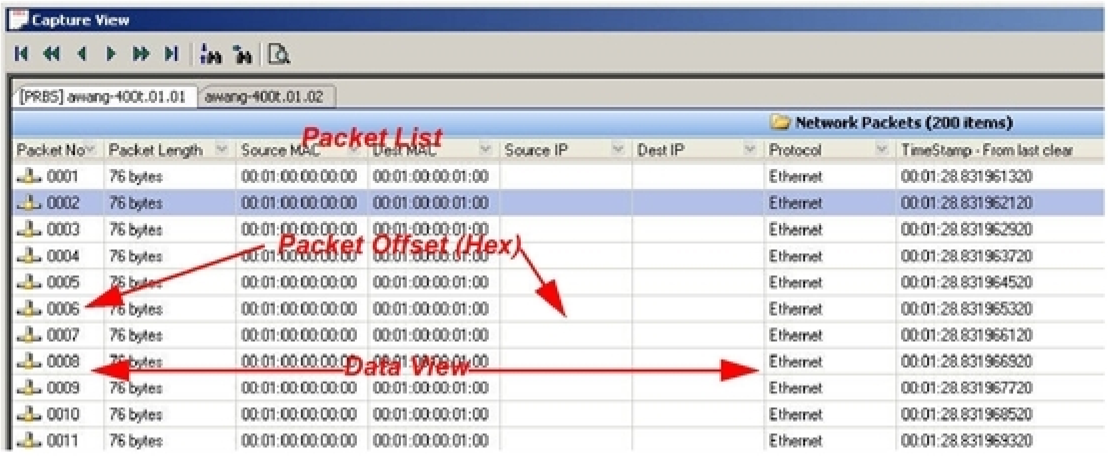
Convert to Stream

The convert to stream buffer takes all of the highlighted packets in the packet list and converts them to individual streams (one packet in length) for the port. Each newly converted stream is added to the end of the set of streams. Note that only 255 streams are allowed if a port's transmit mode is set to streams and 15,872 total packets if set to flows. This feature is not available for some modules.

PRBS Mode Capture

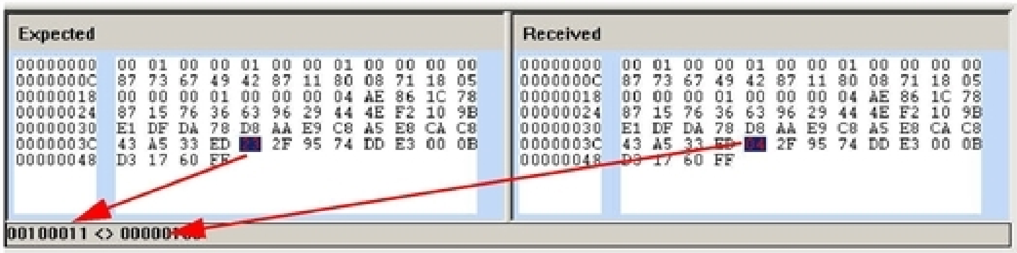
When PRBS mode is selected for transmit and receive, the capture view dialog has the configuration shown in *Figure:Capture View Dialog–PRBS Version*. There is no Packet Tree view (as in the standard variation). In this example, a TXS4 card has been configured in a loopback fashion to transmit and receive packet streams in PRBS mode.

Figure:Capture View Dialog–PRBS Version



In the data view (lower) panel, the Expected packet configuration is displayed on the left, and the Received packet on the right. This enables bit comparison between the two. Differences are highlighted in red. Select any byte in the data view, and a bit comparison will be revealed on the bottom frame.

Figure:Bit Comparison Example



Chapter 15 - Statistic View

The Statistic View feature of Ixia IxExplorer allows to view all or a subset of the statistics available for ports. Statistics for multiple ports can be displayed side-by-side for greater insight into overall traffic patterns, and single stream statistics can be viewed:

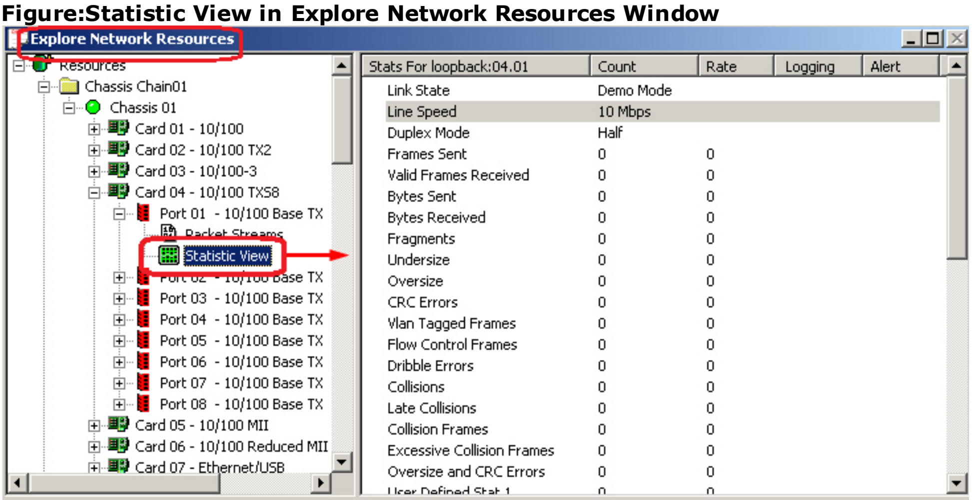
- *Statistic View—Port for single port statistics (in the Explore Network Resources window).*
- *Statistic View—Custom Views for creating Statistic Views for multiple ports.*
- *Stream Statistic Views* for creating Stream Statistic Views for one or more ports.

IxExplorer has the ability to centrally log statistics from any port and to signal alert conditions when a particular statistic goes out of a specified, valid range. Refer to the Statistics Logging and Alerts section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for additional information.

Statistic View—Port

To view the statistics for a single port in the Explore Network Resources window, click *Statistic View* under the port on the tree. The figure in *Figure:Statistic View in Explore Network Resources Window is one sample set of statistics shown for a port on a 10/100 TXS8 load module.*

Figure:Statistic View in Explore Network Resources Window



The counters that are displayed in the statistics windows for each type of load module are the ones that are applicable to the load module type. The 'Rate' column shows the count rate values for each counter in increments per second. The 'Logging' and 'Alert' columns display information if Logging and Alerts are enabled on the chassis and configured for the statistics. *Statistics Logging and Alerts* for additional information.

See the 'Available Statistics' appendix of the *Ixia Platform Reference Manual* for a description of the statistics which are counted for each card type.

NOTE

Derived Statistics
Some statistics are derived from calculations based on other statistics. For

NOTE example, 'Bits Sent' is derived from the 'Bytes Sent' statistic. To clear a derived statistic, the statistic on which it is based must also be cleared.

NGY Fault Handling

IEEE Requirements

IEEE 802.3ae, section 46.3.4 defines how a Reconciliation Sublayer (RS) shall respond to Local and Remote Faults. Response to a Local Fault is to immediately cease sending traffic on the transmit data path (even if doing so truncates a frame) and to send continual Remote Faults. Response to a Remote Fault is to stop sending MAC data (completing any frame that is being transmitted) and to send continual idles.

NGY Operation

NGY load modules have a single statistic for Faults called Link Fault State. This statistic is real-time and indicates the current state of the port's Reconciliation Sublayer (RS) state machine. The possible stat values are as follows:

- No Fault
- Local Fault
- Remote Fault

Features that force deviation from IEEE spec

NOTE In general, if a NGY port appears to be transmitting according to the Frames Sent statistic, be aware that Link Fault State may override this.

Tx Ignores Rx Link Faults

This feature is enabled through the Link Fault Signaling tab of Port Properties. When the feature is enabled, the Fault statistic will continue to indicate the RS state of the port; however, the transmit-side response will behave as if no fault was received. That is to say, Remote Faults will not be sent as a response to Local Fault and Idles will not be forced as a response to Remote Fault, even though Link Fault State indicates the board is in a Fault state.

Transmit Ignores Link Status

This feature is enabled through the Transmit Modes tab of Port Properties. When the feature is enabled, a port will be permitted to transmit under conditions that would normally inhibit transmit. For instance, a port that has no link and is not in diagnostic loopback will appear in IxExplorer as red color, and will normally not be permitted to transmit. Enabling this feature will allow transmit. When the feature is enabled, the statistic called Link State will indicate 'Ignore Link'.

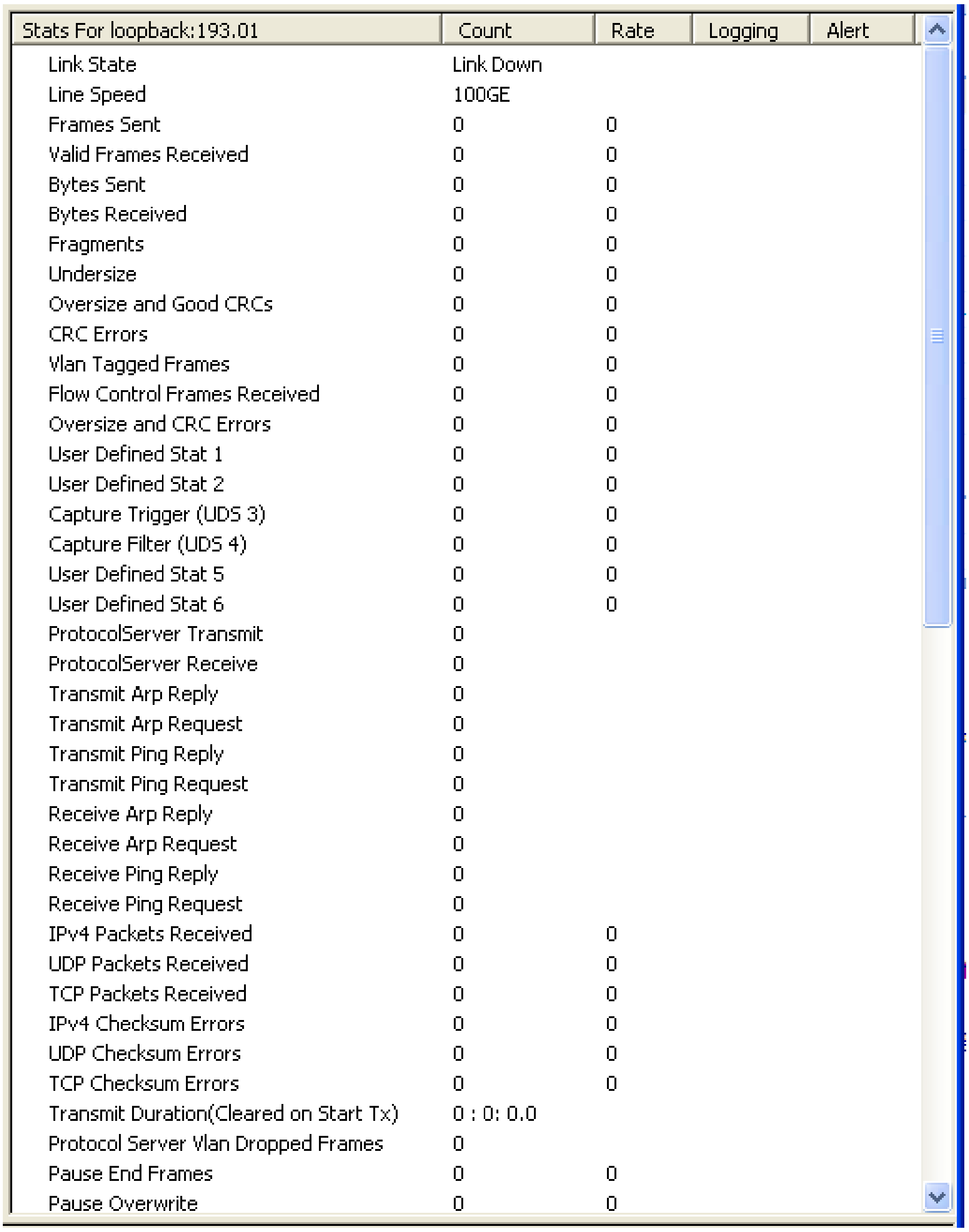
Note that if the port is in Fault, enabling this feature and forcing transmit may result in misleading results. The port shown in the following stat view (*Figure:Statistic View for NGY, Ignore Link Status*) is ignoring link (see Link State statistic), is in Remote Fault (see Link Fault State statistic), yet appears to be transmitting (see Frames Sent Rate statistic). The reality is that no frames are actually leaving the port because the port is in Remote Fault. This is because the block that maintains the transmit statistics is located before the block that forces idles as a response to Remote Fault.

Figure:Statistic View for NGY, Ignore Link Status

	A	B
1	Name	loopback:02.01
2	Link State	Ignore Link
3	Line Speed	10GE LAN
4	Frames Sent	164,624,279
5	Frames Sent Rate	14,880,954
6	Valid Frames Received	0
7	Valid Frames Received Rate	0
8	Bytes Sent	10,535,953,80
9	Bytes Sent Rate	952,380,945
10	Bytes Received	0
11	Bytes Received Rate	0
12	Fragments	0
13	Undersize	0
14	Oversize	0
15	CRC Errors	0
16	Link Fault State	Remote Fault
17	Scheduled Transmit Duration	0 : 0: 0.0
18	Bytes Sent / Transmit Duration	21,740,528
19	Bits Sent	84,287,630,43
20	Bits Sent Rate	7,619,047,560
21	Bits Received	0
22	Bits Received Rate	0
23	Central Chip Temperature(C)	45
24	Port Chip Temperature(C)	45
25	Port CPU Status	Ready
26	Port CPU DoD Status	Ready

Lava Statistics View

Figure:Statistic View for Lava



Stats For loopback:193.01	Count	Rate	Logging	Alert
Link State	Link Down			
Line Speed	100GE			
Frames Sent	0	0		
Valid Frames Received	0	0		
Bytes Sent	0	0		
Bytes Received	0	0		
Fragments	0	0		
Undersize	0	0		
Oversize and Good CRCs	0	0		
CRC Errors	0	0		
Vlan Tagged Frames	0	0		
Flow Control Frames Received	0	0		
Oversize and CRC Errors	0	0		
User Defined Stat 1	0	0		
User Defined Stat 2	0	0		
Capture Trigger (UDS 3)	0	0		
Capture Filter (UDS 4)	0	0		
User Defined Stat 5	0	0		
User Defined Stat 6	0	0		
ProtocolServer Transmit	0			
ProtocolServer Receive	0			
Transmit Arp Reply	0			
Transmit Arp Request	0			
Transmit Ping Reply	0			
Transmit Ping Request	0			
Receive Arp Reply	0			
Receive Arp Request	0			
Receive Ping Reply	0			
Receive Ping Request	0			
IPv4 Packets Received	0	0		
UDP Packets Received	0	0		
TCP Packets Received	0	0		
IPv4 Checksum Errors	0	0		
UDP Checksum Errors	0	0		
TCP Checksum Errors	0	0		
Transmit Duration(Cleared on Start Tx)	0 : 0: 0.0			
Protocol Server Vlan Dropped Frames	0			
Pause End Frames	0	0		
Pause Overwrite	0	0		

Figure:Statistic View for Lava (Continued.)

Stats For loopback:193.01	Count	Rate	Logging	Alert
Scheduled Frames Sent	0	0		
Asynchronous Frames Sent	0	0		
Port CPU Frames Sent	0	0		
Link Fault State	No Fault			
Local Faults	0			
Remote Faults	0			
Scheduled Transmit Duration	0 : 0: 0.0			
Bytes Sent / Transmit Duration	0			
Bits Sent	0	0		
Bits Received	0	0		
Port CPU Status	Not Present			
Port CPU DoD Status	Not Ready			
Frames Received with Coding Errors	0	0		
Frames Received with /E/ error Character	0	0		
TxSchedulerOverlay Fpga Temperature(C)	0			
TxFmx Fpga Temperature(C)	0			
Capture1 Fpga Temperature(C)	0			
Latency1 Fpga Temperature(C)	0			
Pcpu Fpga Temperature(C)	0			
PCS Sync Errors	0	0		
PCS Illegal Codes	0	0		
PCS Remote Faults	0	0		
PCS Local Faults	0	0		
PCS Illegal Ordered Set	0	0		
PCS Illegal Idle	0	0		
PCS Illegal SOF	0	0		
PCS Out Of Order SOF	0	0		
PCS Out Of Order EOF	0	0		
PCS Out Of Order Data	0	0		
PCS Out Of Order Ordered Set	0	0		
PHY Chip Temperature(C)	0			
Transmit Neighbor Solicitations	0			
Transmit Neighbor Advertisements	0			
Receive Neighbor Solicitations	0			
Receive Neighbor Advertisements	0			

HSE 100GE Load Module Statistics

The statistics support for HSE 100GE load module has been added with new statistic fields per port and per PCS Lane. The new statistics are mentioned in the following table:

Table:HSE 100GE Load Module Statistics

Statistics Per Port	Statistics Per PCS Lane
Link Fault State	Physical and PCS lane address assignments
PCS Sync Errors	Sync header lock
PCS Illegal Codes	PCS lane marker lock
PCS Remote Faults	PCS lane marker map
PCS Local Faults	Relative lane skew
PCS Illegal Ordered Set	Synch header error count

Statistics Per Port	Statistics Per PCS Lane
PCS Illegal Idle	PCS lane marker error count
PCS Illegal SOF	BIP-8 Error Count
PCS Out Of Order SOF	Lost synch header lock
PCS Out Of Order EOF	Lost PCS lane marker lock
PCS Out Of Order Data	
PCS Out Of Order Ordered Set	

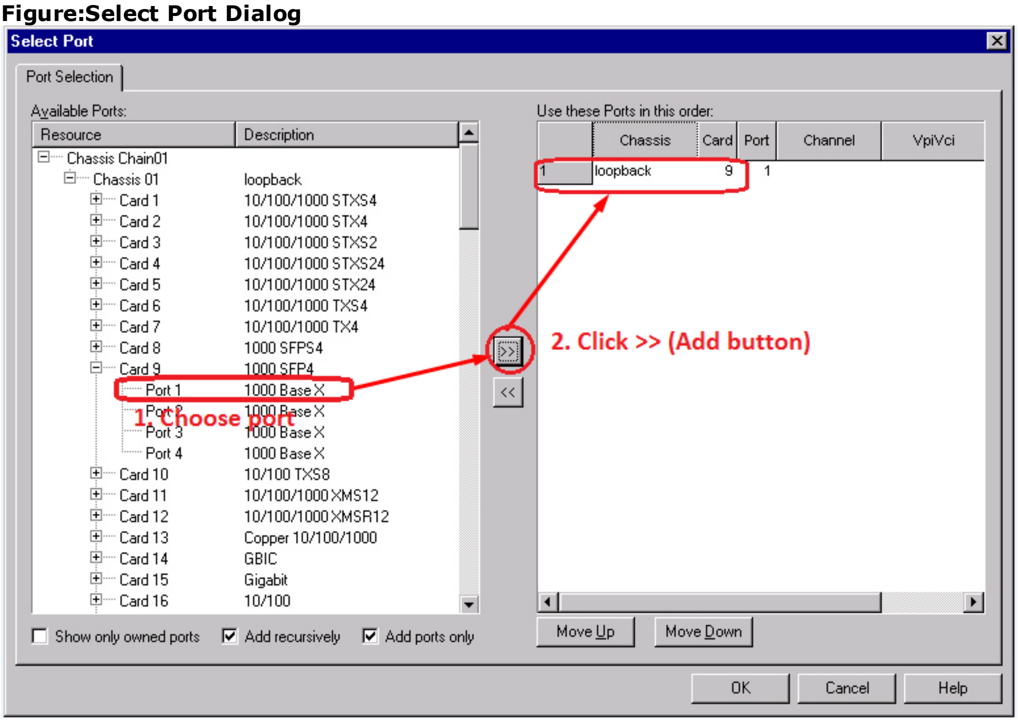
Statistic View—Custom Views

Use the Statistic View, accessed in the lower part of the Resources tree list, to display multiple ports' statistics side-by-side.

Selecting Ports for the Statistic View

To create a Statistic View for one or more ports, highlight *Statistic View* near the bottom of the Explore Network Resources list, right-click, and then select *New*. The *Select Port* dialog opens, allowing to select ports for viewing statistics in a side-by-side display, as shown in *Figure:Select Port Dialog*.

Figure:Select Port Dialog



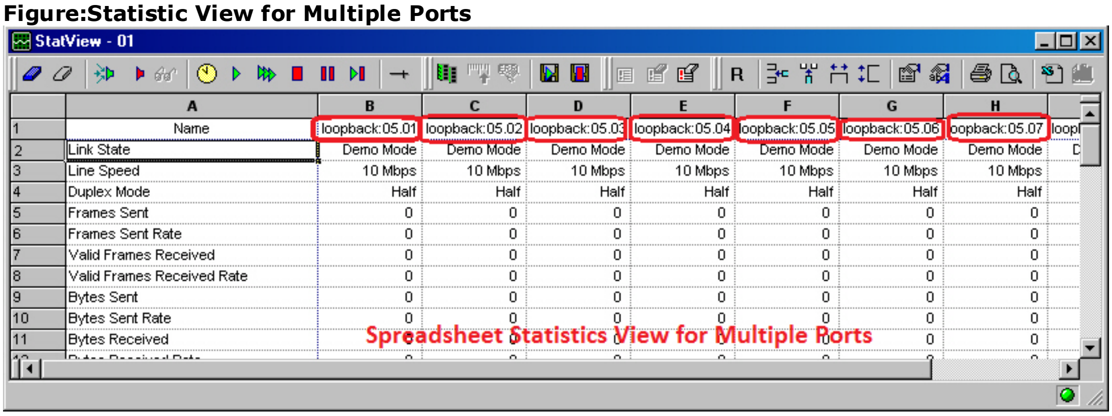
On the left side of the window, highlight the desired ports using either the shift-click or control-click methods, and then click the >> (Add) button to place them in a list on the right side of the window. Then click *OK*, and the statistics window will appear.

The *Add recursively* check box enables the capability for adding groups of ports at one time. Enable the *Add recursively* check box. Then select/highlight a higher level item in the list: Card (load module), Chassis, or Chassis Chain. Click the >> (Add) button, and all of the ports listed under that higher level item will be added to the list of active ports in the right pane.

NOTE For a description of the Select Port dialog, *Select Port Dialog*.

The *Statistic View* dialog is shown in *Figure:Statistic View for Multiple Ports*.

Figure:Statistic View for Multiple Ports



It is possible to include a counter that does not exist in this view by default. From a statistics window that contains the desired counter, users can drag-and-drop the counter into the multiple ports *Statistic View* dialog using the left button on the mouse. The order of the list of counters in the window can be rearranged using the same drag-and-drop method. Full control over transmit and capture operations, as well as operations related to statistics and their display are available from the Statistic View toolbar.

By selecting any of the column titles, additional operations may be invoked. *Figure:Spreadsheet Statistic View Pop-Up Menu* shows an example of the pop-up menu that it presented when a column header is selected.

NOTE The tx and rx stats that appear in Statistic View are continuously synching as IxServer polls the ports that are communicating with each other. However, if the link between two ports is down, the Statistic View will not be updated, and so the tx and rx stats in the Statistic View will not match. It may appear that more frames are received than are transmitted, or vice-versa. This behavior applies only to the following load modules:

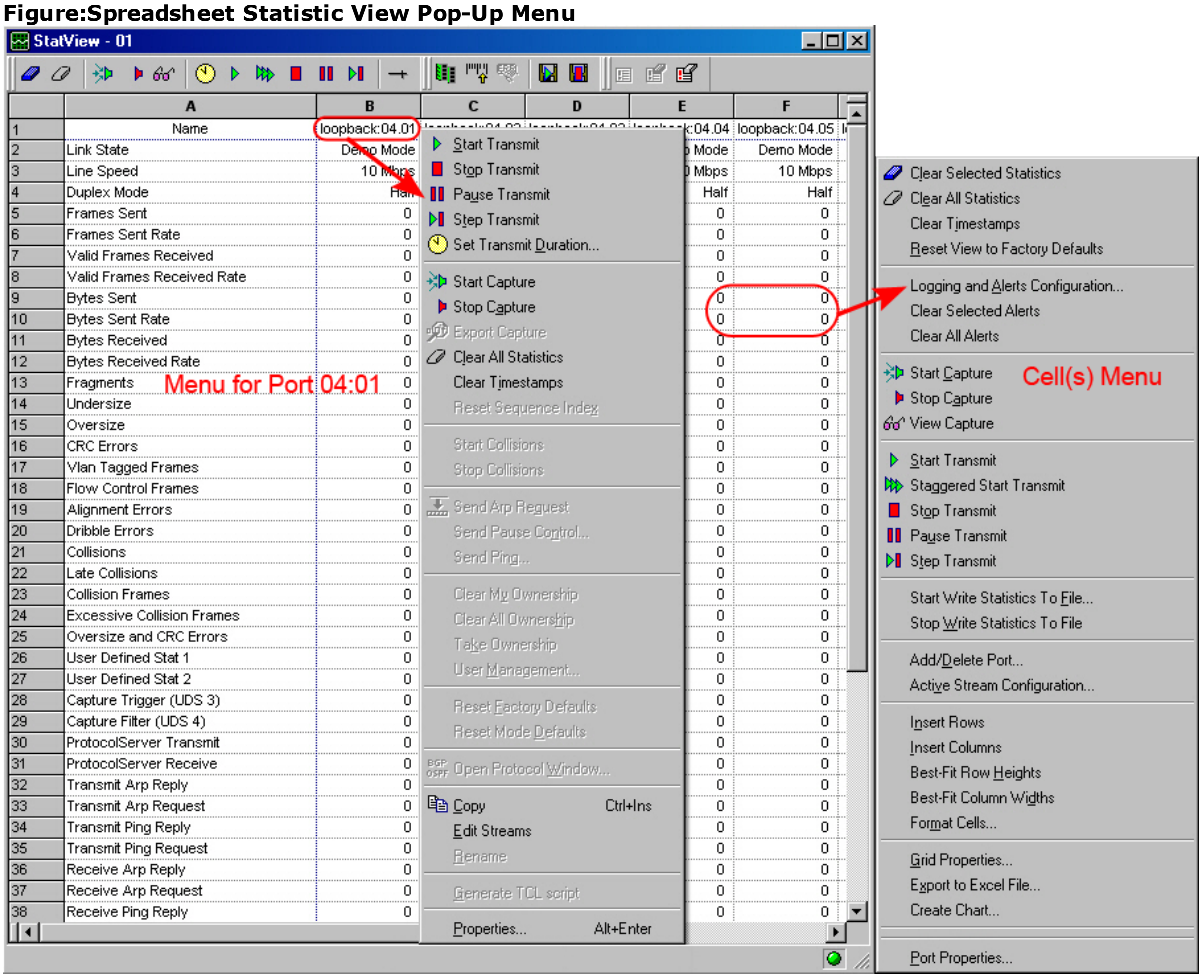
Copper 10/100/100 (LM1000T-5)

GBIC (LM1000GBIC)

Gigabit (LM1000SX)

10/100 (LM100TX)

Figure:Spreadsheet Statistic View Pop-Up Menu

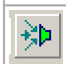
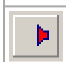


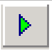
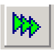
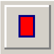
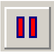
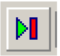
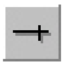
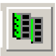
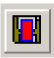
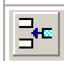
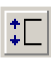
The operations available on the Column pop-up menu are a subset of the commands available from the Explore Resources port pop-up menu (*Ports*). *Selection of the Edit Streams item invokes the Frame Data Tab for the first stream for the port (Frame Data Tab for additional information).*

Spreadsheet Statistic View Toolbar

The icons/options in the spreadsheet type Statistic View toolbar are described in *Table:Statistic View—Spreadsheet Type Toolbar Options.*

Table:Statistic View—Spreadsheet Type Toolbar Options

Toolbar Icon	Pop-Up Menu Option	Operation
	Clear Selected Statistics	Resets the selected statistics for the port(s) back to all 0's.
	Clear All Statistics	Resets the statistics for all ports back to all 0's.
	Start Capture	Starts the capture operation on the selected port(s).
	Stop Capture	Stops the capture operation on the selected port(s).
	Capture View	Displays the *Capture View* dialog. *Capture View* for additional information.

Toolbar Icon	Pop-Up Menu Option	Operation
	Set Transmit Duration	Displays the *Set Transmit Duration* dialog which allows to control the length of the stream transmission. *Set Transmit Duration* for additional information.
	Start Transmit	Starts the transmit operation on the selected port(s).
	Start Staggered Transmit	Starts the transmit operation on the selected ports. A delay is inserted between one port's start transmission and the next.
	Stop Transmit	Stops the transmit operation on the selected port(s).
	Pause Transmit	Pauses the transmit operation on the selected port(s).
	Single Step Stream	Sends a single packet on each of the selected ports.
	Global Rate Slide Bar	Sets the line rate for ports in the Statistic View. *Global Line Rate Configuration*.
	Add/Delete Ports	Opens the *Select Port* dialog, where one or more ports can be added to or deleted from the Statistic View. *Selecting Ports for the Statistic View*.
	Active Stream Configuration	Opens the *Active Streams* dialog, which allows frame size and inter-packet gap to be varied over a set of ports. *Active Stream Configuration*.
	Insert Single BERT Error	(Available only for BERT mode) Inserts a single Bert error into the data stream.
	Start Write Statistics to File	Starts logging of statistics to a file. *Start Write Statistics to File*.
	Stop Write Statistics to File	Stops logging of statistics to a file. *Stop Write Statistics to File*.
	Logging and Alerts Configuration	Displays the *Logging and Alerts* dialog. *Statistics Logging and Alerts for additional information.*
	Clear Selected Alerts	Clears the alerts in highlighted cells of the Statistic View.
	Clear All Alerts	Clears the alerts in all cells of the Statistic View.
	Reset View to Defaults	Resets the view to the factory-default settings.
	Insert Rows	Inserts a row below the currently selected row.
	Insert Columns	Inserts a column to the right of the currently selected cell or column. This option may be used for setting up a blank area in which an Excel-style formula may be entered. *Grid Properties—Display Settings*.
	Best-Fit Row Heights	For all of the selected rows, adjusts the height of the row so as to just fit the contents of all of the columns.

Toolbar Icon	Pop-Up Menu Option	Operation
	Best-Fit Column Width	For all of the selected columns, adjusts the width of the columns so as to just fit the contents of all of the rows.
	Grid Properties	Controls the grid properties of spreadshseet. Refer to *Grid Properties—Display Settings.*
	Format Cells	Controls the formatting of the text within cells. Refer to *Cells Format Dialog.*
	Print	Displays a print dialog, so the Statistic View grid can be printed (does not include the toolbar).
	Print Preview	Displays the a preview of the Statistic View grid as it will appear in a printed format.
	Export to Excel File	Allows part or all of the spreadsheet to exported to an Excel compatible spreadsheet file. Refer to *Spreadsheet—Export to Excel File Dialog.*
	Create Chart	Creates a chart from selected areas of the spreadsheet. Refer to *Using Chart View*.

Statistic View Operations

Excel Spreadsheet Capabilities

The spreadsheet view follows most of the behavior characteristics of an Excel spreadsheet.

Formulas for manipulating received statistical data may be created in the spreadsheet-style Statistic View. Add a new (empty) column to the right of the existing columns that contain port data. Select/highlight the last column on the right, and then click the *Insert Column* icon ( ) on the toolbar. Select a convenient cell in the new column, and enter the equal sign '=' to indicate the start of a formula. Use the standard Excel techniques for performing mathematical operations on the numerical contents of various cells in the spreadsheet. Each cell is indicated by a combination of the column letter and row number, such as 'B9.'

Statistics Logging and Alerts

If visual alerts (see the Statistics Logging and Alerts section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*) are configured and enabled, the cell containing the statistic displays a color to indicate the alert status of that statistic for the port. The color coding is described below:

- **Clear** (background color of spreadsheet)—no alert has been configured.
- **Green**—an alert has been configured, but no alert is active.
- **Red**—an alert is active, which indicates that an out-of-range condition exists.
- **Yellow**—an alert was active, but the condition is now within range, and a user acknowledgment is pending. This serves as an alert history indicator. If the user then clears the statistic, by using the *Clear Selected Statistics* or *Clear All Statistics* icons (and) or menu options, the color will turn green.

An example follows for a link state statistic that has been previously configured to use Logging and Alerts:

- A link is down due to a physical disconnect (connector is pulled out of port interface)—statistic turns red.
- The interface is reconnected—statistic turns yellow.
- Click the stat and then click the *Clear Selected Statistics* or *Clear All Statistics* icons (and) in the toolbar—statistic turns green.

These are the default colors. The alert status colors may be modified in the *Tools* > *Options* > *Alerts* dialog. Refer to *Chassis Properties—Logging and Alerts*.

Statistic View Options

Some of the options available for Statistic Views are described in more detail in the following sections:

- *Start Write Statistics to File*
- *Stop Write Statistics to File*
- *Active Stream Configuration*
- *Global Line Rate Configuration*
- *Grid Properties—Display Settings*
- *Cells Format Dialog*
- *Spreadsheet—Export to Excel File Dialog*
- *Chart View Dialog*

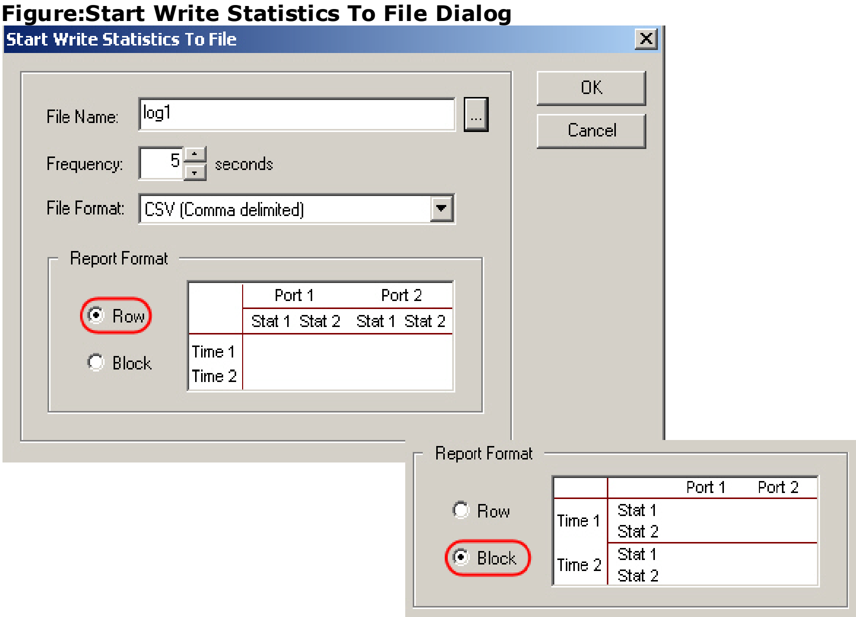
Start Write Statistics to File

In addition to displaying statistics on the screen, IxExplorer is able to write statistics to a disk file. The Start Write Statistics To File mode is entered by selecting the *Start Write Statistics to File* icon ()on the Statistic View tool bar, as shown in *Figure:Start Write Statistics To File Icon*.

Figure:Start Write Statistics To File Icon

The *Start Write Statistics to File* dialog allows a number of formatting parameters to be set, as shown in .

Figure:Start Write Statistics To File Dialog



The fields in this dialog and their usage are described in *Table:Start Write Statistics To File Dialog*.

Table:Start Write Statistics To File Dialog

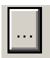
Field	Usage
File Name	The name of the file on the disk to write to.
	This button provides access to a standard Windows *Save As* dialog, as shown in *Figure:Save As Dialog*. If no directory is provided in the file name, the directory into which IxExplorer was loaded will be used (`c:\Program Files\Ixia` by default).
Frequency	(in seconds) Specifies how often statistics are written to the file.
File Format	Determines how each line of output is displayed. The choices are: • **CSV** (Comma delimited)—all items are separated by a single comma. • **Formatted text** (Space Delimited)—columns are lined up by the insertion of spaces. • **Text** (Tab Delimited)—all items are separated by a single tab character.
Report Format	The output may be formatted in one of two methods: • **Row**—the output is formatted as shown in *Figure:Sample Output for Row Format Output with Formatted Text*. • **Block**—the output is formatted as pictured below *Figure:Sample Output for Block Format Output with Formatted Text*.

Figure:Save As Dialog

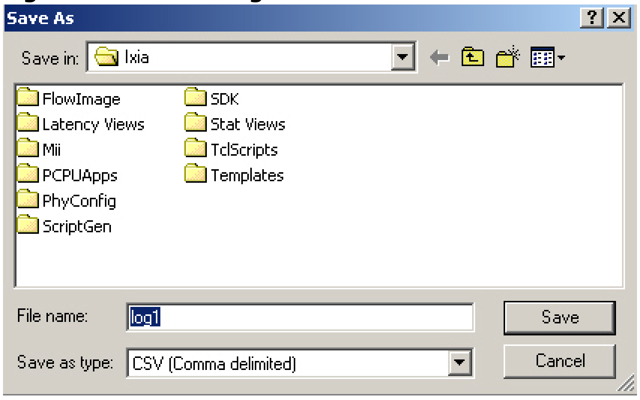


Figure:Sample Output for Row Format Output with Formatted Text

```
                    "127.0.0.1:01.01"
                    "Link State"  "Line Speed"  "Duplex Mode" "Frames Sent" "Frames Sent Rate"

01-25-1999    20:53:52      "Down" "1000" "Full" "0"    "0"    "0"    "0"    "0"    "0"
01-25-1999    20:53:57      "Down" "1000" "Full" "0"    "0"    "0"    "0"    "0"    "0"
01-25-1999    20:54:03      "Down" "1000" "Full" "0"    "0"    "0"    "0"    "0"    "0"
01-25-1999    20:54:08      "Down" "1000" "Full" "0"    "0"    "0"    "0"    "0"    "0"
```

Figure:Sample Output for Block Format Output with Formatted Text

```
                    "127.0.0.1:01.01"    "127.0.0.1:01.02"    "127.0.0.1:02.01"    "127.0.0.1:02.02"

01-25-1999    21:26:28      "Link State"  "Down" "Down" "Down" "Down"
              "Line Speed"  "1000" "1000" "1000" "1000"
              "Duplex Mode" "Full" "Full" "Full" "Full"
              "Frames Sent" "0"    "0"    "0"    "0"
              "Frames Sent Rate"   "0"    "0"    "0"    "0"
              "Valid Frames Received"     "0"    "0"    "0"    "0"
              "Valid Frames Received Rate"       "0"    "0"    "0"    "0"
              "Bytes Sent"  "0"    "0"    "0"    "0"

01-25-1999    21:26:33      "Link State"  "Down" "Down" "Down" "Down"
              "Line Speed"  "1000" "1000" "1000" "1000"
              "Duplex Mode" "Full" "Full" "Full" "Full"
              "Frames Sent" "0"    "0"    "0"    "0"
              "Frames Sent Rate"   "0"    "0"    "0"    "0"
              "Valid Frames Received"     "0"    "0"    "0"    "0"
              "Valid Frames Received Rate"       "0"    "0"    "0"    "0"
              "Bytes Sent"  "0"    "0"    "0"    "0"
```

Stop Write Statistics to File

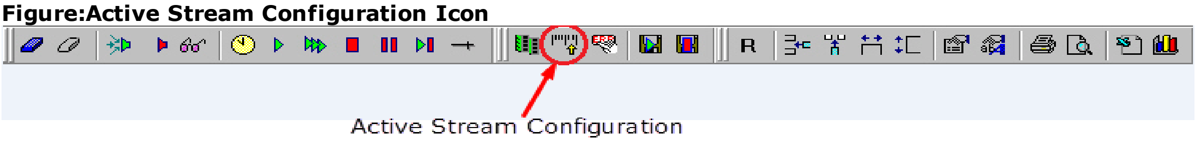
Output to statistics write files may only be stopped when IxExplorer is terminated or the *Stop Write To File* icon ()is selected from the Statistic View toolbar, as shown in *Figure:Stop Write Statistics To File Icon*.

Figure:Stop Write Statistics To File Icon

Active Stream Configuration

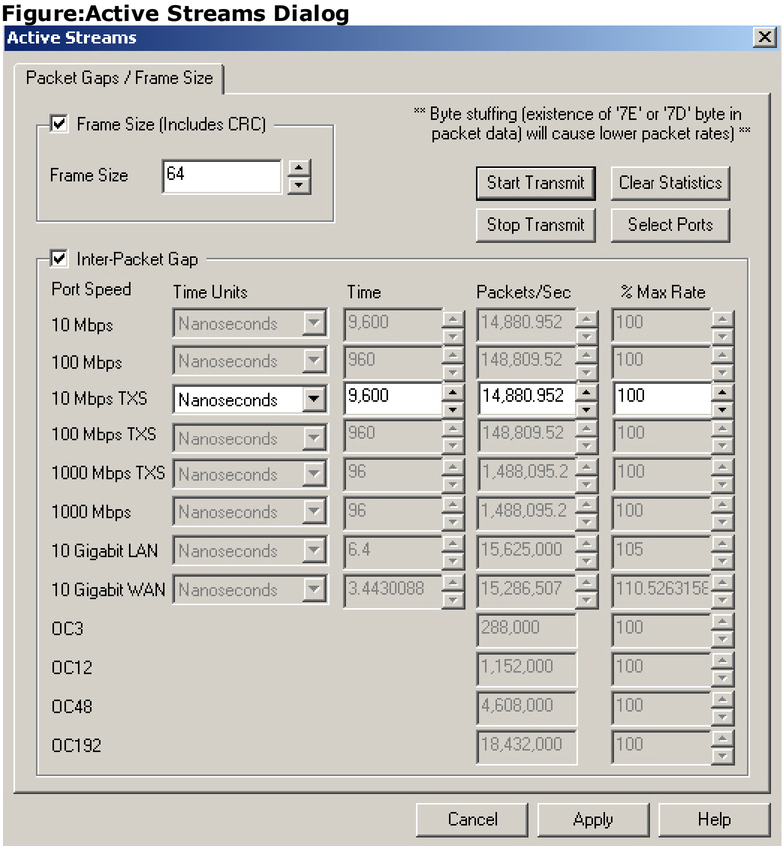
The *Active Stream Configuration* option of the multiple Statistic Views is a unique feature that allows threshold testing by varying frame size and inter-packet gap across a range of ports, while monitoring a set of statistics. During the operation of active streams, the first stream for the applicable ports is set to contiguous packet mode, and then reset after the adjustments are completed.

Figure:Active Stream Configuration Icon



When the *Active Stream Configuration* icon ( ) is selected, the *Active Streams* dialog is displayed, as shown in *Figure:Active Streams Dialog*.

Figure:Active Streams Dialog



NOTE When editing the Frame Size, Time, Packets/Sec, and % Max Rate fields directly it is not necessary to select the Apply button (the Apply button is grayed out). The changes take effect immediately.

The fields and controls in this dialog are described in *Table:Active Streams Dialog*.

Table:Active Streams Dialog

Control	Usage
Start Transmit	Starts the transmit process, using the other settings that override frame size and inter-packet gap for the selected ports. If the transmit sequence on the selected ports is infinite, there is no need to stop and start the transmit operation.
Stop Transmit	Stops the transmit process on the selected ports.
Clear Statistics	Clears the statistics on the selected ports.

Control	Usage
Select Ports	Presents a dialog identical to the one used to select the members of the statistics group. The selections in this list are the only ones that will be subject to the changes made in Active mode.
Frame Size (Includes CRC)	If the check box is selected, this box allows the frame size of transmitted packets to be set in a range from the minimum to maximum compatible with the ports and frames being applied. The number may be typed directly into the box or incremented/decremented with the up/down arrows. The *Apply* button must be clicked before any change goes into effect.
Inter-Packet Gap	If the check box is selected, this box allows the inter-packet gap for the selected ports/line rates to be varied. Separate controls are available for ports that are operating at different speeds. Time units available are: • Nanoseconds • Microseconds • Milliseconds • Seconds The gap may be modified in any of three ways: • Time—the number of time units (N/A to POS modules). • Packets/Sec—the number of packets per second. The gap will be adjusted so as to allow the required number of packets to be sent. • % Max Rate—as a percentage of the maximum rate obtainable. The *Apply* button must be clicked before any change goes into effect.
Apply	The *Apply* button must be clicked before any change goes into effect.

Global Line Rate Configuration

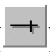
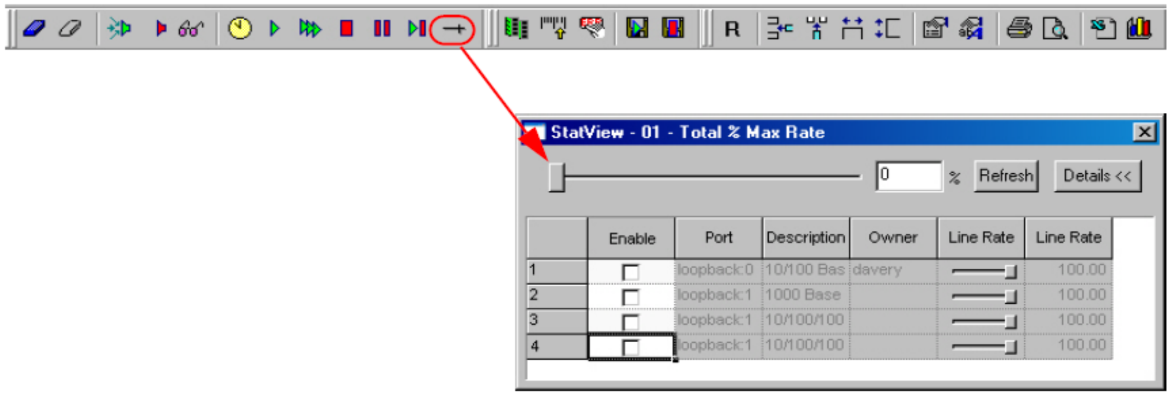
The *Global Line Rate* icon () allows to change the line rate for ports in the Statistic View. The slide bar will change the total percentage of the maximum line for each port indicated port. Selecting this icon opens the *Total % of Max Rate* dialog box. *Figure:Total % Max Rate Dialog* shows the *Total % Max Rate* dialog box.

Figure:Total % Max Rate Dialog



The *Table:Total % Max Rate Fields* describes the fields on the *Total % Max Rate* dialog.

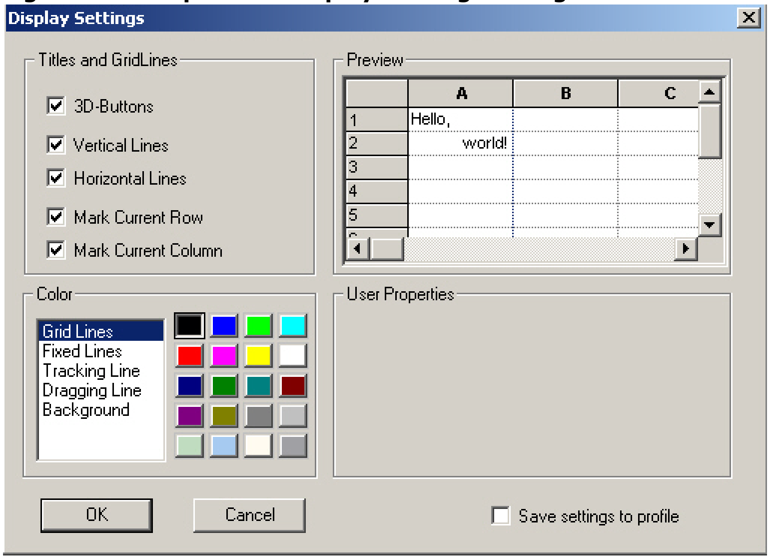
Table:Total % Max Rate Fields

Field	Usage
Slide Bar	Adjusts the percentage of the maximum line rate for all ports selected in the list. When this bar is moved, the percentage number to the right is changed.
Percentage	Shows the percentage number for the line rate usage for all selected ports. When this number is changed, the Slide Bar moves.
Details	Selecting this button displays or hides the fields listed for individual Latency Views.
Enable	This check box enables the use of the line rate slide bar and other configurable port options.
Port	Specifies the port number by chassis, card slot, and port.
Description	Describes the port type (that is, 10/100 base TX).
Owner	Shows the port owner (if applicable).
Line Rate	A slider bar for adjusting the percentage of the max line rate for a particular Statistic View. When this is moved, the percentage number to the right changes.
Line Rate	A percentage number used for adjusting the max line rate for the Statistic View. When this change, the slider bar to the left moves.

Grid Properties—Display Settings

The *Display Settings* dialog is shown in *Figure:Grid Properties—Display Settings Dialog*.

Figure:Grid Properties—Display Settings Dialog



The fields in the dialog are described in *Table:Grid Properties—Display Settings Dialog*.

Table:Grid Properties—Display Settings Dialog

Field	Sub-Field	Usage
Titles and Grid-lines	3D-Buttons	Provides shading for the column and row labels making them appear as buttons.
	Vertical Lines	Draws vertical lines between columns.
	Horizontal Lines	Draws horizontal lines between rows.
	Mark Current Row	Causes the current row's label to appear declicked.
	Mark Current Column	Causes the current column's label to appear declicked.
Color	Grid Lines	Sets the default color for all grid lines.
	Fixed Lines	Sets the color for the line separating the heading rows and the body of the chart.
	Tracking Line	Sets the color for the line separating the heading rows and the body of the chart, when the area is highlighted.
	Dragging Line	The color of the line used to indicate the new position of a relocated column or row.
	Background	Sets the color for the part of the spreadsheet window that has no data grid.
Preview		Shows a preview of the selections made in the display.

Cells Format Dialog

The *Cells Format* dialog consists of five tabs for configuring custom grid formats for the Statistic View, as described in the following sections:

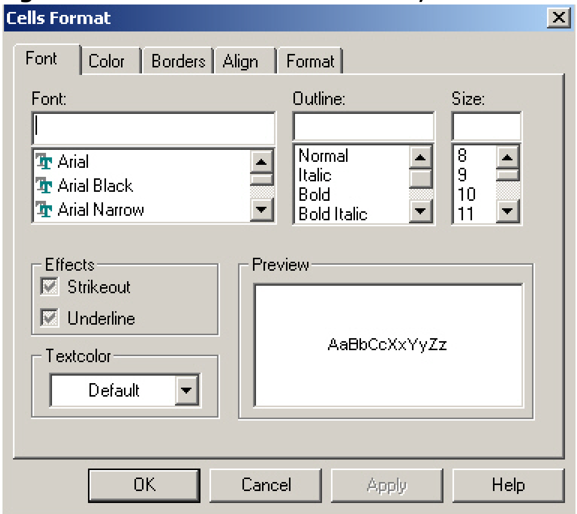
- *Font Tab*
- *Color Tab*
- *Borders Tab*

- *Align Tab*
- *Format Tab*

Font Tab

The *Font* tab controls the fonts used within cells and is shown in *Figure:Statistic View—Cells Format, Font Tab*.

Figure:Statistic View—Cells Format, Font Tab



Where a field is blank, or the check box is dimmed (as in the *Strikeout* and *Underline* attributes in the figure above), then the spreadsheet default is applied. The fields in this dialog are described in *Table:Statistic View—Cells Format, Font Tab Fields*.

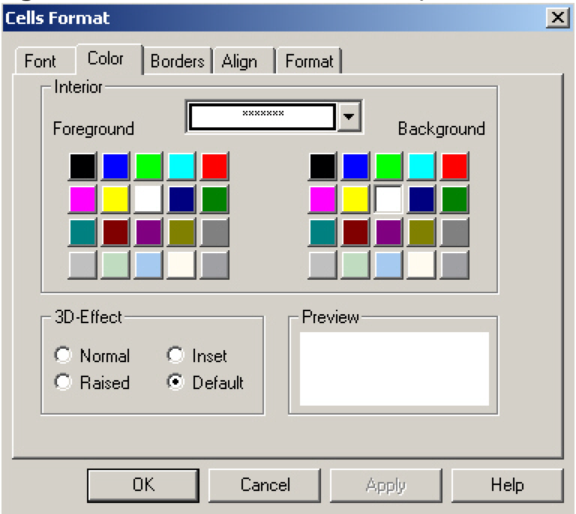
Table:Statistic View—Cells Format, Font Tab Fields

Field	Usage
Font	Selects the font to be used in the selected cells. Selects from the system installed fonts.
Outline	Selects the representation of the font: normal, italic, bold, bold-italic, not bold, and not italic.
Size	Selects the font size to be used in the selected cells. A font size may be selected from the list, or typed directly into the box.
Effects	Selects strikeout and or underline for the selected cells.
Textcolor	Selects the color for text in the selected cells.
Preview	Previews the results of the selections.

Color Tab

The *Color* tab is used to set the color used within cells and is shown in *Figure:Statistic View—Cells Format, Color Tab*.

Figure:Statistic View—Cells Format, Color Tab



The fields in the tab are described in *Table:Statistic View—Cells Format, Color Tab Fields*.

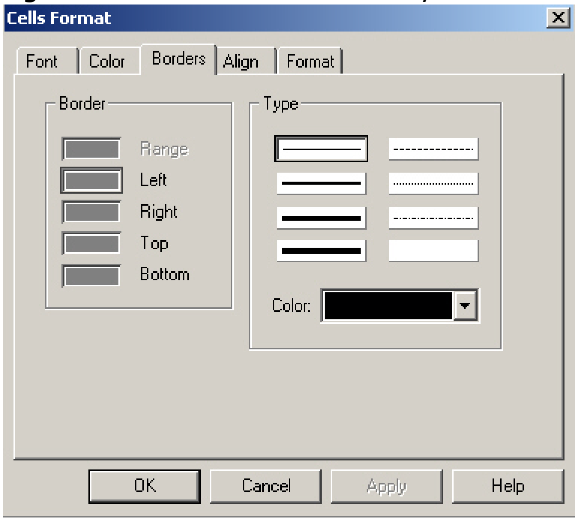
Table:Statistic View—Cells Format, Color Tab Fields

Field	Usage
Top Drop Down Box	Selects a black and white background pattern, rather than a combination of colors. The initial selection of '******' indicates use of the spreadsheet default.
Foreground	Selects the foreground color used to display text. Selection of either a foreground or background color overrides any black and white selection.
Background	Selects the background color used in the selected cells. Selection of either a foreground or background color overrides any black and white selection.
3D-Effect	Selects the display effect of the selected cells. The choices are: • Normal—a flat display. • Raised—the cells appear raised up. • Inset—the cells appear declicked. • Default—the spreadsheet default is used.
Preview	Previews the results of the selections.

Borders Tab

The *Borders* tab, used to place border lines around cells, is shown in *Figure:Statistic View—Cells Format, Borders Tab*.

Figure:Statistic View—Cells Format, Borders Tab



The fields in this tab are described in *Table:Statistic View—Cells Format, Borders Tab Fields*.

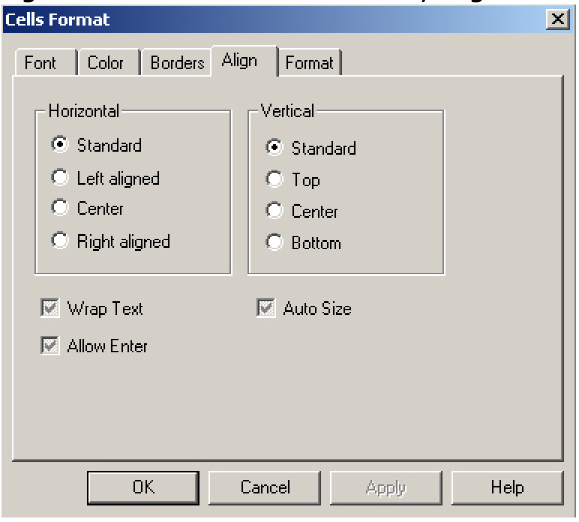
Table:Statistic View—Cells Format, Borders Tab Fields

Field	Usage
Border	Select which side or sides of the cells to place border lines along. Any combination of left, right, top, and bottom.
Type	Select the type of border line to apply. The left column offers different line widths, and the right column offers different line styles.
Color	Select the line color from the list.

Align Tab

The *Align* tab, used to set the alignment of the text within the cells, is shown *Figure:Statistic View—Cells Format, Align Tab*.

Figure:Statistic View—Cells Format, Align Tab



Where a check box is dimmed in the tab, the spreadsheet default is applied. The fields in this tab are described in *Table:Statistic View—Cells Format, Align Tab Fields*.

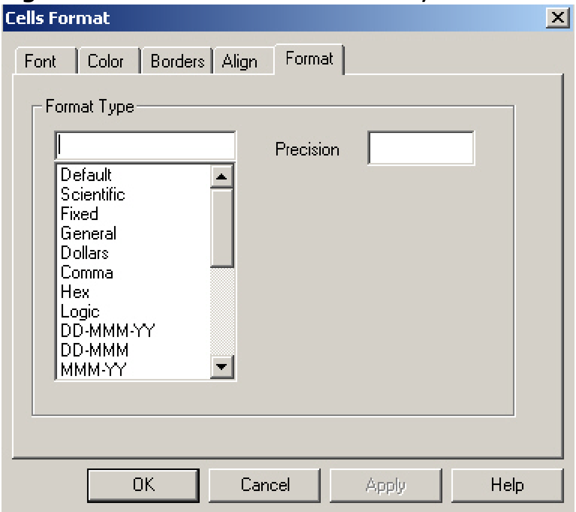
Table:Statistic View—Cells Format, Align Tab Fields

Field	Usage
Horizontal	Select the horizontal alignment of text in the selected cells. One of standard (spreadsheet default), left alignment, centered, or right aligned.
Vertical	Select the vertical alignment of text in the selected cells.
Wrap Text	If selected and not dimmed, wraps text that exceeds the cell's width onto a new line within the cell.
AutoSize	If selected and not dimmed, the column width expands to hold the entered text.
Allow Enter	If selected and not dimmed, the *Enter* key causes a new line to be started in the cell.

Format Tab

The *Format* tab, used to define the format of data in the cells, is shown in .

Figure:Statistic View—Cells Format, Format Tab



The fields in the tab are described in *Table:Statistic View—Cells Format, Format Tab*.

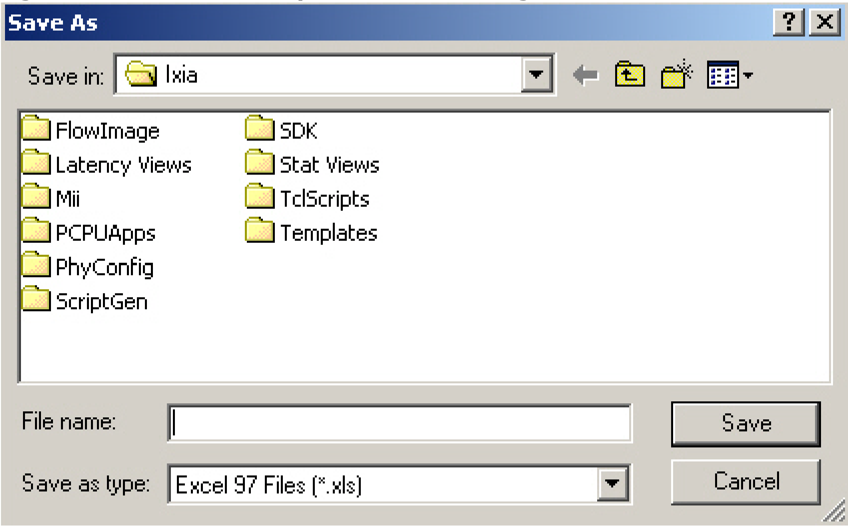
Table:Statistic View—Cells Format, Format Tab

Field	Usage
Format Type	Select one of the standard numeric formats.
Precision	The precision/scientific notation used for the numeric format (for example, hex = 0x0).

Spreadsheet—Export to Excel File Dialog

The export to Excel file *Save As* dialog is shown *Figure:Statistic View—Export to Excel Dialog*.

Figure:Statistic View—Export to Excel Dialog



The standard file *Save As* dialog allows the selection/specification of a file name for the saved file, which is stored in Excel format.

Using Chart View

The charting process may be performed either on the instantaneous, real-time statistics data or on static data obtained when testing has stopped. The process of charting starts with the selection of one or more ranges of data on the spreadsheet.

For example, in the following fictitious spreadsheet with the indicated selection (shown in *Figure:Logging and Alerts Dialog–Single Stat*), the vertical bar chart corresponding to the selection follows in *Figure:Statistic View—Sample Chart*.

Figure:Statistic View—Chart Data Selection

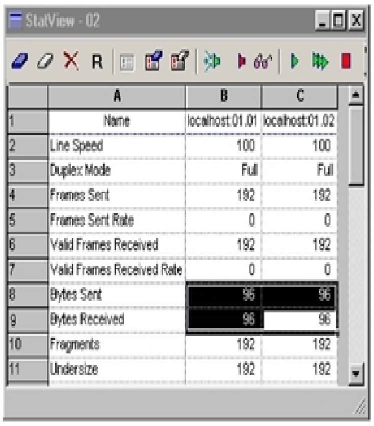
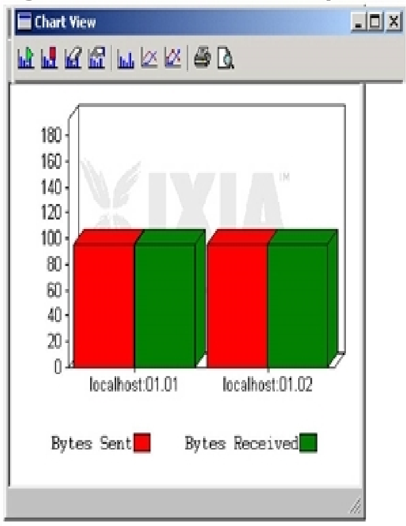


Chart View Dialog

Press the *Create Chart* icon () in the Statistic View spreadsheet toolbar to display the *Chart View* dialog. An example is shown in *Figure:Statistic View—Sample Chart*.

Figure:Statistic View—Sample Chart



The format of the chart may be changed through the use of the *Chart Properties* icon ()at the top of the *Chart View* dialog, as shown in *Figure:Statistic View—Chart Toolbar*. See the *Chart Properties* window for configuration specifics.

Figure:Statistic View—Chart Toolbar

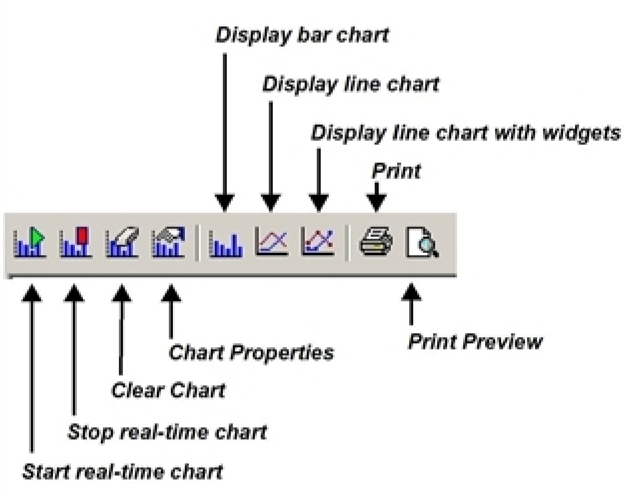
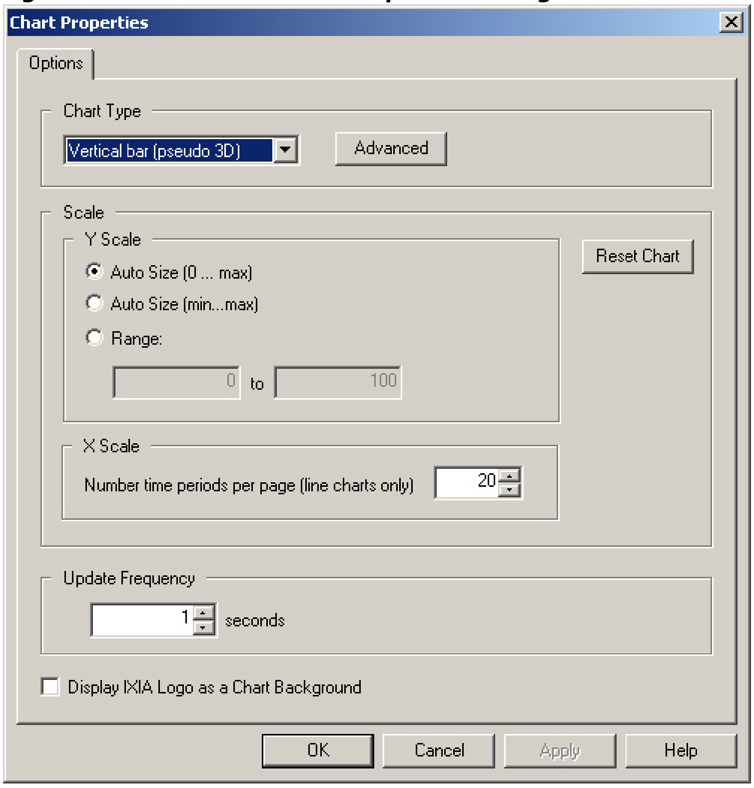


Chart Properties

The *Chart Properties* icon () provides dialogs that allows for scale specification and chart type selection, as shown in .

Figure:Statistic View—Chart Properties Dialog



The fields on this dialog are described in *Table:Statistic View—Chart Properties Dialog Fields*.

Table:Statistic View—Chart Properties Dialog Fields

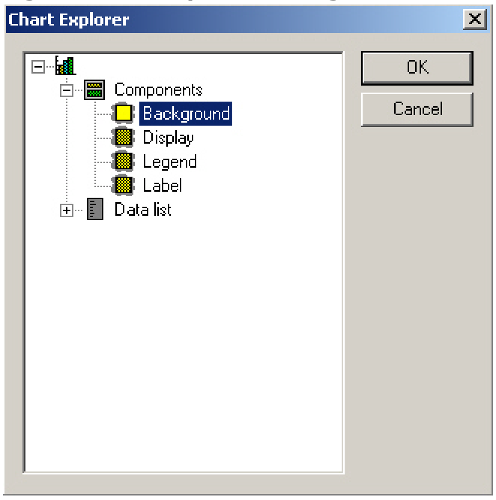
Boxed Area	Field	Usage
Chart Type	List	Lists the different types of charts that are available. The choices available and illustrations are available in the discussion of charting. *Chart View Dialog*.
	Advanced...	This button makes available a series of dialogs that present each component of the chart in a form that may be individually customized in any way through the Chart Explorer window, as described in *Chart Explorer Dialog*.
Scale - Y Scale	Auto Size (0 ... max)	Allows the chart to automatically scale in size.
	Auto Size (min...max)	Allows the chart to automatically scale in size.
	Range	Allows the vertical scale to be set explicitly.
	From	Low vertical scale value.
	To	High vertical scale value.
X Scale	Number of time periods per page (line charts only)	Select the number of time periods which will be displayed in the line chart along the x-axis.
Reset Chart		Resets the chart to its default configuration.

Boxed Area	Field	Usage
Update Frequency		Select the time interval between updates of the data displayed in the chart.
Display IXIA logo as a Chart Background		If selected, the IXIA logo will appear as a back-ground in the chart.

Chart Explorer Dialog

The *Chart Explorer* dialog is displayed when the *Advanced...* button is clicked, and is shown in *Figure:Chart Explorer Dialog*.

Figure:Chart Explorer Dialog



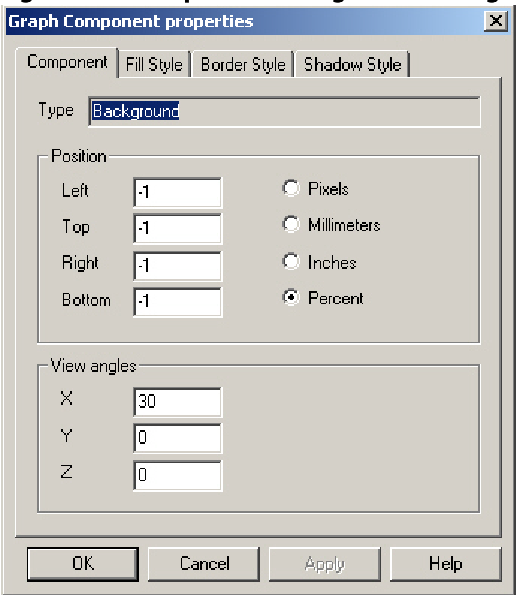
The components listed in this window allow to access many standard graphics properties for configuring the Chart View. The following dialogs can be displayed by double-clicking the appropriate item in the list:

- *Background Dialog*
- *Display Dialog*
- *Legend Dialog*
- *Label Dialog*

Background Dialog

The *Background* dialog provides with four tabs that allow customization of the graphic back-grounds for the charts, as shown in *Figure:Chart Explorer—Background Dialog*.

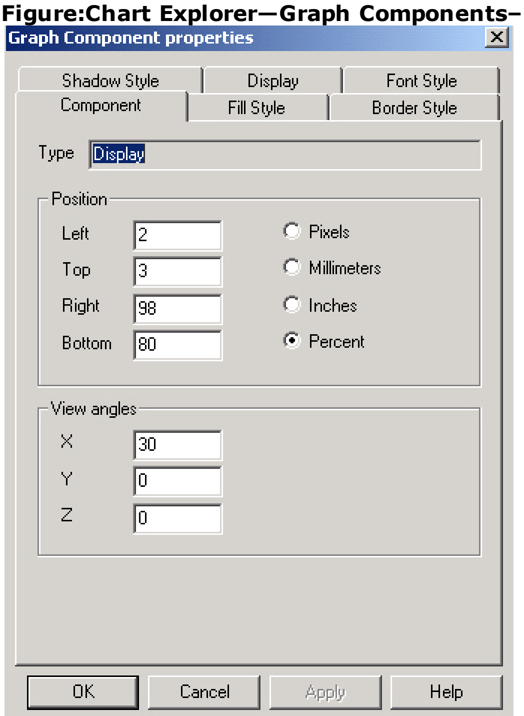
Figure:Chart Explorer—Background Dialog



Display Dialog

The *Display* option provides with six tabs which allow customization of the display properties for the charts, as shown in *Figure:Chart Explorer—Graph Components–Display*.

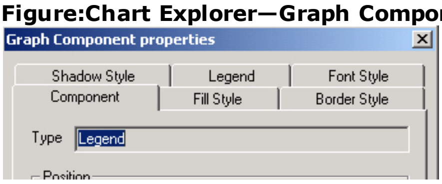
Figure:Chart Explorer—Graph Components–Display



Legend Dialog

The *Legend* option provides with six tabs which allow customization of the legends for the charts, as shown in *Figure:Chart Explorer—Graph Components–Legend*.

Figure:Chart Explorer—Graph Components–Legend



Label Dialog

The *Label* option provides with six tabs which allow customization of the labels to be used in the charts, as shown in *Figure:Chart Explorer—Graph Components–Label*.

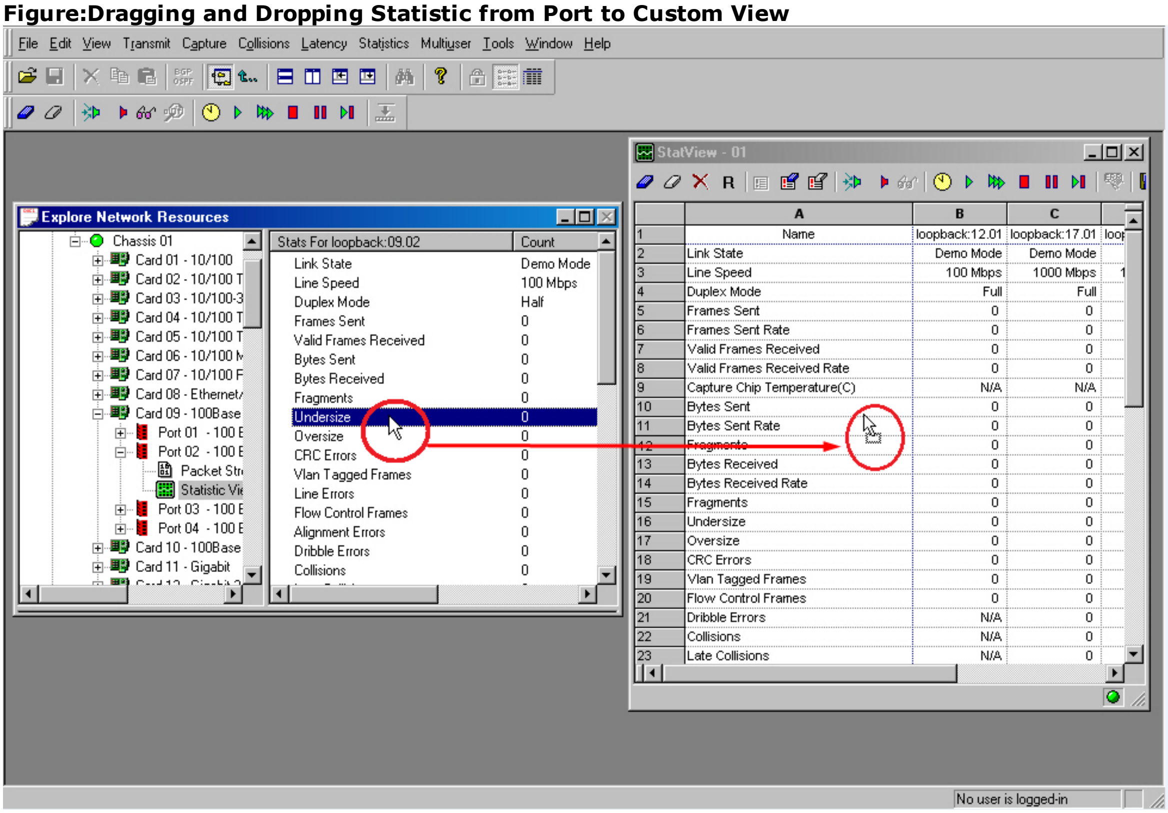
Figure:Chart Explorer—Graph Components–Label

Adding Fields and Ports to Custom Views by 'Drag and Drop'

Fields and their related ports can be dragged from a Port Statistic View and dynamically added to an existing Custom Statistic View. The steps to accomplish this are:

1. Create a Custom Statistic View as described in *Statistic View—Custom Views* above. Leave the view open in the IxExplorer window.
2. Open a Port Statistic View as described in *Statistic View—Port* above.
3. Select a field (or fields) in the Port Statistic View, and drag it (or them) to the Custom Statistic View. *Figure:Dragging and Dropping Statistic from Port to Custom View* demonstrates this action.

Figure:Dragging and Dropping Statistic from Port to Custom View



The selected fields appears in the Custom View. If the port from which the fields were dragged was not originally a member of the Custom View, this action adds the port to the custom view.

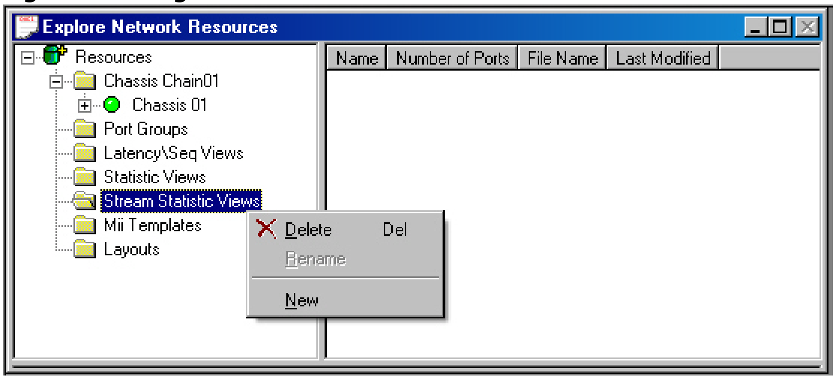
To remove the newly added fields, delete the port from the custom view, as described in *Statistic View—Custom Views* above.

Stream Statistic Views

Stream Statistic Views allow to see statistics for specified streams on all TXS/SFP port module types. To view the statistics for a single stream in the Explore Network Resources window, right-click *Stream Statistic View* folder in the Resources view.

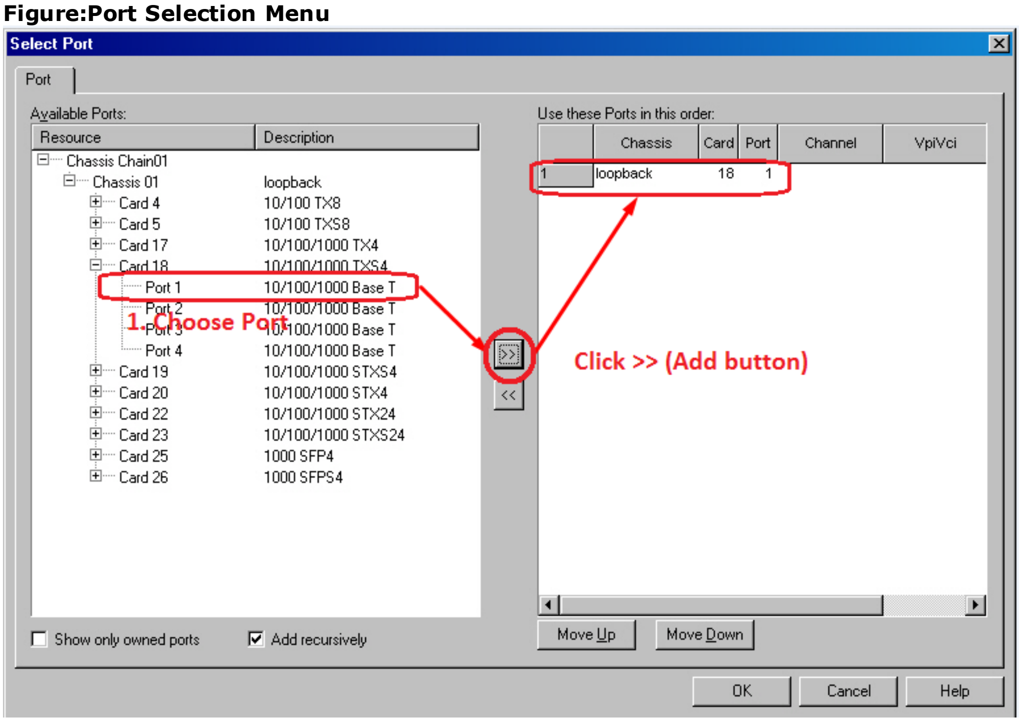
Figure:Creating a New Stream Statistic View shows the Stream Statistic View right-click menu.

Figure:Creating a New Stream Statistic View



Selecting the New option opens the *Select Port* dialog. The *Select Port* dialog is shown in *Figure:Port Selection Menu*.

Figure:Port Selection Menu

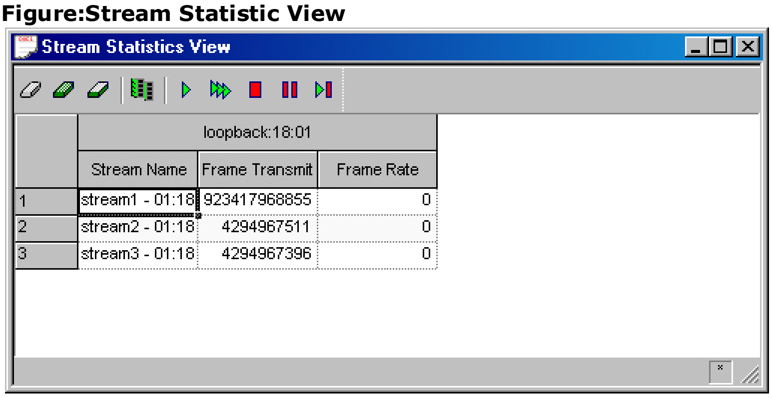


To select streams to show statistics, select a port or ports in the left pane and then the >> button (to Add). Once all ports that have streams to track have been added to the list, click **OK**.

NOTE For a description of the Select Port dialog, *Select Port Dialog*.

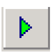
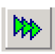
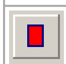
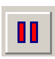
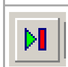
The *Stream Statistic View* dialog displays the per stream statistics. The *Stream Statistic View* dialog is shown in *Figure:Stream Statistic View*.

Figure:Stream Statistic View



Each port is shown with its configured streams. The controls on this dialog are explained in *Table:Stream Statistic View Operation*.

Table:Stream Statistic View Operation

Icon	Field/Control	Usage
	Clear All Statistics	Resets all statistics back to all 0's.
	Clear Stream Statistics	Resets the selected stream statistics for back to all 0's. At least one stream must be highlighted for this icon to be active.
	Clear All Stream Statistics	Resets the statistics for all streams back to all 0's.
	Add/Delete Ports	Opens the *Select Port* dialog, where one or more ports can be added to or deleted from the Statistic View. *Selecting Ports for the Statistic View*.
	Start Transmit	Starts the transmit operation on the selected stream(s).
	Start Staggered Transmit	Starts the transmit operation on the selected streams. A delay is inserted between one port's start transmission and the next.
	Stop Transmit	Stops the transmit operation on the selected stream(s).
	Pause Transmit	Pauses the transmit operation on the selected stream(s).
	Single Step Stream	Sends a single packet on each of the selected streams.

Icon	Field/Control	Usage
	Stream Name	The name of the stream on the selected port.
	Frame Transmit	The total number of frames transmitted on the port through the selected stream.
	Frame Rate	The frame rate of the stream.

Statistics Logging and Alerts

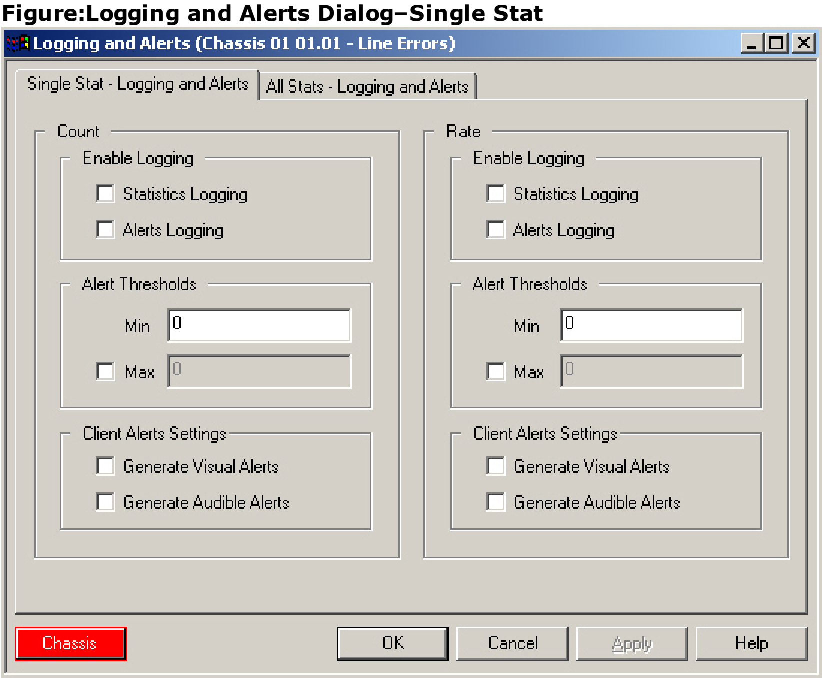
Statistics Logging and Alerts only operates in conjunction with the spreadsheet view of statistics. The spreadsheet view is configured in the *Tools > Options > Statistics View* tab; refer to Statistic Views . *Statistics Logging and Alerts may be configured through the Logging and Alerts dialog, which is accessed by clicking the Logging and Alerts Configuration icon (**), or by right-clicking a cell and selecting Logging and Alerts Configuration. The Logging and Alerts dialog is shown in Figure:Logging and Alerts Dialog–Single Stat. There are two tabs on the dialog:*

- *Single Stat–Logging and Alerts*—allows configuration of logging and/or alerts for a related pair of statistics.
- *All Statistics– Logging and Alerts*—allows configuration of logging and alerts for multiple statistics.

Single Stat–Logging and Alerts

For specifying logging and alerts for a single statistic, click the *Single Stat - Logging and Alerts* tab, which is shown in *Figure:Logging and Alerts Dialog–Single Stat*.

Figure:Logging and Alerts Dialog–Single Stat



This tab allows configuration of logging and/or alerts for a related pair of statistics. The first is a raw count of events and the other is the rate per second of the count. Regardless of which is selected, both may be configured at the same time. For example, if either the *Frames Sent* or *Frames Sent Rate* is selected in the spreadsheet with the right mouse button, then the same dialog will be presented, which will allow alerts for both statistics to be configured. The fields and controls in this dialog are described in *Table:Logging and Alerts Dialog–Single Stat Fields*.

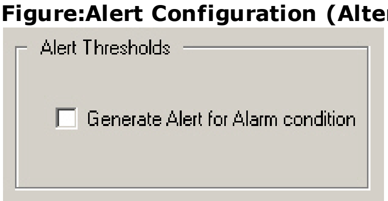
Table:Logging and Alerts Dialog–Single Stat Fields

Area	Field	Usage
Count		The left side of the dialog configures the count form of the statistic.
Enable Logging	Statistics Logging	If selected, statistics logging is enabled for the selected count statistic.
	Alert Logging	If selected, alert logging is enabled for the selected count statistic.
Alert Thresholds	Min	If alert logging or either client alert is enabled, this value specifies the low alert threshold. Measured values below this value will generate logs and/or alerts.
	Max	If alert logging or either client alert is enabled and the check box is selected, then this value specifies the upper alert threshold. Measured values above this value will generate logs and/or alerts.
	(Alternate to Min/Max)) Generate Alert for Alarm Condition	When the alert is configured for a condition which cannot be defined by numerical threshold values, a single check box is provided for enabling an alert for alarm condition applicable to that parameter.
Client Alerts Settings	Generate Visual Alerts	If selected, enables visual alerts on the client station for configured parameters. These would be made visible in the Statistic View spreadsheet with a red, green, or yellow background in the cell for that statistic on the affected port.
	Generate Audible Alerts	If selected, enables audible alerts on the client station for configured parameters. These alerts would be in the form of a beeping noise from the PC speakers. The Statistic View spreadsheet window must be open for these to take effect.
Rate		The right side of the dialog configures the rate form of the statistic.
Enable Logging	Statistics Logging	If selected, statistics logging is enabled for the selected rate statistic.
	Alert Logging	If selected, alert logging is enabled on the chassis for the selected rate statistic.
Alert Thresholds	Min	If alert logging or either client alert is enabled, this value specifies the low alert threshold. Measured values below this value will generate logs and/or alerts.
	Max	If alert logging or either client alert is enabled and the check box is selected, then this value specifies the upper alert threshold. Measured values above this value will generate logs and/or alerts.
Client Alerts	Generate	If selected, enables visual alerts on the client station for

Area	Field	Usage
Settings	Visual Alerts	configured parameters. These would be made visible in the Statistic View spreadsheet with a red, green, or yellow background in the cell for that parameter on the affected port.
	Generate Audible Alerts	If selected, enables audible alerts on the client station for configured parameters. These alerts would be in the form of a beeping noise from the PC speakers. The Statistic View spreadsheet window must be open for these to take effect.
Chassis	Chassis Button	This button invokes the *Logging and Alerts* tab of the *Chassis Properties* dialog which allows logging and alerts to be configured for the chassis as a whole. Refer to *Chassis Properties—Logging and Alerts*.

For state conditions, where an allowable range with threshold values is not applicable, the Alert Thresholds section is shown in *Figure:Alert Configuration (Alternate display)*.

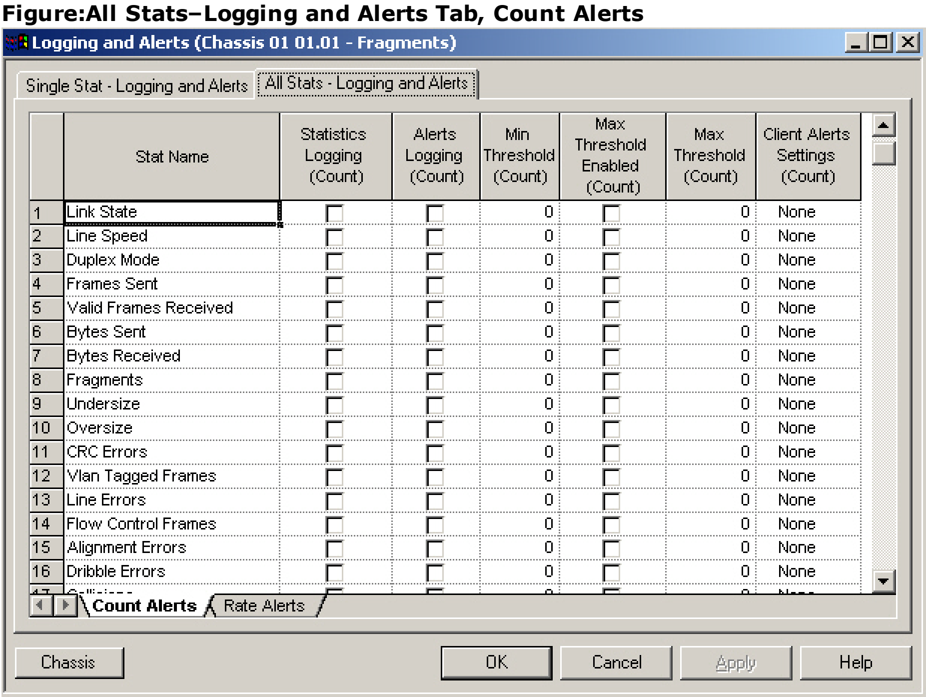
Figure:Alert Configuration (Alternate display)



All Statistics– Logging and Alerts

For specifying logging and alerts for multiple statistics, click the *All Stats–Logging and Alerts* tab, which is shown in *Figure:All Stats–Logging and Alerts Tab, Count Alerts*.

Figure:All Stats–Logging and Alerts Tab, Count Alerts



The *All Stats–Logging and Alerts* tab has two sub-tabs along the bottom edge: *Count Alerts* and *Rate Alerts*. The columns allow to configure statistics logging and/or alerts for all of the statistics for the port. The screen can be scrolled left-to-right to access all of the columns. The columns are selectable; right-clicking a column heading displays a pop-up menu with options for modifying the column properties.

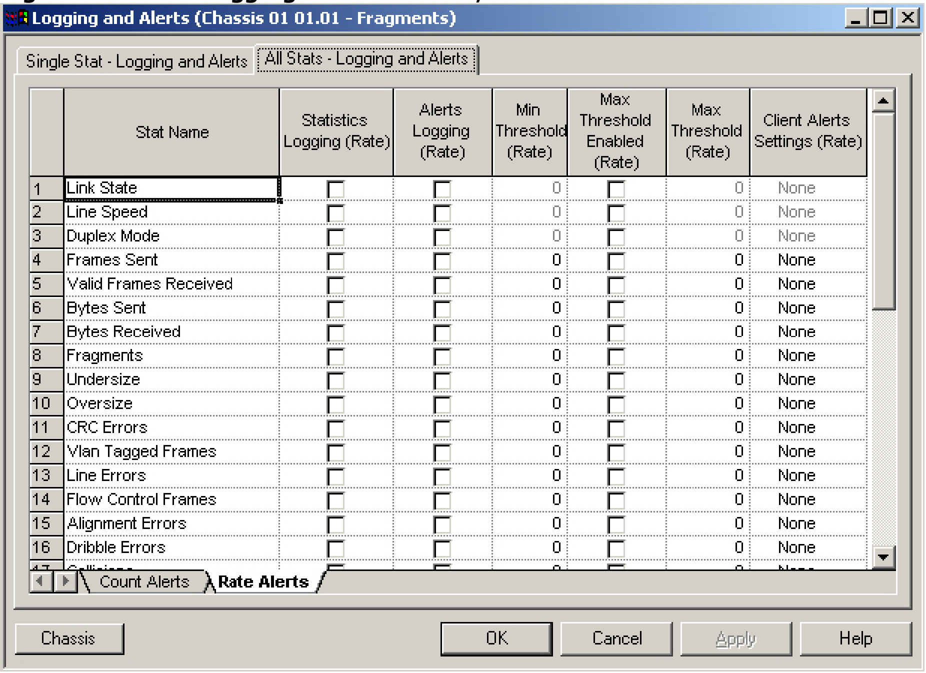
Columns and controls for the *Count Alerts* sub-tab are described in *Table:All Stats–Logging and Alerts Tab, Count Alerts*.

Table:All Stats–Logging and Alerts Tab, Count Alerts

Field	Usage
Stat Name	The name of the statistic which is being monitored for this port.
Statistics Logging (Count)	If selected, statistics logging is enabled for the statistic for this port.
Alerts Logging (Count)	If selected, alert logging is enabled for the statistic for this port.
Min Threshold (Count)	If alert logging or either client alert is enabled, this value specifies the lower alert threshold. Measured values below this value will generate logs and/or alerts.
Max Threshold Enabled (Count)	If alert logging or either client alert is enabled and the check box is selected, then the corresponding Maximum Threshold value in the next column specifies the upper threshold value. Measured values above this value will generate logs and/or alerts.
Max Threshold (Count)	If alert logging or either client alert is enabled and the Maximum Threshold (Enabled) check box is selected, then this value specifies the upper alert threshold. Measured values above this value will generate logs and/or alerts.
Client Alerts Settings (Count)	Selects the type of Alerts settings to be enabled. Select the cell in this column to open the alert setting list. Select one of: • **None**—Indicates that no client alerts are enabled for this statistic for this port. • **Audio**—Enables audible alerts on the client station for configured statistics in the form of a beeping noise from the PC speakers. The Statistic View spreadsheet window must be open for these to take effect. • **Visual**—Enables visual alerts on the client station for configured statistics. These would be made visible in the Statistic View spreadsheet with a red, green, or yellow background in the cell for that statistic on the affected port. • **Audio + Visual**—Enables both visual and audible alerts (as described above) for this statistic for this port.

Logging and Alerts for multiple statistics can be also configured for rates by using the *Rate Alerts* sub-tab as shown *Figure:All Stats–Logging and Alerts Tab, Rate Alerts* .

Figure:All Stats–Logging and Alerts Tab, Rate Alerts

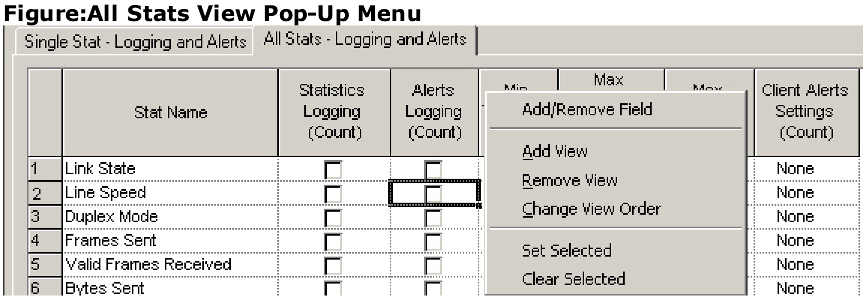


This spreadsheet uses the same set of columns as the *Count Alerts* sub-tab, but applies to rate-based alerts. *Table:All Stats–Logging and Alerts Tab, Count Alerts* for an explanation of the fields and columns.

Logging and Alerts Dialog–All Stats–Configuring Views

The *All Stats* tab in the *Logging and Alerts* dialog can be configured to suit varied needs. Right-click a column heading on the *Count Alerts* or *Rate Alerts* sub-tab (which are the default views), to display the pop-up menu shown *Figure:All Stats View Pop-Up Menu*.

Figure:All Stats View Pop-Up Menu



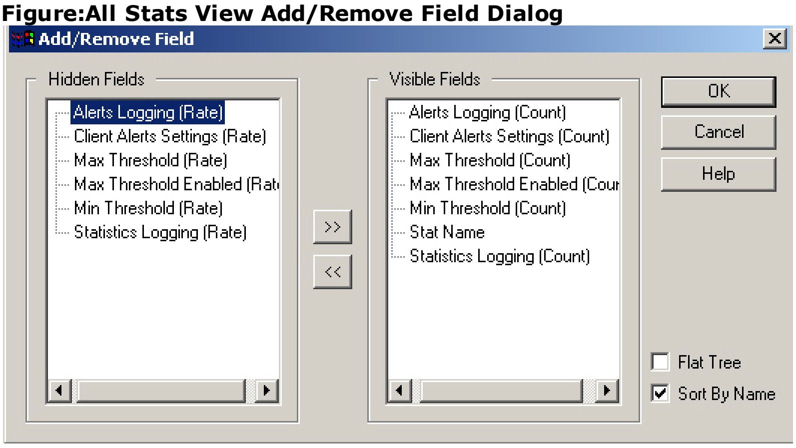
The pop-up menu allows to select the following options.

- *Add/Remove Field Option*
- *Add View Option*
- *Remove View*—deletes the currently displayed view sub-tab from the *All Stats* tab.
- *Change View Order Option*
- *Set Selected*—you can enable all of the highlighted parameters at one time.
- *Clear Selected*—you can disable all of the highlighted parameters at one time.

Add/Remove Field Option

To add or remove a field (column), right-click the column and select *Add/Remove Field*, and the dialog shown in *Figure:All Stats View Add/Remove Field Dialog* will be presented.

Figure:All Stats View Add/Remove Field Dialog

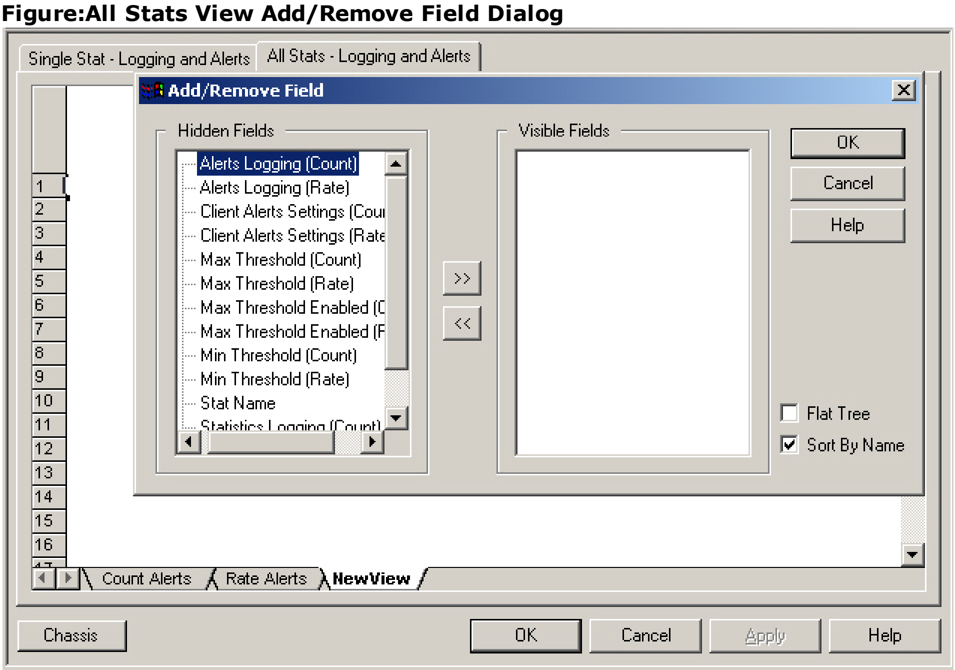


Highlight field names in the *Hidden Fields* list in the left pane, and click the >> button to move them to the *Visible Fields* list in the right pane. To remove fields from the view, highlight and move the field names to the left pane using the << button.

Add View Option

To add another view (a sub-tab, such as the *Count Alerts* or *Rate Alerts*) containing only specific columns, right-click an existing sub-tab and select *Add View* in the pop-up menu, and the dialog shown in will appear.

Figure:All Stats View Add/Remove Field Dialog

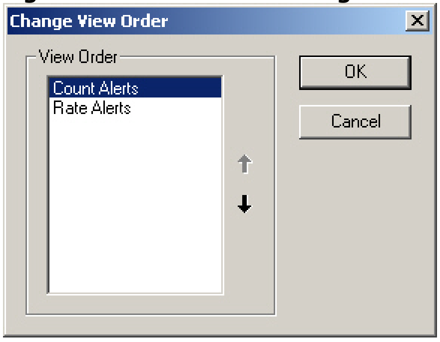


Select the fields/columns to be displayed in the new view, using the same method used with the *Add/Remove Field* dialog described above. Enter a name for the new view in the tab at the bottom of the view window.

Change View Order Option

Click the *Change View Order* option on the pop-up menu to display the *Change View Order* dialog as shown in . This dialog is used to change the order of the tab labels shown at the bottom edge of the *All Stats* tab.

Figure:All Stats View—Change View Order



Use the arrow buttons to move a selected view feature up or down.

NOTE This section describes the function of the Logging and Statistics Change View dialog. There is a similar dialog found for the Stream Grid in the main IxExplorer window. It functions in the same manner.

Customizing the Stream Edit Window for more information about the Stream Grid.

Chapter 16 - Packet Group Statistic View

Packet Group Statistic View

The Packet Group Statistic View allows the latency data (including Inter-Arrival Time) to be collected from one or more ports that are configured to receive packet groups. Packets representing different types of traffic profiles can be associated with packet group identifiers (PGIDs). The receiving port measures the minimum, maximum, and average latency in real time for each packet belonging to different groups. Measurable latencies include Instantaneous Latency, where each packet is associated with one group ID only, and Latency Over Time, where multiple PGIDs can be placed in 'time buckets' with fixed durations.

Data may be viewed as a spreadsheet and/or charted. For certain modules, data related to sequence checking error thresholds may also be monitored in this view.

To display latency/sequence checking data for one or more ports side-by-side, right-click *Packet Group Statistic Views* (under *Global Views*) in the tree and select *New*, or choose a previously defined view in the detail pane. Selecting *New* will open a window where one or more ports may be selected to view the data in a side-by-side display. Latency data is shown in the form of a spreadsheet labeled *Packet Group Statistic View*. Some modules also support *Latency over Time* and *Inter-Arrival Time*. Latency Reports appear as additional, named spreadsheets in the same display.

NOTE There may be a minimum frame size necessary to support latency measurements on particular load modules. Refer to the appropriate chapter in the Reference Manual for limits.

For more information on Latency, Sequence Checking, and Inter-Arrival Time, see the following sections in the 'Theory of Operation: General' chapter in the *Ixia Platform Reference Manual*:

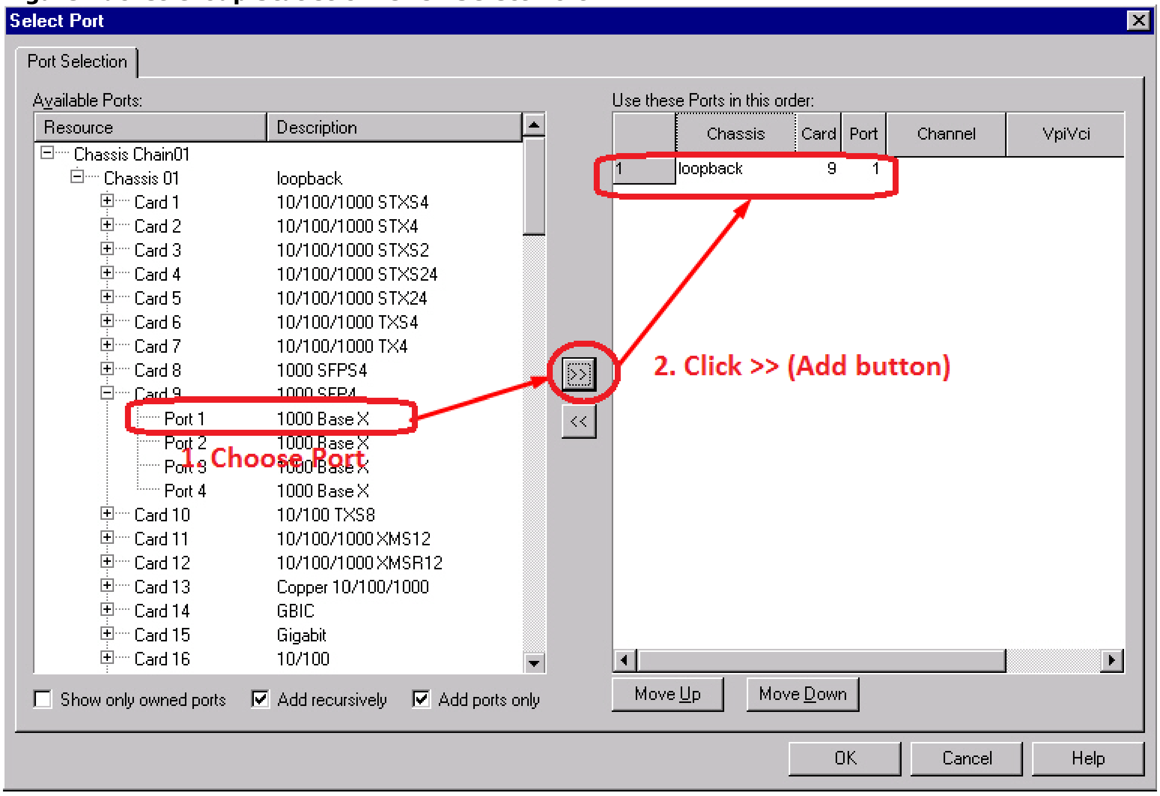
- Packet Group Operation
- Latency/Jitter Measurements
- Sequence Checking Operation

Port Selection

The Packet Group Statistic Views *Select Port* dialog for selecting new or additional ports is shown in *Figure:Packet Group Statistic Views—Select Port*.

NOTE For a description of the Select Port dialog,*Select Port Dialog*.

Figure:Packet Group Statistic Views—Select Port



On the left side of the window, highlight the desired ports using either the shift-click or control-click methods, and then click the *Add* button to place them in a list on the right side of the window. After selections are complete, click *OK*, and the *Packet Group Statistic View* spreadsheet will appear.

Any port may be selected, but latency measurements will not occur unless several things are set up correctly (see the Port Data Capture Capabilities section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for a full description of packet group and latency operation). Configuration requirements are described below:

NOTE	Type-3 cards may not be used to transmit packet group data.

- The Receive Mode on the ports in the latency group must be set for Packet Groups or Wide Packet Groups. *Receive Mode Tab for the setting of latency groups and associated parameters.*
- The transmitting port or ports must be configured to generate packet group data in the manner that the selected receive ports expect. *Instrumentation Box* for setting up Packet Group mode on transmitting ports.
- When ports support sequence checking with threshold error, a combination Latency/sequence Checking View may be set up. The ports must also have sequence checking enabled for receive modes. *Advanced Sequence Checking* for further information.

Packet Group Stats/Sequence Checking Data Display

The Packet Group Statistics View has different modes which are described in the following sections:

Packet Groups View

A Packet Groups view for a group with a single member (a Gigabit port) is shown in *Figure:Packet Group Statistics View—Packet Group Receive Mode*. This view is set up for latency measurements only, without the sequence checking option.

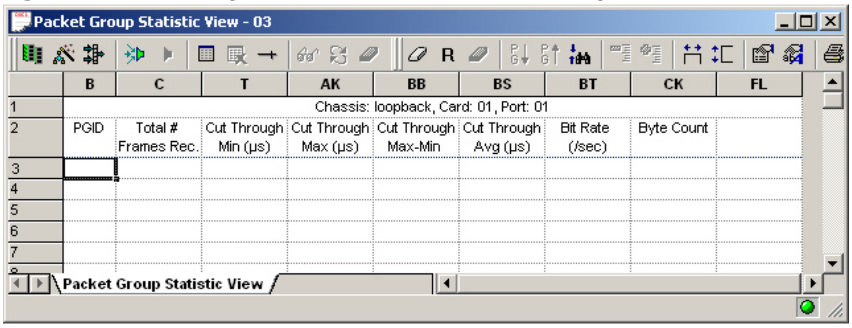
CAUTION For OC-192c POS legacy modules (in packet group mode)—

When performing latency measurements, the following restrictions apply:

1024 or fewer packet group IDs **should** be used if different frame sizes are used at full line rate.

More than 1024 packet group IDs **may** be used at line rate and varying frame sizes, so long as the frame sizes are between 256 and 1024 bytes.

Figure:Packet Group Statistics View—Packet Group Receive Mode



Each port in the packet group is displayed in a set of columns, with a blank column between ports. The first row of the display specifies the port. The second row has the column headings for the latency parameters. *Refer to Figure:Packet Group Statistic Views—Select Port* for explanations of these headings.

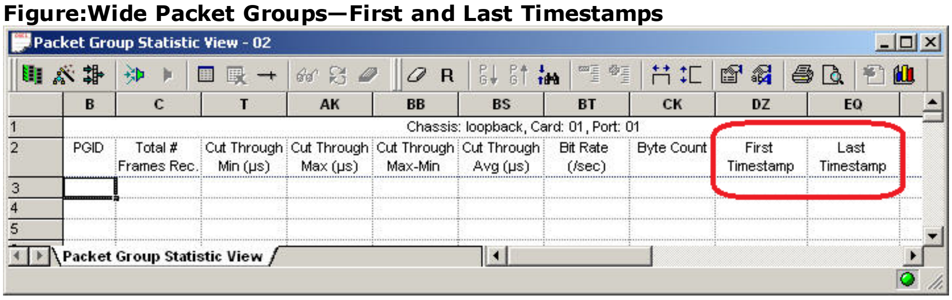
NOTE When Wide Packet Groups are used, two extra columns for First and Last Timestamp are included. See Wide Packet Groups.

The rest of the rows contain latency data. For instantaneous latency, some rows may be appear to be empty, but this is due to the lack of received data with the Packet Group ID that corresponds to that row.

Wide Packet Groups

If the *Wide Packet Groups* check box is selected in the *Receive Mode* tab, the Packet Group Statistics View for the port will contain two additional columns, for First Timestamp and Last Timestamp, as shown in *Figure:Wide Packet Groups—First and Last Timestamps*.

Figure:Wide Packet Groups—First and Last Timestamps



The column headings in this view are described in *Table:Wide Packet Groups Statistics View* .

Table:Wide Packet Groups Statistics View

Column Heading	Description
PGID	The Packet Group ID (PGID) is used as a row ID for latency data concerning packets that contain this PGID.
Total # Frames Rec.	The number of packets received with this specific PGID, since the last reset of the data.
Cut Through Min (us)	The minimum delay seen on packets with this specific PGID, measured in microseconds.
Cut Through Max (us)	The maximum delay seen on packets with this specific PGID, measured in microseconds.
Cut Through Max-Min	Maximum delay minus minimum delay.
Cut Through Avg (us)	The average delay seen on packets with this specific PGID, measured in microseconds.
Bit Rate (bit/sec)	The instantaneous bit rate seen on the port, measured in bits per second.
Byte Count	The total number of bytes seen on the port.
First Timestamp	The received timestamp for the first incoming packet. The 6-byte timestamp value for the first packet received with this particular PGID. This value is exclicked, in hex, as multiples of the basic system clock (20 ns intervals).
Last Timestamp	The received timestamp for the last incoming packet. The 6-byte timestamp value for the last packet received with this particular PGID. This value is exclicked, in hex, as multiples of the basic system clock (20 ns intervals).
Standard Deviation	Only available if latency bin is enabled for wide packet group mode. Shows the standard deviation in the latency for the bin.

Delay Variation Measurement Mode

This mode in Receive properties, Wide Packet Groups, Latency/Jitter configuration enables the system to measure delay variation between consecutive frames that are not out of sequence. For details, *Delay Variation Measurement Mode*.

In addition to the statistics for Wide Packet Groups (above,*Table:Wide Packet Groups Statistics View*), the following are specific to the Delay Variation measurement.

Table:Delay Variation Measurement Statistics

Column Heading	Description
DV Min (us)	The smallest of all delay variations measured for a specific flow from the start of statistic collection
DV Max (us)	The largest of all delay variations measured for a specific flow from the start of statistic collection
DV Max -Min (us)	The mathematical subtraction of Min DV from Max DV
DV Avg (us)	Boxcar average value of all the valid delay variations from the start of statistic collection. This is calculated by dividing the total sum of all DV by the number of received frames.
DV Short Term Avg	Boxcar average value of all the valid delay variations from the last time this value was read.

Packet Group/Sequence Checking View

The headings for the Packet Group/Sequence Checking View are shown in *Figure:Packet Group/Sequence Checking View*. The sequence checking information is based on error conditions related to a threshold value defined in the sequence checking dialog for the port's receive mode. **No** error condition exists when the current sequence number is **one** greater than the previous sequence number. The error conditions are described in *Table:Packet Group/Sequence Checking View*

For more information on Sequence Checking using threshold values, *Advanced Sequence Checking*.

CAUTION For OC-192c POS legacy modules (in packet group mode).

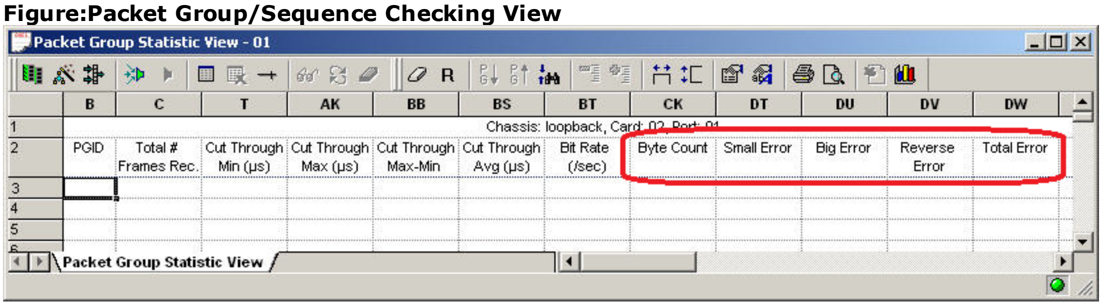
When performing latency measurements, the following restrictions apply:

1,024 or fewer packet group IDs should be used if different frame sizes are used at full line rate.

More than 1,024 packet group IDs may be used at line rate and varying frame sizes, so long as the frame sizes are between 256 and 1,024 bytes.

When performing sequence checking, no more than 1,024 packet group IDs should be used.

Figure:Packet Group/Sequence Checking View



The possible options displayed as column headings in the spreadsheet are described in *Table:Packet Group/Sequence Checking View*.

Table:Packet Group/Sequence Checking View

Column Heading	Description
PGID	The Packet Group ID (PGID) is used as a row ID for latency data concerning packets that contain this PGID.
Total # Frames Rec.	The number of packets received with this specific PGID, since the last reset of the data.
Cut Through Min (us)	The minimum delay seen on packets with this specific PGID, measured in microseconds.
Cut Through Max (us)	The maximum delay seen on packets with this specific PGID, measured in microseconds.
Cut Through Max-Min	Maximum delay minus minimum delay.
Cut Through Avg (us)	The average delay seen on packets with this specific PGID, measured in microseconds.
Bit Rate (bit/sec)	The instantaneous bit rate seen on the port, measured in bits per second.
Byte Count	The total number of bytes seen on the port.
No Error	When the current sequence number is **one** greater than the previous sequence number. Refer to *Advanced Sequence Checking*.
Small Error	A 'Small Error' is counted when the current sequence number minus the previous sequence number is less than or equal to the error threshold (set by software) and not negative. Refer to *Advanced Sequence Checking*.
Big Error	A 'Big Error' is counted when the current sequence number minus the previous sequence number is greater than the error threshold. Refer to *Advanced Sequence Checking*.
Reverse Error	A 'Reverse Error' is counted when the current sequence number is less than the previous sequence number. Refer to *Advanced Sequence Checking.*
Total Error	The 'Total Error' is the sum of all of the sequence checking errors, including: small, bit, and reverse. Refer to *Advanced Sequence Checking*.

The process of collecting latency data starts with deciding whether to perform a single set of measurements or handling multiple time slices.

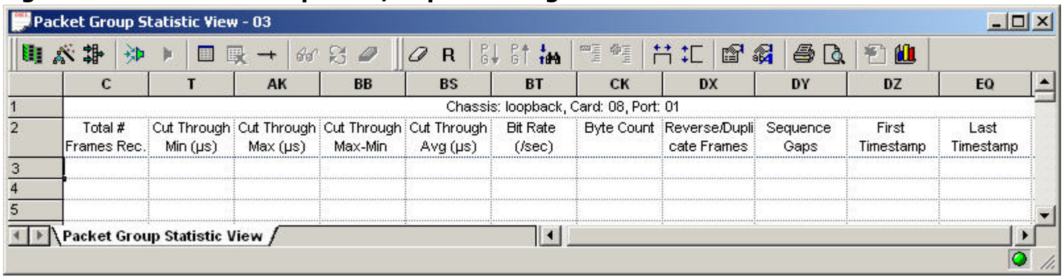
Switched-Path Duplicate/Gap Checking

If the port's *Receive Mode* tab is set up with these two conditions:

- the *Wide Packet Groups* check box is selected and
- the *Switched-Path Duplicate/Gap Checking* option button is selected in the *Sequence Checking* tab,

then the Packet Group Statistic View for the port will contain two additional columns, for *Reverse/Duplicate Frames* and *Sequence Gaps*, as shown in the following figure.

Figure:Switched-Path Duplicate/Gap Checking View



The extra options displayed as column headings in the spreadsheet are described in *Table:Switched-Path Duplicate/Gap Checking*.

Table:Switched-Path Duplicate/Gap Checking

Column Heading	Description
Reverse/Duplicate Frames	The number of reversed or duplicate frames that arrive on the port. This is used in test switched-path operations. A duplicate frame is a frame that arrives more than once with the same sequence ID, and a reverse frame is counted when the current sequence number is less than the previous sequence number. In most situations, these numbers should be the same.
Sequence Gaps	Records the number of gaps in a sequence, that is, if packets 1, 2, 3, 5 arrive there would be a count of 1 gap.

The remaining columns are explained in *Table:Wide Packet Groups Statistics View*.

Refer to the Switched-Path Duplicate/Gap Checking Mode section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information.

Wide Packet Groups/Sequence Checking—Advanced Sequence Tracking

If the port's **Receive Mode** tab is set up with these three conditions:

- the **Wide Packet Groups** check box is enabled,
- the **Sequence Checking** check box is enabled, and
- the **Late Threshold** value is added in the **Advanced Sequence Tracking** option,

then, five additional statictics appear in the **Packet Group Statistic View** tab. *Configuring Advanced Sequence Tracking of Frame* for more information.

NOTE

Advanced Sequence Tracking options are available in the following load modules:

LSM XMVDC16

ASM XMV 10/100/1000

LSM XM 10/100/1000

FCM GXM

Configuring Advanced Sequence Tracking of Frame

The following steps help to configure the parameters in the IxExplorer application, using relevant load modules, to set advanced sequence tracking options to a frame of data.

To configure Advanced Sequence Tracking, do the following:

1. Click the port that is in transmit mode in the left pane, and then double-click **Packet Streams** in the right pane.

   The Frame/Stream Data tab appears.

2. Double-click any value in one of the rows of the **Frame/Stream Data** table.

   The Stream Properties dialog box appears.

3. In the **Frame Data** tab, select the **Packet Groups** and the **Sequence Checking** check boxes under **Instrumentation Offsets** pane. Note that selecting the **Packet Groups** check box automatically selects the **Time Stamp** check box as well.
4. Click **Ok**.
5. Click the port that is in receive mode in the left pane, and then double-click **Filters, Statistics, Receive Mode** in the right pane.

   The Chassis dialog box appears.

6. Click the **Receive Mode** tab.
7. Select the **Wide Packet Groups** and the **Sequence Checking** check boxes under the **Mode** pane.
8. In the **Sequence Checking** tab, click **Advanced Sequence Tracking**.

   The Late Threshold box is made available.

9. In the **Late Threshold** box**,** type a value in the range of 1 to 19,555.
10. Click **Apply,** and then click **OK** to go back to the **Explore Network Resources** window.
11. In the left pane, scroll to locate the **Global Views** folder, and then double-click the folder to expand it.

    The subfolders under the Global Views folder appears.

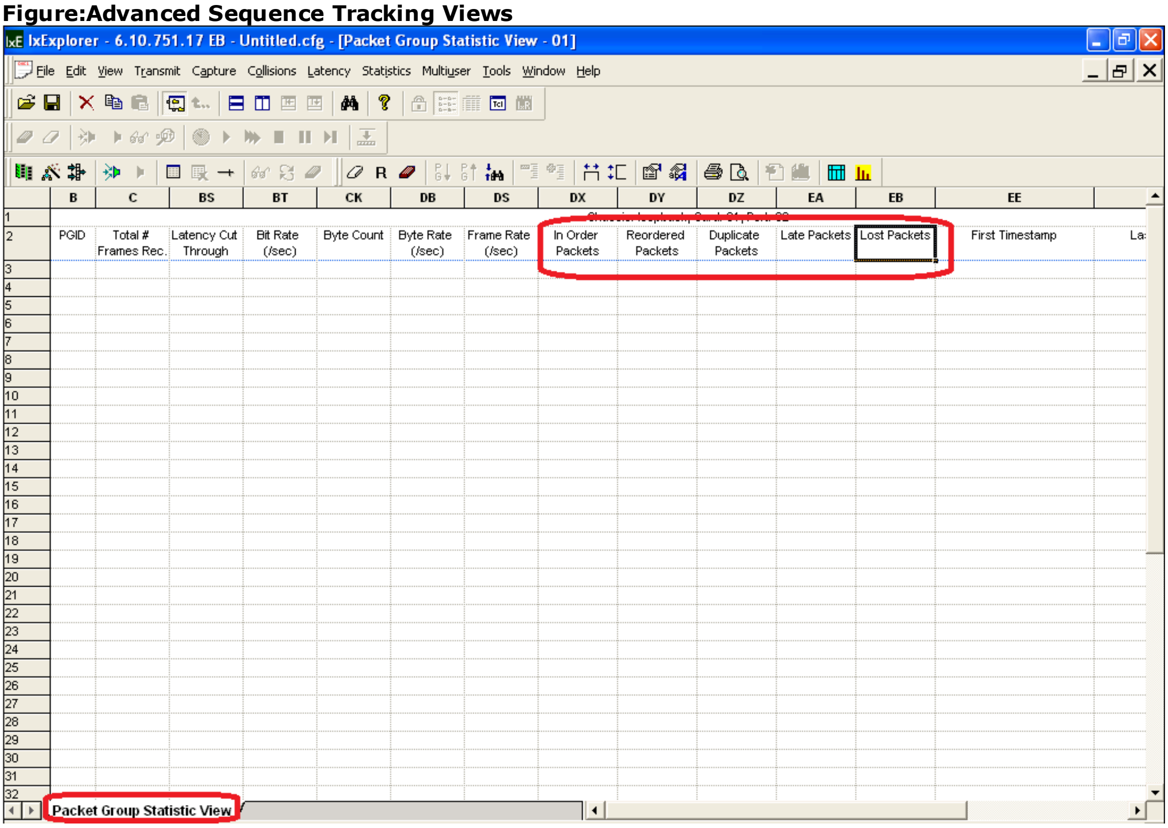
12. Right-click the **Packet Group Statistic Views** folder to open a shortcut menu.
13. Click **New**.

    The Select Port dialog box appears.

14. Select the port that you have configured in receive mode in the preceeding steps, and then click  to add the port to the right pane.
15. Click **OK**.

The **Packet Group Statistic View** window appears where you can view the advanced sequence tracking options.

Figure:Advanced Sequence Tracking Views



The additional advanced sequence tracking options for a frame are described in the following table.

Table:Advanced Sequence Tracking Views Option

Field	Description
In Order Packets	Count of received packets that contain sequence numbers equal to or greater than expected. The expected value is set to one greater than the largest sequence number received. When packets are in order, the frames are received when expected. The **In Order** count is derived by software in the following manner: • Lost = Received Frames - Duplicate - Reordered - Late
Reordered Packets	Count of received packets that contain sequence numbers that are less than expected, but were not counted as Duplicate, and are greater than or equal to the Late Threshold value.
Duplicate Packets	Count of packets that were determined to be duplicates. A received test packet is a duplicate if its value falls within the current sequence run. (A sequence run is a series of sequence numbers from the received test packets that is equal to or less than expected. The sequence run ends when the received sequence number is greater than expected, creating a gap in the series, and a new sequence run is initiated). The sequence run contains all of the sequence numbers from the start of the series up to one less than the expected value. Consequently, a

Field	Description
	received sequence number that falls within the current series must be a duplicate. Received sequence numbers are not checked against previous sequence runs. Therefore, undetected duplicate packets are counted as **Reordered** or **Late**.
Late Packets	Count of received packets that contain sequence numbers that are less than expected, were not counted Duplicate, and are less than the Late Threshold value. Received sequence numbers that are less than expected are due to packets that arrived later than the adjacent packets of the transmitted packet sequence. The threshold may be adjusted to allow these packets to be classified as Reordered (if they arrive before the Late Threshold) or Late (if they arrive after the Late Threshold).
Lost Packets	Frames that were counted as Unknown, but later arrive (and counted as Reordered or Late) are referred to as **Lost**. The **Lost** count can be derived by software in the following manner: • Lost = Unknown - Reordered - Late NOTE It is possible that this equation results in a negative number, which the software treats as 0.

Inter-Arrival Time

If the port's *Receive Mode* tab is set up with these conditions:

- the *Latency/IAT Bins (Inter-Arrival Time)* check box is enabled in the *Wide Packet Groups* tab, and
- the *Inter-Arrival Time* check box is selected in the *Latency/Jitter tab*,

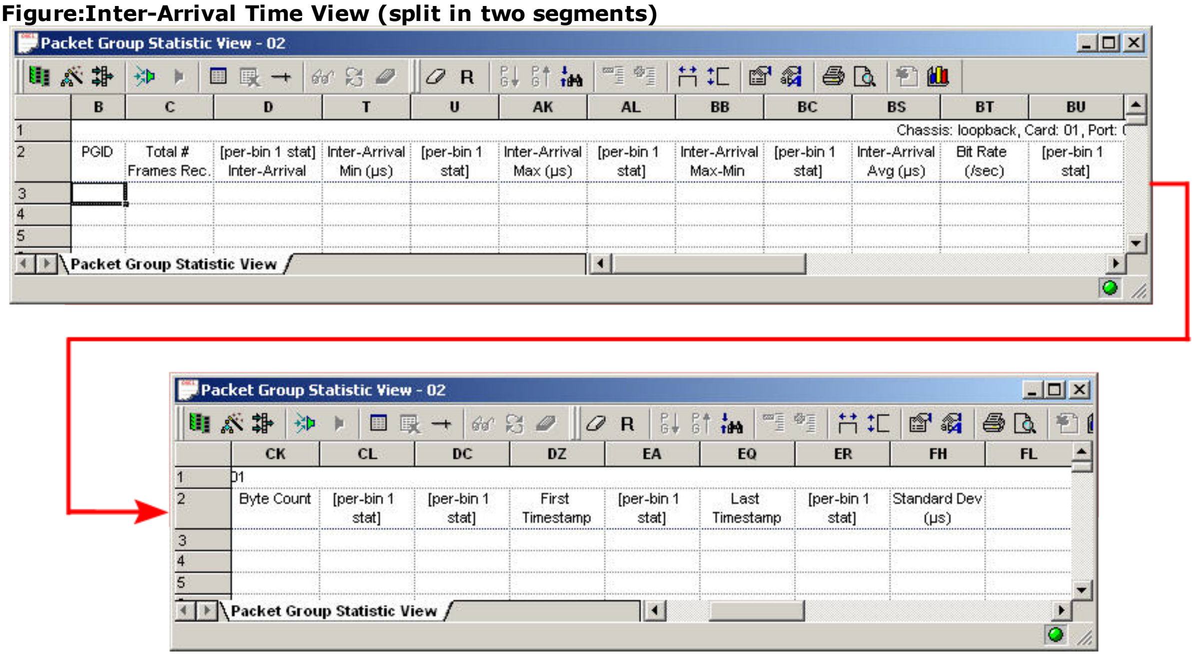
  or

- the *Rate Monitoring* mode is selected (which automatically selects Inter-Arrival Time latency),

then the Inter-Arrival Time view is displayed when creating a Packet Group Statistic View. This view is shown in .

For more information on Inter-Arrival Time, see the *Ixia Platform Reference Manual*.

Figure:Inter-Arrival Time View (split in two segments)



The headings for the columns of data collected in the Inter-Arrival Time view are described in *Table:Inter-Arrival View Columns*

Table:Inter-Arrival View Columns

Field	Description
PGID	The Packet Group ID (PGID) is used as a row ID for inter-arrival time data concerning packets that contain this PGID.
Total # of Frames Rec	The total number of frames received for this PGID.
(per-bin 1 stat) Inter-Arrival	For each listed column statistic, a corresponding bin column is listed for each configured inter-arrival time bin. For information on inter-arrival *Time Bins Configuration*, see *Latency/IAT Bins Configuration*.
Inter-Arrival Min (us)	The smallest packet-to-packet gap in microseconds.
Inter-Arrival Max (us)	The largest packet-to-packet gap in microseconds.
Inter-Arrival Max-Min	The difference between the inter-arrival maximum and minimum values. This measurement is peak to peak inter-arrival time.
Inter-Arrival Avg (us)	The sum of all the packet to packet gaps, divided by the total number of packets.
Bit Rate (/sec)	The instantaneous bit rate seen on the port, measured in bits per second.
Byte Count	The total number of bytes seen on the port.
First Timestamp	(in 'raw' format) The 6-byte timestamp value in the first packet received with this particular PGID. This value is exclicked, in hex, as multiples of the basic system clock (20 ns intervals).
Last Timestamp	(in 'raw' format) The 6-byte timestamp value in the last packet received with this particular PGID. This value is exclicked, in hex, as multiples of the basic system clock (20 ns

Field	Description
	intervals).
Standard Deviation (us)	The standard deviation between expected packet gap and actual packet gaps.

PRBS Mode

Pseudo Random Binary Sequence (PRBS) checking mode is available in the following load modules:

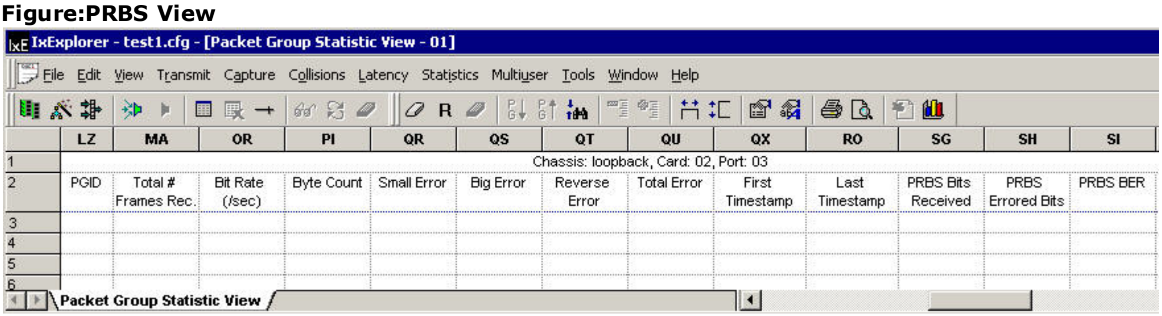
- LM1000STXS4 family
- LM1000TXS4 family
- LM1000SFPS4 family
- OLM1000STXS24 family
- LSM1000XMS12 family
- LSM1000XMV family (not in Data Center Mode)
- ASM1000XMV12
- NGY LSM10GXM family (not in Data Center Mode)

When the port is in PRBS mode, all latency-related statistics are removed and the following per-PGID statistics are added:

- PRBS Bits Received
- PRBS Errored Bits
- PRBS BER

The PRBS view is shown in *Figure:PRBS View*.

Figure:PRBS View



The headings for the columns of data collected in the PRBS view are described in *Table:PRBS View Columns*.

Table:PRBS View Columns

Field	Description
PRBS Bits Received	The number of bits in PRBS payload
PRBS Errored Bits	The number of bits in PRBS payload that are corrupted (that is, ‘in error’)
PRBS BER	The ratio of PRBS Errored Bits to PRBS Bits Received

Table:Packet Format in PRBS Mode shows the packet format when enabled in PRBS mode.

Table:Packet Format in PRBS Mode

Mode : PRBS	Signature 12 bytes	**PGID** 4 bytes	**Sequence** **#** 4 bytes	**PRBS** **Lock** **Pattern** 4 bytes	Header CRC 4 bytes	N-Byte PRBS payload	Reserved	TS 4 bytes	FCS 4 bytes

Rate Monitoring Mode

Rate Monitoring mode is available in the following load modules:

- LSM10GXM family (NGY)
- LSM1000XMV family
- ASM1000XMV12X

The stats for Inter-Arrival Time latency mode will be available when the Receive Mode is set to *Rate Monitoring* mode, as well at the two stats listed below.

The headings for the columns of data collected in the Rate Monitoring view are described in *Table:Rate Monitoring Columns*.

Table:Rate Monitoring Columns

Field	Description
Below Threshold Timestamp	Below threshold timestamp is the time at which the Inter-Arrival Time crossed below the programmed IAT threshold value for the last time. The last time the IAT was greater than the threshold value. Displayed in nanoseconds.
Above Threshold Timestamp	The Above threshold timestamp is the time at which the Inter-Arrival Time crossed above the programmed IAT threshold value for the first time. The first time the IAT was less than the threshold value. Displayed in nanoseconds.

Per PGID Checksum Error Stats Mode

In Per PGID Checksum Error Stats mode, per-flow checksum error statistics will be provided for Tcp\Udp and IPV4 checksum errors.

This mode is available in the following load modules:

- LSM10GXM family (NGY)
- LSM1000XMV family
- ASM1000XMV12X

When the port is in this mode, the following per-PGID statistics are added:

- IPv4 Checksum Errors
- UDP Checksum Errors
- TCP Checksum Errors

Latency/Jitter Options

The Packet Group Statistics View toolbar (*Figure:Packet Group Statistics View Toolbar*) contains the *Options* icon (). Clicking the *Options* icon displays the *Latency Options* dialog, which presents the latency options available, depending on the capability of the load module. These options tabs are described in the following sections:

- *Latency Type Tab*—available for modules that support latency over time (which requires support for sequence checking receive mode). It allows to choose between instantaneous latency (the default) and latency over time.
- *Latency Statistics Tab*—controls the manner in which the received data rate is displayed.
- *Latency Update Interval Tab*—available for all modules that support latency testing.

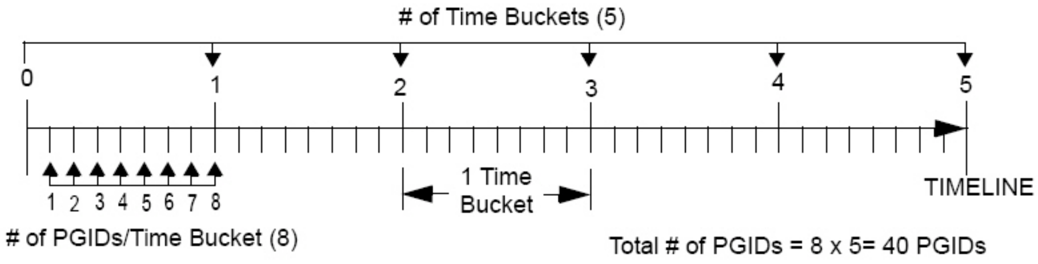
Latency Type Tab

For those load modules that support Latency testing and Sequence Checking, there are two types of Real-Time Latency measurement available:

- **Instantaneous** (default)—Latency measured for all received data (continuous). Up to 57,344 packet group IDs (PGIDs) may be used.
- **Latency Over Time**—Latency measured for a number of time intervals of equal length, called 'time buckets' or 'time bins.' The example diagram in *Figure:Multiple Latency Time Measurements—Example* demonstrates the relationship between the time buckets/bins and PGIDs.

NOTE For the remainder of this chapter, 'Time Bucket' and 'Time Bin' are interchangeable terms.

Figure:Multiple Latency Time Measurements—Example



The timeline is equally divided into a *# of Time Buckets,* each of which is ONE *Time Bucket Duration* in length. A time bucket duration can range anywhere from nanoseconds to hours, depending on the user configuration.

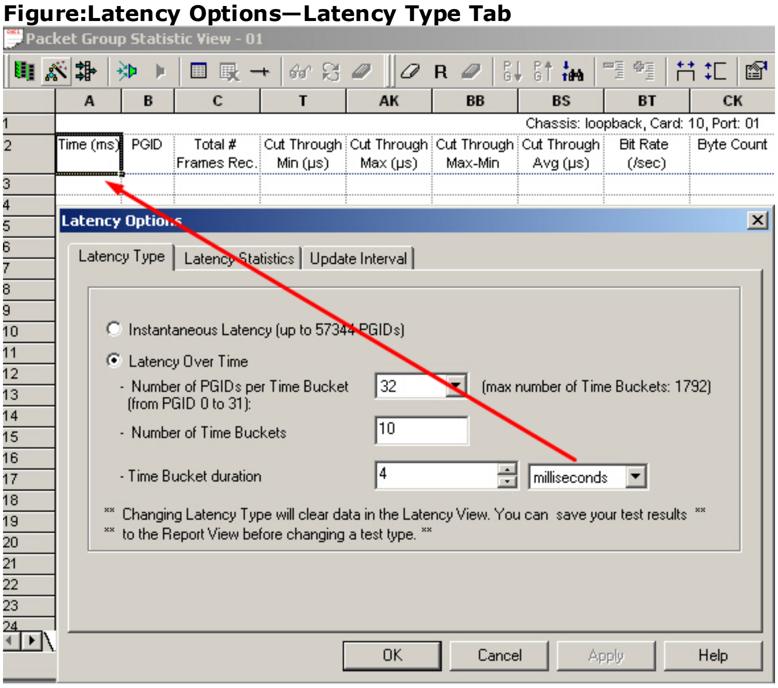
The maximum number of time buckets that can be handled is determined by the number of PGIDs in each bucket. The product of the number of time buckets and the number of PGIDs must be no more than 57,344 (131072 for Time Bins). The number (count) of PGIDs starts at 1 and increments by powers of 2—that is, 2, 4, ..., up to 8,192, and then jumps to 57,344 (Time Bins continue exponentially up to 131,072).

NOTE The actual PGID numbers start at 0, and increase up to a maximum of 57,343 (131072 for Time Bins).

When the time bucket duration is set, the *Time (units)* column appears in the spreadsheet.

The *Latency Type* tab in the *Latency Options* dialog is shown in *Figure:Latency Options—Latency Type Tab*.

Figure:Latency Options—Latency Type Tab



The two options available are described in *Table:Latency Options—Latency Type Tab*.

NOTE Changing the latency type will clear data in the Latency View. Test results are saved by creating a Latency report before changing a test type.

Table:Latency Options—Latency Type Tab

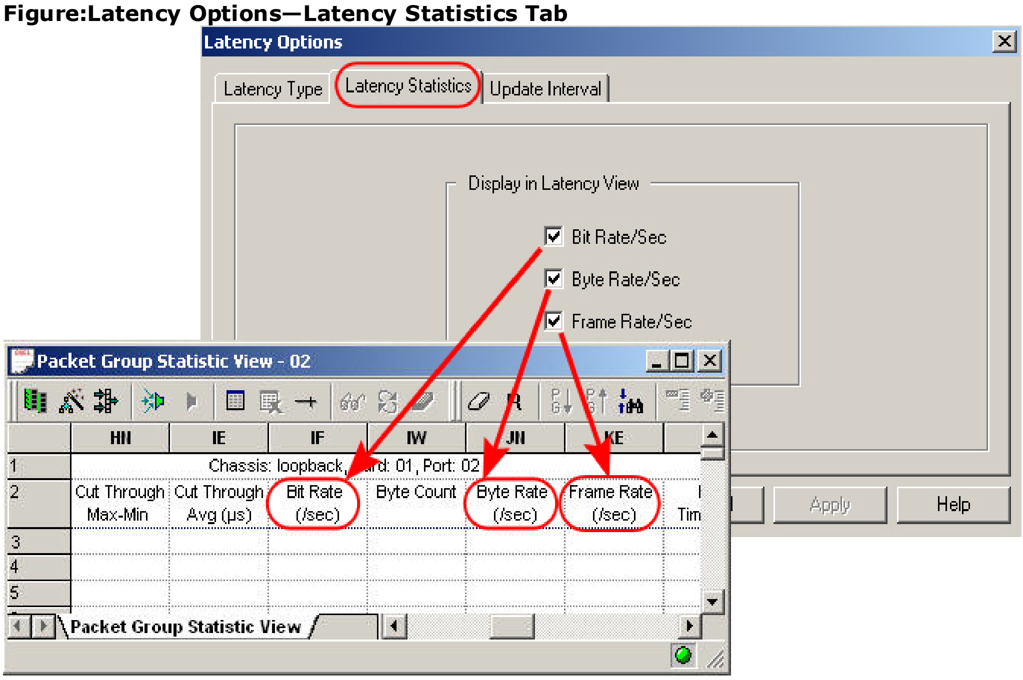
Option	Field/Control	Description
Instantaneous Latency (default)		All of the measurements over time are stored in a single set of values.
Latency Over Time (available for modules which have sequence checking enabled)		Multiple measurements are made for a specified number of PGID's.
	Number of PGIDs per Time Bucket.	Select the number of PGID's to be processed per time bucket–from the dropdown list.
	Number of Time Buckets	The total number of time buckets to be used. (The maximum number of Time Buckets available is indicated as a comment displayed next to the *number of PGIDs per Time Bucket* field.)
	Time Bucket Duration	The time duration of each time bucket. When this field is active, the Time (*units*) column appears in the spreadsheet. Units of time available are: • nanoseconds • microseconds

Option	Field/Control	Description
		• milliseconds • seconds • minutes • hours

Latency Statistics Tab

The *Latency Statistics* tab of the *Latency Options* dialog controls the manner in which the received data rate is displayed, and is shown in *Figure:Latency Options—Latency Statistics Tab*. Display of the received data rate is **optional**. Any number of the data rate displays can be added to the Packet Group Statistics View.

Figure:Latency Options—Latency Statistics Tab



The controls in this tab are described in *Table:Latency Options—Latency Statistics Tab.*

Table:Latency Options—Latency Statistics Tab

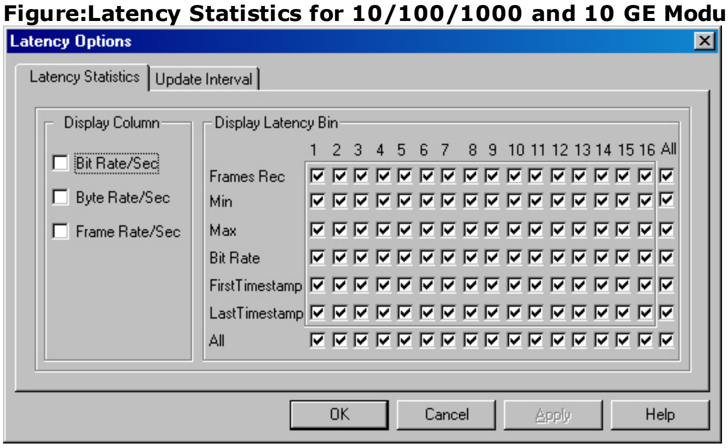
Section	Field/Control	Description
Display in Latency View	Bit Rate/Sec	When selected, the Packet Group Statistics View dialog will contain a column for displaying the received data rate in bits per second.
	Byte Rate/Sec	When selected, the Packet Group Statistics View dialog will contain a column for displaying the received data rate in bytes per second.
	Frame Rate/Sec	When selected, the Packet Group Statistics View dialog will contain a column for displaying the received data rate in frames per second.

10/100/1000 and 10 Gigabit Ethernet load modules have a different *Latency Statistics* tab that incorporates statistics for the Latency Bin feature, and is described in *Latency Statistics with Latency Bins*.

Latency Statistics with Latency Bins

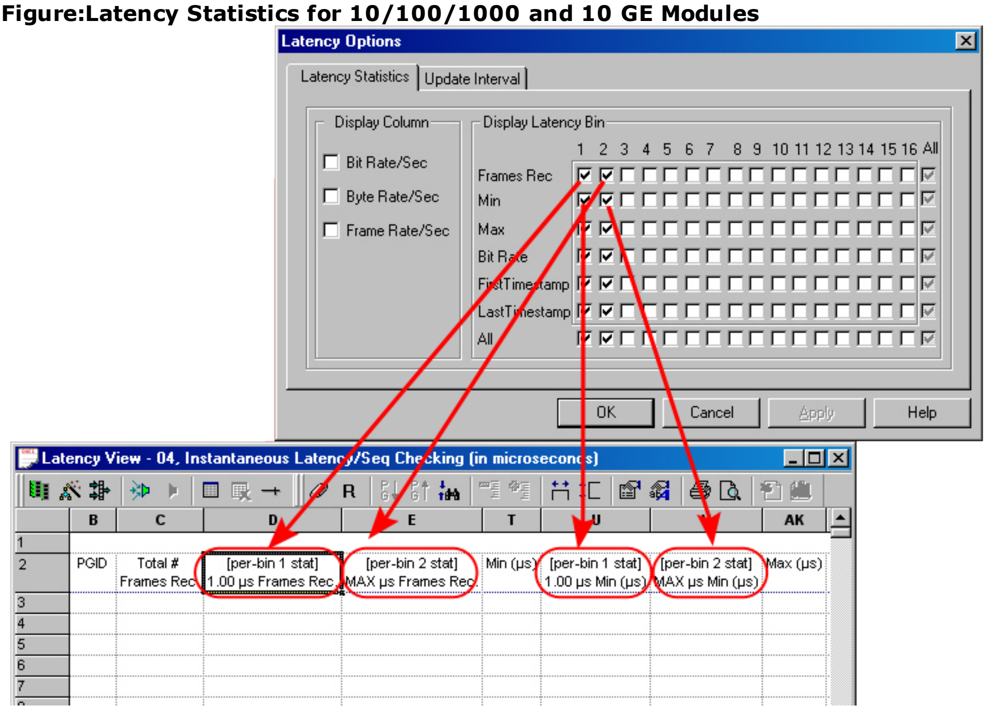
For 10/100/1000 and 10 Gigabit Ethernet modules, the *Latency Statistics* tab has additional options for the Latency Bin feature. The options for Latency Bin features on the *Latency Statistics* tab page are shown in *Figure:Latency Statistics for 10/100/1000 and 10 GE Modules*.

Figure:Latency Statistics for 10/100/1000 and 10 GE Modules



The statistics appear in the Packet Group Statistics View dialog under the port being used. Each latency bin (from 1 to 16) receives its own column for each listed statistic, as shown in *Figure:Latency Statistics for 10/100/1000 and 10 GE Modules*.

Figure:Latency Statistics for 10/100/1000 and 10 GE Modules



The check boxes shown in the Display Column are described in *Table:Latency Options—Latency Statistics Tab*. The Latency Bin options in the Display Latency Bin section are described in *Table:Latency Bin Statistics*.

Table:Latency Bin Statistics

Section	Field/Control	Description
Display Latency Bin	Frames Rec	Selecting this check box displays the total num-

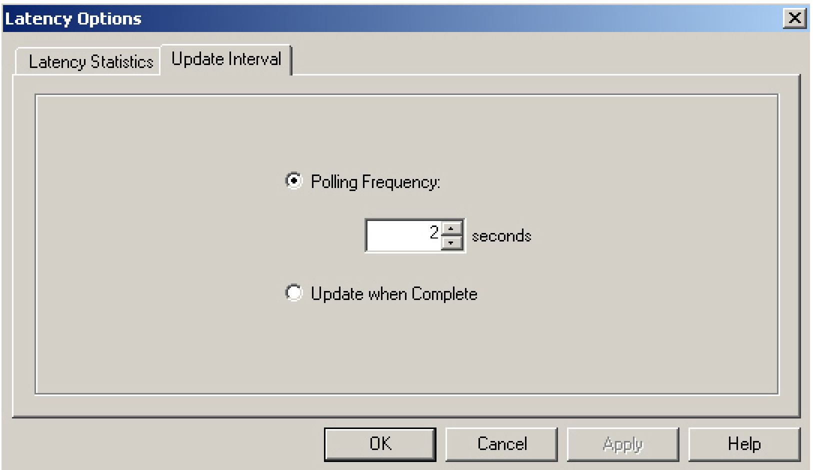
Section	Field/Control	Description
		ber of frames received during the latency test in the Packet Group Statistics View.
	Min	Selecting this check box displays the minimum latency value received during the latency test in the Packet Group Statistics View, measured in microseconds.
	Max	Selecting this check box displays the maximum latency value received during the latency test in the Packet Group Statistics View, measured in microseconds.
	Bit Rate	Selecting this check box displays the bit rate of the latency test during the latency test in the Packet Group Statistics View.
	First Timestamp	Selecting this check box displays the first timestamp received during the latency test in the Packet Group Statistics View.
	Last Timestamp	Selecting this check box displays the last timestamp received during the latency test in the Packet Group Statistics View.
	All (vertical)	Selecting this check box activates all of the fields for a specified Latency Bin.
	All (horizontal)	Selecting this check box activates the selected statistic for all ports.

The default is for all statistics for all Latency Bins to be displayed. Statistics will only appear for the number of Latency Bins that have been specified in Wide Packet Mode Latency/IAT Bins.

Latency Update Interval Tab

The Latency *Update Interval* tab in the *Latency Options* dialog controls the type and timing of screen updates, and is shown in *Figure:Latency Options—Update Interval Tab*.

Figure:Latency Options—Update Interval Tab



The fields and controls in this tab are described in *Table:Latency Options—Update Interval Tab*.

Table:Latency Options—Update Interval Tab

Field/Control	Description
Polling Frequency	When selected, the data in the Packet Group Statistics View dialog will be updated at the frequency selected in the *Polling Frequency* field, in seconds.
Update when Complete	When selected, the Packet Group Statistics View dialog data will not be displayed until the latency measurements are complete.

The update interval selected will affect the update of the Packet Group Statistics View dialog while the view is scrolled. A large update interval may cause scrolled screens to appear to have no data until the next update occurs.

Start/Stop Latency

The process of collecting latency data is performed through the use of the Packet Group Statistics View toolbar, shown in *Figure:Packet Group Statistics View Toolbar*.

NOTE

Clear Timestamps on Transmit and Receive ports together **BEFORE** starting Latency measurements.

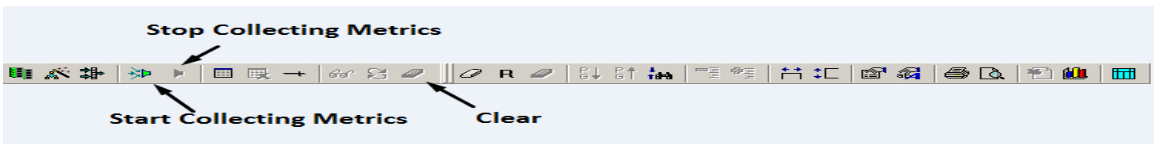
Some methods for clearing timestamps on multiple ports simultaneously are listed below:

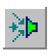
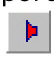
Create a Port Group for all of the transmit and receive ports to be used in the Latency measurement. Right-click the Port Group name in the details list, and select Clear Timestamps.

If all of the Transmit and Receive ports are on a single card, and no other ports on that card are being used for other purposes, highlight the card in the Network Resources list, and go to the main menu bar. Click Transmit or Capture and select Clear Timestamps from the dropdown menu.

Create a Statistic View for all of the transmit and receive ports to be used in the Latency Measurement. In the Statistic View, highlight ALL of the port names in the column headers. Right-click the highlighted port names and select Clear Timestamps from the pop-up menu.

Figure:Packet Group Statistics View Toolbar



The *Start Collecting Metrics* icon  should be used before any transmit is started on ports feeding the ports in the Packet Group Statistics View. The *Stop Collecting Metrics* icon 

should be used after all latency data has been received. A number of other commands are not available while latency data is being collected. The *Clear* icon may be used to erase collected data in preparation for a new run.

The spreadsheet contents are updated during the latency data collection process, as dictated by the *Update Interval* tab of the *Latency Options* dialog.

Packet Group Statistics View Toolbar

The set of operations available in the Packet Group Statistics View, either from the main menu bar or from the latency toolbar are shown in *Table:Packet Group Statistics View Operations*.

Table:Packet Group Statistics View Operations

Operation	Toolbar Icon	Description
Add/Delete Ports		Opens a dialog allowing ports to be added and/or removed to the latency group. *Port Selection*.
Latency Options		Opens the *Latency Option* dialog which allows the latency measurement type to be adjusted. See *Latency/Jitter Options*.
Port Receive Mode		Opens the *Receive Mode* tab for the current port. See *Receive Mode Tab*.
Start Collecting Metrics		Starts the latency operation. See *Start/Stop Latency* Clear Timestamps for all ports before starting a Latency test.
Stop Collecting Metrics		Stops the latency operation. See *Start/Stop Latency*
Clear		Clears collected latency data. See *Start/Stop Latency*
Reset View to Defaults	R	Resets all of the Packet Group Statistics View options to their defaults.
Create Latency Report		Creates a latency report in the form of an additional spreadsheet which is a snapshot of the current data. See *Latency Reports*.
Delete Latency Report		Deletes the current latency report. See *Latency Reports*.
Global Line Rate		Sets the total percentage of the maximum port rate. See *Total % Max Rate*.
View PRBS Capture		View the captured PRBS packets and show the errored bits.
Refresh PRBS Capture		Refresh capture buffer with captured packets from Start capture until latest ones.
Clear PRBS Capture		Clear current PRBS capture buffer.
Clear Selected PGID Stats		Clear selected PGID stats NOTE (Not supported in Packet Group mode.)
Next Packet Group		Moves the cursor to the first row of the next packet

Operation	Toolbar Icon	Description
		group in the display. See note below.
Previous Packet Group		Moves the cursor to the first row of the previous packet group in the display. See note below.
Go To Packet Group		Opens the *Go To* dialog. This dialog allows to Move the cursor to the first row of the specified packet group. See *Go to Packet Group*.
Hide Empty Rows		During latency measurements, blank rows may will appear for empty packet group ids. This selection causes those rows to be omitted from the display. See *Latency Reports*.
Show Empty Rows		This selection reverses the previous selection. See *Latency Reports*.
Best-Fit Column Widths		For the selected column(s), the width of the column is adjusted to just fit the widest data in that column(s).
Best-Fit Row Height		For the selected row(s), the height of the row is adjusted to just fit the tallest data in the row(s).
Grid Properties		Opens a dialog that allows the adjustment of the visible grid. See *Grid Properties—Display Settings*.
Format Cells		Sets the formatting for display in the selected cells. See *Cells Format Dialog*.
Print		Prints the contents of the current spreadsheet — either live data or a latency report.
Print Preview		Allows the printout of the contents of the current spreadsheet—either live data or a latency report—to be previewed before printout.
Export Data to Excel File		Exports the current data to a file in Excel spreadsheet form. A standard file save dialog allows the naming and placement of the output file.
Create Chart		Opens a dialog that allows the creation of a chart in a number of formats. See *Using Chart View*.
Latency View Options		Opens a dialog that allows changing the latency view to list the ports vertically. See *Latency View Options*.

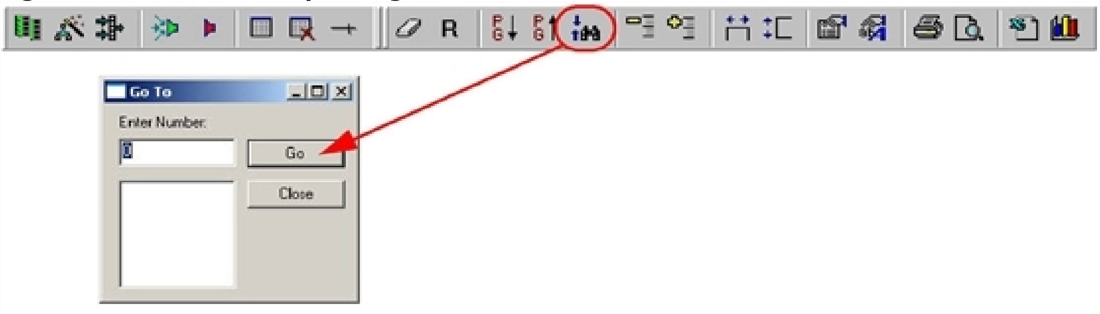
NOTE When there is a large number of PGIDs listed in the Packet Group Statistics View/Latency report, it may be necessary to use the vertical scroll bar to move up and down in the list of PGIDs.

Also, for instantaneous latency, the PGIDs may not be continuous, and some rows may appear to be empty, but this is due to the lack of received data with the packet group ID that corresponds to that row. Additional data may be present for larger PGID numbers.

Go to Packet Group

The *Go to Packet Group* icon allows to advance the cursor to a specified Packet Group in the Packet Group Statistics View grid. Selecting this icon opens the *Go To* dialog, as shown in *Figure:Go To Packet Group Dialog*.

Figure:Go To Packet Group Dialog



Enter the packet group number in the field shown and select the *Go* button. The cursor in the Packet Group Statistics View grid moves to the first instance of the Packet Group.

The number searched on is saved in the window below the *Enter Number* field. It can be reselected for another search at a later time. Once the *Go To* dialog is close, all entries are cleared.

Clear Selected PGID Stats

The Clear Selected PGID Stats icon allows to clear statistics of selected rows in Packet Group Statistics View while latency is running. To use the feature, highlight any combination of PGID rows and click the icon. The stats are cleared on those highlighted rows.

NOTE Currently this feature is only supported by these load modules:

LM1000(S)TX(S)4/24
LSM1000XMS(R)12
LSM1000XMV(R)16
ASM1000XMV12X
LSM10G1-01, LSM10GL1-01, and LSM10GXL6-01
MSM2.5G and MSM10G
10/100/1000 STXS4
10/100/1000 STX4
10/100/1000 STXS2
10/100/1000 STXS24
10/100/1000 STX24
10/100/1000 TXS4
10/100/1000 TX4
1000 SFPS4
1000 SFP4
10/100/1000 XMS12
10/100/1000 XMSR12
10/100/1000 XMSP12
10/100/1000 LSM XMV16
10/100/1000 LSM XMVR16
10/100/1000 LSM XMVDC16
10/100/1000 LSM XMVDC12
10/100/1000 LSM XMVDC8
10/100/1000 LSM XMVDC4
10/100/1000 LSM XMVDC4
10/100/1000 ASM XMV12X
10GE LSM XM8

NOTE

10GE LSM XM8XP
10GE LSM XM8S
10GE LSM XMR8S
10GE LSM XM8 10GBASE-T
10GE LSM XMR8 10GBASE-T
10GE LSM XM8 10GBASE-T
10GE LSM XMR8 10GBASE-T
NGY-NP8
10GE LSM
10GE LSM XM3
10GE LSM XMR3
10GE LSM XL6
10G MSM
2.5G MSM
100GE/BERT LSM XMV1
40GE/BERT LSM XMV1

Total % Max Rate

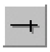
The *Global Line Rate* icon  allows to change the line rate for ports in the Packet Group Statistics View. The slide bar will change the total percentage of the maximum line for each port indicated port. Selecting this icon opens the *Packet Group Statistic View—Total % of Max Rate* dialog box.

Figure:Total % Max Rate Dialog

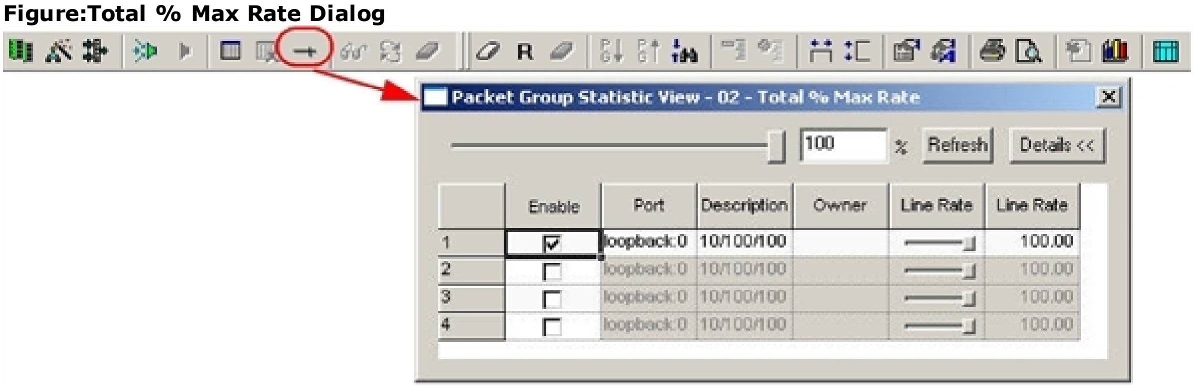


Table:Total % Max Rate dialog describes the fields on the *Packet Group Statistic View—Total % of Max Rate* dialog.

Table:Total % Max Rate dialog

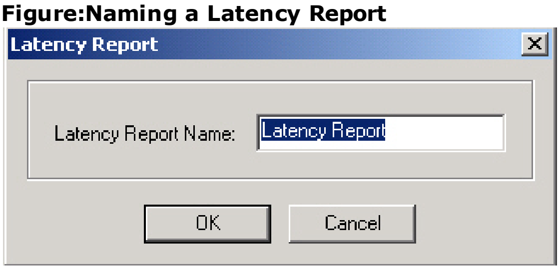
Field	Usage
Slide Bar	Adjusts the percentage of the maximum line rate for the entire list of Packet Group Statistics Views. When this bar is moved the percentage number to the right is changed.
Percentage	Shows the percentage number for the line rate usage. When this number is changed, the Slide Bar moves.
Details	Selecting this button displays or hides the fields listed for individual Packet Group Statistics Views.
Enable	This check box enables the use of the line rate slide bar.

Field	Usage
Port	Specifies the port number by chassis, card slot, and port.
Description	Describes the port type (that is, 10/100 base TX).
Owner	Shows the port owner (if applicable).
Line Rate	A slider bar for adjusting the percentage of the max line rate for a particular Packet Group Statistics View. When this is moved, the percentage number to the right changes.
Line Rate	A percentage number used for adjusting the max line rate for the Packet Group Statistics View. When this change, the slider bar to the left moves.

Latency Reports

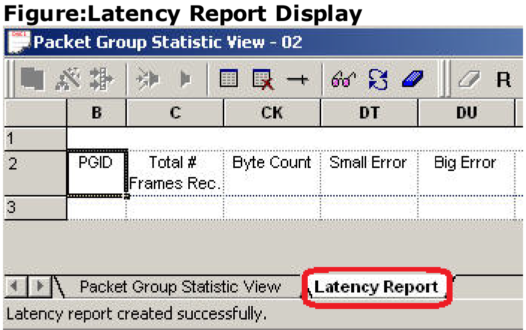
A Latency Report is a copy of the Instantaneous Latency data, displayed as an additional tabbed view in the spreadsheet. We recommend creating a Latency Report, as soon as the Latency test setup is completed, for saving the collected data. When the *Create Report* icon  is clicked, the *Latency Report* dialog appears which allows the specification of the report name, as shown in *Figure:Naming a Latency Report*.

Figure:Naming a Latency Report



The named Latency Report is displayed by clicking the named tab at the bottom of the *Packet Group Statistics View* dialog, as shown in *Figure:Latency Report Display*.

Figure:Latency Report Display



Note that the port operation icons cannot be accessed from a latency report. While viewing a latency report, the *Hide Empty Rows* and *Show Empty Rows* icons  and  are active in the toolbar, and these commands may be used to hide empty rows in the spreadsheet or show them again. These rows are due to the lack of data with the Packet Group ID that corresponds to that row.

The *Export Data to Excel File* icon  can be used to save a copy of the latency report to disk in Excel spreadsheet format. A dialog allows the naming and placement of the Excel file.

NOTE The Export Data to Excel File icon is only active and usable after an Ixia latency report has been created and you select the Latency Report tab. Excel also does not allow to export more than 21 ports of information at one time; attempting this causes Excel to crash.

Using Chart View

The charting process may be performed either on the Packet Group Statistics View data or on data in a latency report. Charts may be used to follow 'live' data, or to analyze data after data collection has been stopped. The process of charting starts with the selection of one or more ranges of data on the spreadsheet.

An example of this process is shown for the following fictitious spreadsheet example shown in *Figure:Packet Group Statistics View with Data for a Single Parameter Selected*, with the indicated data selected. The chart corresponding to the selected data is shown in *Figure:Latency Chart with Data for a Single Parameter*.

Figure:Packet Group Statistics View with Data for a Single Parameter Selected

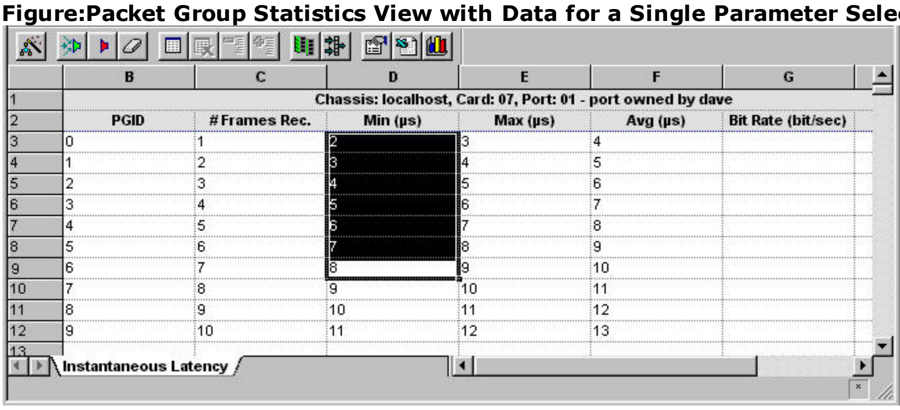
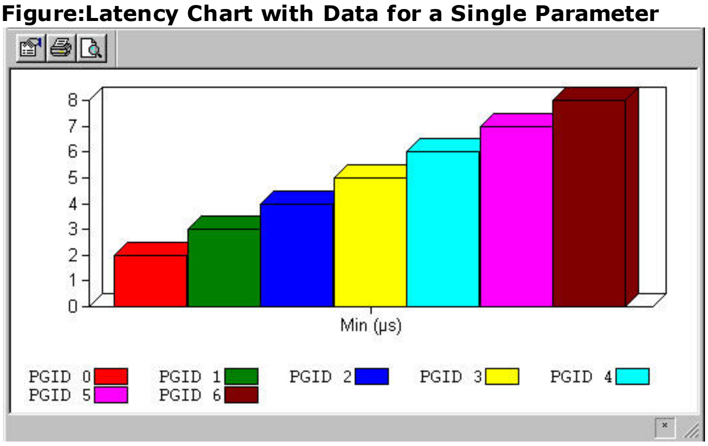
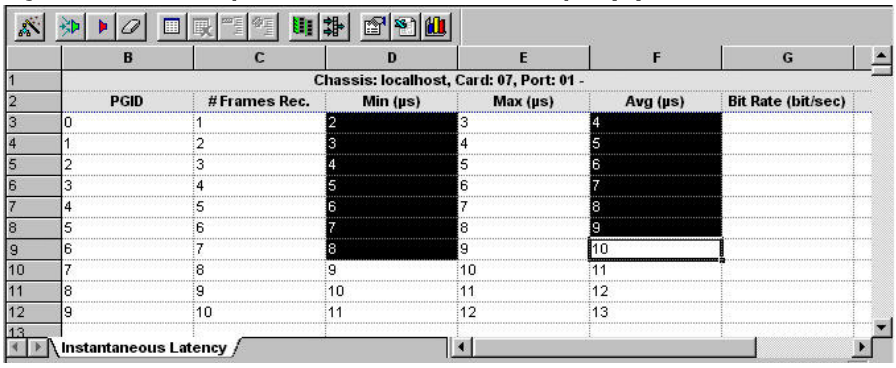


Figure:Latency Chart with Data for a Single Parameter



Multiple selections of data can be made within one spreadsheet, as shown in *Figure:Packet Group Statistics View with Multiple (2) Parameters Selected*.

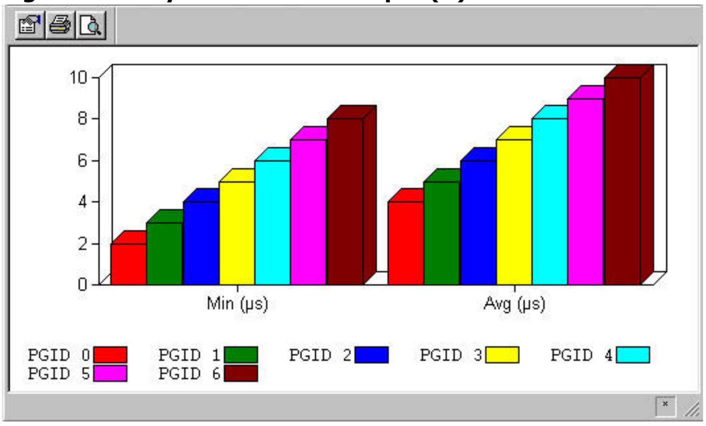
Figure:Packet Group Statistics View with Multiple (2) Parameters Selected



	B	C	D	E	F	G
1	Chassis: localhost, Card: 07, Port: 01 -					
2	PGID	# Frames Rec.	Min (µs)	Max (µs)	Avg (µs)	Bit Rate (bit/sec)
3	0	1	2	3	4	
4	1	2	3	4	5	
5	2	3	4	5	6	
6	3	4	5	6	7	
7	4	5	6	7	8	
8	5	6	7	8	9	
9	6	7	8	9	10	
10	7	8	9	10	11	
11	8	9	10	11	12	
12	9	10	11	12	13	
13						

The corresponding display is shown in *Figure:Latency Chart with Multiple (2) Parameters Selected*.

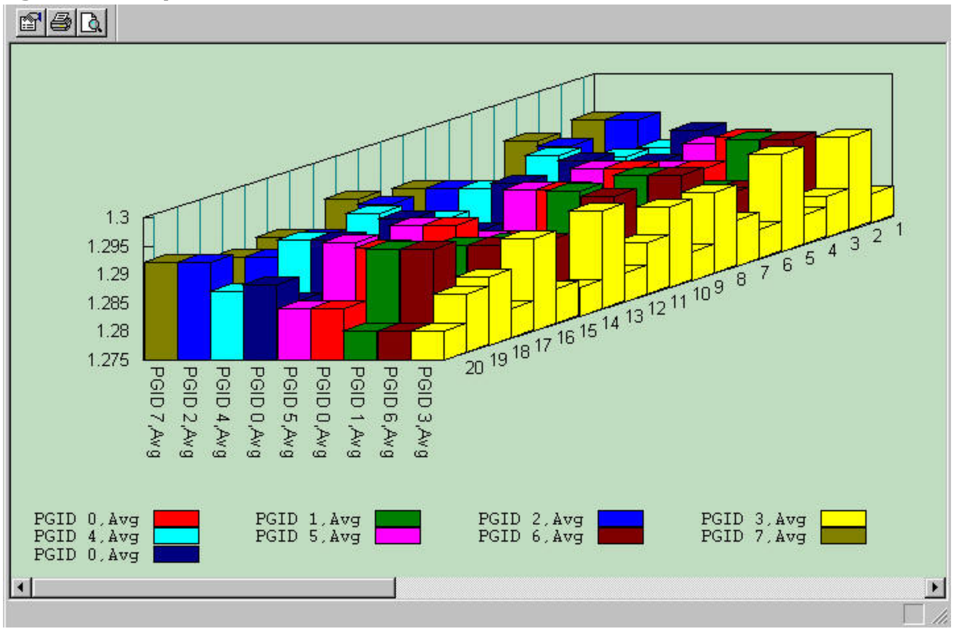
Figure:Latency Chart with Multiple (2) Parameters Selected



The contents of an active chart may be changed by making a new selection of data in the spreadsheet, and then either selecting the *Chart* icon  or dragging and dropping the selection into the chart. Ensure to grab the selection at its edge.

Charts can be made during latency over time measurements as well. Included in *Figure:Latency over Time 3d 'Manhattan' Chart* is a 3D 'Manhattan' chart of the average latency over time for a number of packet groups.

Figure:Latency over Time 3d 'Manhattan' Chart



The format of the chart may be changed through the use of the *Chart Properties* icon  in the toolbar at the top of the Chart View window, as shown in *Figure:Chart View Toolbar*.

Figure:Chart View Toolbar

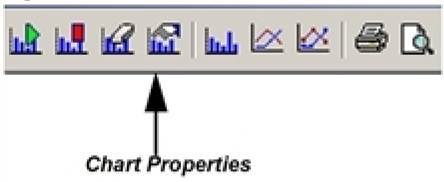


Chart Properties

The *Chart Properties* icon  displays dialogs that allows for scale specification and chart type selection.

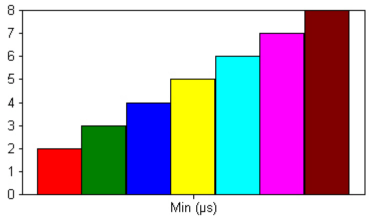
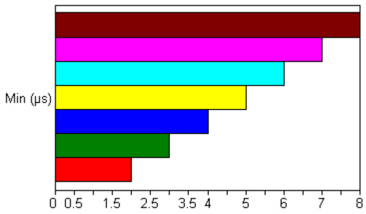
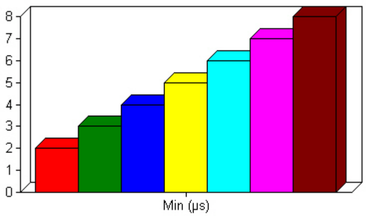
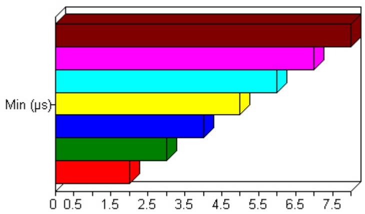
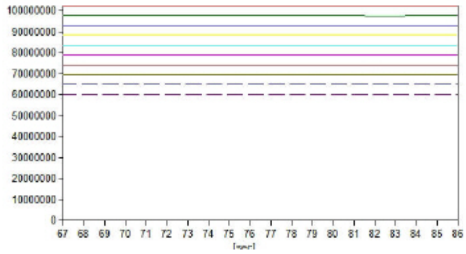
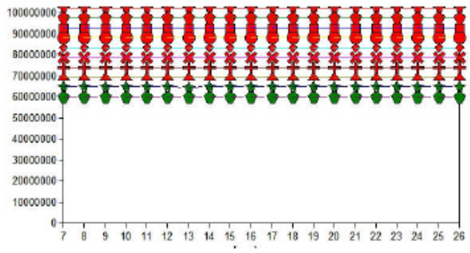
Chart Properties (in Statistic View) for additional information.

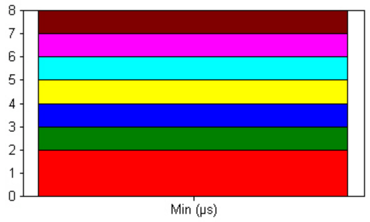
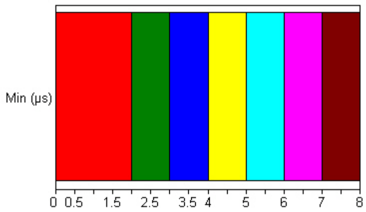
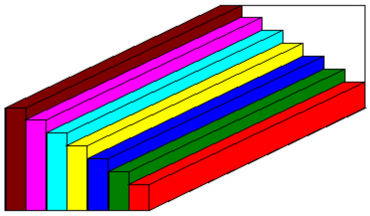
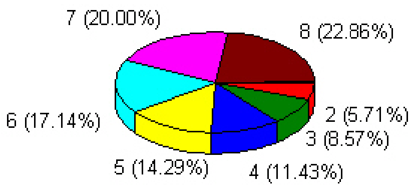
Chart Types

Within the *Chart Properties* dialog, the type of chart can be selected from the *Chart Type* list. Examples of Latency charts from this list are shown in *Table:Chart Types*.

Table:Chart Types

Type	Example
Vertical Bar	

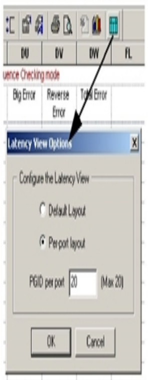
Type	Example
	
Horizontal Bar	
Vertical bar (pseudo 3D)	
Horizontal bar (pseudo 3D)	
Line Plot	
Line Plot with Widgets	
Vertical stacked bar	

Type	Example
	
Horizontal stacked bar	
3D ‘Manhattan’	
Pie Chart	

Latency View Options

When the Latency View Options icon is clicked, a dialog opens (*Figure:Latency View Options Dialog*) to allow changing the latency view to list the ports vertically. You can toggle between the default layout (horizontal) and the per-port layout (vertical). You can also configure the maximum number of PGIDs to be displayed (up to 20).

Figure:Latency View Options Dialog



[This page intentionally left blank]

Chapter 17 - Card Properties

Card Properties Dialog

The *Card Properties* dialog displays a number of properties related to the port's operation (*Card Properties*). *The display varies according to the type of card.*

The complete specifications for the various types of boards can be found in the *Ixia Platform Reference Manual*. See the following chapters:

- Impairment Load Modules
- Xcellon-Lava Load Modules
- Power over Ethernet Load Modules
- 10/100/1000 Load Modules
- Network Processor Modules
- 40/100 Gigabit Ethernet Load Modules
- 10 Gigabit Ethernet Load Modules
- OC-12 ATM/POS Load Modules
- 10/100 Load Modules
- 10GE LAN/WAN and OC192 POS Load Modules
- OC12c / OC3c Load Modules
- OC-48c Load Modules
- FCMGXM Load Modules
- Xcellon-Flex Load Modules
- Xcellon-Multis Load Modules
- Xcellon-Multis Reduced Load Modules
- Novus QSPF28 Load Modules
- Novus QSPF28 Reduced Load Modules
- PerfectStorm Load Modules
- Xdensity XDM10G32S/8S Load Modules
- XMVAE Gigabit Ethernet Load Modules
- Stream Extraction Modules

Card Properties

The *Card Properties* dialog for most load modules includes a *General* tab like that shown in the following figure.

NOTE

The General tab for ASM1000XMV12X and LSM1000XMV16 modules provides additional information—*Xcellon-Ultra and ASM1000XMV12X Modules*.

The Card Properties dialog box for Xcellon-Ultra NG load module and the different tab views in this dialog box features the IxN2X capability and the utility to use the load module in IxN2X mode—*Xcellon-Ultra NG Module*.

The General tab for NGY LSM10GXM 4 and 8-port modules features a Clock tab

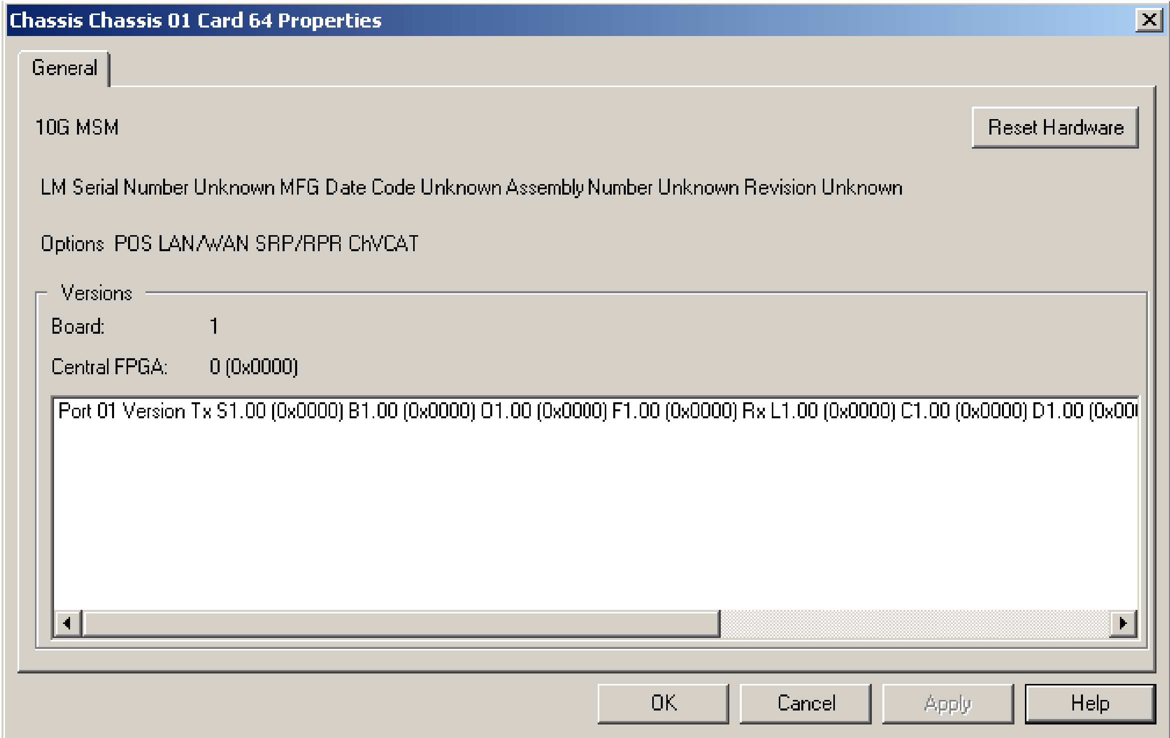
NOTE

for configuring clocking—*NGY LSM10GXM 2, 4 and 8-port Modules*.

The General tab for 10/100/1000 LSM XMVDC16NG 16-port module features the IxN2X capability and the ability to use the module in N2X mode—*LSM XMVDC16NG 16-port Modules*.

The General tab for Xcellon-Multis module provides the general properties of the Multis modules—Xcellon-Multis General.

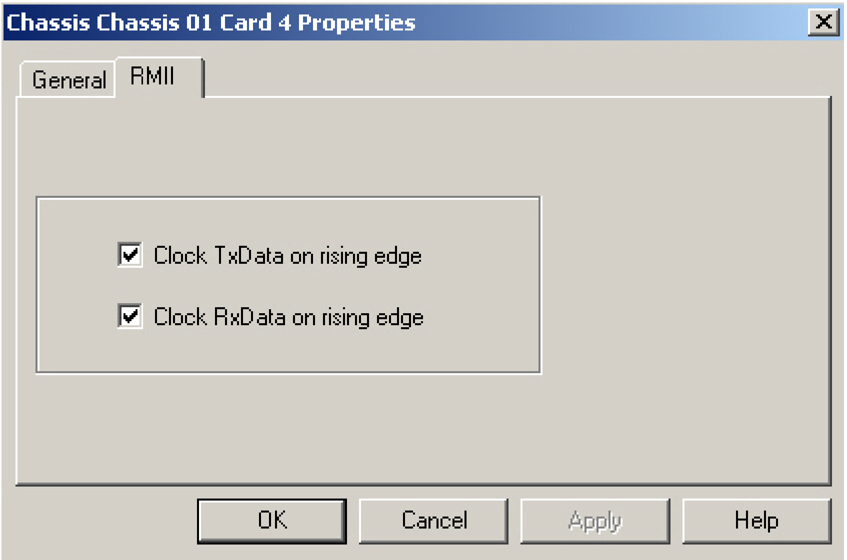
Figure:General Card Properties



The *General* tab shows the board version, load module serial number, date of manufacture, and revision number. It also contains a button for resetting the hardware to factory defaults.

The 10/100 Reduced MII card properties window contains an additional *RMII* tab for the clock setting. This tab is shown in the following figure.

Figure:RMII Card Properties for 10/100 Reduced MII Cards

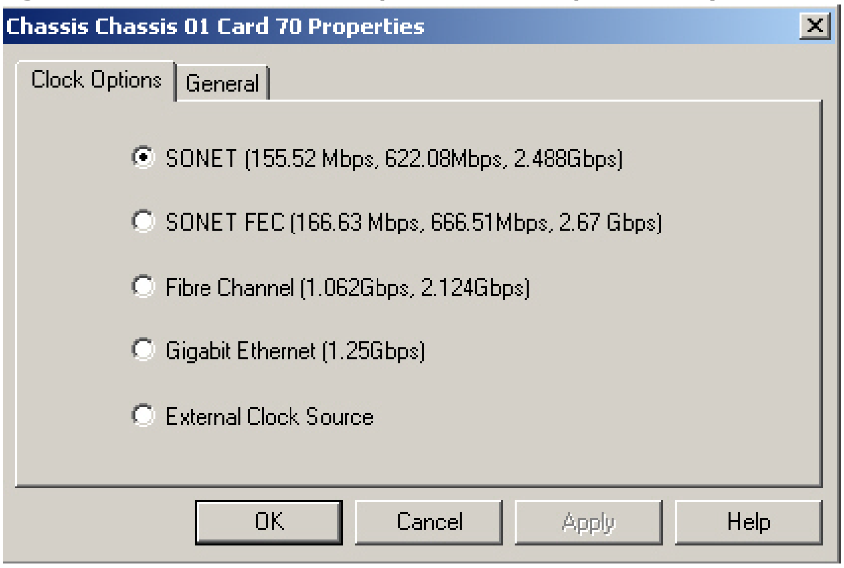


The *Clock Tx/Rx Data on rising edge* boxes allows a shift of 180 degrees on these clocks to accommodate for delays between the DUT and the Ixia Reduced MII port.

Unframed BERT

For the unframed BERT modules, some of the data rates must be enabled through the *Clock Options* tab of the *Card Properties* dialog, as shown in the following figure.

Figure:Unframed BERT Card Properties—Clock Options Tab (shown for Multi-Rate)



The dialog shown here is for the Multi-Rate unframed BERT module. The dialog for the Single-Rate unframed BERT module contains a subset of these options. The data rate selections are described in the following table:.

Table:Data Rates for Unframed BERT

Data Rate	Usage
SONET	Includes: 155.52 Mbps (OC-3c data rate)

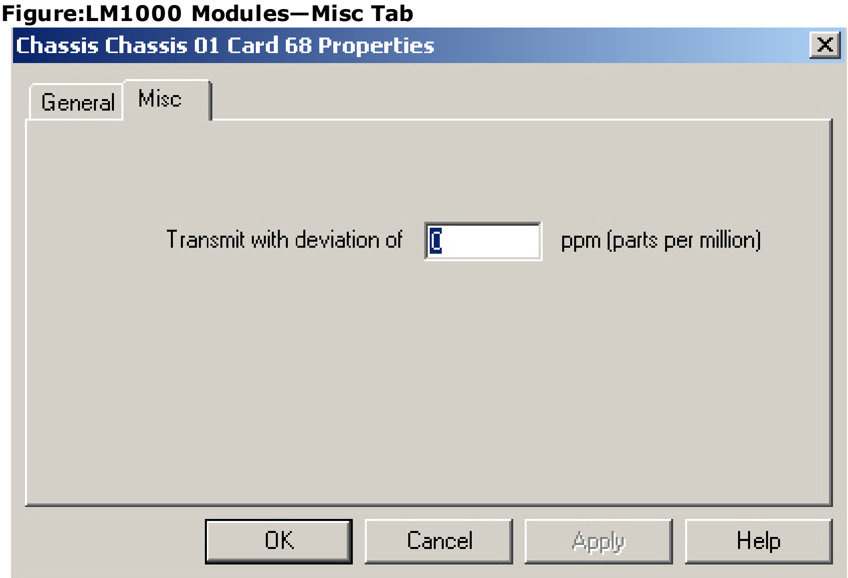
Data Rate	Usage
	622.08 Mbps (OC-12c data rate) 2.488 Gbps (OC-48c data rate)
SONET FEC	SONET with Forward Error Correction. Includes: 166.63 Mbps (OC-3c FEC data rate) 666.51 Mbps (OC-12c FEC data rate) 2.67 Gbps (OC-48c FEC data rate)
Fibre Channel	Includes: 1.062 Gbps - the basic fibre channel rate 2.124 Gbps - 2X the basic fibre channel rate
Gigabit Ethernet	1.25 Gbps
External Clock Source	With this option is selected, the clock is derived from the external device.

LM1000 and LM10GE Modules—Misc Dialog

For the LM1000SFP(S)4, LM1000(S)TX(S), and LM10GE modules there is an additional *Misc* tab located in *Card Properties* dialog, as shown in the following figure.

The same *Misc* tab applies to the LSM1000XMV16 and ASM1000XMV12X modules.

Figure:LM1000 Modules—Misc Tab



This dialog allows to adjust the line transmit frequency for the card/ module. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the card. LM1000 cards can be adjusted by up to +/- 102 ppm–(0.0102%) above or below that initial rate—to test frequency compatibility per IEEE 802.3. LM10GE cards can be adjusted from 0 to -2500 ppm (-0.25%) below that initial rate.

All LM1000 cards/modules that are configured with the same deviation value, within a chassis chain, will remain locked together at that same frequency, permitting long-term testing. LM10GE cards/modules are clocked on a per card basis.

NOTE 10GE LSM and MSM family modules have this feature, but it is controlled in the General tab of the Port Properties dialog.

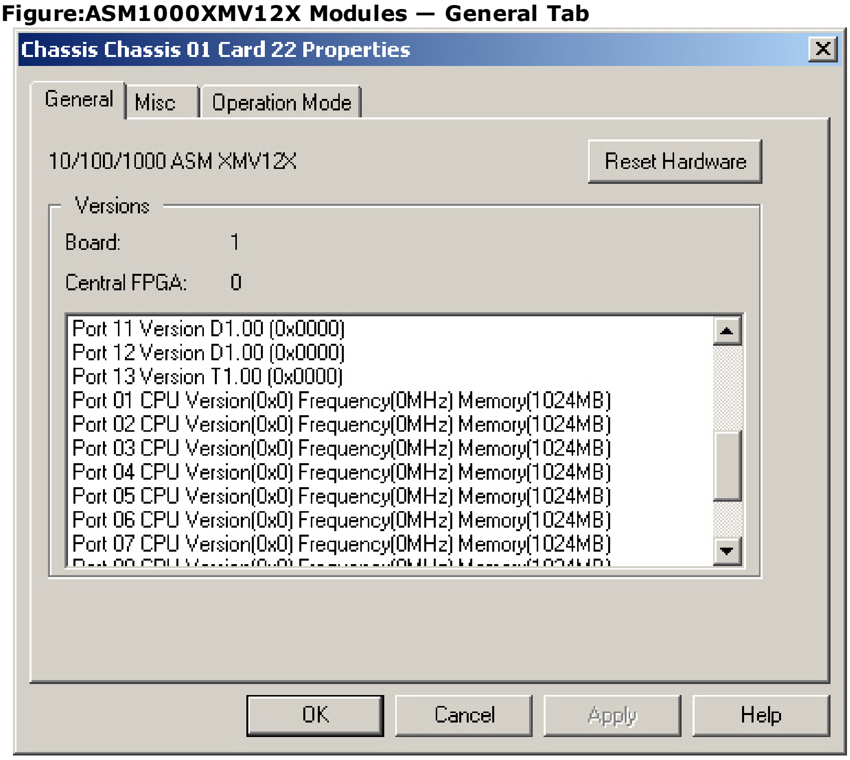
Xcellon-Ultra and ASM1000XMV12X Modules

The Xcellon-Ultra XP, NP, and ASM1000XMV12X modules *Card Properties* dialog *General* tab is shown in the following figure.

The LSM1000XMV16 module has the same *General* tab functionality.

The *General* tab shows the board version and FPGA revision level for the board as well as the FPGA versions for each port on the card. It also contains a button for resetting the hardware to factory defaults. Also displayed (by scrolling downward) are Power PC version, Power PC speed, and SODIMM memory size.

Figure:ASM1000XMV12X Modules — General Tab

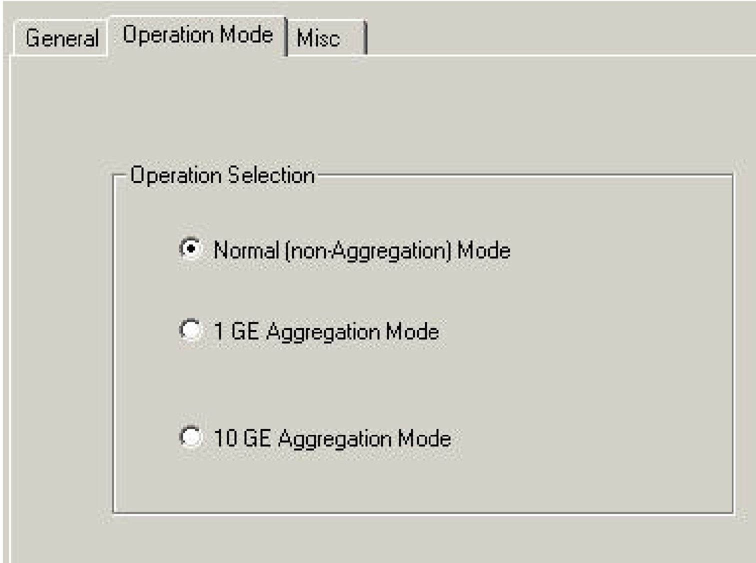


Operation Mode

The Xcellon-Ultra and ASM1000XMV12X modules have an *Operation Mode* tab which is used to select between the three modes of operation for the module. The *Operation Mode* tab is shown in the following figure. The three modes are:

- Normal (non-aggregation) Mode–twelve 10/100/1000Mbps ports that provide L2-L7 functionality the same as the LSM1000XMV16 load module, including Stream Control, Capture and Latency features.
- 1 GE Aggregation Mode–any of the twelve PCPUs aggregated to any of 12 GE test ports through the switch fabric.
- 10 GE Aggregation Mode–twelve PCPUs aggregated to one 10GE test port through the switch fabric. The 10GE port is for application traffic only, providing no support for hardware stream engine.

Figure:Operation Mode Tab for ASM1000XMV12X



Misc Tab

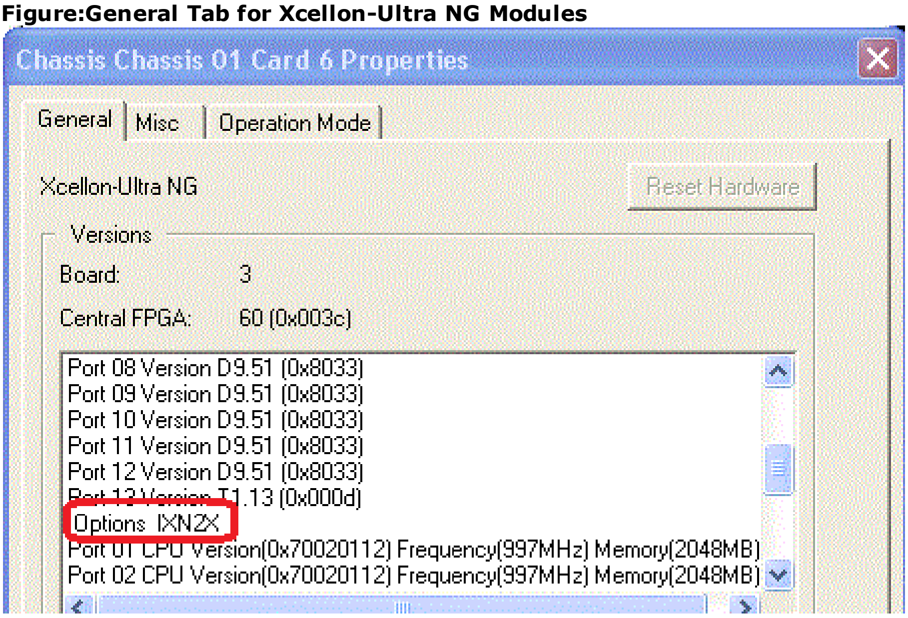
The Xcellon-Ultra and ASM1000XMV12X modules *Card Properties* dialog has the *Misc* tab when in normal (non-aggregated) mode. The Misc tab functionality is identical to that described in *LM1000 and LM10GE Modules—Misc Dialog*.

Xcellon-Ultra NG Module

The Xcellon-Ultra NG module is the Fusion-Enabled version of the existing Ixia Xcellon-Ultra NP and XP load modules. The Xcellon-Ultra NG module is capable of running in IxN2X mode.

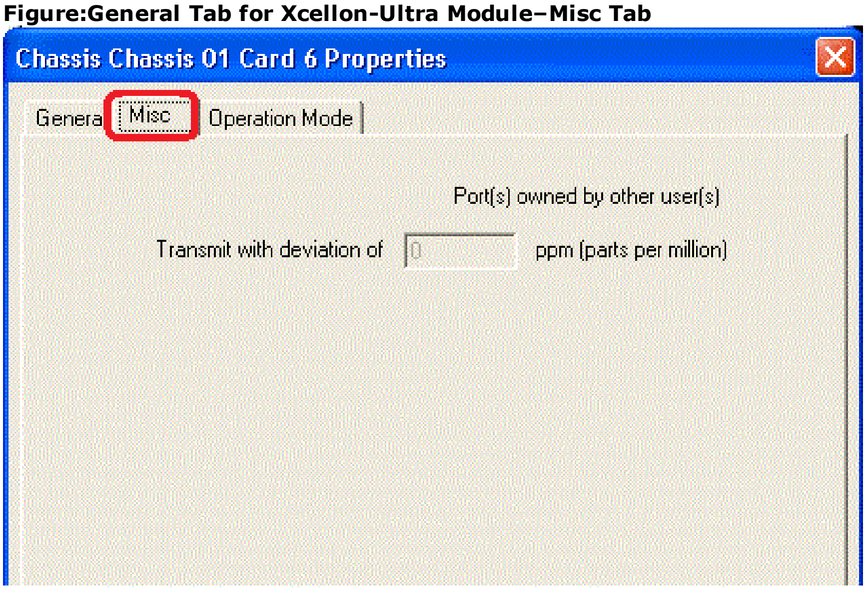
The **General** tab in **Card Properties** dialog box is shown in the following figure. The IxN2X capability appears in the **General** tab.

Figure:General Tab for Xcellon-Ultra NG Modules



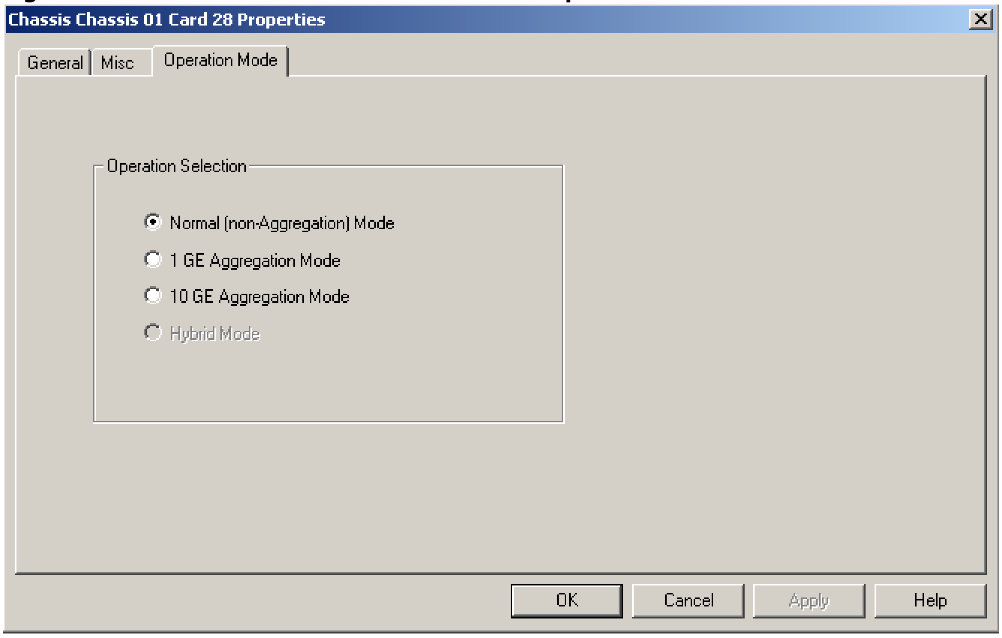
The Misc dialog box for Xcellon-Ultra NG card properties is shown in the following figure.

Figure:General Tab for Xcellon-Ultra Module–Misc Tab



The Operation Mode dialog box for Xcellon-Ultra NG card properties is shown in the following figure.

Figure:General Tab for Xcellon-Ultra Module–Operation Mode Tab



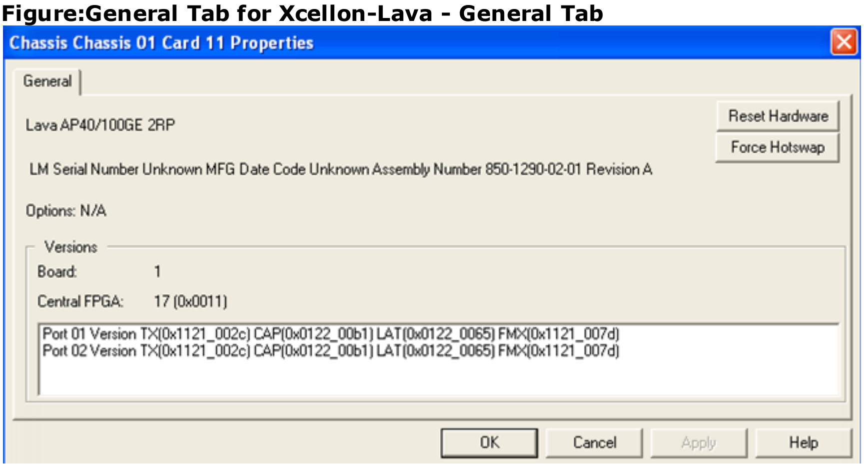
The features of partition, aggregation and multicast are mainly used by the IxLoad and IxNetwork applications. IxExplorer can display the current state of the Xcellon-Ultra card. An operation mode option named **Hybrid** Mode is added to represent the state that Xcellon-Ultra card has multiple partition groups. A radio button named **Hybrid Mode** is added in Xcellon-Ultra card **Properties** dialog box in the **Operation Mode** tab. The other options in the **Operation Mode** are Normal (non-aggregation) Mode, 1 GE Aggregation Mode, and 10 GE Aggregation Mode. In this dialog box, you can switch Xcellon-Ultra card to other modes from hybrid mode, but cannot switch it to hybrid mode from other modes. When partition groups are created through IxTclHal, the operation mode will be set to hybrid mode, and be displayed in IxExplorer.

Xcellon-Lava Module

The ***General*** tab shows the board version and FPGA revision level for the board as well as the FPGA versions for each port on the card. It contains a button for resetting the hardware to factory defaults. There is another button Force Hotswap which will emulate physical removal and insertion of the load module. This is done for diagnostic purposes. We recommend the use of this test with guidance from Ixia.

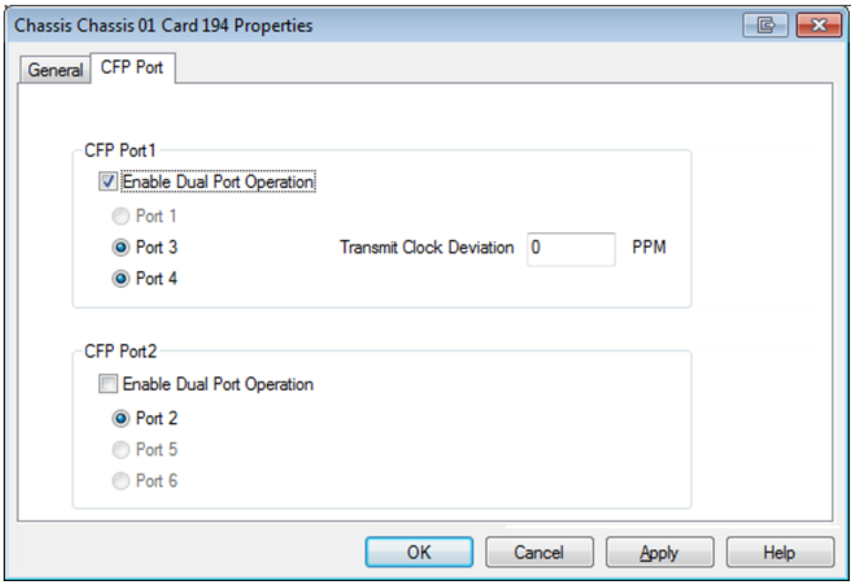
Xcellon-Lava module card properties dialog **General** tab is shown in the following figure:

Figure:General Tab for Xcellon-Lava - General Tab



Xcellon-Lava module card properties dialog **CFP Port** tab is shown in the following figure:

Figure:General Tab for Xcellon-Lava - CFP Port Tab



This is present in Port Properties view, and allows CFP to be placed into Single Port or Dual Port operation. CFP Mode operation is not automatic; user must select desired mode of operation. There are two types of mode:

- **Single Port Operation**: CFP provides one port of 40G or 100G. Speed is selected in a Port Property.
- **Dual Port Operation**: CFP provides two ports of 40G, when using CFP-to-QSFP+ Dual-Port Interface Adapter.

Each of the two ports can be owned independently, but if ownership is not exclusive by one user, the following operation will not be allowed by either owner:

- CFP Mode change to Single Port Operation
- Clock PPM adjustment
- Reset Hardware (under Card Properties) – not to be confused with Reboot CPU, which is not restricted

The limitations for the Dual Port Operation are as follows:

- BERT functionality not available
- Capture buffer is half the capacity of Single Port Operation
- Value List memory is half that of Single Port Operation
- TX Flow sequence memory is half that of Single Port Operation
- Sequence Checking memory is half that of Single Port Operation
- PPM adjustment is per CFP (pair of QSFP ports)
- DCE support not available at this time
- Front panel LEDs not functional

Xcellon-Multis Module

General

The ***General*** tab shows the board version and FPGA revision level for the board as well as the FPGA versions for each port on the card. The Reset Hardware button in this dialog allows you to reset the hardware to factory defaults.
Examples of the card properties dialog **General** tab for the Multis CXP and QSFP load modules are shown in the following figures:

Figure:Xcellon-Multis CXP- General Tab

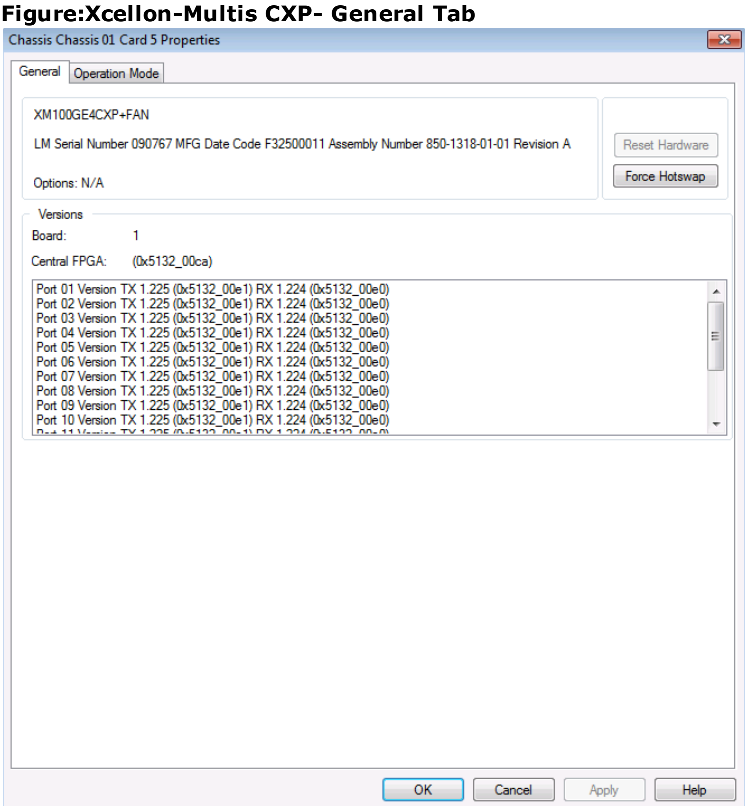
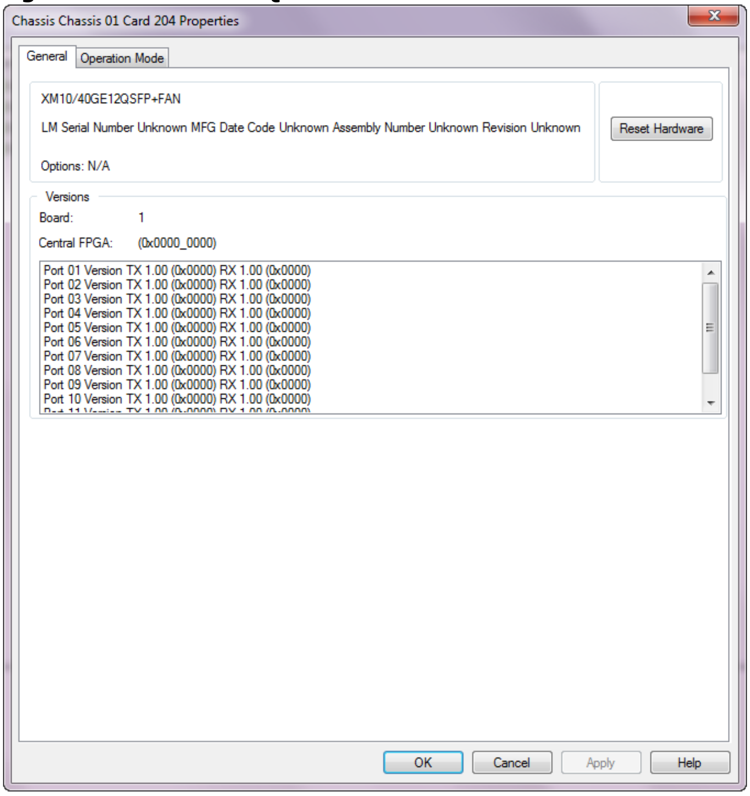


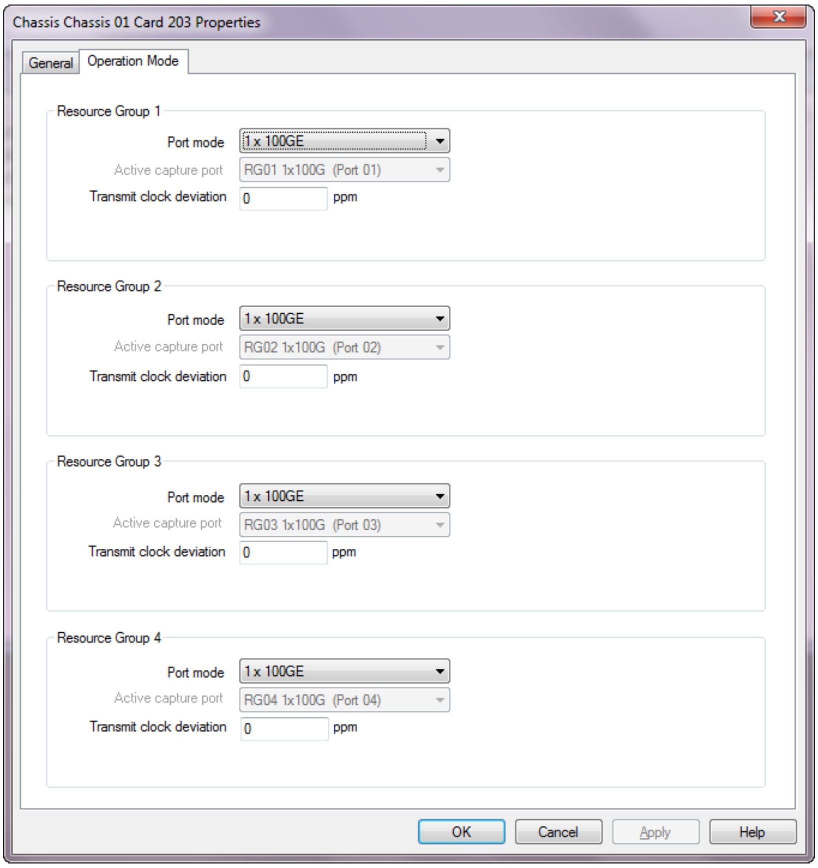
Figure:Xcellon-Multis QSFP- General Tab



Operation Mode

The Xcellon-Multis modules have an **Operation Mode** tab which is used to select the mode of operation for the module.

The *Operation Mode* tab is shown in the following figure.



The Xcellon-Multis card has four Ethernet ports with 100GE speeds. The card has a transceiver corresponding to each port. In each port, you can insert a FanOut cable which fans the output into multiple ports instead of using the original port.

You need to select the mode from the Port mode list for each Resource Group. Options include the following:

- 100GE Normal Mode–4 ports of 100GE speed
- 3x40GE Fan-out Mode–3 ports of 40GE speed using Fan-out cables
- 3x10GE Fan-out Mode–3 ports of 10GE speed using Fan-out cables
- 8x10GE Fan-out Mode–8 ports of 10GE speed using Fan-out cables
- 4x25GE Normal Mode–1 port of 100 GE speed converts to 4 ports of 25 GE speed within a single Resource Group using QSFP28 form factor

  2x25GE Normal Mode–A subset of the 4x25G mode, and has the same capabilities except that only 2 ports of the port group are activated. This mode is available with the 4x25G license.
- 1X50GE Normal Mode–1 ports of 50GE speed

The following Xcellon-Multis card types are supported:

- XM100GE4CXP
- XM100GE4CXP+FAN
- XM40GE12QSFP+FAN
- XM100GE4CXP+FAN+10GE
- XM10/40GE12QSFP+FAN

- XM10/40GE6QSFP+FAN
- XM100GE4CFP4
- XM100GE4CFP4+ENH
- XM100GE4QSFP28
- XM100GE4QSFP28+ENH
- XM100GE4QSFP28+ENH+25G
- XM100GE4QSFP28+ENH+25G+50G
- XMR10GE16SFP+FAN
- XMR10GE32SFP+FAN

For more information on Xcellon-Multis cards, see *Ixia Platform Reference Guide*.

The Active capture port field shows the port in the Resource Group on which you can perform data capture.

NOTE You can perform data capture only on a single port within a Resource Group. You can activate multiple ports but if you try to capture more data on more than one, then it fails with an error message.

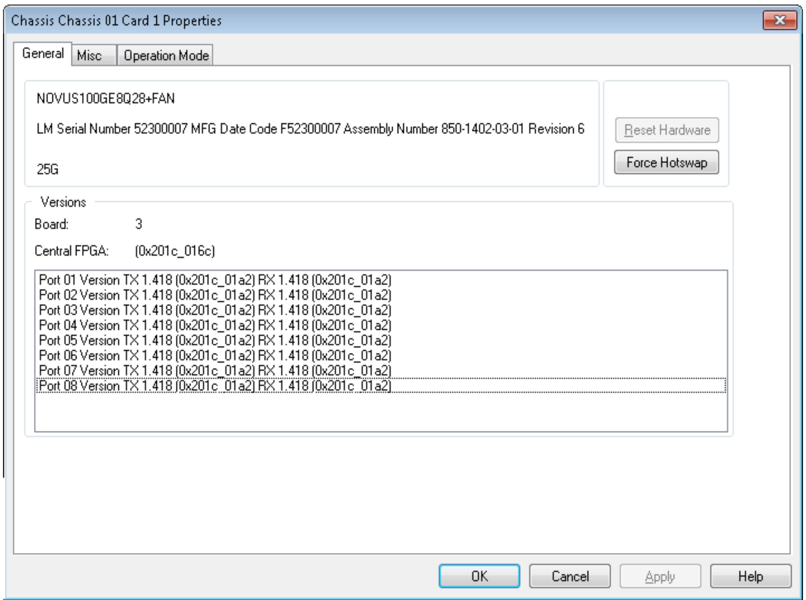
In the Transmit clock Deviation box, enter the line transmit frequency for the Multis card. The initial rate is controlled by the chassis chain reference clock. You can then adjust the line transmit frequency for the card.

Novus Module

General

The ***General*** tab shows the board version and FPGA revision level for the board as well as the FPGA versions for each port on the card. The Reset Hardware button in this dialog allows you to reset the hardware to factory defaults.
Examples of the card properties dialog **General** tab for the Novus load modules are shown in the following figures:

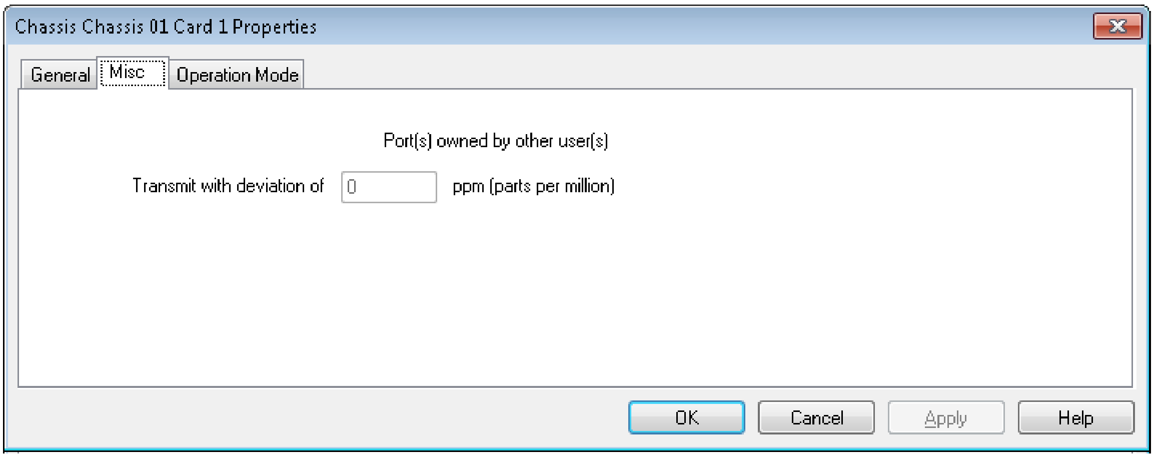
Figure: Novus-General Tab



Misc

The Novus module Card Properties dialog has the Misc tab when in normal (non-aggregated) mode. The Misc tab functionality is identical to that described in LM1000 and LM10GE Modules—Misc Dialog.

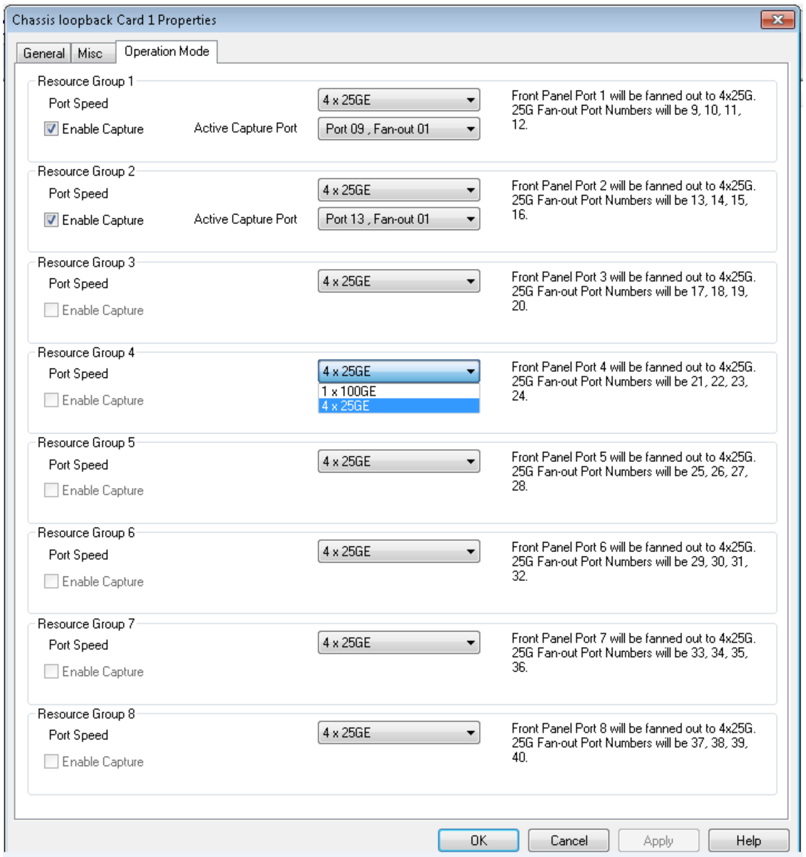
Figure: Novus-Misc Tab



Operation Mode

The Novus modules have an **Operation Mode** tab which is used to select the mode of operation for the module.

The ***Operation Mode*** tab is shown in the following figure:



The Novus card has eight Ethernet ports with 100GE speeds. The card has a transceiver corresponding to each port. In each port, you can insert a FanOut cable which fans the output into multiple ports instead of using the original port.

You need to select the speed from the Port speed list for each Resource Group. Options include the following:

- 100 GE Normal Mode - 8 ports of 100 GE speed
- 4x25GE Normal Mode–1 port of 100 GE speed converts to 4 ports of 25GE speed within a single Resource Group using QSFP28 form factor

The following Novus card types are supported:

- NOVUS100GE8Q28+FAN
- NOVUS100GE8Q28+FAN+25GE

For more information on Novus cards, see *Ixia Platform Reference Guide*.

The Enable Capture checkbox shows the port in the Resource Group on which you can perform data capture.

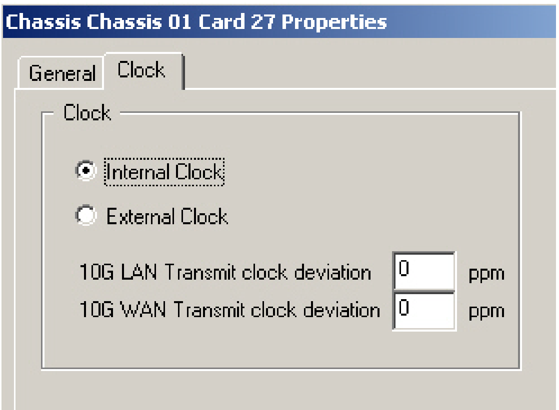
NOTE You can enable capture only on two ports in a card.

NGY LSM10GXM 2, 4 and 8-port Modules

The *Card Properties* dialog box of the LSM10GXM 2, 4 and 8-port modules has a *General* tab identical to that shown in the following figure.

It also features a *Clock* tab, for configuring clocking, shown in the following figure:

Figure:clock Tab for LSM10GXM Modules

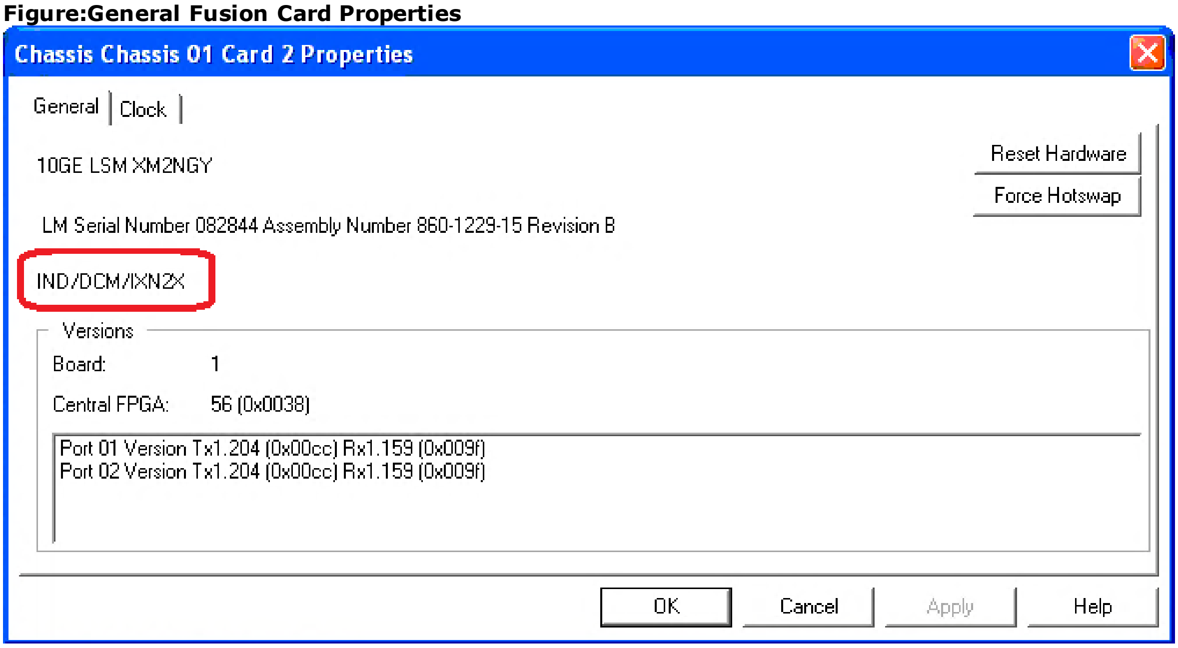


Select **Internal** clock and set the transmit clock deviation using this dialog, or select **External** clock. Details are provided in *Table:10GE LSM LAN/WAN General Tab Configuration*.

Fusion enabled NGY Modules

10GLSMXM2NG, 10GLSMXM4NG and 10GLSMXM8NG are the fusion enabled versions of the existing Ixia 10GLSMXM2XP, 10GLSMXM4XP, 10GLSMXM8XP. These modules are capable of running in IxN2X mode. The General Tab in Card Properties dialog box is shown in the following figure. The IXN2X capability appears in the General tab. The remaining tabs are identical to the non-Fusion enabled load modules.

Figure:General Fusion Card Properties

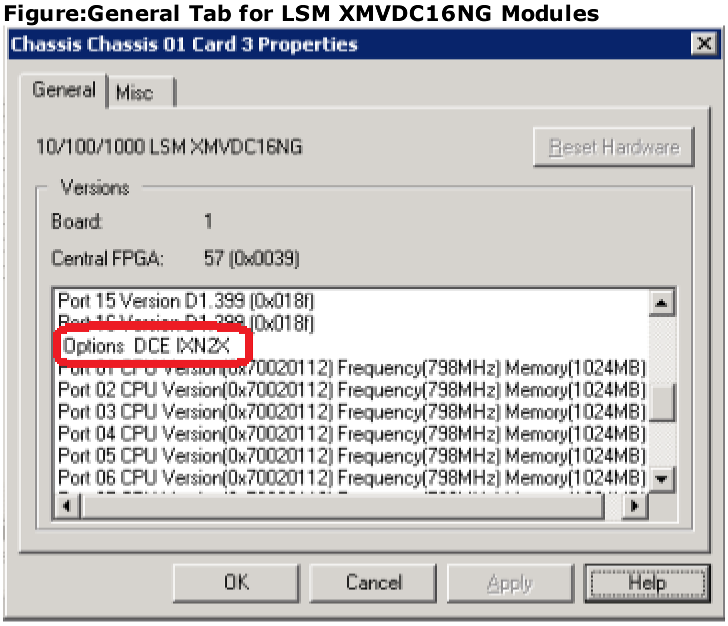


LSM XMVDC16NG 16-port Modules

The LSM XMVDC16NG module is the Fusion-Enabled version of the existing Ixia XMVDC16 module. The LSM XMVDC16NG module is capable of running in IxN2X mode.

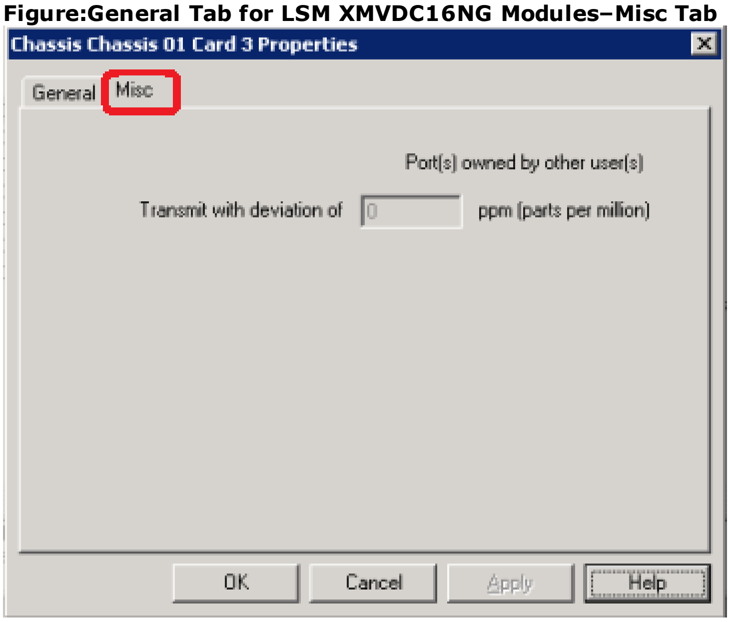
The **General** tab in **Card Properties** dialog box is shown in the following figure. The IxN2X capability appears in the **General** tab.

Figure:General Tab for LSM XMVDC16NG Modules



The Misc dialog box for LSM XMVDC16NG card properties is shown in the following figure.

Figure:General Tab for LSM XMVDC16NG Modules–Misc Tab



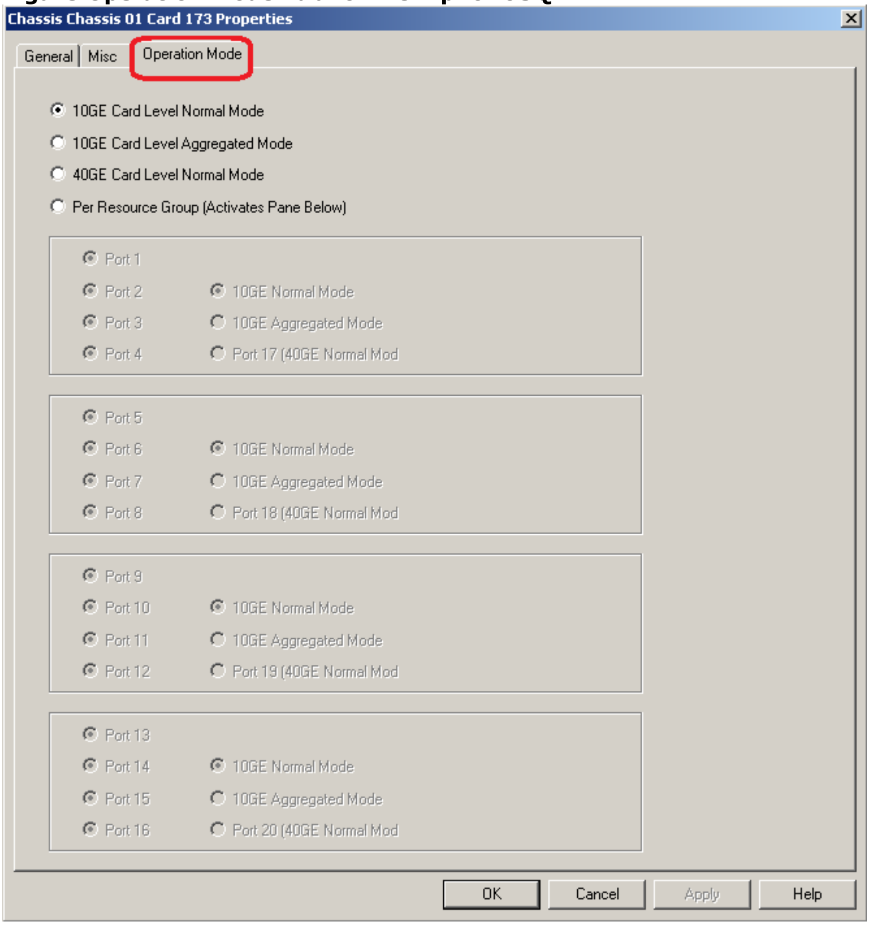
FlexAP1040SQ

The 10/40 Gigabit Ethernet Accelerated Performance is a 6-port load module with SFP+ interfaces and 4-ports of QSFP+ 40GE interfaces with full performance L2-7 support.

Operation Mode

The **Operation Mode** dialog box for FlexAP1040SQ card properties is shown in the following figure:

Figure:Operation Mode Tab for FlexAp1040SQ



The different card level modes can be set in the **Operation Mode** dialog box.

Power over Ethernet Modules

Power over Ethernet modules have two additional tabs in the Card Properties dialog:

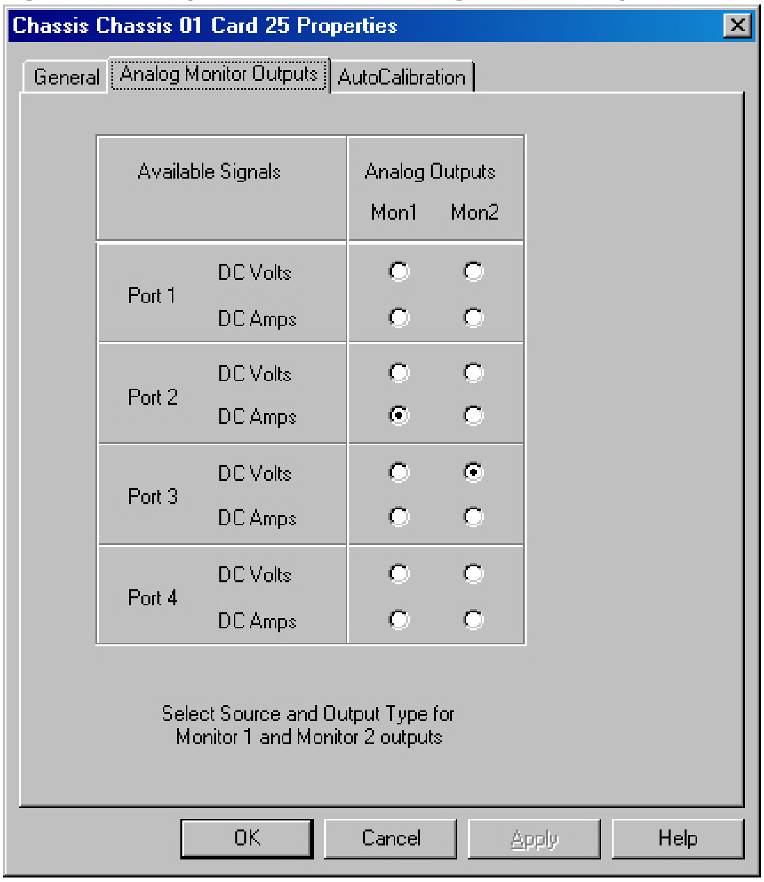
- *Monitor Analog Outputs Tab*
- *AutoCalibration Tab*

Monitor Analog Outputs Tab

Power of Ethernet (PoE) modules have a special tab for controlling how to monitor the analog outputs. The monitor outputs provide a signal to an external measuring device (such as an oscilloscope).

The *Monitor Analog Outputs* tab in the *Card Properties* dialog is shown in the following figure.

Figure:Card Properties for PoE—Analog Monitor Outputs Tab



There are two monitors that can be set (Monitor 1 and 2), both on the same port or on separate ports.

The controls for the *Analog Monitor Outputs* tab are explained in the following table.

Table:PoE Analog Monitor Outputs

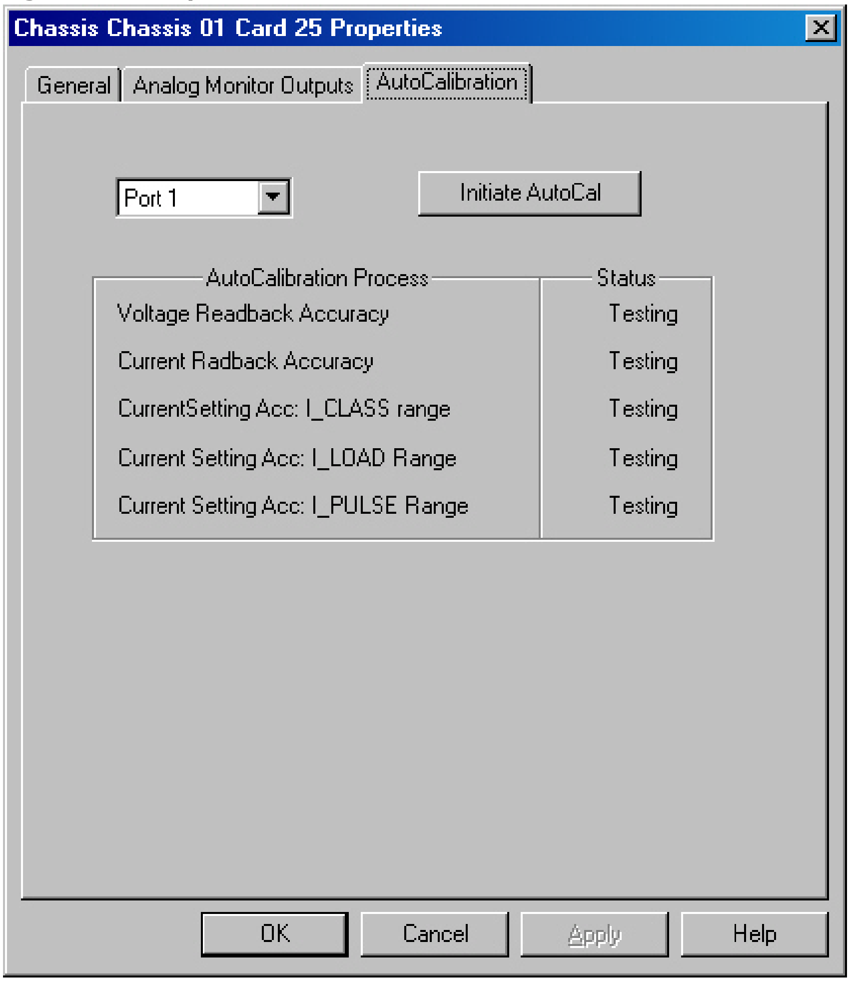
Section	Field/Control	Usage
Available Signals		Displays the available signals for each PoE port.
	DC Volts	Provides a Direct Current voltage measurement.
	DC Amps	Provides a Direct Current amperage measurement.
Analog Outputs		
	Mon1	Use the option buttons to select what output on what port for Monitor 1.
	Mon2	Use the option buttons to select what output on what port for Monitor 2.

AutoCalibration Tab

During the regular chassis start-up sequence, all ports in the chassis are tested and calibrated. The PoE module ports can be re-calibrated at anytime using the *AutoCalibration* tab.

This tab is accessed by right-clicking a module in the Resources window, selecting the *Properties* menu options, then selecting the *AutoCalibration* tab. The *AutoCalibration* tab is shown in the following figure.

Figure:Card Properties for PoE—AutoCalibration Tab



The controls in this tab page are described in the following table:

Table:PoE AutoCalibration

Field/Control	Usage
Port List	Allows to pick a port for calibration. Selectable ports are limited to ports on the current card.
Initiate AutoCal	Selecting this button initiates the calibration sequence.
Auto Calibrate Process	Displays the various tests that are run on the selected port to verify it can be used. The categories are: • Voltage Readback Accuracy • Current Readback Accuracy • CurrentSetting Acc: I_CLASS Range • CurrentSetting Acc: I_LOAD Range • CurrentSetting Acc: I_PULSE Range
Status	Shows the status of a particular test. The possible statuses are:

Field/Control	Usage
	• Testing—In process of testing. • Pass—Port has passed this test. • Fail—Port has failed this test.

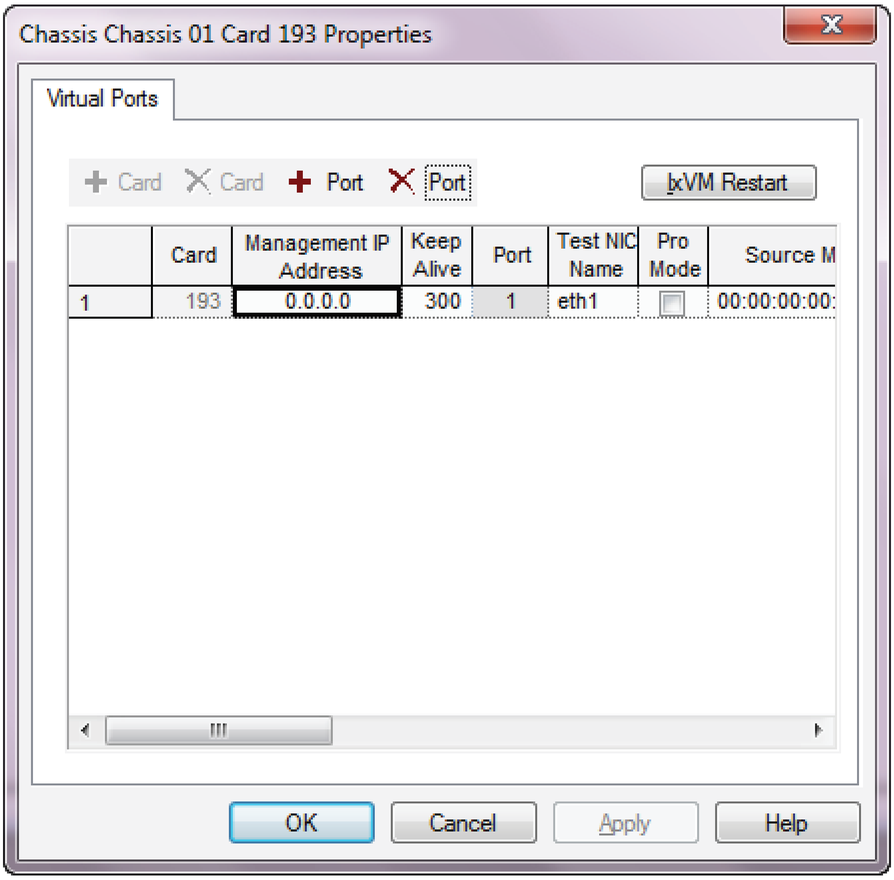
Testing statistics can be viewed in the IxServer main window. For more information on the IxServer main window, see the *IxServer User Guide*.

Virtual Load Modules

The Ixia Virtual load module has the Virtual Ports tab in the Card Properties dialog.

Virtual Ports Tab

The Card Properties - Virtual Ports tab is shown in the following figure.Table 17-4. Card Properties for Virtual Ports Tab.



The controls for the Virtual Ports tab are explained in the following table.

Section	Field/Control	Description
	Card	The card number.
	Management IP Address	Management IP address of the Linux machine with the IxVM software agent installedMan-

Section	Field/Control	Description
		agement IP address of the Linux machine with the IxVM software agent installed.
	Keep Alive	The keep-alive timeout in seconds. Each IxVM card has a keep-alive mechanism between the virtual chassis and the virtual card. In case either of these two components do not send or receive a keep-alive message for a certain amount of time, then the virtual card will disconnect from the virtual chassis.
	Port	The name of the port on the IxVM card to be used for traffic generation and measurement.
	Test NIC Name	Name of the virtual interface that will be used as a traffic generator. Virtual interface must be created before adding the port.
	Pro Mode	Denotes the promiscuous or non-promiscuous mode in which a virtual port is added to a virtual card.
	Source MAC	The first source MAC address to be generated for the stream.
	Link MTU	MTU value of test interface from a virtual machine. The minimum value is 1500 and the maximum value is 9000 and should be changed mainly when there are control plane frames bigger than 1500.
	Line Speed (Mbps)	Select the line speed. Options include the fol-

Section	Field/Control	Description
		lowing: 100MBPS 1000MBPS: 1 Gb speed 10000MBPS: 10 Gb speed
+ Port		Adds a port to the virtual load module.
✕ Port		Removes a port from virtual the load module.
IxVM Restart		Restarts the virtual machine.

Chapter 18 - Port Properties — 10/100/1000 Ethernet Family

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog is a display that corresponds to the module type. The following sections describe the functions and configuration of the 10/100/1000 Ethernet family of module port properties.

Port properties for the various Ethernet family module types are described in the following sections.

- *Port Properties for 10, 100, and/or 1000 Modules* includes the 3 types of modules listed below):
  - *Port Properties for 10, 100, and/or 1000 Modules*
  - *Port Properties for Ethernet Family of Modules* (including TXS Layer-7)
  - *Port Properties for Copper 10/100/1000 Modules*
  - *Port Properties for 10/100/1000 XMV Modules*
- *Port Properties for Gigabit and GBIC Modules*
- *Port Properties for Gigabit and GBIC Modules*
- *Port Properties for Power over Ethernet (PoE)*
- *ALM1000T8/CPM1000T8 Module Port Properties*
- *ELM1000ST2 Module Port Properties*
- *Port Properties for Xcellon-Ultra and ASM1000XMV12X*

Port Properties for 10, 100, and/or 1000 Modules

The Ethernet modules supporting 10, 100, and/or 1000 Mbps operation often have similar port properties, and are grouped together in this section. Many of the same individual *Port Properties* dialogs are used for these modules. The module types included in this group are listed below:

- *Port Properties for 10/100 Modules*
- *Port Properties for Ethernet Family of Modules*
- *Port Properties for Copper 10/100/1000 Modules*
- *Port Properties for 10/100/1000 XMV Modules*

The *Port Properties* dialog is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

Port Properties for 10/100 Modules

The complete specifications for the 10/100 and 100 Mbps modules can be found in the *Ixia Platform Reference Manual*.

The tabbed dialogs in the set indicate the types of properties that may be modified for 10/100, 10/100-3, and 100 Mbps modules. The group of tabs available in each set is dependent on the type of module. The list of available tabs follows:

- *Auto Negotiation Tab*
- *Advanced MII Tab*(*MII Register* Files for additional information on *MII registers*.)
- *Flow Control Tab*
- *Collision Backoff Algorithm Tab*
- *Forced Collisions Tab*
- *Status Tab*
- *Transmit Modes for 10/100 Modules* (Not available for 100-3 modules.)

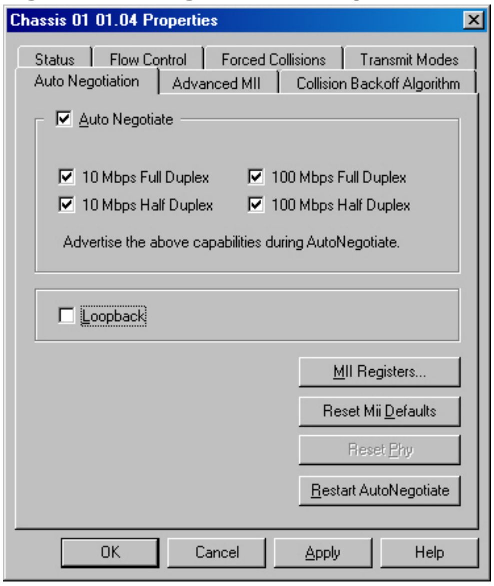
The *Port Properties* dialog is access by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

Auto Negotiation Tab

The *Auto Negotiation* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Auto Negotiation* tab.

Auto negotiation controls how the port communicates with other ports. The *Auto Negotiation* tab offers access to the Auto Negotiation and Loopback properties. This tab is shown in the following figure:

Figure:Auto Negotiation Tab (shown for 10/100 module)



The fields and controls in this tab are described in the following table:

Table:Auto Negotiation Tab

Field/Control	Description
Auto Negotiate	If selected, allows auto negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during AutoNegotiation.
10 Mbps Full Duplex	If selected, auto negotiate will advertise 10 Mbps full duplex operation.
10 Mbps Half Duplex	If selected, auto negotiate will advertise 10 Mbps half duplex operation.
100 Mbps Full Duplex	If selected, auto negotiate will advertise 100 Mbps full

Field/Control	Description
	duplex operation.
100 Mbps Half Duplex	If selected, auto negotiate will advertise 100 Mbps half duplex operation.
Loopback	If selected, the port is set to internally loopback from transmit to receive.
MII Registers...	Allows the current MII register values to be read and written. *MII Register Files* for additional information on MII Registers.
Reset MII Defaults	Resets all of the port's properties back to the default settings.
Reset Phy	Does not apply to this module; it is always dimmed.
Restart AutoNegotiate	When pushed, the Auto Negotiate sequence is restarted.

The MII Control register pages for different modules vary somewhat, based on the module.

Advanced MII Tab

The *Advanced MII* tab allows for the proper association of MII register labels with the actual hardware in use (for example, a port). It is initially set to use the appropriate default template that corresponds to one of the PHYs in use on that Ixia module card. Additions or corrections can be made, and even saved under a different template name.

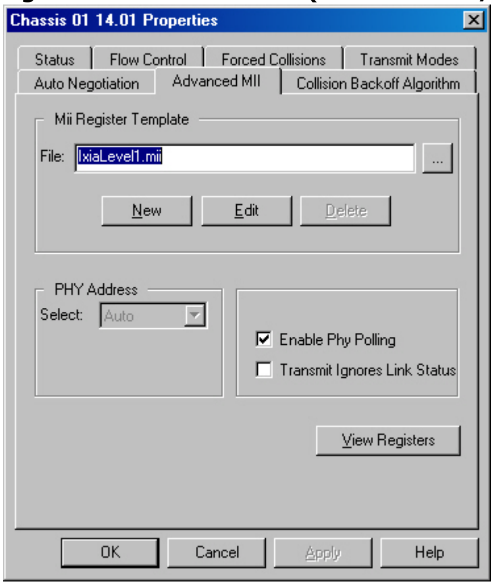
The *Advanced MII* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Advanced MII* tab. The tab for a port is shown in the following figure:

NOTE Note:*MII Register Files* for additional information on MII Registers.

For Copper 10/100/1000 modules, *Advanced MII for Copper 10/100/100 Modules.*

For 10GE modules, *10GE Port Properties–Advanced MII*.

Figure:Advanced MII Tab (shown for 10/100 module)



The upper part of the tab, labeled *MII Register Template*, is used to control the selection and editing of an MII register template file. MII Register Template files hold the register definitions. The lower part of the dialog allows the PHY address to be set. The fields and controls in this tab are described in the following table:.

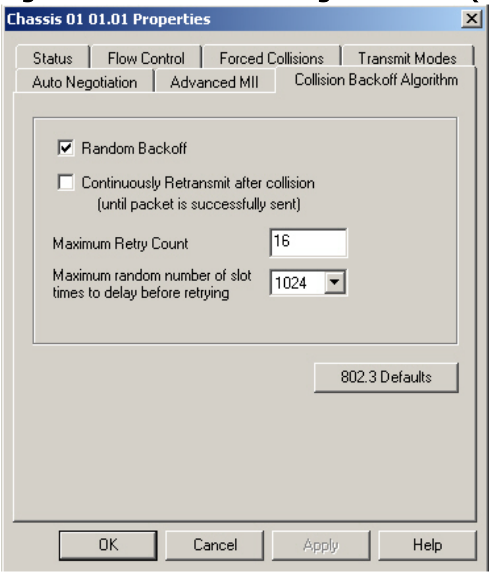
Figure:Advanced MII Tab

Section	Field/Control	Description
MII Register Template	File	The name of the MII register file.
	Browse	Opens up a standard Windows file browsing window in the directory `C:\Program Files\Ixia\MII`, looking for files that end in *.mii*.
	New	Allows the creation of a new MII register Template file. *New/Edit MII Register Template Setup—Management Page* for operational details.
	Edit	Allows the editing of the indicated file. *New/Edit MII Register Template Setup—Management Page* for operational details.
	Delete	Deletes the current file after a confirmation dialog.
PHY Address	Select:	Allows the address of the PHY to be set to Auto or a constant from 0 to 31.
	Enable Phy Polling	If selected, then the PHY is continuously polled during MII setup operation.
	Transmit ignores link status	If selected, will allow transmission of packets even if the link is down.

Collision Backoff Algorithm Tab

The *Collision Backoff Algorithm* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Collision Backoff Algorithm* tab. The *Collision Backoff Algorithm* tab for 10/100 modules is shown in the following figure:

Figure:Collision Backoff Algorithm Tab (shown for 10/100 module)



Refer to the Forced Collision Operation section in the 'Theory of Operation: General' chapter of the Ixia Platform Reference Manual for additional information on forced collisions.

The options and controls available on the *Collision Backoff Algorithm* tab are as follows:

Table:Collision Backoff Algorithm Tab

Field/Control	Description
Random Backoff	When a collision occurs, wait a random amount of time before retrying the transmission. The *Maximum Retry Count* and *Maximum number of random slot times to delay before retrying* settings below govern how often and how long retries will be attempted.
Continuously Retransmit After Collision (until packet is successfully sent)	When a collision occurs, continuously retransmit the packet until the *Maximum Retry Count* is reached.
Maximum Retry Count	The maximum number of retries that will be attempted for each packet.
Maximum random number of slot times to delay before retrying	Each successive retry operates by selecting a slot time over a range that doubles with each retry (2, 4, 8,..., 1024). This value controls the maximum number of slot times used.
802.3 Defaults	Restores the IEEE 802.3 standard default values for *Maximum Retry Count* (16) and *Maximum number of random slot times to delay before retrying*

Field/Control	Description
	(1024).

The *Apply* button can be used to immediately change the port's properties without leaving the tab; the *OK* button performs the same function and exits the tab as well.

Flow Control Tab

NOTE For NGY module, *NGY Port Properties–Flow Control*.

For Xcellon-Flex module, *Flex Port Properties—Flow Control*.

For XDM10G32S module, *XDM10G32S Port Properties—Flow Control*.

For Xcellon-Multis module,*Xcellon-Multis Port Properties—Flow Control*.

For Novus module, *Novus Port Properties—Flow Control*.

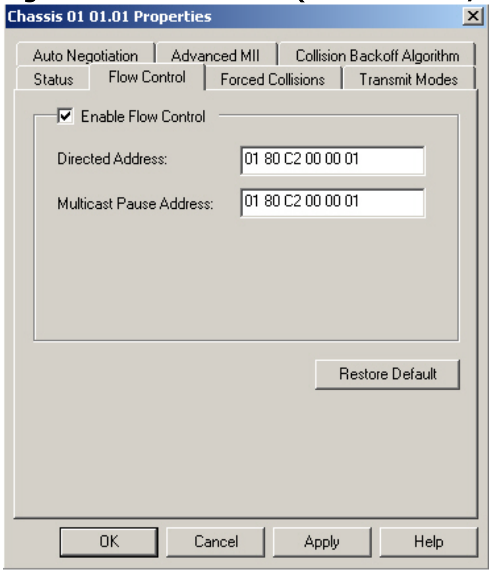
When a port is receiving data at a faster rate than it can handle from another, directly connected port, the receiving port can send a MAC control PAUSE frame to the sending port to temporarily halt transmission of frames. The PAUSE function is defined in IEEE 802.3.

NOTE For 10GE module Flow Control, *10GE Port Properties–Flow Control*

For 10/100 TXS8, 1000SFPS4, and 10/100/1000 TXS4 module Flow Control, *Flow Control Tab for Ethernet Modules*

The *Flow Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The behavior of the port's link layer (MAC) flow control may be set with the *Flow Control* tab, shown in the following figure:

Figure:Flow Control Tab (shown for 10/100 module)



The options and controls available for the *Flow Control* tab are described in the following figure:

Table:Flow Control Tab

Field/Control	Description
Enable Flow Control	Must be selected in order for the port's MAC flow control mechanisms to be enabled.
Directed Address	This is the MAC address that the port will listen on for a directed pause message.
Multicast Pause Address	This is the MAC address that the port will listen on for a multicast pause message.
Restore Default	Resets both the Directed Address and Multicast Pause Address back to the default value of *01 80 C2 00 00 01.*

Forced Collisions Tab

Forced collisions can be generated on the receive side of a port on certain modules, when the port is in half-duplex mode. Forced collisions operate by generating data as information is being received. The collision takes the form of a number of 4-bit nibbles generated at a specific offset within a packet. A number of consecutive collisions are generated, followed by a non-colliding period. This combination of collisions and non-colliding periods can be repeated indefinitely, or for a specified number of repetitions. See the Port Data Capture Capabilities section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for a full explanation of the theory of forced collision operation.

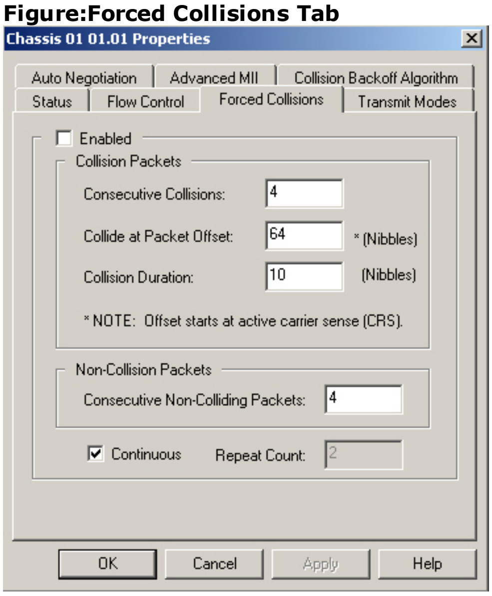
Collisions must be separately started, before capture. See *IxExplorer Operation* for ways to initiate collisions.

The *Forced Collisions* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Forced Collisions* tab.

NOTE The forced collision algorithm on the T-5 and 10/100 load modules does not generate a preamble and SFD as part of the collision. This may cause some PHYs not to detect the collision. This is not a problem with collisions occurring during normal operation (not initiated due to a forced collision).

The tab used to control forced collisions is shown in the following figure. (Forced Collisions are not supported on 10/100 TXS8, 10/100/1000 TXS4, or 1000 SFPS4 modules.)

Figure:Forced Collisions Tab



The options and controls available in the *Forced Collisions* tab are described in the following figure:

Table:Forced Collisions Tab

Section	Field/Control	Description
Enabled		This box must be selected to enable the generation of forced collisions.
Collision Packets	Consecutive Collisions	The number of consecutive collisions to generate at a time. Collisions take place on the first received packet after enabled.
	Collide at Packet Offset	The offset from the beginning of packet active carrier sense (the beginning of the preamble) to the start of the collision, measured in nibbles.
	Collision Duration	The duration of each collision, measured in nibbles.
Non-Collision Packets	Consecutive Non-Colliding Packets	The number of packets that will not be modified after each time that the programmed consecutive collisions have occurred.
	Continuous	If selected, the pattern of collisions and non-collisions is repeated indefinitely.
	Repeat Count	If continuous is not selected, this value is the number of times that the pattern of collisions/non-collisions is repeated.

The *Apply* button can be used to immediately change the port's properties without leaving the tab. The *OK* button performs the same function and exits the tab as well.

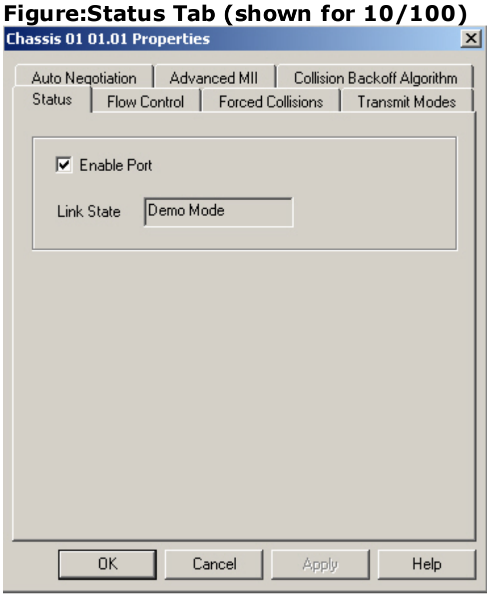
Status Tab

NOTE For VM Port Status tab properties, *VM Port Properties—Status*.

The *Status* tab displays the link state and allows the port to be disabled manually. This feature also automatically disables a port which has a hardware fault—at power up or at run time. It allows the chassis to restart without taking the time to check the status of this port. The port can also be disabled if a hardware fault occurred, or for some other purpose. The *Enable Port* check box is enabled by default.

The *Status* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Status* tab. The *Status* tab is shown in the following figure. (Type-3 modules do not support this capability.)

Figure:Status Tab (shown for 10/100)

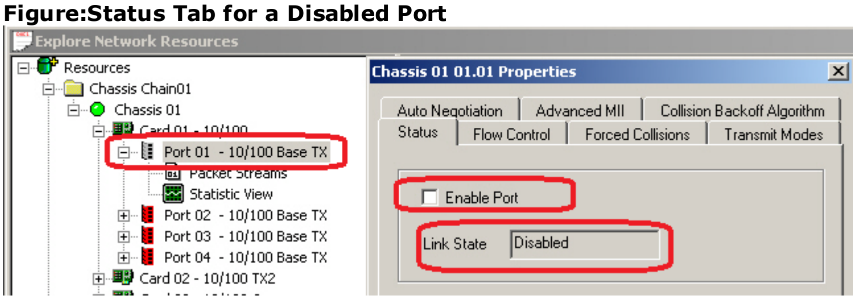


The display of the status of the link is also shown in the Statistic View for this port. The possible states are:

- Hardware Fault
- Disabled, Busy
- Link Up
- Link Down
- Loopback
- WriteMII
- Demo Mode
- empty (no status displayed if the chassis is disabled)

The port can be disabled by selecting the check box to remove the checkmark and then pressing the *Apply* button. The display will then read 'Disabled,' and the port icon in the Resources tree will be changed to gray, as shown in the following figure:

Figure:Status Tab for a Disabled Port



Transmit Modes for 10/100 Modules

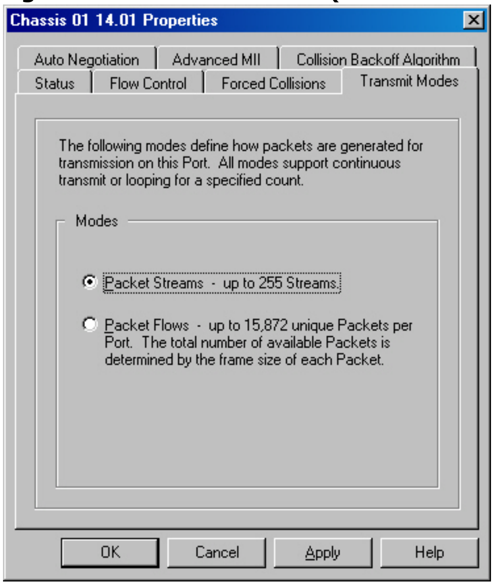
The *Transmit Modes* tab controls the basic transmit mode of the port. These modes define how packets are generated for transmission on the port. All modes support continuous transmit or looping for a specified count.

The *Transmit Modes* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Transmit Modes* tab. The *Transmit Modes* tab for 10/100 modules is shown in the following figure:

NOTE *Transmit Modes Tab for Ethernet Modules* for information on the Transmit Modes tab for those modules.

Transmit Modes for Gigabit Modules for information on the Transmit Modes tab for Gigabit, GBIC, and Copper 10/100/1000 (using Gigabit) modules.

Figure:Transmit Modes Tab (shown for 10/100 module)



The fields and controls for this tab are described in the following table:

Table:Transmit Modes Tab

Field/Control	Description
Packet Streams	Sets the basic operating mode for the port to packet streams. This allows the hardware to generate up to 255 streams. Or, a stream may be programmed for continuous burst or packet generation—generating a continuous, infinite stream.

Field/Control	Description
Packet Flows	Sets the basic operating mode for the port to packet flows. This allows the software to generate up to 15,872 unique packets. Ultimately, the number of packets is determined by the amount of port memory available divided by the size of the packets.

The choice of the file name for image files is arbitrary, but a consistent extension should be chosen to avoid confusion. Although many ports may share the use of a single file, each port must individually specify the file name. The Port Copying operation (*Port Copying Operation*) *will copy this information from port to port if desired. The image files are all kept in the FlowImage sub-directory beneath the Ixia installation directory—usually C:\Program Files\Ixia\FlowImage).*

See the Port Transmit Capabilities section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for a full explanation of streams versus flows.

Port Properties for Ethernet Family of Modules

The Ethernet family of modules (10/100 TXS8, 10/100/1000 TXS4, 1000 SFPS4, 10/100/1000 ALM T8, and so forth) has per-port CPUs. The *Port Properties* dialog for the full-featured TXS modules, as well as the versions that support Layer 2 and 3 capabilities, include the following set of tabs.

- *Auto Negotiation Tab for Ethernet Modules*
- *Advanced MII Tab for Ethernet Modules*(*MII Register Files* for additional information on MII registers.)
- *Status Tab for Ethernet Modules*
- *Flow Control Tab for Ethernet Modules*
- *General Tab for Ethernet Modules*
- *Transmit Modes Tab for Ethernet Modules*
- *OAM Tab for Ethernet Modules*
- *Auto Instrumentation Tab for Ethernet Modules*

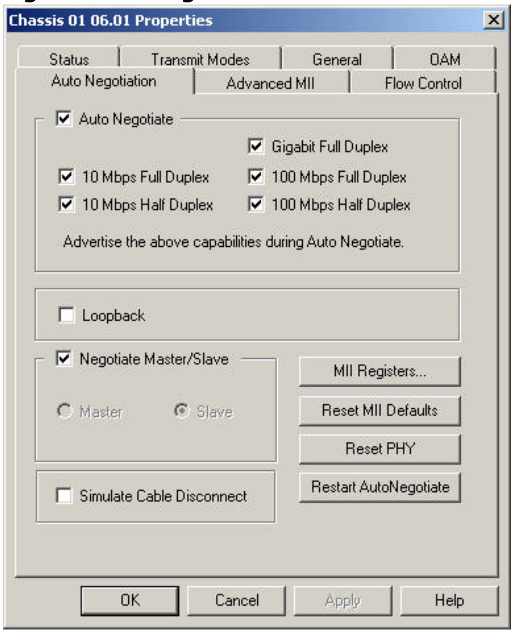
The *Port Properties dialog* is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

Auto Negotiation Tab for Ethernet Modules

Auto negotiation controls how the port establishes communication with other ports. The *Auto Negotiation* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Auto Negotiation* tab.

The *Auto Negotiation* tabs for the Ethernet family of modules are shown in the following figure:

Figure:Auto Negotiation Tabs for Ethernet Modules



The fields and controls in these tabs are described in the following table. The combination of fields and controls available depends on the module.

Table:Ethernet Modules—Auto Negotiation

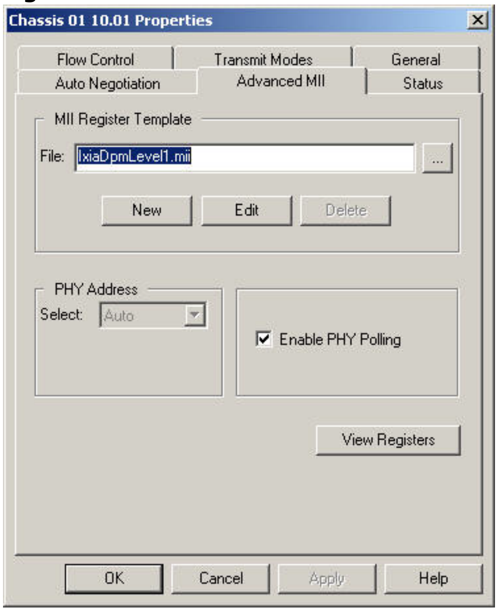
Field/Control	Description
Auto Negotiate	If selected, allows auto negotiation of speed and duplex operation based on the various choices. The capabilities which are selected are advertised during AutoNegotiation.
Gigabit Full Duplex	If selected, auto negotiate will advertise Gigabit (1000 Mbps) full duplex operation.
10 Mbps Full Duplex	If selected, auto negotiate will advertise 10 Mbps full duplex operation.
10 Mbps Half Duplex	If selected, auto negotiate will advertise 10 Mbps half duplex operation.
100 Mbps Full Duplex	If selected, auto negotiate will advertise 100 Mbps full duplex operation.
100 Mbps Half Duplex	If selected, auto negotiate will advertise 100 Mbps half duplex operation.
Loopback	If selected, the port is set to internally loopback from transmit to receive.
Simulate Cable Disconnect	If this is selected, the port acts as if the cable has been disconnected. (Does not apply to the ALM1000T8 and ELM1000ST2 Module.)
Negotiate Master/Slave	If selected, determining which port is Master or Slave is performed **automatically**. (Checking this box will disable the manual option for selecting Master or Slave.
Master	If selected, port will be configured as Master.
Slave	If selected, port will be configured as Slave.
MII Registers...	Allows the current MII register values to be read and writ-

Field/Control	Description
	ten. *MII Register Files* for additional information on MII Registers.
Reset MII Defaults	When this button is clicked, it resets all of the port's MII properties back to the default settings.
Restart PHY	When this button is clicked, it resets the PHY associated with the port through the MII control register.

Advanced MII Tab for Ethernet Modules

The *Advanced MII* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Advanced MII* tab. The *Advanced MII* tab for the 10/100 TXS8, 10/100/1000 TXS4, 1000 SFPS4, ALM1000T8, and ELM1000ST2 modules is shown in the following figure. The format for this tab is the same for all three types of modules, but the file name for the MII Register Template will be different for each one. (The tab shown in *Figure:Advanced MII Tab* for Ethernet Modules is for the 10/100 TXS8 module.)

Figure:Advanced MII Tab for Ethernet Modules



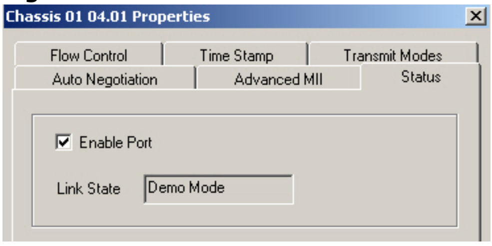
Refer to the following table for information about the fields and controls in this tab.

Status Tab for Ethernet Modules

The *Status* tab displays the link state and allows the port to be disabled manually. This feature also automatically disables a port which has a hardware fault—at power up or at run time. It allows the chassis to restart without taking the time to check the status of this port. The port can also be disabled if a hardware fault occurred, or for some other purpose. The *Enable Port* check box is enabled by default.

The *Status* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Status* tab. The *Status* tab for the 10/100 TXS8, 10/100/1000 TXS4, 1000 SFPS4, 10/100/1000 ALM T8, and 10/100/1000 ELM ST2 modules is shown in the following figure. Refer to *Status Tab* for additional information about the use of the *Status* tab.

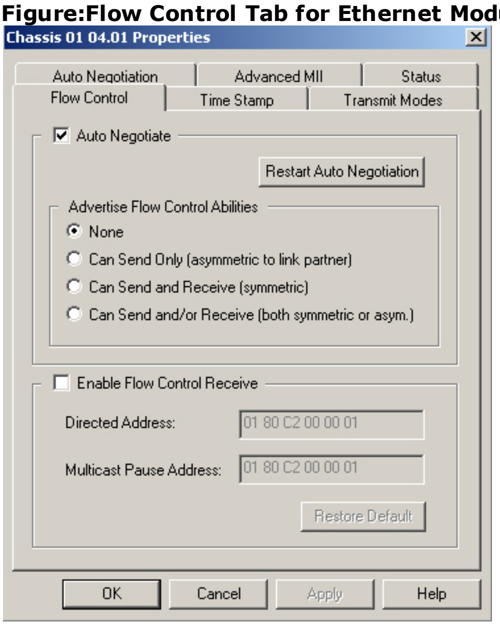
Figure:Status Tab for Ethernet Modules



Flow Control Tab for Ethernet Modules

The *Flow Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The *Flow Control* tab for the 10/100 TXS8, 10/100/1000 TXS4, 1000 SFPS4, 10/100/1000 ALM T8, and 10/100/1000 ELM ST2 modules is shown in the following figure.

Figure:Flow Control Tab for Ethernet Modules



The fields and controls in this tab are described in the following table:

Table:Flow Control Tab for Ethernet Modules

Section	Field/Control	Description
Auto Negotiate		Enables auto-negotiation of flow control capabilities for the port.
	Restart AutoNegotiation	If this button is clicked, it causes the auto-negotiation process to start immediately.
Advertise Flow Control Abilities	None	This and the next three options indicate which set of flow control capabilities are advertised to other ports. This option advertises no capabilities. (No PAUSE, per IEEE 802.3)
	Can Send Only (asym-	This option advertises only send capabilities. (Asymmetric PAUSE toward link partner, per IEEE 802.3)

Section	Field/Control	Description
	metric to link partner)	
	Can Send and Receive (symmetric)	This option advertises both send and receive capabilities. (Symmetric PAUSE, per IEEE 802.3)
	Can Send and/or Receive (both symmetric or asymmetric)	This option advertises all send and receive capabilities in any combination. (Both Symmetric PAUSE and Asymmetric PAUSE toward local device, per IEEE 802.3)
Force Flow Control Receive		Enables receive side flow control handling for the port.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
	Restore Default	If this button is clicked, it restores the default MAC address: 01 80 C2 00 00 01 in both *Directed* and *Multicast Pause Address* fields.

General Tab for Ethernet Modules

The *General* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *General* tab. The *General* tab for 10/100 TXS8, 10/100/1000 TXS4, and 1000 SFPS4 modules allows to configure the placement of the time stamp within a packet, as shown in the following figure:

NOTE If Floating Timestamp is selected in the Auto Instrumentation tab (for modules that have it, such as XMVDC, TXS4 and SFPS4), the Time Stamp Offset options in the General tab will be unavailable–grayed out. This is shown in *Figure:General Tab for TXS4 Module with Floating Timestamp*.

Figure:General Tab for Ethernet Module

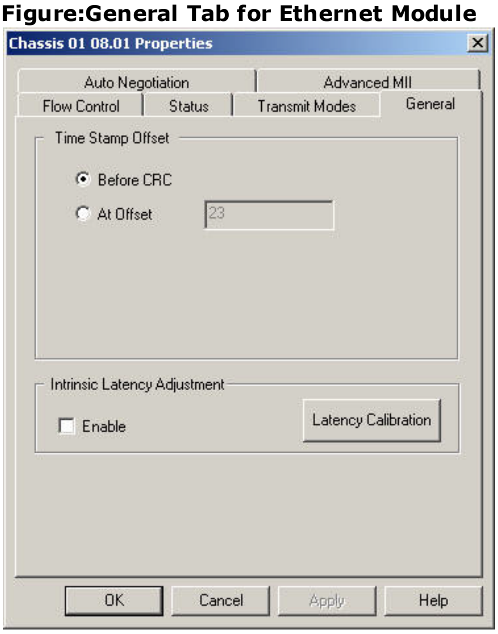


Figure:General Tab for TXS4 Module with Floating Timestamp

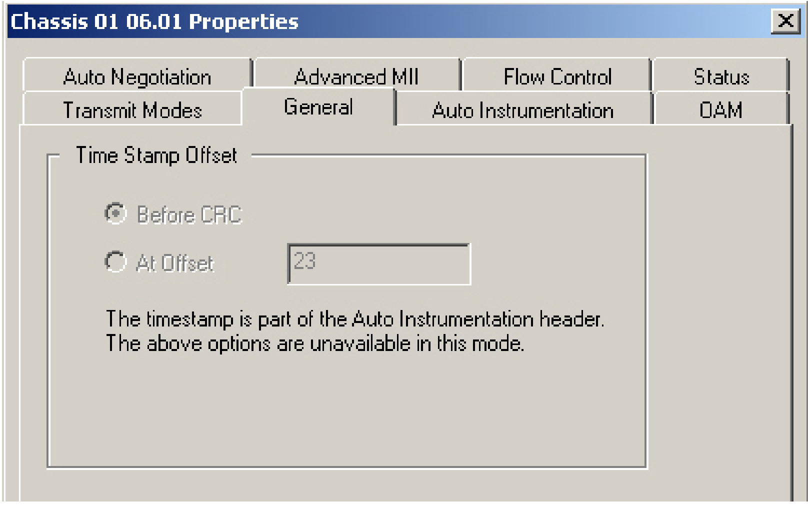
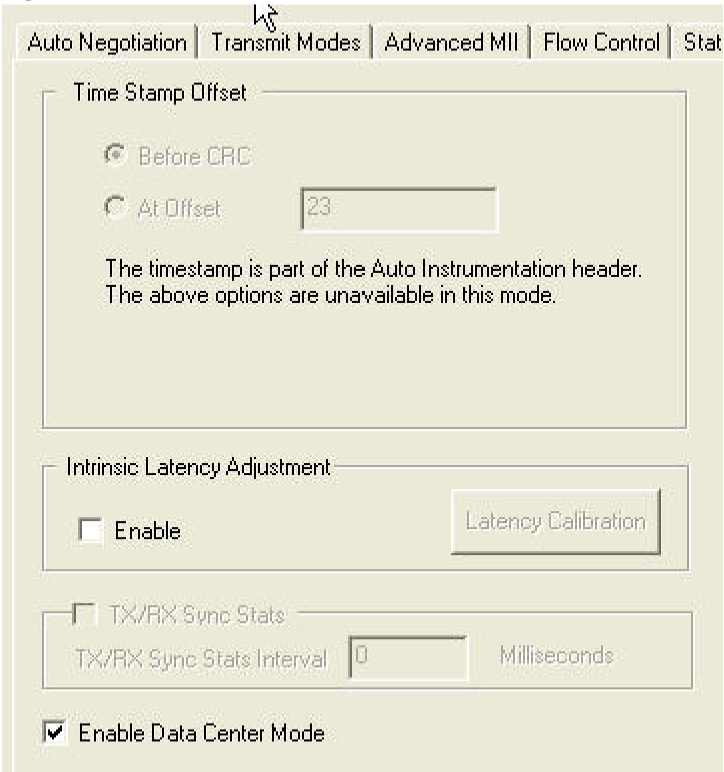


Figure:General Tab for XMVDC Module with Data Center Mode



The text in above reads: ‘The timestamp is part of the Auto Instrumentation header. The above options are unavailable in this mode.’

The fields and controls in this tab are described in the following table.

Table:General Tab for Ethernet Modules

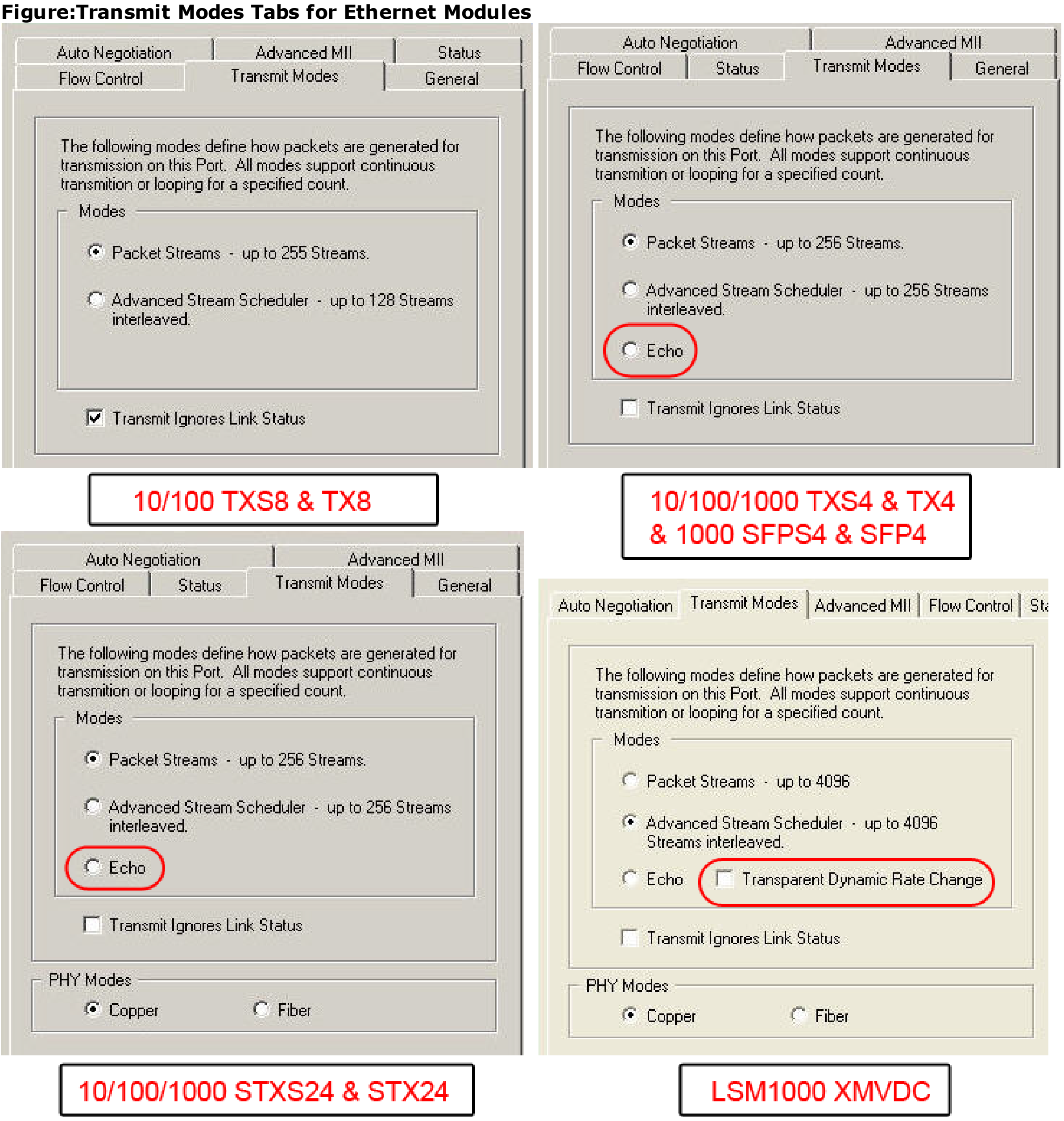
Field/Control	Description
Before CRC	(The default) When this option is selected, the Time Stamp will be inserted into the packet, immediately before the CRC field.
At Offset	When this option is selected, the Time Stamp will be inserted into the packet, starting at the offset (in bytes) from the beginning of

Field/Control	Description
	the packet—as specified in the user-defined field. The offset range is 23 to 12,288. A value outside of this range is automatically set to the nearest valid value (that is, 22 would default to 23, and 12,290 to 12,288). When this option is selected, the following warning appears: WARNING You are changing the default setting of the Time Stamp Offset. This may cause the receiving port to misinterpret the packets. This may also overwrite some of the packet settings.
Intrinsic Latency Adjustment	*Table:10GE LSM XENPAK/XFP General Tab Configuration* for field definitions. For Ethernet modules, this is only available when Auto Negotiate is enabled and capability is set to Gigabit Full Duplex (only).
Enable Data Center Mode	(LSM1000 XMVDC modules) Frame Data for FCoE Support.

Transmit Modes Tab for Ethernet Modules

The *Transmit Modes* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Transmit Modes* tab. The *Transmit Modes* tab for different types of Ethernet modules are shown in the following figure:

Figure:Transmit Modes Tabs for Ethernet Modules



These modules also support the Advanced Stream Scheduler feature, where a number of different streams, depending on the load module, can be interleaved for transmission from one port, to simulate the nature of Internet traffic. The selections available in this tab are described in the following table:

Table:Transmit Modes Tab for Ethernet Modules

Section	Field/Control	Description
Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure up to 255 streams. A stream may be programmed for continuous burst or packet generation— generating a continuous, infinite number of packets.
	Advanced Stream	Up to 128 streams can be interleaved at the

Section	Field/Control	Description
	Scheduler	same time (for 10/100/1000 STXS4 family, up to 256 streams; for XMVDC family, up to 256 streams in Data Center mode, and up to 4096 streams otherwise). Each stream is assigned a percentage of the maximum rate. The streams are mixed in a pseudo-random manner so that each stream's long-term percentage of the total transmitted data is as assigned. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Echo **See the CAUTION below!**	(Not supported on 10/100 TXS8) Sets the basic operating mode for the port to Echo, a Layer 2 Ethernet round-trip mode. (Setting the Echo option in the *Transmit Modes* tab automatically enables the Echo option for the *Receive Mode* tab.) *Echo* for additional information on Echo mode. Also *Echo* for additional information on setting the Transmit Mode to Echo.
Transmit Ignores Link Status		If selected, will allow transmission of packets with the link down.
PHY Modes	Copper	Selected when a copper PHY connector is used (RJ-45).
	Fiber	Selected when a fiber PHY connector is used (SFP transceiver).

CAUTION The following warning message is issued when Echo is selected in the Transmit Modes tab or Receive Mode tab:

'Setting this mode on a live network may cause severe problems. All Ethernet frames with a DA which matches the Receive Filter DA1 will be 'echoed' back onto the network. Setting this mode will IMMEDIATELY start echoing packets. Are you sure you want to set Echo Mode? Yes or No.'

OAM Tab for Ethernet Modules

The *OAM* tab is functionally identical to the one in 10GE load modules.*10GE Port Properties–OAM* for details.

Auto Instrumentation Tab for Ethernet Modules

NOTE
- For NGY modules, see *NGY Port Properties–Auto Instrumentation*
- For FC modules, see *FCM Port Properties—Auto Instrumentation*
- For Flex modules, see *Flex Port Properties—Auto Instrumentation*
- For XDM10G32S module, see *XDM10G32S Port Properties—SFP+*
- For Xcellon-Multis module, see *Xcellon-Multis Port Properties—Auto Instrumentation*

NOTE

- For VM Ports, see *VM Port Properties—Auto Instrumentation*
- For Novus and Novus-R Ports, see *Novus and Novus-R Port Properties—Auto Instrumentation*

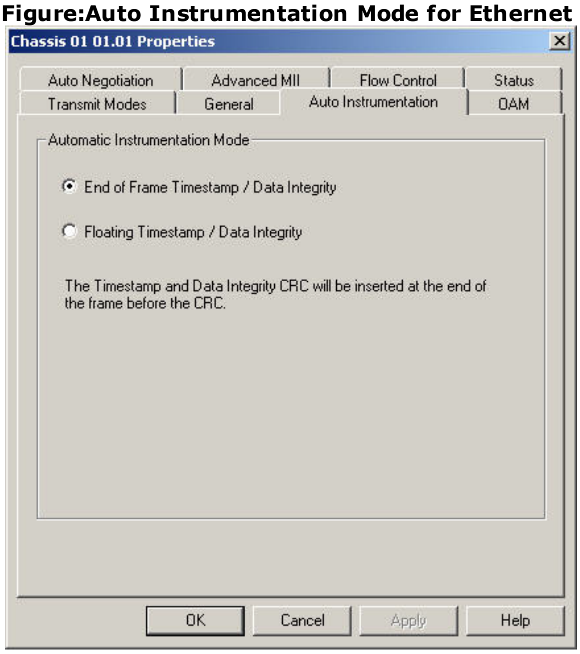
For specified load modules, the timestamp can be inserted into the Auto Instrumentation header instead of the usual locations such as before CRC or at user-specified offset. This is called *Floating Timestamp/Data Integrity*. Timestamp and Data Integrity generation will be stream-based (while the Rx analysis is port-based) if Auto Instrumentation is enabled. The Port Properties Auto Instrumentation tab is shown in the following figure.

The Auto Instrumentation tab is present in the following load modules:

- LM1000STXS4 /24
- LSM1000 XMS12 /XMV16
- ASM1000XMV12X

For MACSec load modules (LSM10GMS-01), *Auto Instrumentation for MACSec Load Modules*.

Figure:Auto Instrumentation Mode for Ethernet Modules, Configuration

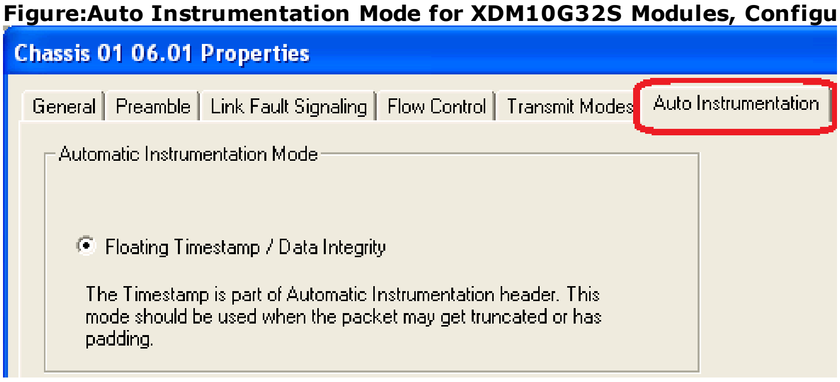


Options on this tab are described in the following table:

Table:Auto Instrumentation Configuration for Ethernet Modules

Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Figure:Auto Instrumentation Mode for XDM10G32S Modules, Configuration



Options on this tab are described in the following table:

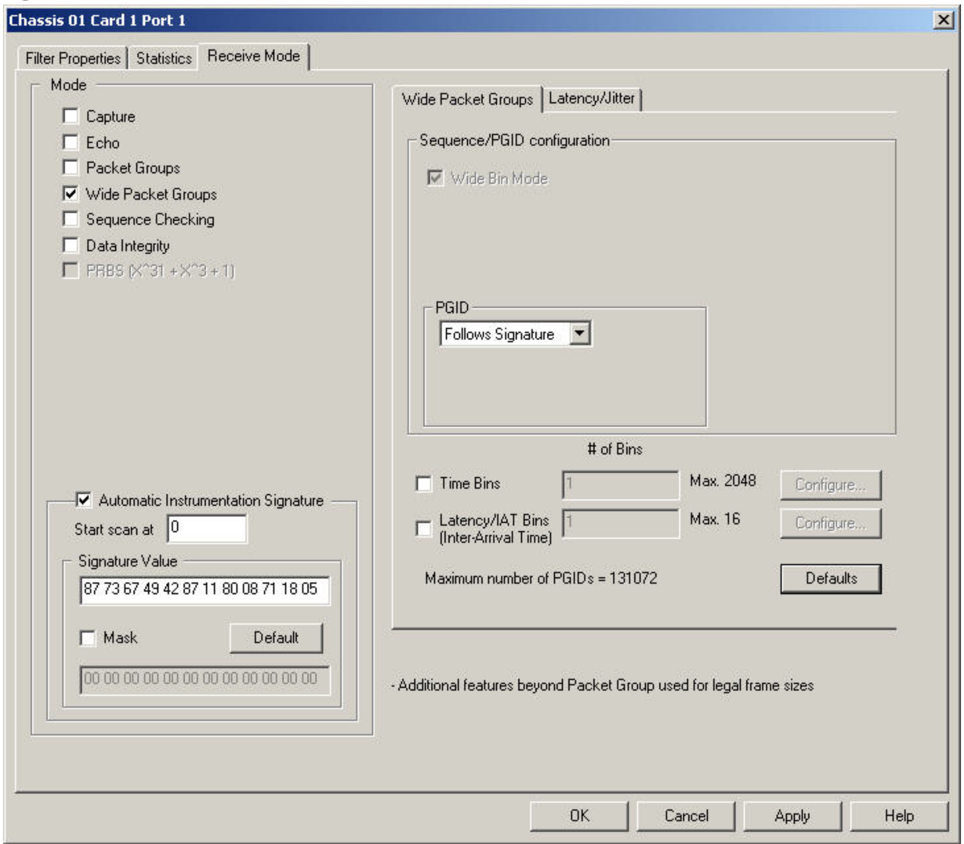
Auto Instrumentation Configuration for XDM10G32S Modules

Field/Control	Description
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

When Floating Timestamp is selected, the Time Stamp Offset options on the *Port PropertiesGeneral* tab are unavailable–grayed out.

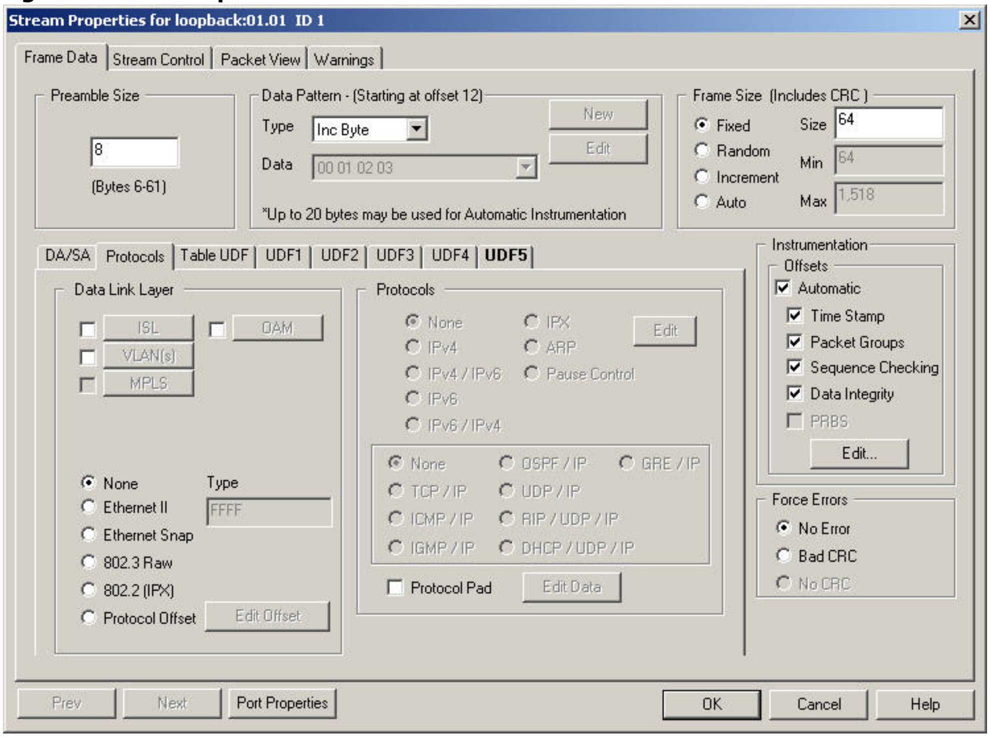
When Floating Timestamp is selected, then in the Receive Mode configuration, PRBS mode is disabled, as shown in the following figure:

Figure:Receive Mode when Auto Instrumentation Mode is Selected



The PRBS option in Packet Streams is also disabled, when Auto Instrumentation mode is selected, as shown in the following figure:

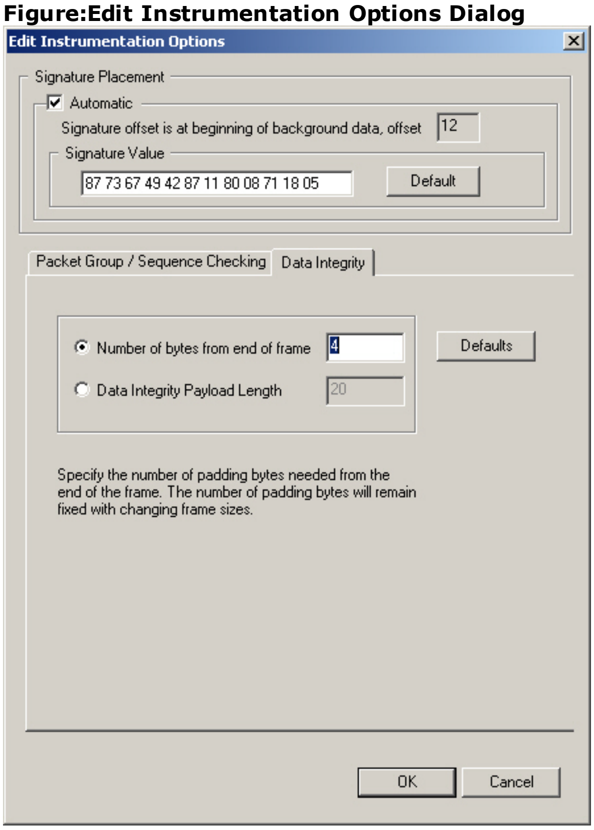
Figure:Stream Properties when Auto Instrumentation Mode is Selected



If Automatic is selected (for Instrumentation), the **Edit** button becomes enabled. When **Edit** is clicked, the **Edit Instrumentation Options** dialog will display, as shown in the following figure:

Edit Instrumentation Options Dialog

Figure:Edit Instrumentation Options Dialog



Data Integrity Tab

In the Edit Instrumentation Options dialog, on the **Data Integrity** tab, enter the 'Number of bytes from end of frame' or specify a 'Data Integrity Payload Length'. The options on this page are described in the following table:

Table:Edit Instrumentation Options

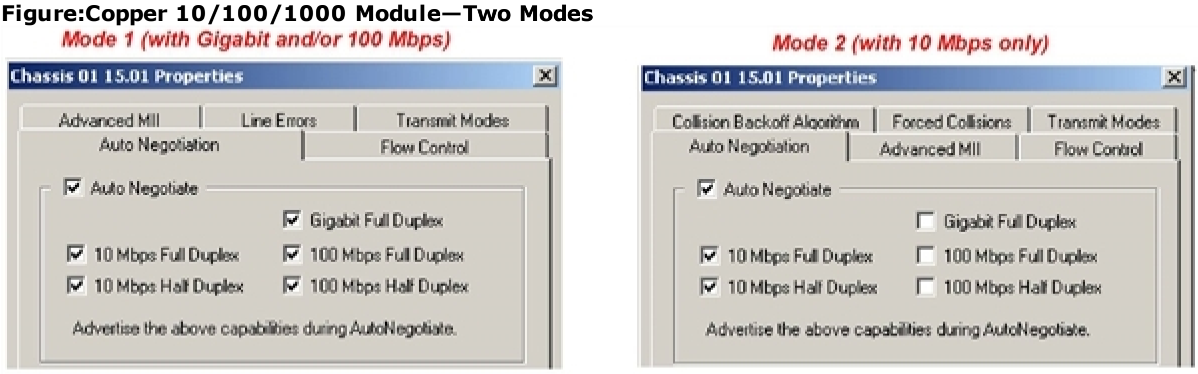
Field/Control	Description
Number of bytes from end of frame	Specify the number of padding bytes needed from the end of the frame. The number of padding bytes will remain fixed with changing frame sizes. Can be any non-negative value, depending on the packet size. (*default = 2 or 4*)
Data Integrity Payload Length	Specify the fixed data integrity payload length. This length will not change with changing frame sizes. (*default = 20*)
Defaults (button)	Resets the two fields (above) to the default values.

Port Properties for Copper 10/100/1000 Modules

The complete specification for the Copper 10/100/1000 modules can be found in the *Ixia Platform Reference Manual*.

There are two sets of configuration tabs—corresponding to the different auto-negotiate modes for the Copper 10/100/1000 module, as shown in the following figure:

Figure:Copper 10/100/1000 Module—Two Modes



The complete list of tabs that make up the sets for the two modes are listed below.

Mode 1: With Gigabit and/or 100 Mbps operation

- *Auto Negotiation for Copper 10/100/1000 Modules*
- *Advanced MII for Copper 10/100/100 Modules*(*MII Register Files* for additional information on MII registers.)
- *Flow Control for Gigabit Modules*
- *Line Errors for Gigabit Modules*
- *Transmit Modes for Gigabit Modules*

Mode 2: With 10 Mbps operation only

- *Auto Negotiation Tab*
- *Advanced MII for Copper 10/100/100 Modules* (*MII Register Files* for additional information on MII registers.)
- *Flow Control Tab*

- *Collision Backoff Algorithm Tab*
- *Forced Collisions Tab*
- *Transmit Modes for 10/100 Modules*

The *Port Properties* dialog is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

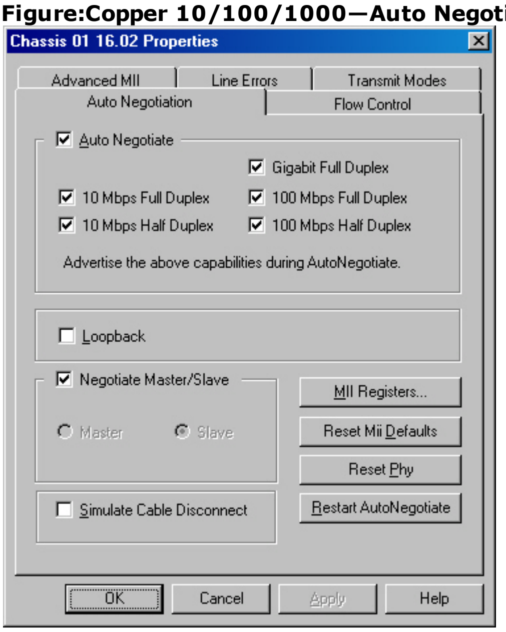
Auto Negotiation for Copper 10/100/1000 Modules

The *Auto Negotiation* tab offers access to the Auto Negotiation and Loopback properties. Auto negotiation controls how the port establishes communications with other ports.

The *Auto Negotiation* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Auto Negotiation* tab. When the module is set to operate at 100 and/or gigabit (Mode 1 in the figure above), the tab appears as shown in the following figure:

NOTE If only 10 Mbps operation has been selected for this port, the Auto Negotiation tab will be the same one used for 10/100 modules. *Auto Negotiation Tab* for additional information.

Figure:Copper 10/100/1000—Auto Negotiation



The fields and controls in this tab are described in the following table:.

Table:Copper 10/100/1000—Auto Negotiation

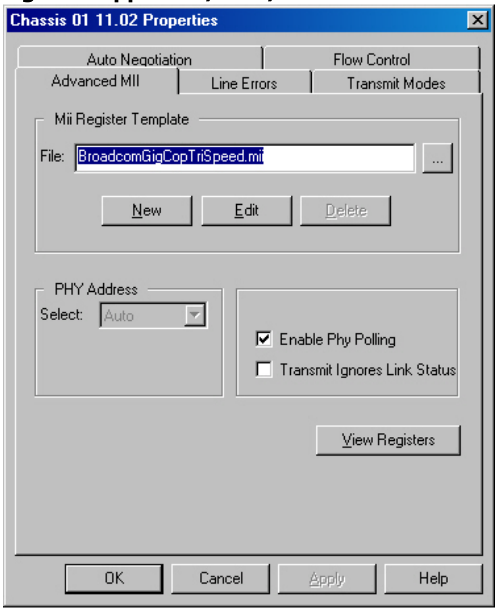
Field/Control	Description
Auto Negotiate	If selected, allows auto negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during Auto Negotiation.
Gigabit Full Duplex	If selected, auto negotiate will advertise Gigabit (1000 Mbps) full duplex operation.
10 Mbps Full Duplex	If selected, auto negotiate will advertise 10 Mbps full duplex operation.
10 Mbps Half Duplex	If selected, auto negotiate will advertise 10 Mbps half duplex

Field/Control	Description
	operation.
100 Mbps Full Duplex	If selected, auto negotiate will advertise 100 Mbps full duplex operation.
100 Mbps Half Duplex	If selected, auto negotiate will advertise 100 Mbps half duplex operation.
Loopback	If selected, the port is set to internally loopback from transmit to receive.
Negotiate Master/Slave	If selected, determining which port is Master or Slave is performed **automatically**. (Checking this box will disable the manual option for selecting Master or Slave).
Master	If selected, port will be configured as Master.
Slave	If selected, port will be configured as Slave.
Simulate Cable Disconnect	If selected, the port will act as if the cable has been disconnected.
MII Registers...	Allows the current MII register values to be read and written. See *MII Register Files* for additional information on MII Registers.
Reset MII Defaults	Resets all of the port's MII properties back to the default settings.
Reset Phy	When pushed, resets the PHY associated with the port through the MII control register.
Restart Auto Negotiate	When pushed, the Auto Negotiate sequence is restarted.

Advanced MII for Copper 10/100/100 Modules

The *Advanced MII* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Advanced MII* tab. The *Advanced MII* tab allows for the proper association of MII registers to the port, as shown in the following figure:

Figure:Copper 10/100/1000 Modules—Advanced MII Tab



The upper box, labeled *MII Register Template*, is used to control the selection and editing of a register template file. Register template files hold the register definitions. The fields and controls in this box are described in the following table:.

Table:Copper 10/100/1000 Modules—Advanced MII Tab

Field/Control	Description
File	The name of the MII Register file.
Browse	Opens up a standard Windows file browsing window in the directory *C:\Program Files\Ixia\MII*, looking for files that end in *.mii*.
New	Allows the creation of a new MII Register Template file. See *New/Edit MII Register Template Setup—Management Page* for operational details.
Edit	Allows the editing of the indicated file. See *New/Edit MII Register Template Setup—Management Page* for operational details.
Delete	Deletes the current file after a confirmation dialog.

The lower part of the tab allows the PHY address to be set. The controls available in this part of the tab are described in the following figure:

Table:Copper 10/100/1000—PHY Address Controls

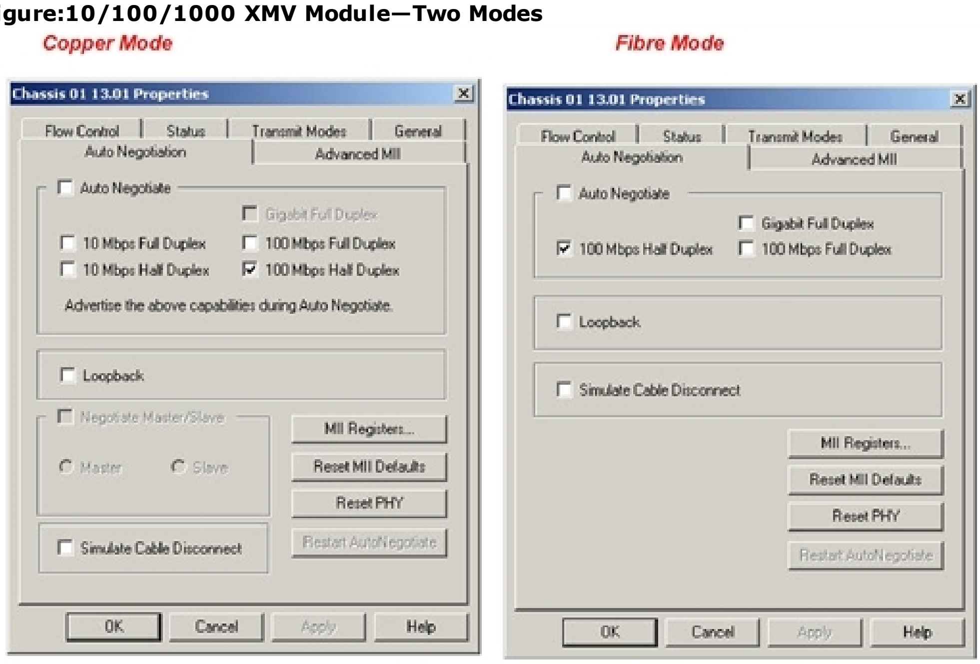
Control	Description
PHY Address	Allows the address of the PHY to be set to Auto or a constant from 0 to 31. (It is set to Auto by default, and manual configuration is disabled.)
Enable Phy Polling	If selected, then the PHY is continuously polled during MII setup operation.
Transmit Ignores Link Status	If selected, will allow transmission of packets with the link down.

Port Properties for 10/100/1000 XMV Modules

The complete specification for the 10/100/1000 XMV modules can be found in the *Ixia Platform Reference Manual*.

There are two sets of Auto Negotiation options—corresponding to the different transmit modes (copper or fibre) for the 10/100/1000 XMV module, as shown in the following figure:

Figure:10/100/1000 XMV Module—Two Modes



In fibre mode, speeds 100 Mbps full duplex and 100 Mbps half duplex are available in addition to gigabit full duplex. In copper mode, 10 Mbps full and half duplex and 100 Mbps full and half duplex are available.

The port properties tabs and options for the 10/100/1000 XMV load modules are also common to other modules.

- For descriptions of the tabs and options of both sets of *Auto Negotiation* options, see in the following table.
- *Advanced MII for Copper 10/100/100 Modules (MII Register Files for additional information on MII registers.)*
- The *Flow Control* tab is the same as the *Flow Control Tab for Ethernet Modules.*
- The *Status* tab is the same as the *Status Tab for Ethernet Modules*
- The *Transmit Modes* is the same as that described in *Transmit Modes Tab in Stream/Capture/Latency Mode*.
- On the *General* tab, *Time Stamp Offset*, *General Tab for Ethernet Modules*.
- Also on the *General* tab, *Intrinsic Latency Adjustment*, *Table:10GE LSM XENPAK/XFP General Tab Configuration for field definitions*.

Port Properties for Gigabit and GBIC Modules

The complete specification for the Gigabit type boards can be found in the *Ixia Platform Reference Manual*.

The dialog tabs indicate the types of properties that may be modified for Gigabit modules. They include the property tabs listed below.

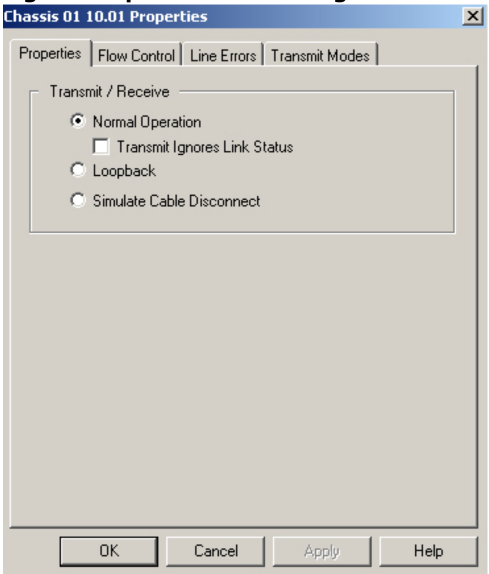
- *Properties for Gigabit Modules*
- *Flow Control for Gigabit Modules*
- *Line Errors for Gigabit Modules*
- *Transmit Modes for Gigabit Modules*

The *Port Properties* dialog is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

Properties for Gigabit Modules

The *Properties* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Properties* tab. The general *Properties* tab common to Gigabit and GBIC modules is shown in the following figure:

Figure:Properties Tab for Gigabit and GBIC Modules



The fields and controls available in this tab are described in the following table:

Table:Properties Tab for Gigabit Modules

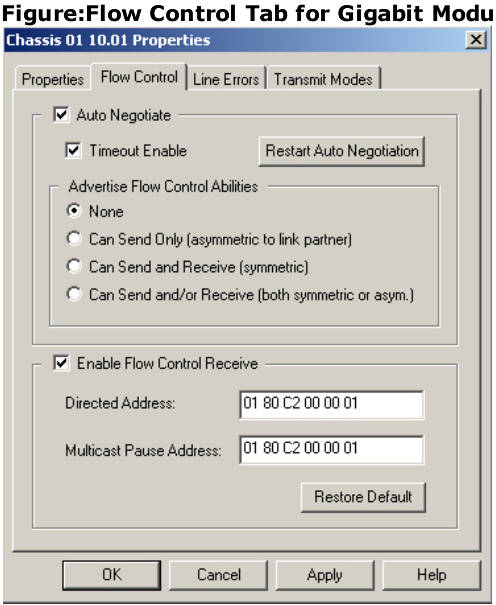
Field/Control	Description
Normal Operation	The port operates normally, as opposed to loopback mode or simulate cable disconnect mode.
Transmit Ignores Link Status	When operating in normal mode, the transmit operation will operate regardless of the link state.
Loopback	The port operates in loopback mode, as opposed to normal or simulate cable disconnect mode.
Simulate Cable Disconnect	The port operates in simulate cable disconnect mode, as opposed to normal or loopback mode.

Flow Control for Gigabit Modules

NOTE For information on Flow Control for 10/100 TXS8, 10/100/1000 TXS4, and 1000 SFPS4 modules, refer to *Flow Control Tab for Ethernet Modules*.

The *Flow Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The *Flow Control* tab for gigabit operation is shown in the following figure. It includes options for setting auto negotiation properties, as well as for flow control.

Figure:Flow Control Tab for Gigabit Modules



The fields and controls in this tab are described in the following table.

Table:Flow Control Tab for Gigabit Operation

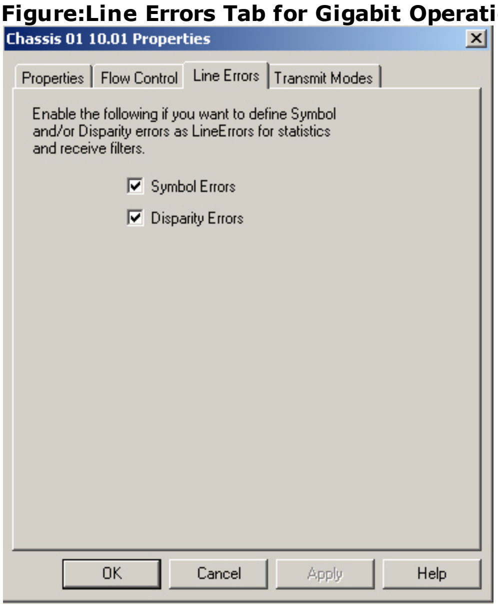
Section	Field/Control	Description
Auto Negotiate		Enables auto-negotiation of flow control capabilities for the port.
	Timeout Enable	Enables timeout during auto-negotiation.
	Restart AutoNegotiation	If this button is clicked, it causes the auto-negotiation process to start immediately.
Advertise Flow Control Abilities	None	This and the next three options indicate which set of flow control capabilities are advertised to other ports. This option advertises no capabilities.
	Can Send Only (asymmetric to link partner)	This option advertises only send capabilities.
	Can Send and Receive (symmetric)	This option advertises both send and receive capabilities.
	Can Send and/or Receive (both symmetric or asymmetric)	This option advertises all send and receive capabilities in any combination.

Section	Field/Control	Description
Force Flow Control Receive		Enables receive side flow control handling for the port.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	This is the MAC address that the port will listen on for a multicast pause message.
	Restore Default	Restores the default MAC address: 01 80 C2 00 00 01 in both *Directed* and *Multicast Pause Address* fields.

Line Errors for Gigabit Modules

The *Line Errors* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Line Errors* tab. The *Line Errors* tab for gigabit operation is shown in the following figure:

Figure:Line Errors Tab for Gigabit Operation



The two check boxes control how symbol and disparity errors are considered with respect to capture and statistics operation. If a check box is selected, then that type of error will be included with Line Errors. The Line Errors category is one of the statistics for Gigabit ports and may be used in the definition of any of the User Defined Statistics, as well as Capture triggers and filters.

Transmit Modes for Gigabit Modules

The *Transmit Modes* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Transmit Modes* tab. The *Transmit Modes* tab for Gigabit modules, including GBIC and Copper 10/100/1000 modules running at gigabit speed, is shown in the following figure. (There is no *Transmit Modes* tab for Gigabit-3 modules.)

Figure:Transmit Modes for ASM XMV12x

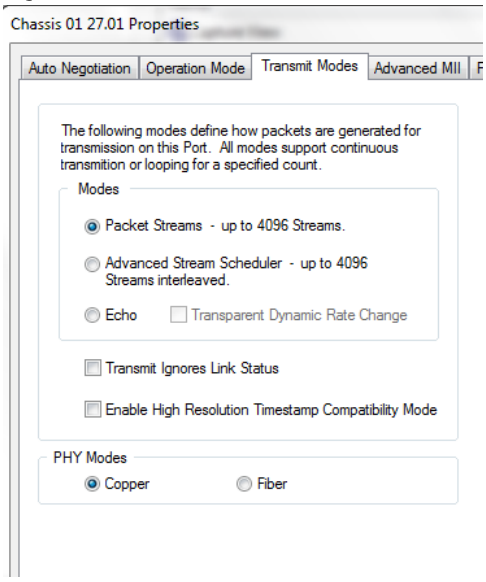


Figure:Transmit Modes for LSM XMVD16

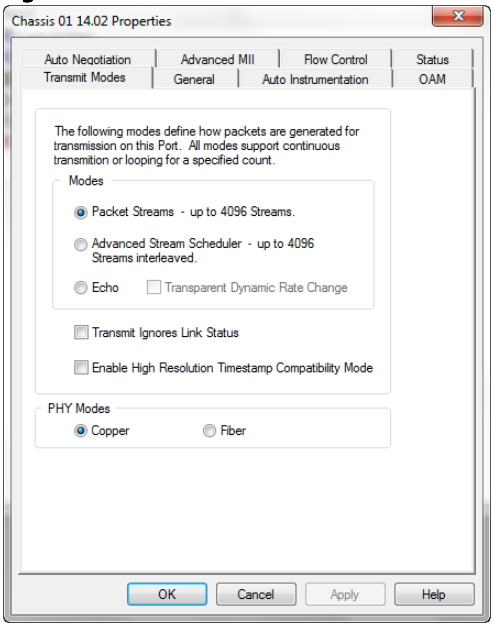


Figure:Transmit Modes for LSM XMVDC12

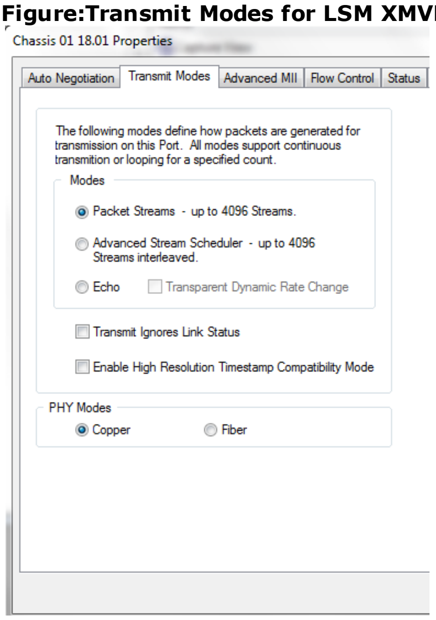
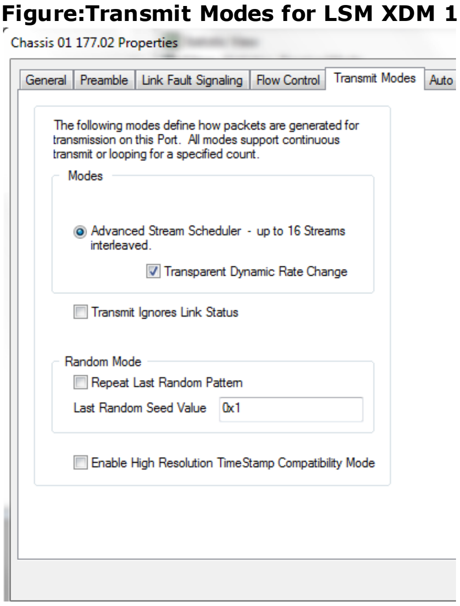


Figure:Transmit Modes for LSM XDM 10GMSM



The controls in this tab are described in the following table.

Table:Transmit Modes Tab for Gigabit Modules

Field/Control	Description
Packet Streams	Sets the basic operating mode for the port to packet streams. This allows to configure up to 255 streams. A stream may be programmed for continuous burst or packet generation—generating a continuous, infinite number of packets.
Advanced Stream Scheduler	Up to 4096 streams can be interleaved at the same time for LSM XMV16 and LSM XMVDC12, and up to 16 streams for XDM 10GMSM. Each stream is assigned a percentage of the maximum rate. The streams are mixed in a pseudo-random manner so that each stream's long-term percentage of the total transmitted data is as assigned. Refer to *Stream Control for Advanced*

Field/Control	Description
	Streams for additional information on Advanced Streams.
Echo **See the CAUTION below!**	Sets the basic operating mode for the port to Echo, a Layer 2 Ethernet round-trip mode. (Setting the Echo option in the *Transmit Modes* tab automatically enables the Echo option for the *Receive Mode* tab.) Also Echo for additional information on Echo mode. Also Echo for additional information on setting the Transmit Mode to Echo.
Transparent Dynamic Rate Change	If selected, the dynamic rate control will allow rate change across counters, for this port.
Transmit Ignores Link Status	If selected, will allow transmission of packets with the link down.
Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the Ixia Platform Reference Guide.
Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Enable High Resolution Timestamp Compatibility Mode	Select the check box to allow the traffic to be sent and received by next gen load modules supporting high resolution timestamp without DI error. This feature is valid only in LAN and WAN mode with Packet stream and concurrent scheduler. This feature is not available in other modes like TSO/LRO, IxN2X or Offload mode.
PHY Modes - Copper	Selected when a copper PHY connector is used (RJ-45).
PHY Modes - Fiber	Selected when a fiber PHY connector is used (SFP transceiver).

CAUTION The following warning message is issued when Echo is selected in the Transmit Modes or Receive Mode tabs:

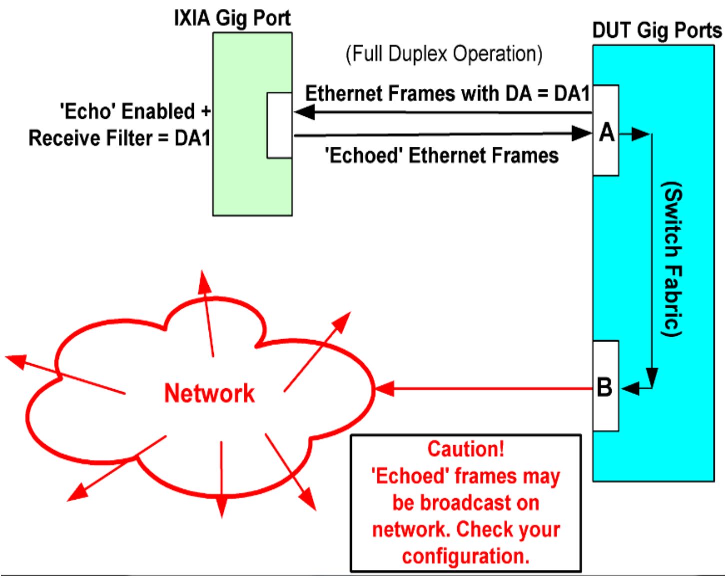
'Setting this mode on a live network may cause severe problems. All ethernet frames with a DA which matches the Receive Filter DA1 will be 'echoed' back onto the network. Setting this mode will IMMEDIATELY start echoing packets. Are you sure you want to set Echo Mode? Yes or No.'

Echo

The gigabit TXS modules (10/100/1000 TXS4 and TX4, 1000 SFPS4 and SFP4, and 10/100/1000 STXS24 and STX24), Gigabit, GBIC, and Copper 10/100/1000 (running in

Gigabit mode) load modules offer an additional feature–Layer 2 Echo. This feature operates in conjunction with gigabit rates in full duplex mode, for testing Ethernet loopback mode at up to wire speed. A diagram of the Echo features is shown in the following figure:

Figure:Gig Echo Diagram



The transmitting side (the DUT) sends one or more streams of simple Ethernet frames. Currently, the DA and DA Mask in the Stream Properties/Frame Data page is used for the Gig Echo transmit.The minimum valid length of an incoming frame is 16 bytes, which includes the MAC DA (with DA mask), MAC SA, and CRC. A preamble of at least 8 bytes must precede the incoming Ethernet frame. The minimum length of a valid incoming frame is 16 bytes (for DA + SA + CRC).

In Echo mode, when the frames are received, the MAC DA and MAC SA will be swapped, a standard 8-byte preamble will be inserted for each echoed frame (no matter how long the preamble is on the received frame), and the CRC will be recalculated before the frame is echoed back. If an incoming frame has a bad CRC, the frame will be retransmitted with a bad CRC. For Gigabit, GBIC, and Copper 10/100/1000 (running Gigabit mode), Layer 3 Capture options will not be included, but all other capture and statistics options will be available. (These capture and statistics options are not currently available for the 10/100/1000 TXS4 and 1000 SFPS4 modules.) The transmitted frames will support only the gigabit statistics. The Echo feature supports VLAN-encapsulated Ethernet or SNAP Ethernet frames.

To control the amount of traffic echoed back onto the network, the receiving port will echo ONLY received frames which matched a specified DA1 (Destination Address) set as a receive filter. *DA/SA Values* for additional information.

Echo for additional information on setting the Receive Mode to Echo.

Port Properties for Power over Ethernet (PoE)

The Power Over Ethernet (PoE) load module (PLM1000T4-PD) is a special purpose, 4-channel electronic load. It is intended to be used in conjunction with Ixia ethernet traffic generator/analyzer load modules to test devices that conform to IEEE std 802.3af.

There are two versions of the PoE load module: 20 Watt dissipation and 30 Watt dissipation. The two versions have slightly different controls, noted below.

For an overview of PoE, refer to the Power over Ethernet section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The following sections explain the use of the PoE controls:

- *PoE Basic Setup*
- *PoE Advanced Signatures*
- *PoE Advanced Load Control*
- *PoE Voltage Threshold*
- *PoE Acquisition*

The *Port Properties* dialog is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option.

PoE Basic Setup

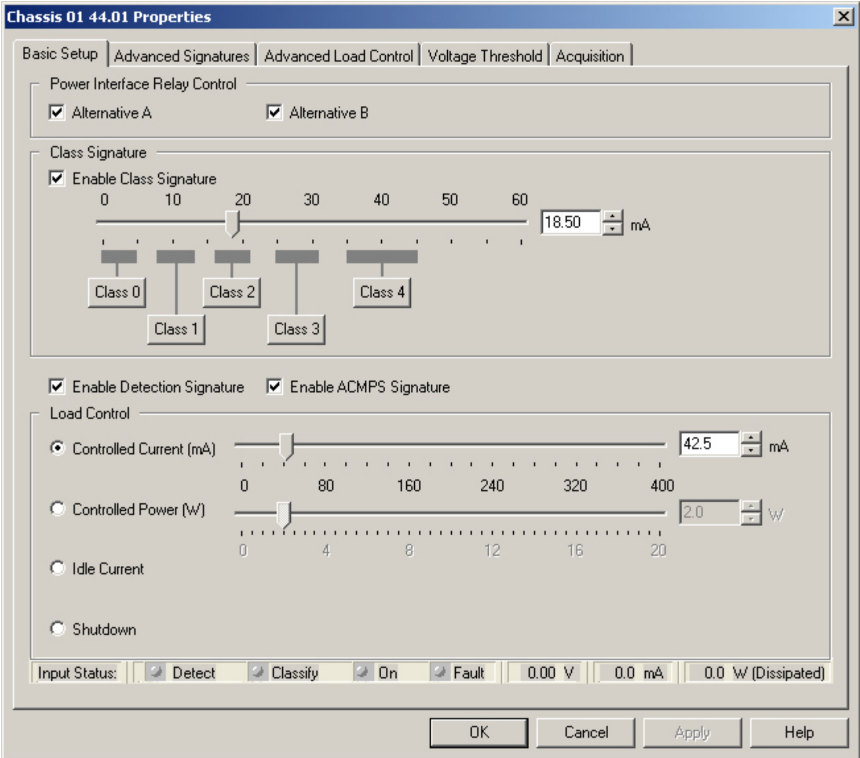
The *Basic Setup* tab allows to set the following:

- What load type will be used in the emulated Powered Device (PD) (Alternative A and/or Alternative B).
- Allows to quickly set the signatures.
- Emulate PD power requirements based on a selected class.

The selected class in this tab will determine the emulated PD characteristics when viewed by a Power Sourcing Equipment (PSE).

The *Basic Setup* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Basic Setup* tab. The *Basic Setup* tab is shown in the following figure:

Figure:Basic Setup Tab (20W PoE Load Module)



The controls shown in this tab are explained in the following table:

Table:Input Relays Controls

Section	Field/Control	Usage
Power Interface Relay Control		Allows the selection of the load method of the physical interface (Alternative A or Alternative B). Note that mid span PSEs only supply Alternative B power.
Class Signature		Sets the emulated class. (This function is also available in *PoE Advanced Signatures*.)
	Enable Class Signature	This check box enables the class signature, and allows for the detection of power requirements by class. Selecting this check box also enables the remainder of the group box.
	Slide Bar	The slide bar can be used to set the power requirements for the emulated PD. The signal value can also be set with the number field to the far right.
	Class buttons	Selecting one of these buttons sets the Current Class value to the default signaling current associated with the selected class.
Enable Detection Signature		Selecting this check box enables the nominal detection signature for the selected class. If not enabled, the emulated PD will not have a detection signature.
Enable AC MPS Signature		Selecting this check box provides an Alternating

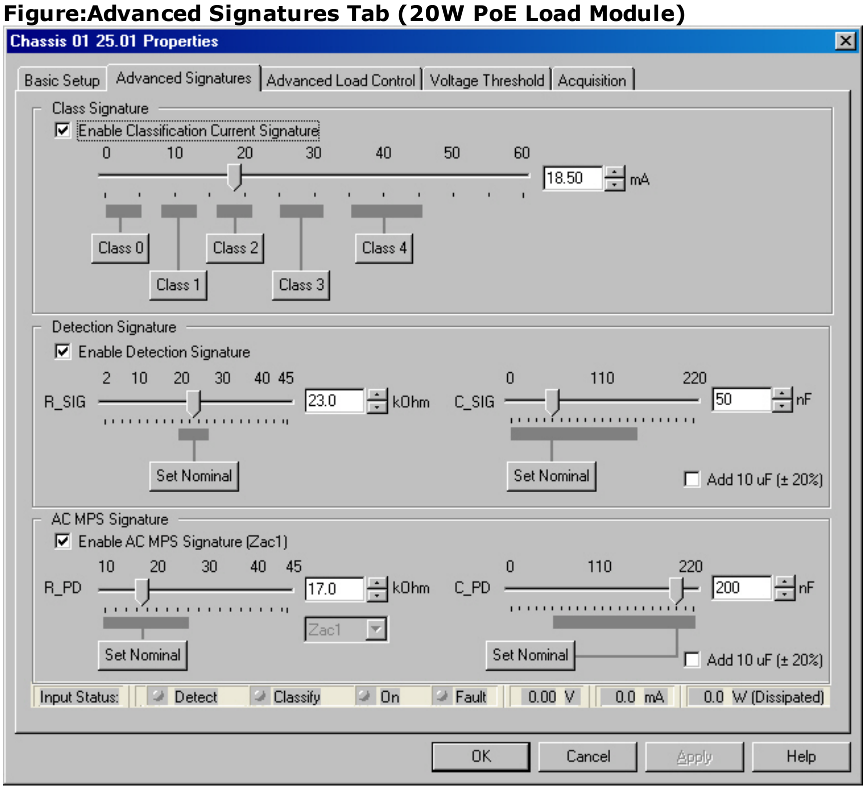
Section	Field/Control	Usage
		Current Maintain Power Signature for the selected class. If not enabled the emulated PD will not have an AC MPS.
Load Control		Allows to set the emulated PD's load operation mode. (This function is also available in *PoE Advanced Load Control*.)
	Controlled Current	Sets the emulated PD to require constant current. This slide bar sets the current requirements for the emulated PD in mAmps. The current setting can also be set by entering a number in the number field. For 20W card the max is 400 mA. For 30W card, the max is 600 mA.
	Controlled Power	Sets the PD to require constant power. This slide bar sets the power requirements for the emulated PD in watts. The power setting can also be set by entering a number in the number field.
	Standby	Sets the PD to standby mode, requiring only 10 mA of current.
	Shutdown	Sets the PD to shutdown mode.
Input Status		The bar at the bottom of the tab displays the current status of the attached PSE device. This information is visible on all PoE dialogs and tab pages.
	Detect	When green, shows the PSE is in the detection phase.
	Classify	When green, shows the PSE is in the classification phase.
	On	When green, shows that the PSE is supplying power to the PD.
	Fault	When red, indicates that the PSE has performed an illegal operation. The PoE disconnects under a fault condition until the PSE resets.
	Input Voltage	The voltage being sent from the connected PSE device, exclicked in volts.
	Input Current	The amperage being sent from the connected PSE device, exclicked in mAmps
	Power (Dissipated)	The power provided from the PSE device, in Watts.

PoE Advanced Signatures

The *Advanced Signatures* tab page allows for the selection and manipulation of the PD signatures. Signatures are used by the PSE to determine what the power requirements are for the PD.

The *Advanced Signatures* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Advanced Signature* tab. Following figure shows the *Advanced Signatures* tab page.

Figure:Advanced Signatures Tab (20W PoE Load Module)



The controls on the *Advanced Signatures* tab page are explained in the following table:

Table:Advanced Signatures Configuration

Section	Field/Control	Usage
Class Signature		Allows to set the emulated PD class signature.
	Enable Classification Current Signature	This check box enables the class signature, and allows for the detection of the class and power requirements. Selecting this check box also enables the load slide bar and class buttons.
	Slide Bar	The slide bar can be used to signal the power requirements for the emulated PD. The value can be manipulated using the slide bar or the number field to the far right.
	Class Buttons	Selecting one of these buttons sets the *Current Class* value to the default signaling current of the selected class.
Detection Signature		Allows to manipulate the PD detection signatures. Detection signatures signal the PSE that a PD is on line and waiting to be powered.
	Enable Detection Signature	Enables the detection signatures for this port, and the R_SIG and C_SIG slide bars.
	R_SIG KOhm	The resistance signature, in kilo Ohms. This set-

Section	Field/Control	Usage
		ting is manipulated using the slide bar or the number field to the right of the bar.
	C_SIG nF	The capacitance signature, in nano Farads. This setting is manipulated using the slide bar or the number field to right of the bar.
	Set Nominal	Pressing this button sets the detection signatures to their nominal levels. The nominal levels are shown by the black bar.
	Add 10uF	Selecting this check box adds a 10 micro Farads capacitance to the detection signature.
AC MPS Signature		Allows to manipulate the Alternating Current Maintain Power Signature.
	Enable AC MPS Signature	Enables the AC MPS signature and slide bar operation.
	R_PD KOhm	Sets the resistance for the emulated PD AC MPS signature, in kilo Ohms. This setting is manipulated using the slide bar or the number field to the far right of the bar. The range of this slide bar is dependent on the Zac setting: Zac1–10 to 45 KOhms Zac2–200 to 1200 KOhms (only on 30W PoE load modules
	C_PD nF	Sets the capacitance requirements for the emulated PD AC MPS signature, in nano Farads. This setting is manipulated using the slide bar or the number field to the far right of the bar.
	Set Nominal	Pressing this button sets the AC MPS resistance and current requirements settings to their nominal values based on the selected class.
	Zac1/Zac2 Toggle	This pull-down menu allows to select either Zac1 or Zac2 AC MPS signature. It also changes the R_PD slide bar range, noted above. Zac 1/2 is the impedance signature sent by the PD informing the PSE to maintain power (*Z* is common notation for impedance, and *AC* is alternating current). Zac1 is the impedance range for maintaining power, while Zac2 is the range for removing power. Zac2 is only available on 30W PoE load modules. In 20W PoE load modules, this control is always set to Zac1.
	Add 10uF	Selecting this check box adds a 10 micro Farads requirement to the AC MPS signature.

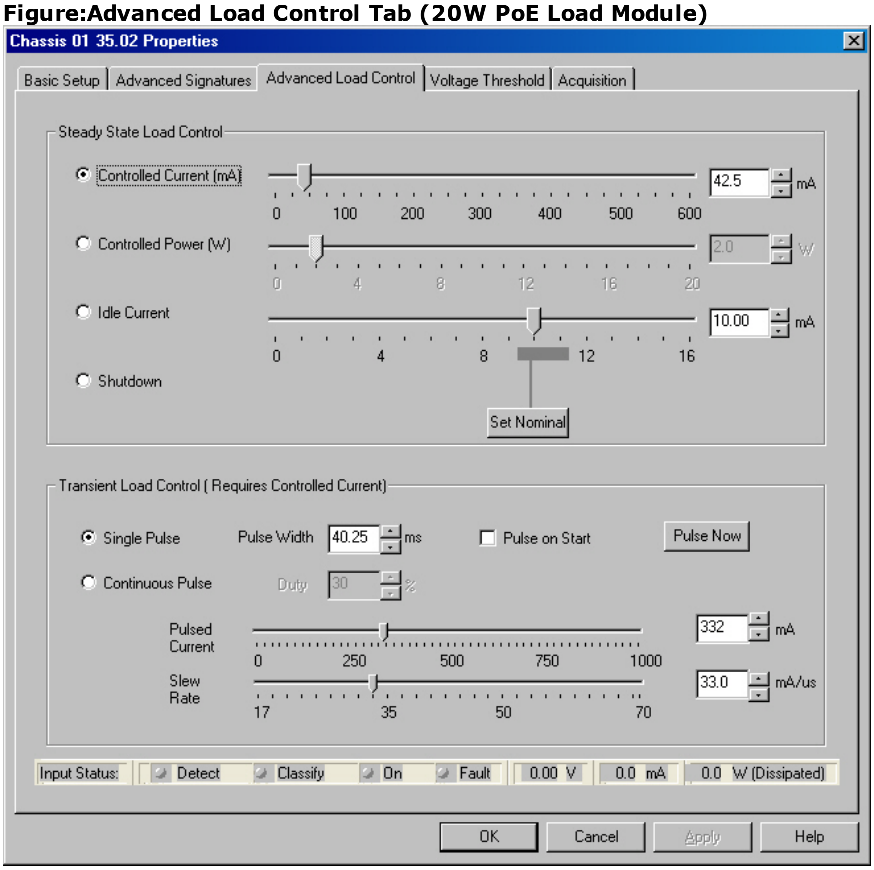
The Status settings are described in *Table:Input Relays Controls*.

PoE Advanced Load Control

Once the PSE has detected and classified the emulated PD, it should provide power to the port. The *Advanced Load Control* tab page allows to control the emulated PDs power requirements. It also allows for the insertion of power 'pulses,' which change the PD load from short periods of time.

The *Advanced Load Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Advanced Load Control* tab. The *Advanced Load Control* tab page is shown in the following figure:

Figure:Advanced Load Control Tab (20W PoE Load Module)



The controls on the *Advanced Load Control* tab are explained in the following table:

Table:Advanced Load Control Configuration

Section	Field/Control	Usage
Steady State Load Control		Selects the type of PD load requirements the port emulates.
	Controlled Current	Sets the emulated PD to require constant current. This slide bar sets the current requirements for the emulated PD, in milli Amps. The current setting can also be manipulated by entering a number in the number field.
	Controlled Power	Sets the PD to require constant power. This slide bar sets the power requirements for the emulated PD, in Watts. The power setting can

Section	Field/Control	Usage
		also be manipulated by entering a number in the number field. There are two ranges for this control, depending on which version of the load module being used: • 20W version–0 to 20 Watts • 30W version–0 to 30 Watts
	Standby	Sets the PD to standby mode, requiring only 10 mA of current.
	Shutdown	Sets the PD to shutdown mode.
Transient Load Parameters		Allows for the creation of Load variations from the PSE in the form of a pulse, or a repeating pulse.
	Single Pulse	Selecting this option button sets up a single pulse that conforms to the values indicated by the slide bars. The pulse is initiated when the *Pulse Now* button is selected.
	Pulse Width	Sets how long the new pulse current level lasts, in microseconds.
	Pulse on Start	Selecting this check box begins a single pulse each time the PSE starts to supply power.
	Pulse Now	Selecting this button begins the requested pulse. This button is only active after the pulse parameters have been set, and the *Apply* button selected.
	Continuos Pulse	Selecting this option button repeats the configured pulse indefinitely.
	Duty	Sets the percentage of time that the pulse current is maintained through the steady state current. For example, a setting of 30 percent means that for thirty percent of the load time, the pulse current is maintained.
	Pulse Current	Sets the pulse level, which can be less or greater than the standard current requirement of the PD (in milli Amps), and can be set through the slider or number field to the right of the slide bar.
	Slew Rate	Sets how quickly the pulse level is achieved, in milli Amps per microsecond, and can be set through the slider or number field to the right of the slide bar.

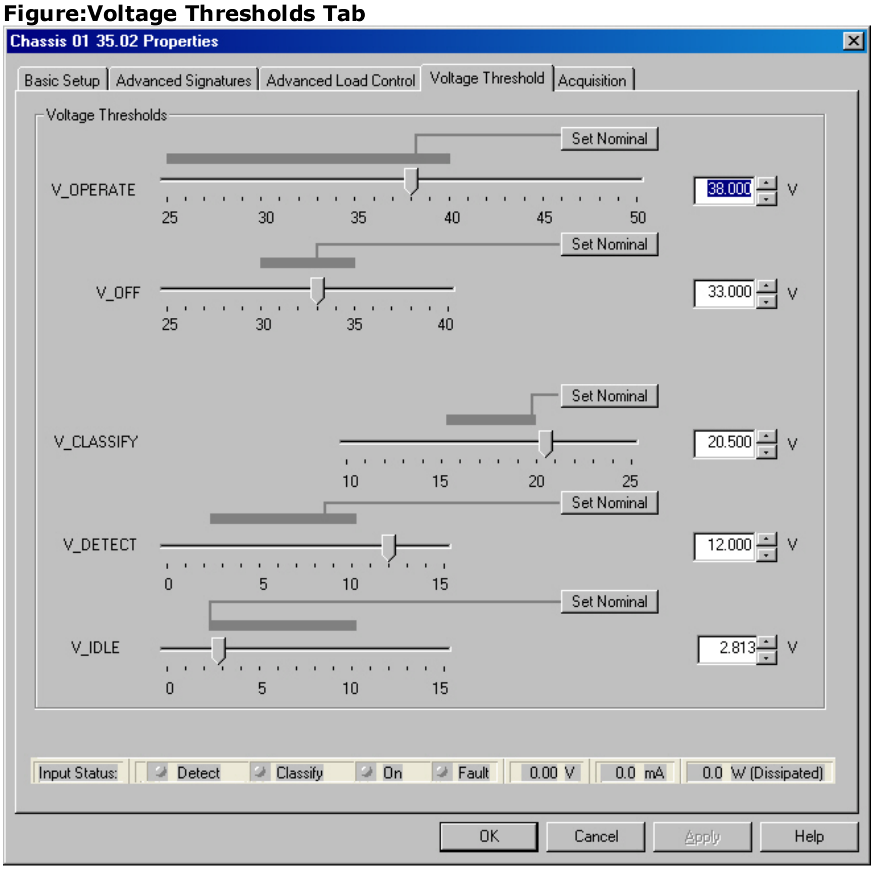
The status settings are described in *Table:Input Relays Controls*.

PoE Voltage Threshold

The voltage threshold settings allow to control the voltage necessary from the PSE for it to detect, classify, and provide power to the emulated PD. As the PSE discovers the emulated PD, the voltage increases to advance the PSE to the next phase.

The *Voltage Threshold* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Voltage Threshold* tab. The *Voltage Thresholds* tab page is shown in the following figure:

Figure:Voltage Thresholds Tab



The controls in this tab page are explained in the following table:

Table:Voltage Threshold Configuration

Field/Control	Usage
V_OPERATE	Sets the input threshold where the PSE load is first applied. The voltage number can be changed using the slide bar or the number field to the right.
V_OFF	Sets the input threshold below which the PSE load is removed. The voltage number can be changed using the slide bar or the number field to the right.
V_CLASSIFY	Sets the maximum voltage for the emulated PD classification stage. Between this setting and V_DETECT, the classification currents are presented to the PSE by the PD. The voltage number can be changed using the slide bar or the number field to the right.

Field/Control	Usage
V_DETECT	Sets the maximum voltage for emulated PD detection. Between this setting and V_IDLE, the detection signature impedances are presented to the PSE by the PD. The voltage number can be changed using the slide bar or the number field to the right.
V_IDLE	Sets the minimum detection voltage. No signatures are presented below this threshold value. The voltage number can be changed using the slide bar or the number field to the far right.
Set to Nominal	Any of these button set the selected voltage setting to its nominal position, based on IEEE 802.3af. The black bar shows the nominal range for this setting.

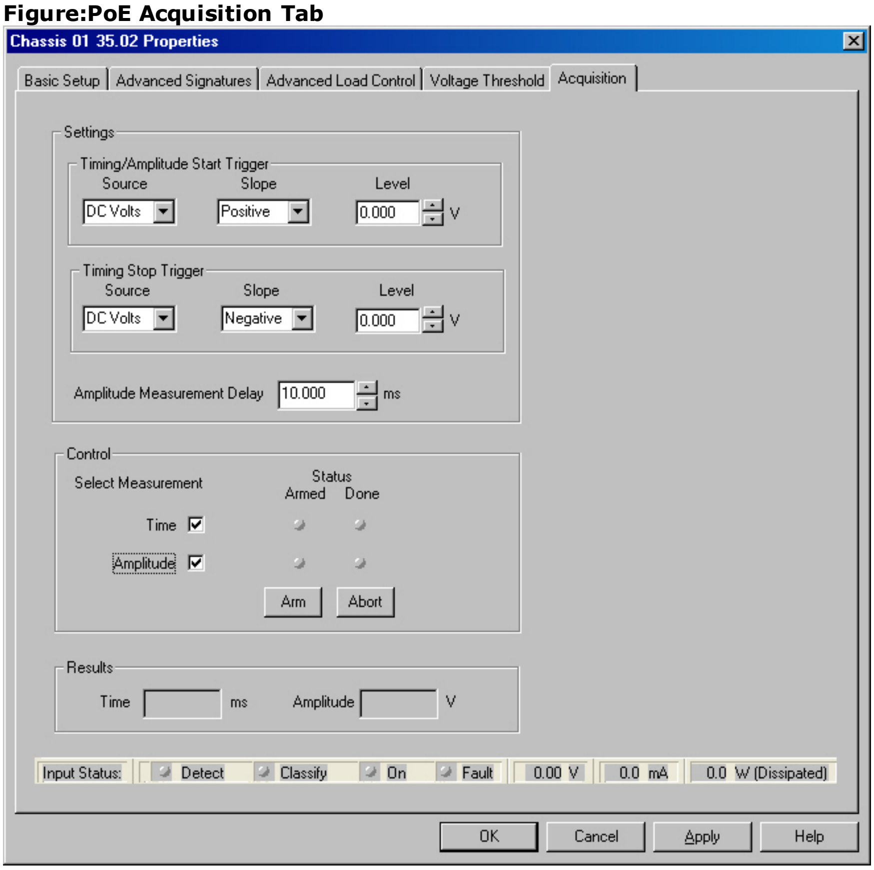
The Status settings are described in the following table:

PoE Acquisition

The *Acquisition* tab is used to set up tests that measure either the time elapsed from a Start trigger position to a Stop trigger position, and/or to measure the amplitude after a set time delay from a Start trigger.

The *Acquisition* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Acquisition* tab. Following figure shows the PoE *Acquisition* tab.

Figure:PoE Acquisition Tab



The controls and settings in the *Acquisition* tab are described in the following table:

Table:Acquisition Configuration

Section	Field/Control	Usage
Settings		Controls how the Start and Stop triggers are employed, as well as the Amplitude Measurement Delay.
	Start Trigger Source	Sets the Start trigger type to either DC Volts or DC Amps. The Start trigger determines when the test starts, based on the amplitude of the incoming voltage or current.
	Start Trigger Slope	Sets the Start trigger slope type, either positive or negative. A positive slope is equivalent to increasing voltage or current, while a negative slope is equivalent to decreasing voltage or current. If a trigger point is reached, but for the opposite slope setting, then the trigger is not activated.
	Start Trigger Level	Sets the amplitude of the Start trigger in either Volts or mAmps (depending on the setting in *Start Trigger Source*). When the trigger is armed, and the incoming voltage or current hits this number then the Start trigger is activated. Note that the Slope setting further qualifies this number.
	Stop Trigger Source	Sets the Stop trigger type to either DC Volts or DC Amps. The Stop trigger determines when the test ends, based on the amplitude of the incoming voltage or current. This setting is only valid for Time tests.
	Stop Trigger Slope	Sets the Stop trigger slope type, either positive or negative. A positive slope is equivalent to increasing voltage or current, while a negative slope is equivalent to decreasing voltage or current. If a trigger point is reached, but for the opposite slope setting, then the trigger is not activated. This setting is only valid for Time tests.
	Stop Trigger Level	Sets the amplitude of the Stop trigger in either Volts or mAmps (depending on the setting in *Stop Trigger Source*). When the trigger is armed, and the incoming voltage or current hits this number then the Start trigger is activated. Note that the Slope setting further qualifies this number.

Section	Field/Control	Usage
		This setting is only valid for Time tests.
	Amplitude Meas-urement Delay	Sets the length of an Amplitude test, in micro-seconds. When the Start trigger is activated, the value of the input signal is measured after the elapsed time. This setting is only valid for Amplitude tests.
Control		Controls the type of test, and the arming of tests.
	Select Meas-urement	Sets the type of test to be run, either a Time test, an Amplitude test, or both. Selecting the Time check box activates the Stop Trigger fields, while selecting the Amplitude check box activates the *Amplitude Measurement Delay* field. Both tests can be selected and run at the same time.
	Status	Shows the current status of a Time or Amplitude test. When the Arm light is green, the test is armed, and will start when the Start trigger is reached. When the Done light is green, the test has completed. Tests must be armed before they can initiate.
	Arm	Selecting this button arms a selected test. Tests are selected using the Select Measurement check boxes.
	Abort	Selecting this button disarms a selected test. Tests are selected using the Select Meas-urement check boxes.
Results		Displays the test results for both tests.
	Time	For Time tests, lists the time between the Start trigger activation and Stop trigger activation. For Amplitude tests, lists the time set in the *Amplitude Measurement Delay* field.
	Amplitude	For Time tests, lists the Amplitude set in the Stop trigger point. For Amplitude tests, lists the Amplitude at the end of the Amplitude Meas-urement Delay.

The Status settings are described in the following table:

ALM1000T8/CPM1000T8 Module Port Properties

The ALM100T8 load module is a Layer 7-only version of Ixia TXS Ethernet modules and has 8 ports, each with an embedded CPU running the Linux operating system. It is currently designed to support two Layer 7 test applications — Ixia’s Chariot and IxLoad software. It supports the PING and ARP protocols, as well as independent SDK applications.

The CPM1000T8 is identical to the ALM1000T8, only with more memory (2 Gigabytes).

For information on Ixia's IxChariot and IxLoad software, refer to the following manuals:

- *IxChariot Quick Start Guide*
- *IxChariot User Guide*
- *IxLoad User Guide*

The complete specifications for the ALM1000T8 and CPM1000T8 load modules can be found in the *Ixia Platform Reference Manual*.

The properties and capabilities of the ALM1000T8 and CPM1000T8 load module are described in the following sections:

- *Port Properties for Ethernet Family of Modules* (this chapter).
- *Statistics Tab*
- *Statistic View*
- *Card Properties*

Note that the ALM1000T8 and CPM1000T8 does *NOT* support the following functions:

- Frame Data Protocols support
- Filter/Receive mode support
- Time stamp support
- Transmit Modes
- Packet Streams

ELM1000ST2 Module Port Properties

Ixia's Encryption Load Module (ELM) enables high performance testing of IPSec VPN devices and networks. With its custom hardware-based security processor in conjunction with Ixia's IxVPN test suite, the ELM offers an extremely scalable solution for validating the performance of IPSec VPN gateways. The ELM emulates the functional requirements of today's VPN network with its extensive IPSec security features such as data encryption, device authentication and credential, data integrity, address hiding, and security-association (SA) key aging.

The ELM, in conjunction with Ixia's IxVPN, implements a full IPSec and IKE protocol stack. It can emulate thousands of secure gateways and clients, creating thousands of IPSec tunnels. Using multiple ports, a single Ixia test system can scale to test the largest IPSec VPN gateways and networks. Once the tunnels are set up, IxVPN measures the encryption and decryption performance of the IPSec gateway using standard RFC 2544 test methodology. This solution can also be combined with Ixia's IxChariot, enabling application emulation using real world Layer 4-7 traffic over secured networks.

For information on IxVPN, see the *IxVPN User's Guide*. For information on IxChariot, see:

- *IxChariot Quick Start Guide*
- *IxChariot User Guide*

The properties and capabilities of the ELM1000ST2 load module are described in the following sections:

- *Port Properties for Ethernet Family of Modules*(this chapter).
- *Statistics Tab*
- *Statistic View*
- *Card Properties*

Note that the ELM1000ST2 does *NOT* support the following functions:

- Frame Data Protocols support
- Filter/Receive/Statistics (dialog) mode support
- Time stamp support
- Transmit Modes
- Packet Streams

Port Properties for Xcellon-Ultra and ASM1000XMV12X

The Xcellon-Ultra XP, Xcellon-Ultra NP, and ASM1000XMV12X-01 are Ethernet load modules with aggregation capability. The load module provides the following operation modes (which are set in the *Card Properties* dialog):

- 12 ports of 10/100/1000 Mbps that operates in either normal (non-aggregated) mode or 1GE aggregation mode
- 1 port 10GE aggregation

The card operation mode is set in the *Card Properties* dialog; *Xcellon-Ultra and ASM1000XMV12X Modules*.

NOTE The complete specifications for the Xcellon-Ultra XP, NP, and ASM1000XMV12X load modules can be found in the Ixia Platform Reference Manual.

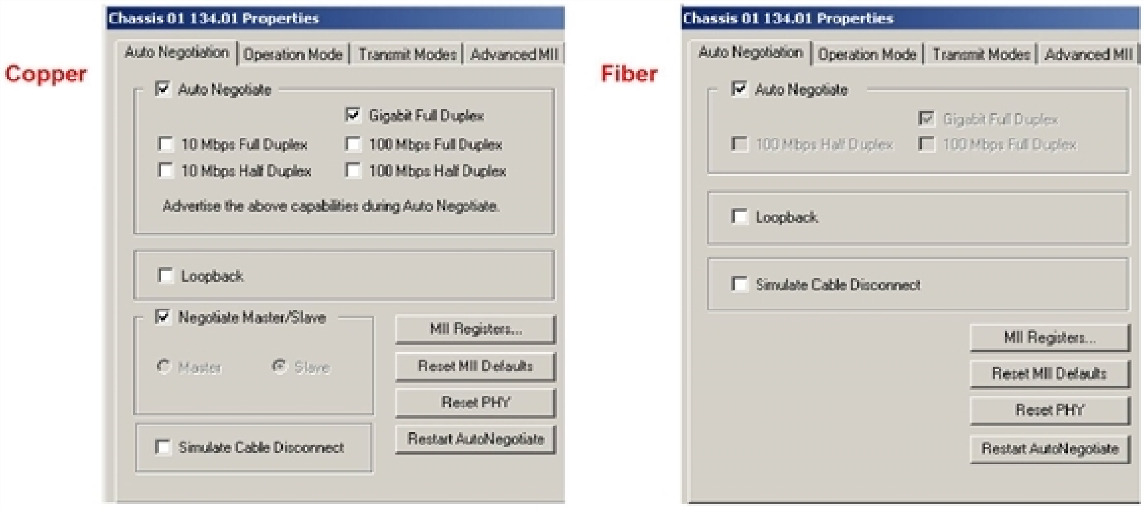
The Port Properties format will differ, depending on the operation mode of the card and the operation and transit modes of the selected port. The Transit Mode (copper or fiber) is set on the Transit Modes tab of the *Port Properties* dialog.

Auto Negotiation

On the Port Properties–Auto Negotiation tab, these are available combinations:

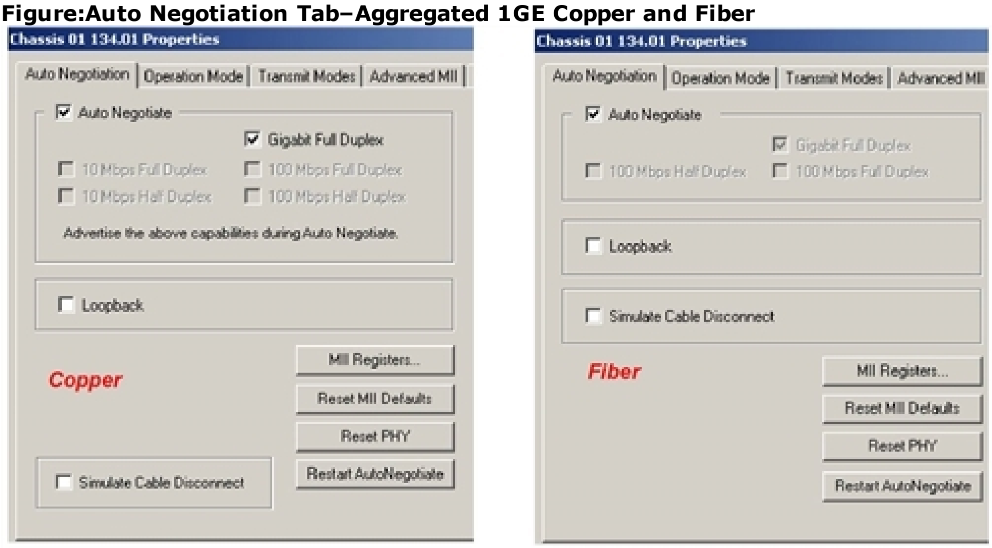
- non-aggregated copper or fiber (shown in *Figure:Auto Negotiation Tab–Non-Aggregated Copper and Fiber*, below)
- 1GE aggregated copper or fiber (*Figure:Auto Negotiation Tab–Aggregated 1GE Copper and Fiber*)
- 10GE aggregated copper and fiber (*Auto Negotiation Tab–Aggregated 10GE Copper and Fiber*)

Figure:Auto Negotiation Tab–Non-Aggregated Copper and Fiber



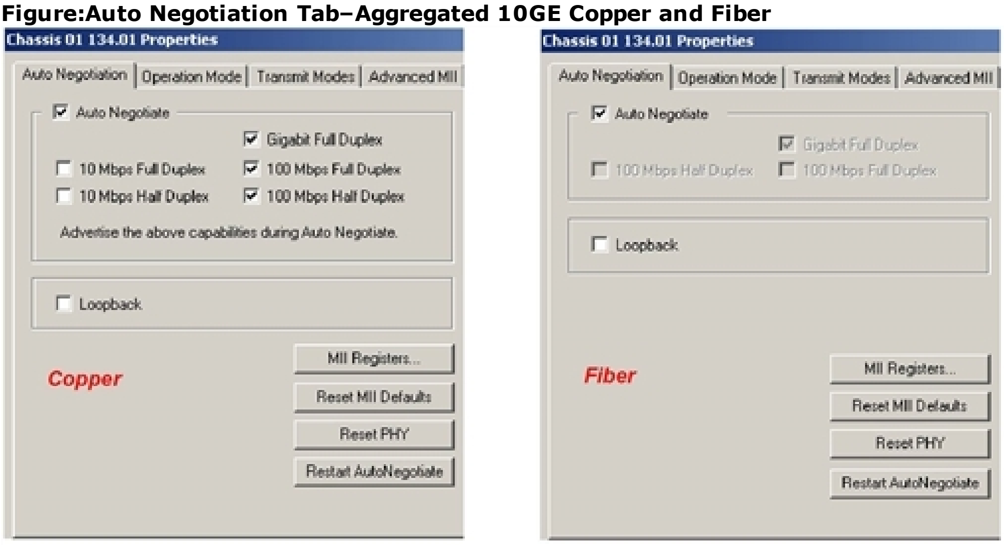
For descriptions of both sets of Auto Negotiation options, in the following figure:

Figure:Auto Negotiation Tab–Aggregated 1GE Copper and Fiber



For descriptions of both sets of Auto Negotiation options, in the following figure:

Figure:Auto Negotiation Tab–Aggregated 10GE Copper and Fiber



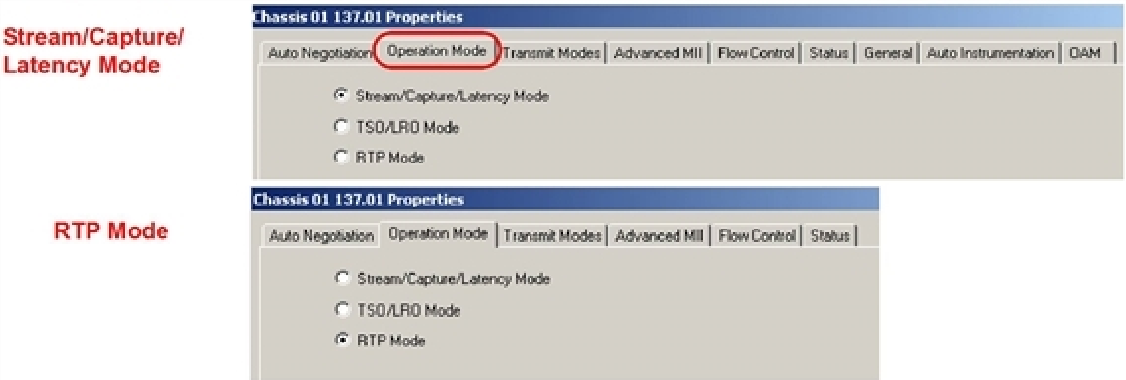
For descriptions of both sets of Auto Negotiation options, in the following table:

Non-Aggregated Port Operation Mode

With the ASM1000XMV12X-01 card in Normal (Non-Aggregated) mode, the port operation mode is (only) Stream/Capture/Latency. (This is the same when this card is in 1GbE Aggregated mode.)

For the Xcellon-Ultra XP and NP load modules, in Normal mode, the Port Operation Mode tab allows selection of Stream/Capture/Latency mode (the default) or RTP mode (Real-time Transport Protocol), or TSO/LRO (Transmit Segmentation Offload/Large Receive Off-load) mode. Depending on the selection, the number and configuration of the other Port Properties tabs will vary, as shown in the following figure:

Figure:Operation Mode Selection in Port Properties (Xcellon-Ultra Card in Normal Mode)



Stream/Capture/Latency Mode

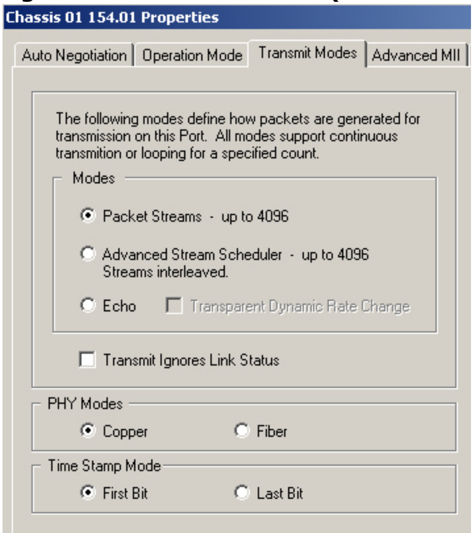
If Stream/Capture/Latency Mode (the default) is selected, then the other tabs will appear as listed below:

- *Transmit Modes*, same as that illustrated in *Transmit Modes Tab in Stream/Capture/Latency Mode*
- *Advanced MII*, practically identical to *Advanced MII for Copper 10/100/100 Modules. (See MII Register Files for additional information on MII registers.)*
- *Flow Control*, same as that described in *Flow Control Tab for Ethernet Modules*
- *Status*, same as that described in *Status Tab for Ethernet Modules*.
- On the *General* tab, *Time Stamp Offset*, same as that illustrated in *General Tab for Ethernet Modules*.
- Also on the *General* tab, *Intrinsic Latency Adjustment*,*Table:10GE LSM XENPAK/XFP General Tab Configuration* for field definitions.
- *Auto Instrumentation*, same as that described in *Auto Instrumentation Tab for Ethernet Modules*.
- *OAM*, same as that illustrated in *OAM Tab for Ethernet Modules*.

Transmit Modes Tab in Stream/Capture/Latency Mode

In non-aggregated or 1GbE Aggregation mode, the Transmit Modes tab offers the choice of PHY Modes, copper or fiber. This *Transmit Modes* tab is also identical in the LSM1000XMV load module family.

Figure:Transmit Modes Tab (Xcellon-Ultra) Stream/Capture/Latency Mode



The fields and controls in this tab are identified in the following table:

Table:Transmit Modes Tab (Xcellon-Ultra) Stream/Capture/Latency Mode

Section	Field/Control	Description
Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 4096 streams. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets up the transmission of up to 4096 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Echo **See the CAUTION below!**	Sets the basic operating mode for the port to Echo, a Layer 2 Ethernet round-trip mode. (Setting the Echo option in the *Transmit Modes* tab automatically enables the Echo option for the *Receive Mode* tab). Echo for additional information on Echo mode. Also Echo for additional information on setting the Transmit Mode to Echo.
Transmit Ignores Link Status	(check box)	If selected, will allow transmission of packets even if the link is down.
PHY Modes	Copper	Selected when a copper PHY connector is used (RJ-45).
	Fiber	Selected when a fiber PHY connector is used (SFP transceiver).
Time Stamp Mode	First Bit	Store and Forward latency mode uses first bit time stamp mode
	Last Bit	Store and Forward latency mode uses last bit time stamp mode

CAUTION The following warning message is issued when Echo is selected in the Transmit Modes tab or Receive Mode tab:

'Setting this mode on a live network may cause severe problems. All Ethernet frames with a DA which matches the Receive Filter DA1 will be 'echoed' back onto the network. Setting this mode will IMMEDIATELY start echoing packets. Are you sure you want to set Echo Mode? Yes or No.'

RTP Mode or TSO/LRO Mode

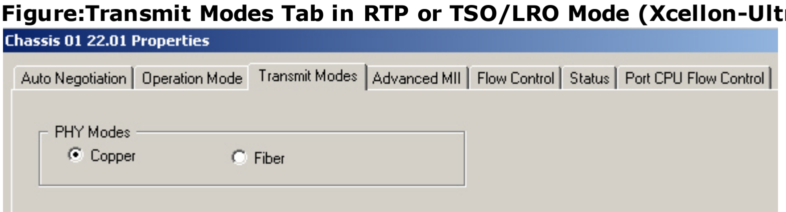
When RTP Mode is selected, IxOS downloads a different FPGA and restarts the CPU. If RTP Mode is selected, then the other Port Properties tabs will appear as listed below:

- *Transmit Modes*, select copper or fiber PHY mode. See the definitions for the PHY Modes in *Table:Transmit Modes Tab (Xcellon-Ultra) Stream/Capture/Latency Mode*.
- *Advanced MII*, the same as *Stream/Capture/Latency Mode*.
- *Flow Control*, the only option is Auto Negotiate. *Flow Control Tab for Xcellon-Ultra Modules*, below.
- *Status*, the same as *Stream/Capture/Latency Mode* above.

Transit Mode Tab in RTP Mode

The *Transmit Modes* tab for the Xcellon-Ultra modules in either RTP or TSO/LRO port operation mode is shown in the following figure. *Table:Transmit Modes Tab (Xcellon-Ultra) Stream/Capture/Latency Mode* for definitions of PHY Modes.

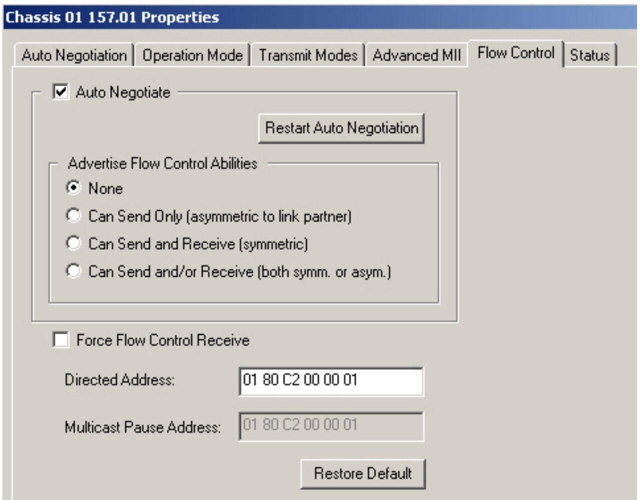
Figure:Transmit Modes Tab in RTP or TSO/LRO Mode (Xcellon-Ultra)



Flow Control Tab for Xcellon-Ultra Modules

The *Flow Control* tab for the Xcellon-Ultra modules in either RTP or TSO/LRO port operation mode is shown in the following figure:

Figure:Flow Control Tab for Xcellon-Ultra Modules



The fields and controls in this tab are described in the following table:

Table:Flow Control Tab for Xcellon-Ultra Modules

Section	Field/Control	Description
Auto Negotiate		Enables auto-negotiation of flow control capabilities for the port.
	Restart AutoNegotiation	If this button is clicked, it causes the auto-negotiation process to start immediately.
Advertise Flow Control Abilities	None	This and the next three options indicate which set of flow control capabilities are advertised to other ports. This option advertises no capabilities. (No PAUSE, per IEEE 802.3)
	Can Send Only (asymmetric to link partner)	This option advertises only send capabilities. (Asymmetric PAUSE toward link partner, per IEEE 802.3)
	Can Send and Receive (symmetric)	This option advertises both send and receive capabilities. (Symmetric PAUSE, per IEEE 802.3)
	Can Send and/or Receive (both symmetric or asymmetric)	This option advertises all send and receive capabilities in any combination. (Both Symmetric PAUSE and Asymmetric PAUSE toward local device, per IEEE 802.3)
Force Flow Control Receive		Enables receive side flow control handling for the port.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
	Restore Default	If this button is clicked, it restores the default MAC address: 01 80 C2 00 00 01 in both *Directed* and *Multicast Pause Address* fields.

Aggregated Modes

With the ASM1000XMV12X-01 card in 1GbE Aggregated mode, the port operation mode is (only) Stream/Capture/Latency. This is the same as the Normal (non-aggregated) mode–*Stream/Capture/Latency Mode*.

For the Xcellon-Ultra XP and NP load modules in 1GbE Aggregated mode, the port operation mode tab allows selection of Stream/Capture/Latency mode (the default) or RTP mode, or TSO/LRO mode. This is the same as the Normal (non-aggregated) mode, which is shown in the following figure.

The tabs that make up the Port Properties sets for the aggregated 1GE mode (copper and fiber) are listed below.

1GE Aggregate Mode:

- *Auto Negotiation, Figure:Auto Negotiation Tab–Aggregated 1GE Copper and Fiber and Figure:Auto Negotiation Tab–Aggregated 10GE Copper and Fiber*
- *Operation Mode, Stream/Capture/Latency mode, RTP, or TSO/LRO mode (however, RTP mode settings are superseded when the card is in aggregated mode). There is no Operation Mode tab when the load module is in 10GbE Aggregated mode. Figure:Operation Mode Selection in Port Properties (Xcellon-Ultra Card in Normal Mode).*
- *Transmit Modes*, select copper or fiber PHY mode. See the definitions for the PHY Modes in *Table:Transmit Modes Tab for Ethernet Modules*.
- *Advanced MII*, *Advanced MII for Copper 10/100/100 Modules (See MII Registers Files for additional information on MII registers.)*
- *Flow Control*, *Flow Control Tab for Xcellon-Ultra Modules*.
- *Status*, *Status Tab for Ethernet Modules*.
- *Port CPU Flow Control*, features a check box to enable/disable the port’s flow control mechanism. *Port CPU Flow Control*.

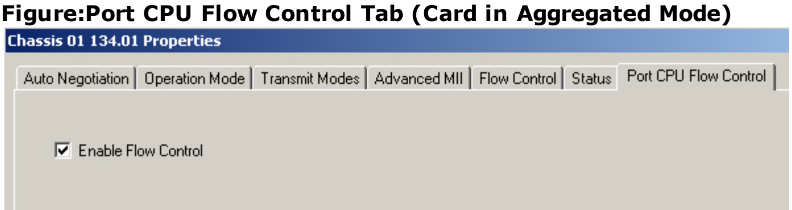
10GE Aggregate Mode:

For the ASM1000XMV12X-01 or Xcellon-Ultra XP and NP load modules in 10GbE Aggregated mode, the 12 Gigabit ports are disabled, and only port 13 *10G LAN XFP–Aggregate*–is operating. The port operation mode tab is not present. The *General* tab is used to select the type of Link and to select Simulate Cable Disconnect. The other tabs do not present configurable options, except the *Flow Control* tab, which allows enabling (or disabling) Flow Control.

Port CPU Flow Control

The Port Properties–Port CPU Flow Control tab is the same in all port operation modes when the card is in 1GbE Aggregate mode (shown in *Figure:Port CPU Flow Control Tab (Card in Aggregated Mode)*). It allows enabling/disabling Flow Control.

Figure:Port CPU Flow Control Tab (Card in Aggregated Mode)



Port/Card Ownership

You can switch the mode of operation on the Xcellon-Ultra or ASM1000XMV12X cards only if you own all ports on the card or if nobody owns any port. The behavior of taking ownership of an individual port is the same as those on other cards; that is, if nobody owns the port, ou can take ownership of the port. If you own the port, you can release ownership on the port. You can take ownership or clear ownership of a port by force.

Application software can enforce its own rules of port ownership.

Import/Export

Port files can be exported and imported even if the card is under a different mode of operation.

- When a port file (that was exported under aggregated mode) is imported back while the card is in normal mode, all the 'hidden' streams will be shown.
- When a port file (that was exported under normal mode) is imported back while the card is in aggregated mode, all the streams will be hidden and the speed will be forced to 1000FD.

Chapter 19 - Port Properties–POS and ATM Families

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog is a display that corresponds to the module type. The following sections describe the functions and configuration of the Packets over SONET (PoS) and ATM family of module port properties.

This chapter also covers several SONET-related special feature options (for example, VSR and SRP) that can be included with the PoS or ATM modules.

Port properties differ for the various module types, and are described in the following sections.

- *Port Properties for Packets over SONET (POS) Modules*
- *Port Properties for BERT*
- *Unframed BERT*
- *Port Properties for VSR*
- *Port Properties for SRP*
- *Port Properties for RPR*
- *Port Properties for GFP*
- *Port Properties for DCC*
- *ATM/POS 622 Modules*

Some (former) port properties are now configured as circuit properties:

- *VCAT Circuit Properties*

NOTE BERT, VSR, SRP, RPR, and DCC are also available on some 10 Gigabit Ethernet and UNIPHY modules.Chapter 20 *Port Properties-10 GE and UNIPHY Families* for more information.

Port Properties for Packets over SONET (POS) Modules

The complete specifications for the Packets over SONET type boards can be found in the following *Ixia Platform Reference Manual* chapters:

- OC-12c/OC-3c Load Module Specifications
- OC-48c Load Module Specifications
- OC-192c Load Module Specifications

The port properties for Packet over SONET modules are configured using the following set of tabs, with the available tab depending on the type of module.

- *General Properties*(2.5G MSM POS only)
- *SONET Properties*
- *PPP Properties*
- *SONET Overhead*
  - *APS K1/K2 Sub-Tab*
  - *J0/J1 Sub-Tab*
  - *SONET Error Insertion*

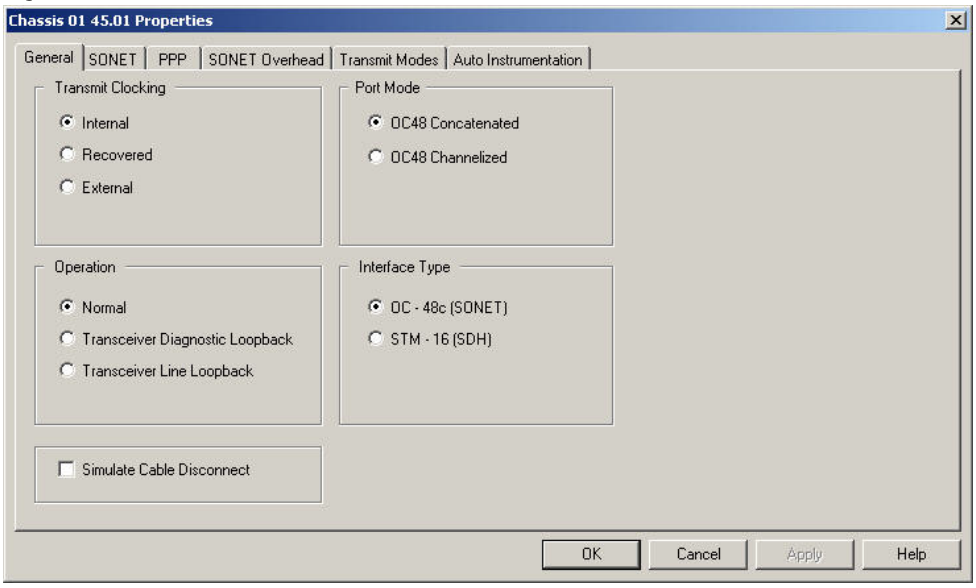
- *Transmit Modes for POS Modules*
- Auto Instrumentation tab, *Auto Instrumentation Tab for Ethernet Modules*(Chapter 18)

General Properties

Figure:2.5G MSM OC-48c POS General Tab shows the 2.5G MSM POS General tab.

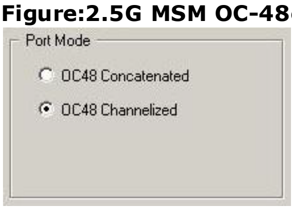
The *General* tab is accessed by right-clicking a port in the Resources window, selecting the *Properties* menu option, then selecting the *General* tab.

Figure:2.5G MSM OC-48c POS General Tab



Board types 2.5G MSM and 10G MSM optionally provide for the selection of Channelized mode (under *Port Mode* on the *General* tab) as shown in *Figure:2.5G MSM OC-48c with Channelized Port Mode Option*.

Figure:2.5G MSM OC-48c with Channelized Port Mode Option



When Channelized mode is selected, the Port Properties window has only *General*, *SONET Overhead*, *Trasmit Modes*, and *Auto Instrumentation* tabs.

Table:General Tab Configuration Options explains the configuration options of the *General* tab.

Table:General Tab Configuration Options

Section	Field/Control	Description
Transmit Clocking	Internal	Use the chassis internal clock.
	Recovered	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal

Section	Field/Control	Description
		clock. Enable this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
	External	If enabled, an external clock source is used.
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disable if FEC is enabled.)
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
Port Mode	OC48 Concatenated	Selects the transmit port mode.
	OC48 Channelized	Selects the channelized mode (on 2.5G MSM and 10G MSM boards only)
Interface Type	OC-48c (SONET)	Optical Carrier level 48 concatenated.
Simulate Cable Disconnect		If this is selected, the port acts as if the cable has been disconnected.

SONET Properties

The port properties SONET tab is shown for several load modules:

- for OC-192c POS modules, *Figure:OC-192c POS—SONET Tab*.
- for OC-48c POS modules, *Figure:OC-48c POS—SONET Tab*.
- for 2.5 MSM POS modules, *Figure:OC-48c POS—SONET Tab*.
- for 10G MSM modules, *Figure:10G MSM—SONET Tab*.
- for older OC-12c/OC-3c POS modules, *Figure:OC-12c/OC-3c POS—SONET Tab*.
- *for UNIPHY 10GE OC-192c POS/BERT, Figure:UNIPHY OC-192c POS.*

The *SONET* tab is accessed by right-clicking a port in the Resources window, selecting the *Properties* menu option, then selecting the *SONET* tab.

NOTE

For information on POS 622 (OC-12c/OC-3c) and ATM 622 port properties, *ATM/POS 622 Modules*.
For information on RPR port properties,*Port Properties for RPR*.
For information on SRP port properties,*Port Properties for SRP*.

Figure:OC-192c POS—SONET Tab

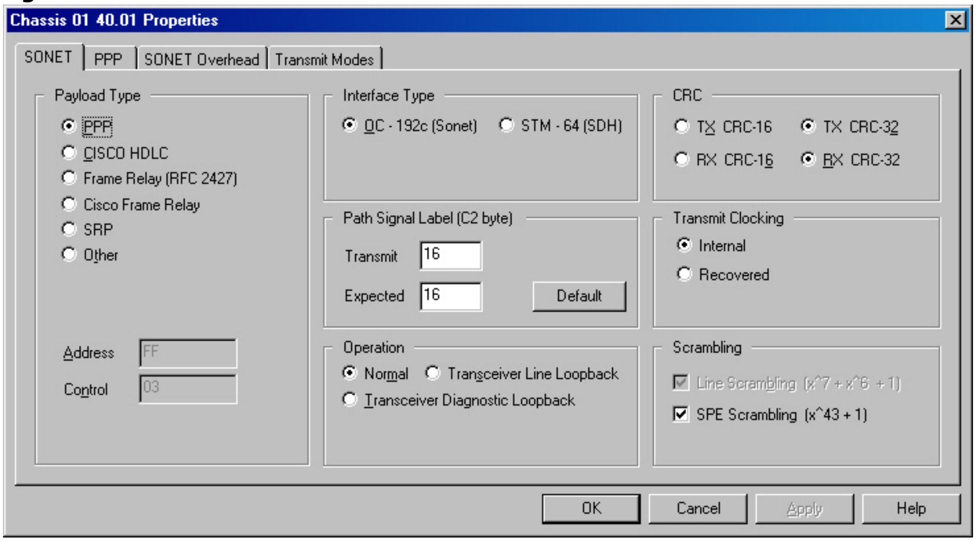


Figure:OC-48c POS—SONET Tab

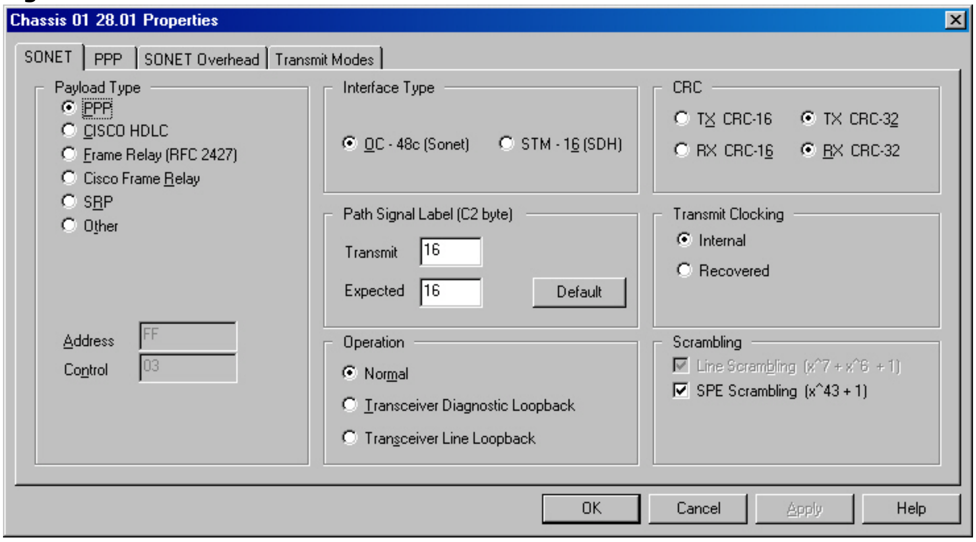
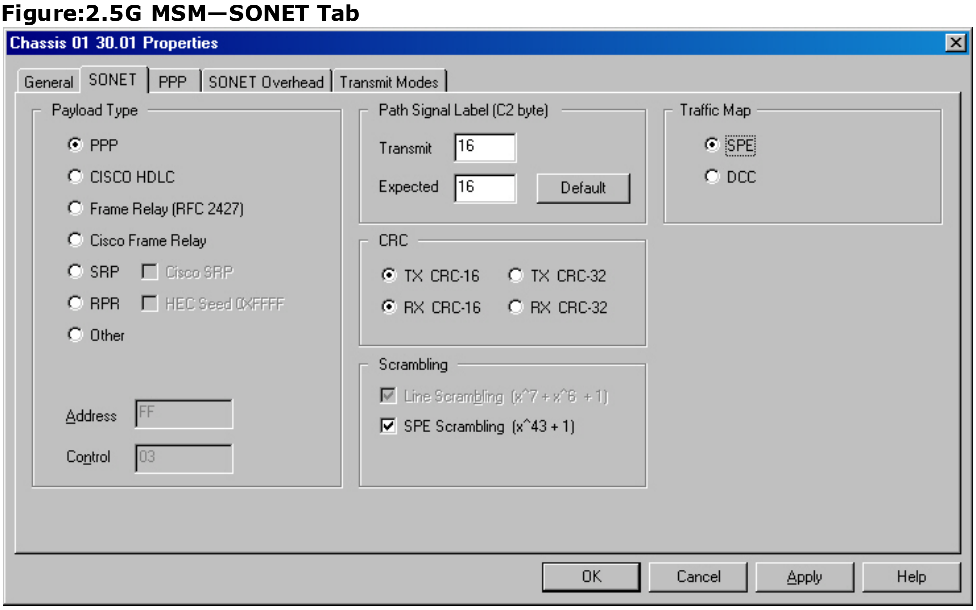
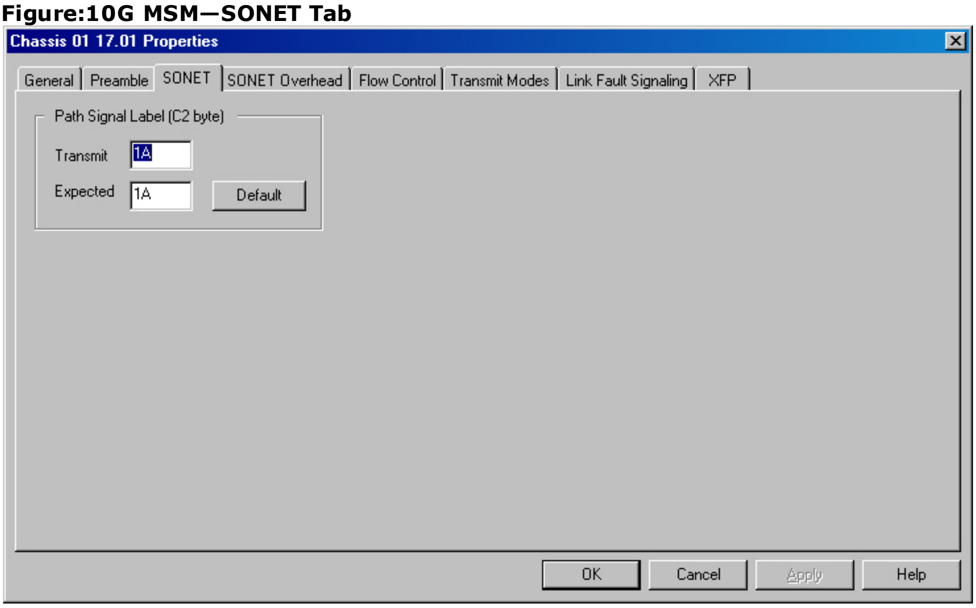


Figure:2.5G MSM—SONET Tab



NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the SONET tab is no longer present. The SONET parameters are configured through the Circuit Properties window. *SONET Circuit Properties*.

Figure:10G MSM—SONET Tab



NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the SONET tab is no longer present. The SONET parameters are configured through the Circuit Properties window. *SONET Circuit Properties*.

Figure:OC-12c/OC-3c POS—SONET Tab

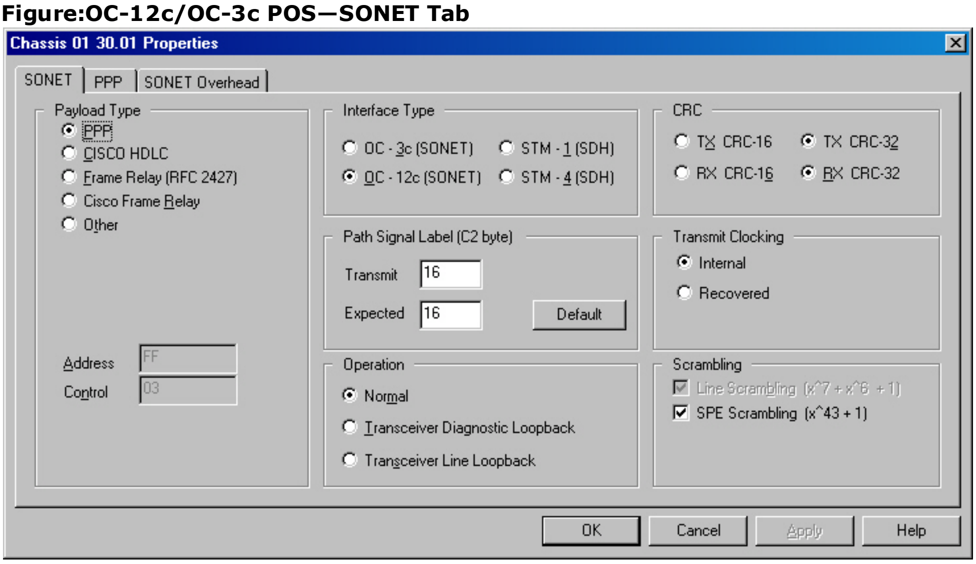
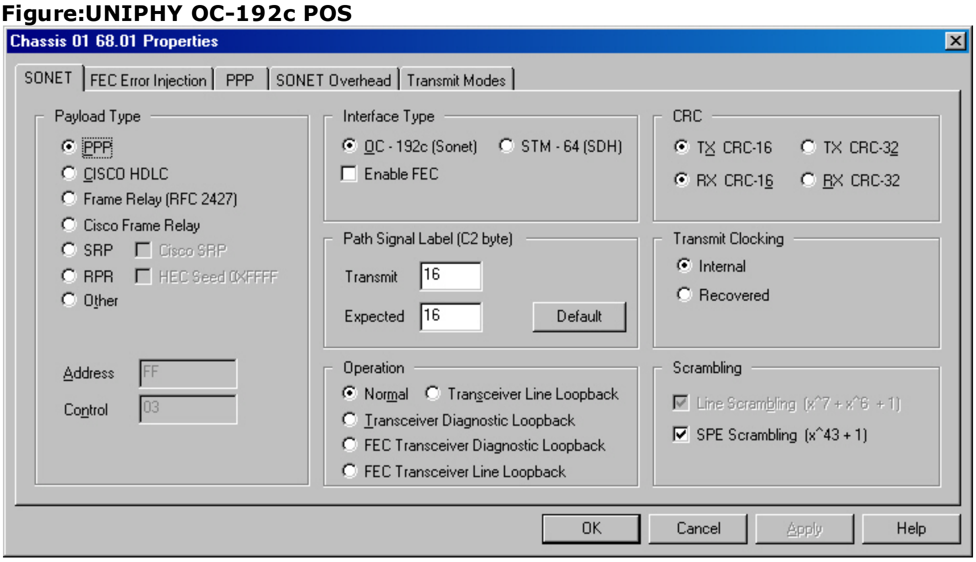


Figure:UNIPHY OC-192c POS



The fields and controls in these tabs are described in *Table:Packet Over SONET (POS)—SONET Tab*.

Table:Packet Over SONET (POS)—SONET Tab

Section	Field/Control	Description
Payload Type		NOTE The choice of Payload Type in this tab is reflected in the Stream Properties/Frame Data/Protocols dialogs.
	PPP	Selects fixed PPP address, control, and protocol header values.
	CISCO HDLC	Selects Cisco proprietary address, control, and protocol header values. HDLC = High-level Data Link Control, a data link layer protocol.
	Frame Relay (RFC 2427)	Selects Frame Relay address, control, and protocol header values.
	Cisco Frame Relay	Selects Cisco proprietary Frame Relay address, control, and protocol header values.
	SRP	Selects Spatial Reuse Protocol (SRP) address, control, and protocol header values. *Port Properties for SRP*. (Not available for OC-12c/OC-3c.) Note that IPv6 is not available when using SRP.
	Cisco SRP	(*SRP* must be selected first.) If selected, Spatial Reuse Protocol header values are implemented per Cisco SRP requirements. Note that IPv6 is not available when using Cisco SRP

Section	Field/Control	Description
	RPR	Selects Resilient Packet Ring (RPR) address, control, and protocol header values. This option is only available for UNIPHY OC-192c, and OC-48c/192c with the optional RPR component. *Port Properties for RPR* for more information. Note that IPv6 is not available when using RPR
	HEC Seed	(*RPR* must be selected first.) If selected, the initial setting of the CRC for the 16 byte header is set to FFFF (all ones). The default setting is all zeros (0000).
	Other	Allows to select values for Address and Control as described in the next two rows.
	Address	When *Other* header is selected, allows the setting of the values for the SONET header address field; otherwise, reflects the fixed values associated with the header choice.
	Control	When *Other* header is selected, allows the setting of the values for the SONET header control field; otherwise, reflects the fixed values associated with the header choice.
Interface Type	OC-12c (SONET)	Optical Carrier level 12 concatenated.
	STM-4 (SDH)	Synchronous transfer mode level 4.
	OC-3c (SONET)	Optical Carrier level 3 concatenated.
	STM-1 (SDH)	Synchronous transfer mode level 1.
	OC-48c (SONET)	Optical Carrier level 48 concatenated.
	STM-16 (SDH)	Synchronous transfer mode level 16.
	OC-192c (SONET)	Optical Carrier level 192 concatenated.
	STM-64 (SDH)	Synchronous transfer mode level 64.
	Enable FEC	Enables FEC information to be included with transmitted data. This also enables the features found on the *FEC Error Injections* tab page, described in *FEC Error Injection*. (Only for UNIPHY 10GE OC-192c POS/BERT.)
	Payload Type	Allows for the selection of the FEC payload type, from the following list: • 02-asy STM-N • 03-bit syn STM-N • 04-ATM • 05-GFP • 10-bit str w o.t. • 11-bit str wo o.t.

Section	Field/Control	Description
		• FE-PRBS This list defines what data type is being simulated in the payload area of the SONET frame. This list is only visible when the *Enable FEC* check box is selected. (Only for UNIPHY 10GE OC-192c POS.)
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted header. (Hex)
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both Transmit and Expected values to the default value (16).
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disable if FEC is enabled.)
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
	FEC Transceiver Diagnostic Loopback	Causes the FEC information to be looped back at the transceiver. (Only for UNIPHY 10GE OC-192c POS/BERT.)
	FEC Transceiver Line Loopback	Causes the data from the receive port to be sent out the transmit port from the FEC Framer. (Only for UNIPHY 10GE OC-192c POS/BERT.)
CRC	TX CRC-16	Selects transmission with 16-bit CRC.
	RX CRC-16	Selects reception with 16-bit CRC.
	TX CRC-32	Selects transmission with 32-bit CRC.
	RX CRC-32	Selects reception with 32-bit CRC.
Transmit Clocking	Internal	Use the chassis internal clock.
	Use Recovered Clock	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal clock. Select this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
	External	Use and external clocking source (such as GPS). For POS/ATM 622 cards only.

Section	Field/Control	Description
Scrambling	Line Scrambling (x^7 + x^6 + 1)	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling (x^43 - 1)	If enabled, data is scrambled with the $x^{43} + 1$ polynomial.
Traffic Map (**Only on 2.5/10G MSM load modules**)	SPE	This is the 'normal' packet stream mode, where streams of packets are transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 256 packet streams may be configured for the port.
	DCC	When this mode is selected, streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Packet Streams.' DCC Packet Streams and Packet Flows for additional information.

SONET Properties

The port properties SONET tab is shown for several load modules:

- for OC-192c POS modules, *Figure:OC-192c POS—SONET Tab*.
- for OC-48c POS modules, *Figure:OC-48c POS—SONET Tab*.
- for 2.5 MSM POS modules, *Figure:OC-48c POS—SONET Tab*.
- for 10G MSM modules, *Figure:10G MSM—SONET Tab*.
- for older OC-12c/OC-3c POS modules, *Figure:OC-12c/OC-3c POS—SONET Tab*.
- *for UNIPHY 10GE OC-192c POS/BERT, Figure:UNIPHY OC-192c POS.*

The *SONET* tab is accessed by right-clicking a port in the Resources window, selecting the *Properties* menu option, then selecting the *SONET* tab.

NOTE For information on POS 622 (OC-12c/OC-3c) and ATM 622 port properties, *ATM/POS 622 Modules*.
For information on RPR port properties,*Port Properties for RPR*.
For information on SRP port properties,*Port Properties for SRP*.

Figure:OC-192c POS—SONET Tab

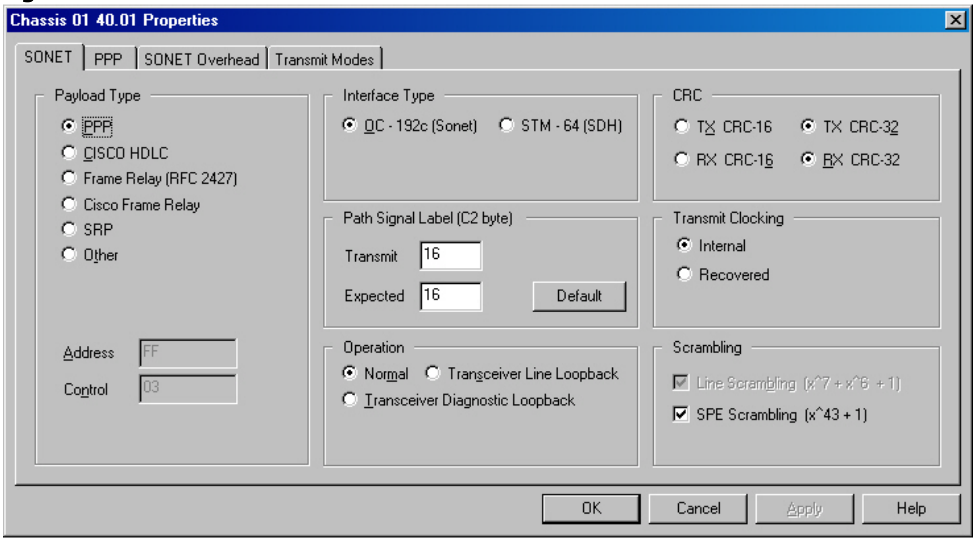


Figure:OC-48c POS—SONET Tab

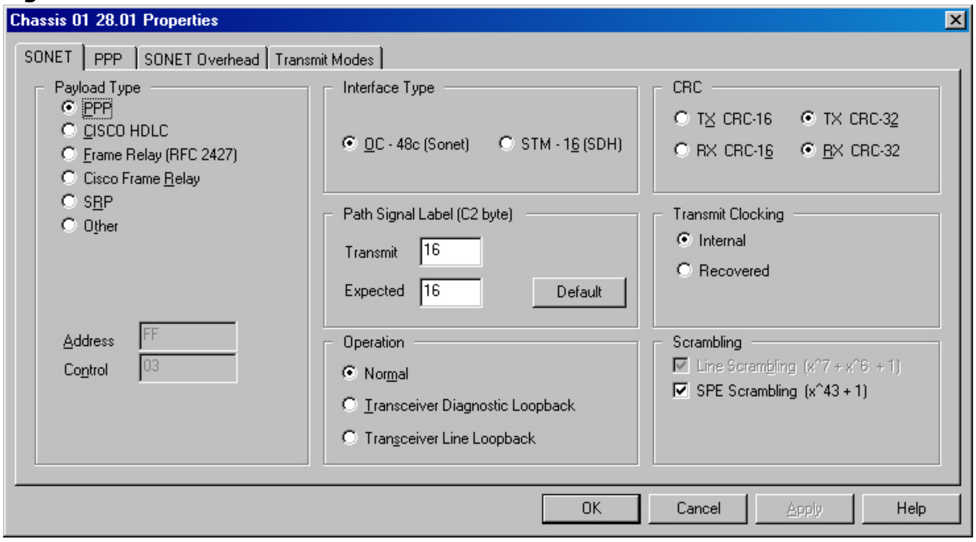
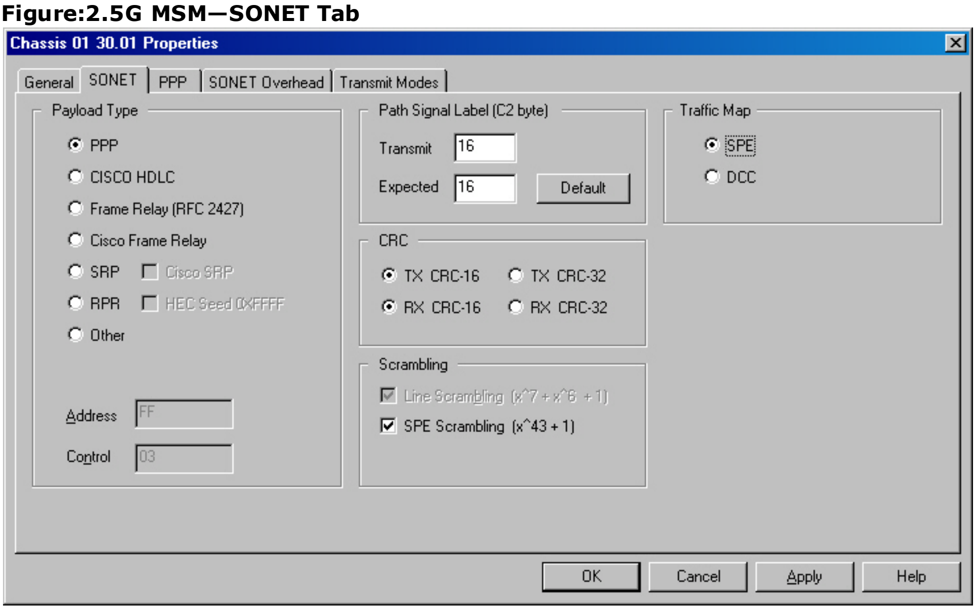


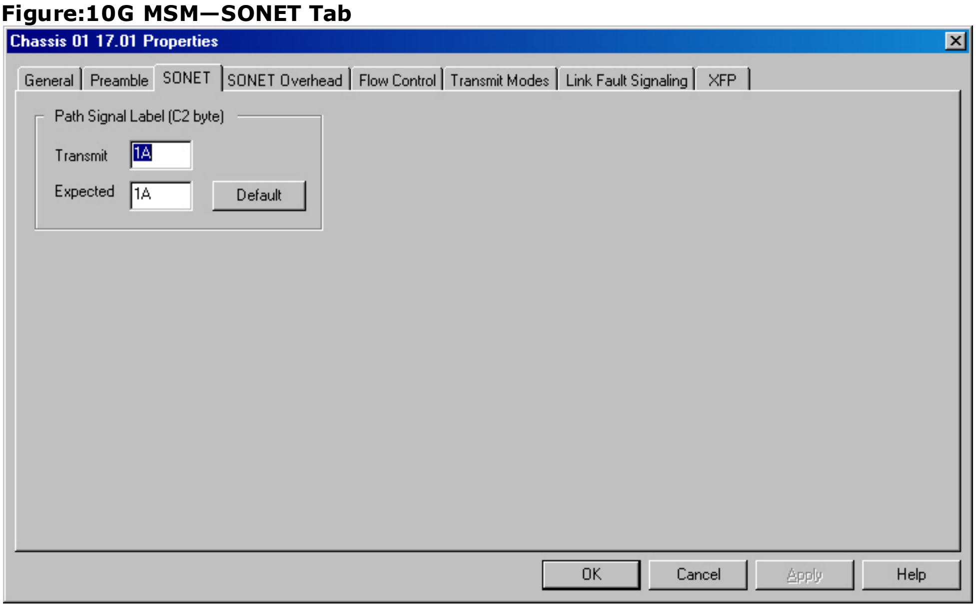
Figure:2.5G MSM—SONET Tab



NOTE

If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the SONET tab is no longer present. The SONET parameters are configured through the Circuit Properties window. *SONET Circuit Properties*.

Figure:10G MSM—SONET Tab



NOTE

If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the SONET tab is no longer present. The SONET parameters are configured through the Circuit Properties window. *SONET Circuit Properties*.

Figure:OC-12c/OC-3c POS—SONET Tab

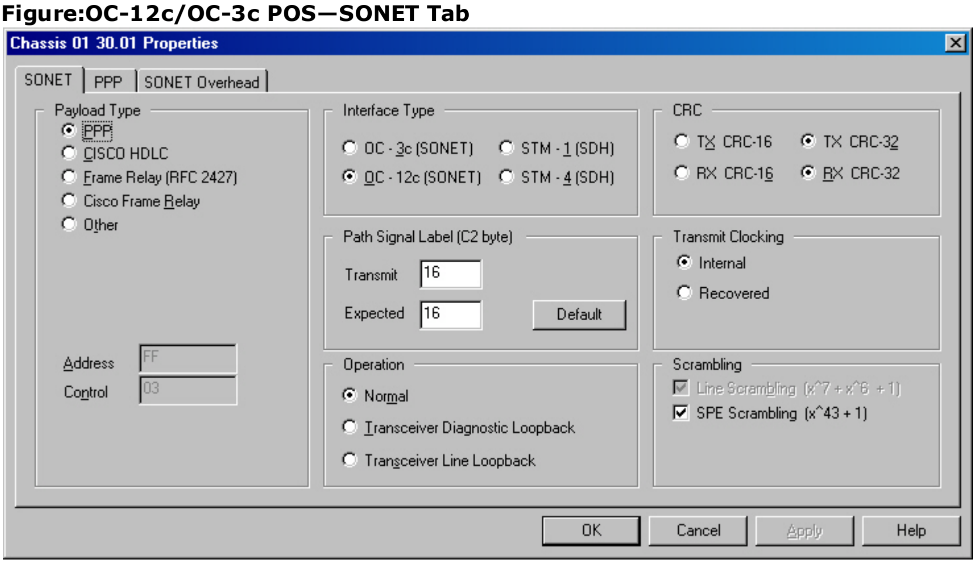
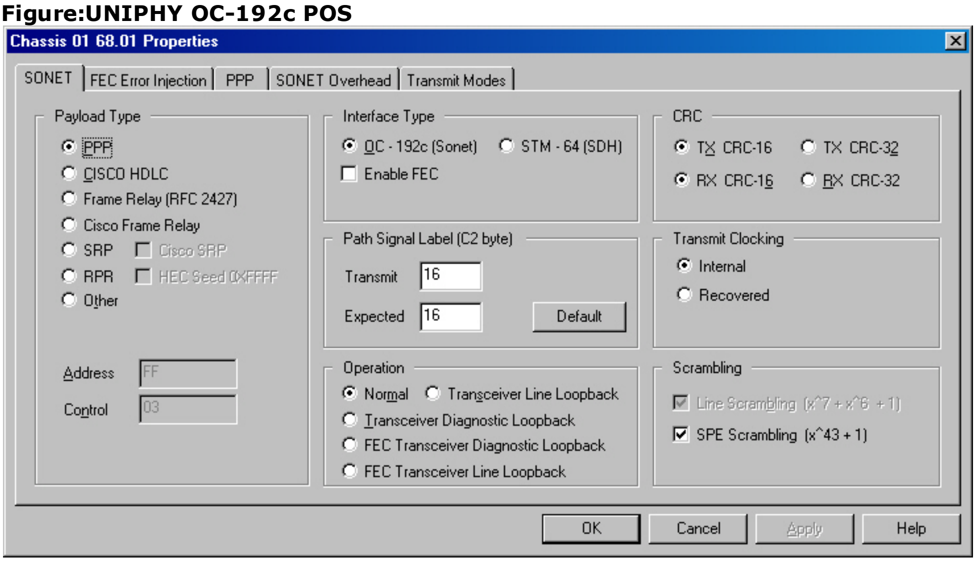


Figure:UNIPHY OC-192c POS



The fields and controls in these tabs are described in *Table:Packet Over SONET (POS)—SONET Tab*.

Table:Packet Over SONET (POS)—SONET Tab

Section	Field/Control	Description
Payload Type		NOTE The choice of Payload Type in this tab is reflected in the Stream Properties/Frame Data/Protocols dialogs.
	PPP	Selects fixed PPP address, control, and protocol header values.
	CISCO HDLC	Selects Cisco proprietary address, control, and protocol header values. HDLC = High-level Data Link Control, a data link layer protocol.
	Frame Relay (RFC 2427)	Selects Frame Relay address, control, and protocol header values.
	Cisco Frame Relay	Selects Cisco proprietary Frame Relay address, control, and protocol header values.
	SRP	Selects Spatial Reuse Protocol (SRP) address, control, and protocol header values. *Port Properties for SRP*. (Not available for OC-12c/OC-3c.) Note that IPv6 is not available when using SRP.
	Cisco SRP	(*SRP* must be selected first.) If selected, Spatial Reuse Protocol header values are implemented per Cisco SRP requirements. Note that IPv6 is not available when using Cisco SRP

Section	Field/Control	Description
	RPR	Selects Resilient Packet Ring (RPR) address, control, and protocol header values. This option is only available for UNIPHY OC-192c, and OC-48c/192c with the optional RPR component. *Port Properties for RPR* for more information. Note that IPv6 is not available when using RPR
	HEC Seed	(*RPR* must be selected first.) If selected, the initial setting of the CRC for the 16 byte header is set to FFFF (all ones). The default setting is all zeros (0000).
	Other	Allows to select values for Address and Control as described in the next two rows.
	Address	When *Other* header is selected, allows the setting of the values for the SONET header address field; otherwise, reflects the fixed values associated with the header choice.
	Control	When *Other* header is selected, allows the setting of the values for the SONET header control field; otherwise, reflects the fixed values associated with the header choice.
Interface Type	OC-12c (SONET)	Optical Carrier level 12 concatenated.
	STM-4 (SDH)	Synchronous transfer mode level 4.
	OC-3c (SONET)	Optical Carrier level 3 concatenated.
	STM-1 (SDH)	Synchronous transfer mode level 1.
	OC-48c (SONET)	Optical Carrier level 48 concatenated.
	STM-16 (SDH)	Synchronous transfer mode level 16.
	OC-192c (SONET)	Optical Carrier level 192 concatenated.
	STM-64 (SDH)	Synchronous transfer mode level 64.
	Enable FEC	Enables FEC information to be included with transmitted data. This also enables the features found on the *FEC Error Injections* tab page, described in *FEC Error Injection*. (Only for UNIPHY 10GE OC-192c POS/BERT.)
	Payload Type	Allows for the selection of the FEC payload type, from the following list: • 02-asy STM-N • 03-bit syn STM-N • 04-ATM • 05-GFP • 10-bit str w o.t. • 11-bit str wo o.t.

Section	Field/Control	Description
		• FE-PRBS This list defines what data type is being simulated in the payload area of the SONET frame. This list is only visible when the *Enable FEC* check box is selected. (Only for UNIPHY 10GE OC-192c POS.)
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted header. (Hex)
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both Transmit and Expected values to the default value (16).
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disable if FEC is enabled.)
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
	FEC Transceiver Diagnostic Loopback	Causes the FEC information to be looped back at the transceiver. (Only for UNIPHY 10GE OC-192c POS/BERT.)
	FEC Transceiver Line Loopback	Causes the data from the receive port to be sent out the transmit port from the FEC Framer. (Only for UNIPHY 10GE OC-192c POS/BERT.)
CRC	TX CRC-16	Selects transmission with 16-bit CRC.
	RX CRC-16	Selects reception with 16-bit CRC.
	TX CRC-32	Selects transmission with 32-bit CRC.
	RX CRC-32	Selects reception with 32-bit CRC.
Transmit Clocking	Internal	Use the chassis internal clock.
	Use Recovered Clock	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal clock. Select this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
	External	Use and external clocking source (such as GPS). For POS/ATM 622 cards only.

Section	Field/Control	Description
Scrambling	Line Scrambling (x^7 + x^6 + 1)	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling (x^43 - 1)	If enabled, data is scrambled with the $x^{43} + 1$ polynomial.
Traffic Map (**Only on 2.5/10G MSM load modules**)	SPE	This is the 'normal' packet stream mode, where streams of packets are transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 256 packet streams may be configured for the port.
	DCC	When this mode is selected, streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Packet Streams.' DCC Packet Streams and Packet Flows for additional information.

PPP Properties

Point to Point Protocol (PPP) properties for Packet over SONET modules are configured using the *PPP* tab, which has three sub-tabs, described in the following sections:

- *PPP Negotiation*
- *PPP Link Control Protocol*
- *PPP Network Control Protocols*

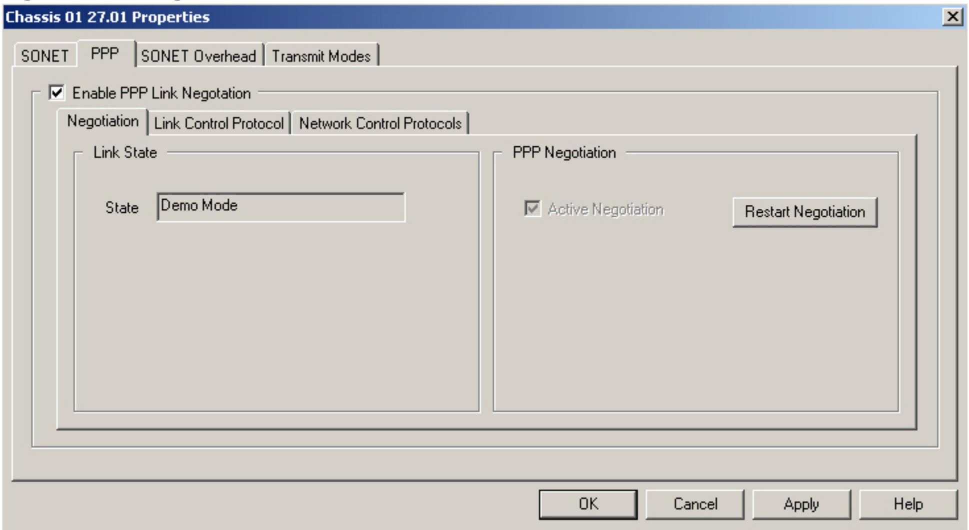
The *PPP* tab is accessed by right-clicking a port, selecting the *Properties* options, then selecting the *PPP* tab in the *Port Properties* dialog.

NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the PPP tab is no longer present. The PPP parameters are configured through the Circuit Properties page. *PPP Circuit Properties*.

PPP Negotiation

The PPP *Negotiation* sub-tab is shown in *Figure:PPP Negotiation Sub-Tab*. This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, then selecting the *Negotiation* sub-tab.

Figure:PPP Negotiation Sub-Tab



The fields and controls in this tab are described in *Table:PPP Negotiation Tab*.

Table:PPP Negotiation Tab

Section	Field/Control	Description
Enable PPP Negotiation		If selected, enables PPP on this port, if a PPP SONET header has already been selected in the *SONET* tab. With PPP enabled, no data traffic will flow until PPP link and network layer negotiation (LCP and NCP) with the peer has successfully completed.
Link State	State	(Read-only) Indicates the current port link state. If PPP is enabled, the fully operational link state is indicated as *PPP Up.*
PPP Negotiation	Active Negotiation	The Ixia port will not wait for the PPP peer to send configuration requests, but will actively attempt to negotiate.
	Restart Negotiation	Clicking this button starts a new PPP negotiation cycle, as follows: • 1—Any data transmission will be stopped. • 2—The PPP link will be dropped. • 3—PPP will attempt to renegotiate. • 4—After successful negotiation, data transmission can be started again.

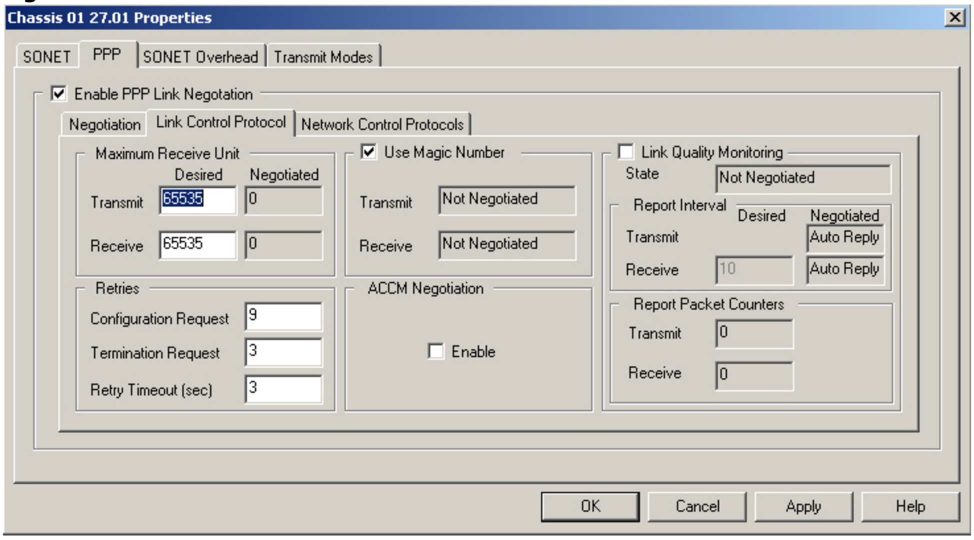
PPP Link Control Protocol

The PPP *Link Control Protocol (LCP)* sub-tab is shown in *Figure:PPP Link Control Protocol Sub-Tab*. It specifies the options and parameters used during LCP negotiation. This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, then selecting the *Link Control Protocol* sub-tab.

NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the PPP tab is no longer present. The PPP

NOTE parameters are configured through the Circuit Properties page. *PPP Link Control Protocol*.

Figure:PPP Link Control Protocol Sub-Tab



NOTE IPv6 has a minimum frame size of 1280 bytes. When using IPv6 over POS ports, it is important to set the desired negotiated Transmit MRU value to 1280 or higher, otherwise protocol interfaces cannot be associated with this port. For more information on protocol interfaces,*Protocol Interfaces*.

The field and controls in this tab are described in *Table:PPP Link Control Protocol Sub-Tab*.

Table:PPP Link Control Protocol Sub-Tab

Section	Field/Control	Description
Maximum Receive Unit	Transmit: Desired	(in bytes) The Maximum Receive Unit (MRU) is the maximum transmit frame size desired.
	Transmit: Negotiated	(Read-only) The maximum transmit frame size actually negotiated.
	Receive: Desired	The maximum receive frame size desired.
	Receive: Negotiated	(Read-only) The maximum receive frame size actually negotiated.
Use Magic Number		If selected, magic number handling is enabled for negotiation and usage. The magic number is used primarily to detect looped connections.
	Transmit	(Read-only) Possible settings: • If Use Magic Number is not selected, then this field will remain *Not Negotiated.* • If *Use Magic Number* is enabled and the peer does not agree to receive magic numbers, then this displays *Disabled.* • If *Use Magic Number* is enabled and the peer agrees to receive magic numbers, then this displays a random value, reflecting the Transmit-Receive from the other card or

Section	Field/Control	Description
		port. • If *Use Magic Number* is enable and the port is set to loopback mode, this field reads *Loopback Detected*.
	Receive	(Read only) Possible settings: • If *Use Magic Number* is not selected, then this field will remain *Not Negotiated.* • If *Use Magic Number* is enabled and the peer does not agree to receive magic numbers, then this will show *Disabled.* • If *Use Magic Number* is enabled and the peer agrees to receive magic numbers, then this displays a random value, reflecting the Transmit-Receive from the other card or port. • If *Use Magic Number* is enabled and the port is set to loopback mode, then this field reads *Loopback Detected*.
Retries	Configuration Request	The number of additional PPP configuration requests to send before beginning the termination process (if the peer is not properly acknowledging them).
	Termination Request	The number of additional PPP termination requests to send before closing down the link (if the peer is not properly acknowledging them).
	Retry Timeout (sec)	The time, in seconds, between retransmissions of successive configuration or termination requests.
ACCM Negotiation	Enable	If selected, enables negotiation of Asynchronous Control Character Mask (ACCM). NOTE Except in special situations (for example, when using non-compliant equipment, or when testing PPP itself), the ACCM Negotiation option be disabled for POS.
Link Quality Monitoring		If selected, enables Link Quality Monitoring (LQM) on the link.
	State	(Read only) Possible states: • **Not negotiated**—LQM has not been negotiated. • **Inactive**—LQM Negotiation has resulted in agreement that LQM will NOT be used on the link. • **Active**—LQM Negotiation has resulted in

Section	Field/Control	Description
		agreement that LQM WILL be used on the link. NOTE: Except in special situations (for example, when using non-compliant equipment, or when testing PPP itself), the ACCM Negotiation option be disabled for POS.
Report Interval	Transmit: Negotiated	(Read-only) Negotiated maximum time in seconds between transmission of consecutive LQR packets from the Ixia port. LQR transmissions may occur faster than the indicated period, because this transmission frequency may be increased by the peer. *Auto-reply* indicates an LQR will be immediately generated and transmitted upon reception of an LQR from the peer, rather than employing an internal timer. (A timer must be maintained by at least one of the peers on the link.)
	Receive: Desired	(Write-only) Desired time in seconds between reception of consecutive LQR packets from the peer. This desired interval is requested during the LQM negotiation process.
	Receive: Negotiated	(Read-only) Negotiated maximum time in seconds between reception of consecutive LQR packets from the peer. *Auto Reply* indicates the peer will generate and transmit an LQR in response to our LQR.
Report Packet Counter	Transmit	(Read-only) This counter records the number of outgoing LQR packets. The count is set to 0 at the beginning of LCP negotiation.
	Receive	(Read-only) This counter records the number of incoming LQR packets. The count is set to 0 at the beginning of LCP negotiation.

PPP Network Control Protocols

PPP Network Control Protocols (NCP) are designed to assign and manage network layer addresses and configuration on Point-to-Point links. PPP allows self-configuration by providing numerous options that can be negotiated with the other peer on the link. Each of the peers describes its capabilities and requirements. NCP packets cannot be exchanged until the PPP negotiation has completed the Link Control Protocol phase, optional authentication phase, and reached the Network-Layer Protocol phase. Exactly one NCP packet can be carried in the Information field of a PPP Data Link Layer frame, with the Protocol Type field set to the corresponding value.

NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the PPP tab is no longer present. The PPP parameters are configured through the Circuit Properties window. *PPP Network Control Protocols*.

The PPP *Network Control Protocols* sub-tab shows the different network protocols that can be negotiated in the IxExplorer GUI. There are individual configuration sub-tabs for each of the protocols, described in the following sections:

- *PPP Network Control Protocol—IP (IPv4)*
- *PPP Network Control Protocols—IPv6*
- *PPP Network Control Protocols—OSI*
- *PPP Network Control Protocols—MPLS*

See the NCP—Network Control Protocols section in the 'Theory of Operation: General' of the *Ixia Platform Reference Manual* for additional information.

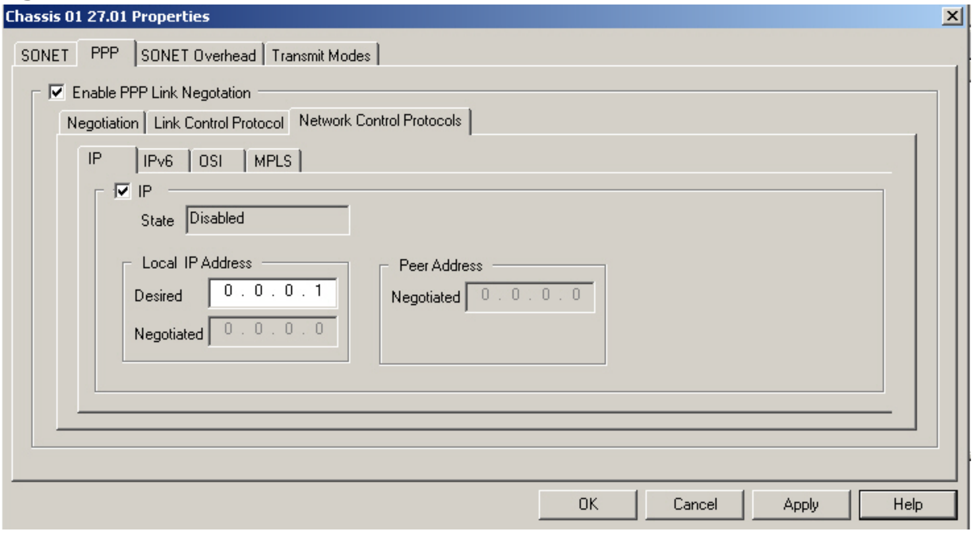
This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, then selecting the *Network Control Protocol* sub-tab.

PPP Network Control Protocol—IP (IPv4)

The PPP Network Control Protocols *IP* sub-tab is shown in *Figure:PPP Network Control Protocols—IP*. This sub-tab is used to configure the Internet Protocol Control Protocol (IPCP) on the link. IPv4 data packets may be exchanged only after the IPv4 control protocol has reached the Opened state.

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, then selecting the *IP* sub-tab.

Figure:PPP Network Control Protocols—IP



The fields and controls for this sub-tab are described in *Table:PPP Network Control Protocols—IP*.

Table:PPP Network Control Protocols—IP

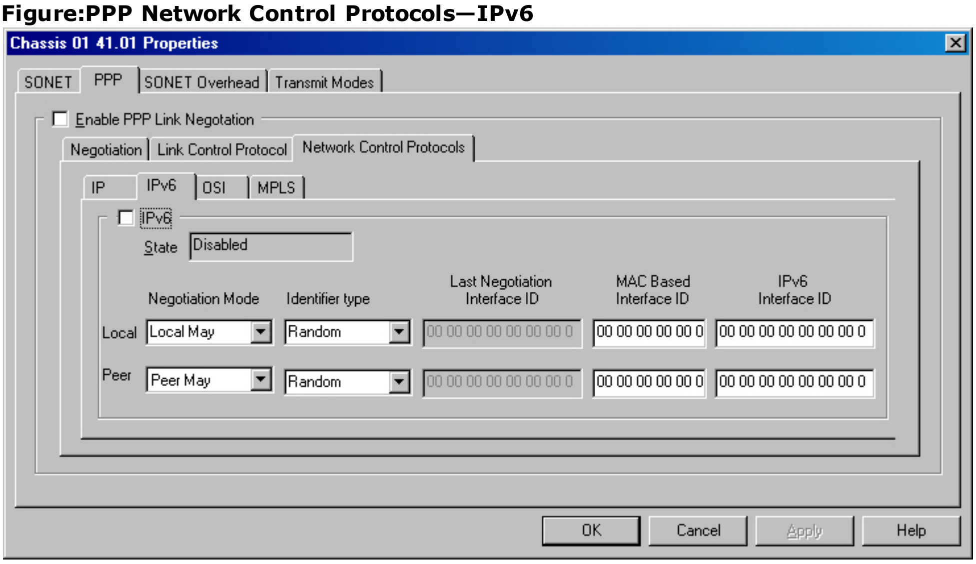
Section	Field/Control	Description
IP	(check box)	If selected, enables the IP(v4) Network Control Protocol.
	State	(Read-only) The IP(v4) protocol state. Choose one of: • Disabled • Closed • Negotiating • Opened
Local IP Address	Desired	The local port's requested IP(v4) address. This information is sent by the local peer to the remote peer, as a Configuration Option in an IPCP Configuration Request packet.
	Negotiated	The local port's negotiated IP(v4) address. The remote peer can accept the desired IPv4 address by sending a Configuration ACK packet. Or, it can provide a different IPv4 address by sending a Configuration NAK packet that includes a new address.
Peer Address	Negotiated	(Read only) The peer's negotiated IP(v4) address.

PPP Network Control Protocols—IPv6

The PPP Network Control Protocols *IPv6* sub-tab is shown in *Figure:PPP Network Control Protocols—IPv6* . This sub-tab is used to configure the Internet Protocol Version 6 Control Protocol (IPv6CP), defined in RFC 2472.

IPv6 data packets may be exchanged only after the IPv6 control protocol has reached the Opened state. This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, then selecting the *IPv6* sub-tab.

Figure:PPP Network Control Protocols—IPv6



For further information on IPv6 and a diagram of the IPv6 Interface ID, see the NCP—Network Control Protocols section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The fields and controls for this sub-tab are described in *Table:PPP Network Control Protocols—IPv6*.

Table:PPP Network Control Protocols—IPv6

<table>
<tr><th>Section</th><th>Field/Control</th><th>Description</th></tr>
<tr><td>IPv6</td><td>(check box)</td><td>If selected, enables the IPv6 Network Control Protocol.</td></tr>
<tr><td></td><td>State</td><td>(Read only). The IPv6 Network Control Protocol state. Choose one of:
• Disabled
• Closed
• Negotiating
• Opened</td></tr>
<tr><td>Local</td><td>Negotiation Mode</td><td>Before the negotiation of the Interface Identifier (IID), the node chooses a tentative Interface-Identifier.
Choose one of:
• Local May—in this mode, the local node may use the IID mode and IID value specified in the fields at the right.
• Local Must—in this mode, the local node must use the IID mode and IID value specified in the fields at the right.
• Peer Must—in this mode, the peer node will supply the local's IID.</td></tr>
<tr><td></td><td>Identifier Type</td><td>The type of Interface Identifier (IID).
It is a Configuration Option sent in the Configuration Request packet. A globally unique, non-zero Interface Identifier is preferred.
Choose one of:
• Last Negotiated—the last Interface Identifier that was negotiated for this link will be used. This value is shown in the read-only Last Negotiation IID field to the right.
• Mac Based—the Interface Identifier (IID) is derived from the MAC address). The IID 'u' (universal/local) bit will be set to zero, to indicate global scope.
• IpV6—the Interface Identifier will be based</td></tr>
</table>

Section	Field/Control	Description
		on the 64-bit EUI-64 identifier. The value is taken 'as is.' • **Random**—the interface identifier will be randomly generated. The IID 'u' (universal/local) bit will be set to zero, to indicate global scope.
	Last Negotiation Interface ID	(Read-only) (a 64-bit value) The last Interface Identifier negotiated for this link.
	Mac based Interface ID	(a 48-bit/6-octet value) It MUST be unique on the link. The MAC Interface Identifier.
	IPv6 Interface ID	(a 64-bit/8-octet value) It MUST be unique on the link. The IPv6 Interface Identifier.
Peer	Negotiation Mode	Choose one of: • **Peer May**—in this mode, the peer node may use the IID mode and IID value specified in the fields at the right. • **Peer Must**—in this mode, the peer node must use the IID mode and IID value specified in the fields at the right. • **Local Must**—in this mode, the local node will assign the IID to the peer (that is, the peer MUST send a configuration request with all 0's).
	Identifier Type	Choose one of: • Last Negotiated • Mac Based • IPv6 • Random
	Last Negotiation Interface ID	(Read-only) The last Interface Identifier negotiated for the peer.
	Mac based Interface ID	The MAC Interface Identifier for the peer.
	IPv6 Interface ID	The IPv6 Interface Identifier for the peer.

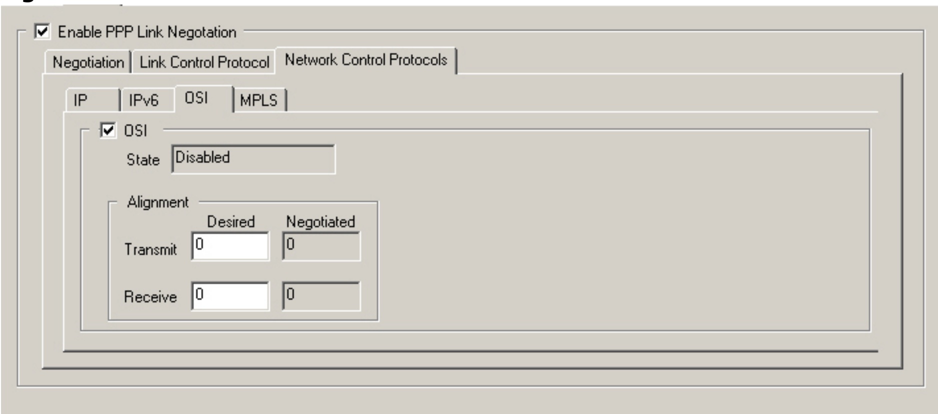
PPP Network Control Protocols—OSI

The PPP Network Control Protocols *OSI* sub-tab is shown in *Figure:PPP Network Control Protocols—OSI.* This tab is used to configure the OSI Network Layer Control Protocol (OSINLCP) Configuration Options, as specified in RFC 1377. OSI data packets may be exchanged only after the OSI control protocol has reached the Opened state.

A single configuration option is provided for this NCP protocol—*Alignment*. OSI packets (for example, IS-IS packets) often have an odd number of bytes in their data link layer headers. PPP packet headers have an even number of bytes. When an OSI packet is encapsulated in a PPP header, the difference in byte alignment may cause processing difficulties upon receipt. To improve the alignment, before transmission one to three leading bytes of zero padding (all zeroes) may be inserted between the end of the PPP header and the beginning of the OSI packet. These extra bytes must be removed upon receipt.

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, then selecting the *OSI* sub-tab.

Figure:PPP Network Control Protocols—OSI



The negotiation for the *Alignment* option is handled separately for each direction on the link, according to the following rules:

- A receiver that needs byte alignment must request this option, including the desired value.
- A receiver that does not need byte alignment must not request this option.
- A sender that wants to implement byte alignment on transmitted packets should send a Configure NAK with the desired value.
- A sender can decline negotiation and can just send the packets with its preferred alignment.
- But, once a non-zero value for alignment has been accepted by a peer, subsequent OSI packets must be sent with the negotiated alignment.

The fields and controls for this sub-tab are described in *Table:PPP Network Control Protocols—OSI*.

Table:PPP Network Control Protocols—OSI

Section	Field/Control	Description
OSI	(check box)	If selected, enables the OSI Network Control Protocol.
	State	(Read only) The OSI protocol state. One of: • Disabled • Closed • Negotiating • Opened

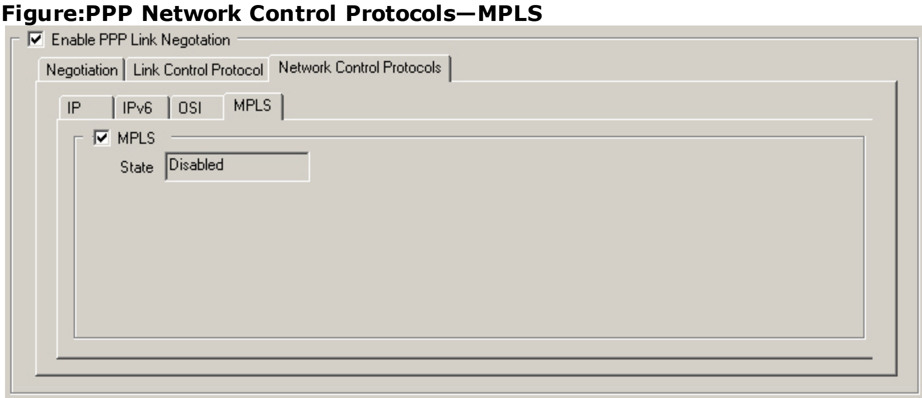
Section	Field/Control	Description
Alignment	Transmit	(in bytes) The byte alignment for Transmit: • Desired • (Read-only) Negotiated
	Receive	(in bytes) The byte alignment for Receive: • Desired • (Read-only) Negotiated

PPP Network Control Protocols—MPLS

The PPP Network Control Protocols *MPLS* sub-tab is shown in *Figure:PPP Network Control Protocols—MPLS.* A node that sends an MPLS configuration request is advertising to its peer that it supports MPLS on that link.

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, and then selecting the *MPLS* sub-tab.

Figure:PPP Network Control Protocols—MPLS



The fields and controls for this sub-tab are described in *Table:PPP Network Control Protocols—MPLS*.

Table:PPP Network Control Protocols—MPLS

Field/Control	Description
MPLS (check box)	If selected, enables the MPLS Network Control Protocol.
State	(Read only) The MPLS protocol state. One of: • Disabled • Closed • Negotiating • Opened

SONET Overhead

The SONET Overhead is configured using the following set of sub-tabs found in the *SONET Overhead* tab:

- *APS K1/K2 Sub-Tab*.
- *J0/J1 Sub-Tab*.

- *SONET Error Insertion*.

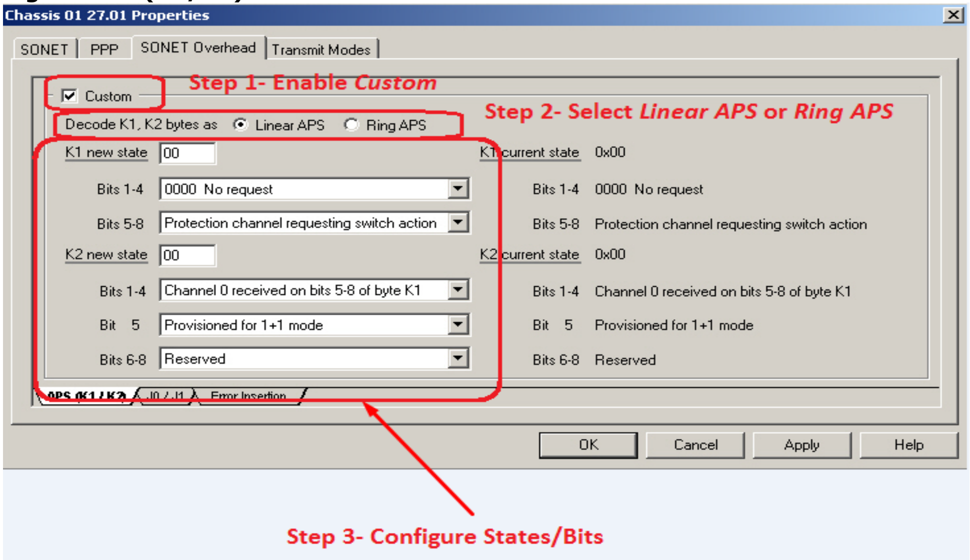
This tab is accessed by right-clicking a port, selecting the *Properties* options and then selecting the *SONET Overhead* tab.

APS K1/K2 Sub-Tab

The *APS K1/K2* sub-tab, shown in *Figure:APS (K1/K2) Sub-Tab* , provides control over the signaling used to control Automatic Protection Switching (APS) on POS modules. It provides control over the contents of transmitted K1 and K2 bytes, as described in ANSI T1.105.01-1998.

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *SONET Overhead* tab, and then selecting the *APS K1/K2* sub-tab.

Figure:APS (K1/K2) Sub-Tab.



The setting of the *Decode K1,K2 bytes as* field controls the interpretation of the remainder of the fields. The two choices are for the Linear APS and Ring APS signaling protocols. For either choice, the left-hand side of the sub-tab allows bytes to be constructed, while the right-hand side displays the current state of the K1 and K2 bytes on the link. Steps 1, 2, and 3 in *Figure:APS (K1/K2) Sub-Tab* show the sequence for configuration.

The remaining fields in this sub-tab and their usage for Linear APS is described in *Table:APS (K1/K2) Sub-Tab—Linear APS*.

Table:APS (K1/K2) Sub-Tab—Linear APS

Section	Field/Control	Description
Custom		Should be set to construct K1/K2 bytes. Otherwise, a no change condition is transmitted.
K1	K1 new state	Allows the construction of the new K1 state byte.
	Bits 1-4	Referred to as the Switch Priority or Condition Bits. Choose one of the following choices, indicated in increasing priority, with their values: • 0000–No request • 0001–Do not revert

Section	Field/Control	Description
		• 0010–Reverse request • 0011– Not used • 0100–Exerciser • 0101– Not used • 0110–Wait to restore
		• 0111– Not used • 1000–Manual switch • 1001– Not used • 1010–Signal degrade - low priority • 1011–Signal degrade - high priority • 1100–Signal fail - low priority • 1101–Signal fail - high priority • 1110–Forced switch • 1111–Lockout protection
	Bits 5-8	Indicates the channel requesting the switch action. Choose one of:
K2	K2 new state	Allows the construction of the new K2 state byte. • Protection channel requesting switch action • 1-14–working channel requesting switch action • Extra traffic channel requesting switch action
	Bits 1-4	Indicates the channel bridged onto a protection channel. Choose one of: • 0–Channel 0 received on bits 5-8 of K1 byte • 1-15–channel bridged onto protection
	Bit 5	Indicates the type of APS provisioning for the line. Choose one of: • Provisioned for 1+1 mode • Provisioned for 1:n mode
	Bits 6-8	Indicates an alarm insertion or switching dir-ectional. Choose one of: • 0–Reserved • 1–Reserved • 2–Reserved • 3–Reserved • 4–Provisioned for unidirectional switching • 5–Provisioned for bidirectional switching • 6–RDI-L • 7–AIS-L

The fields in the sub-tab as interpreted for Ring APS are described in *Table:APS (K1/K2) Sub-Tab—Ring APS*.

Table:APS (K1/K2) Sub-Tab—Ring APS

Section	Field/Control	Description
Custom		Should be set to construct K1/K2 bytes. Otherwise, a no change condition is transmitted.
K1	K1 new state	Allows the construction of the new K1 state byte.
	Bits 1-4	Choose one of the following command choices, indicated in increasing priority, with their values (and acronyms): • 0–No request (NR) • 1–Reverse request [Ring] (RR-R) • 2–Reverse request [Span] (RR-S) • 3–Exerciser [Ring] (EXER-R) • 4–Exerciser [Span] (EXER-S) • 5–Wait-to-restore (WTR) • 6–Manual switch [Ring] (MS-R) • 7–Manual switch [Span] (MS-S) • 8–Signal degrade [Ring] (SD-R) • 9–Signal degrade [Span] (SD-S) • 10–Signal degrade [Protection] (SD-P) • 11–Signal fail [Ring] (SF-R) • 12–Signal fail [Span] (SF-S) • 13–Forced switch [Ring] (FS-R) • 14–Forced switch [Span] (FS-S) • 15–Lockout [Span] or Signal Fail [Protection] (LP-S)
	Bits 5-8	The Ring ID of the node which is the destination of the message. Destination ID range is: 0 - 15.
K2	K2 new state	Allows the construction of the new K2 state byte.
	Bits 1-4	The Ring ID of the source node. Source ID range is: 0 - 15.
	Bit 5	Indicates the path for the message.Choose one of: • 0–Short path code (S) • 1–Long path code (L)
	Bits 6-8	Indicates an alarm insertion or switching type. Choose one of: • 0–Idle • 1–Bridged (Br) • 2–Bridged and Switched (Br and Sw) • 3–Extra traffic on protection (ET)

Section	Field/Control	Description
		• 4–Reserved • 5–Reserved • 6–RDI-L • 7–AIS-L

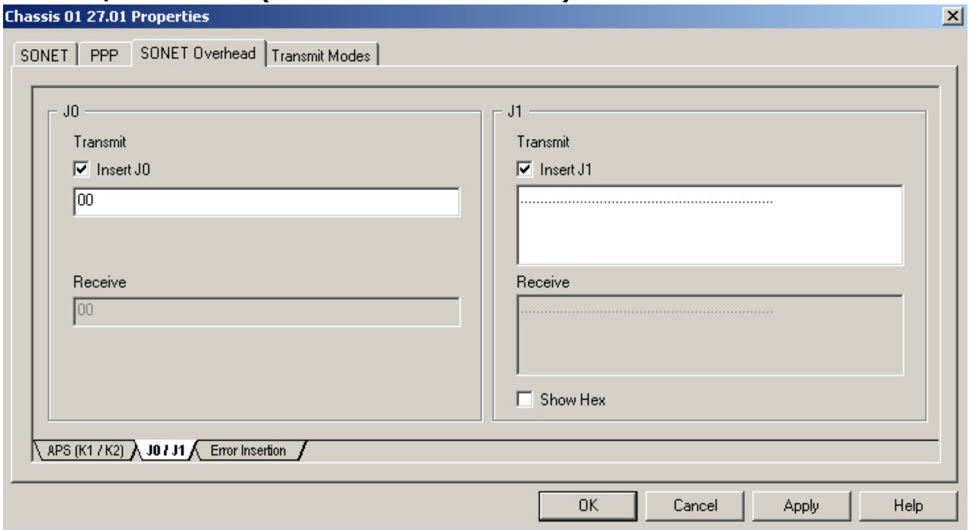
J0/J1 Sub-Tab

The *J0/J1* sub-tab allows to configure and insert J0 and J1 trace messages into the overhead for the SONET frames. The SONET Overhead *J0/J1* sub-tab is shown in *Figure:J0/J1 Sub-Tab (shown for OC-192c POS)*.

NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the J1 sub-tab is no longer present. Only the J0 sub-tab is used.

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *SONET Overhead* tab, then selecting the *J0/J1* sub-tab.

Table:J0/J1 Sub-Tab (shown for OC-192c POS)



The J0 Trace Message is part of the Section Overhead (SOH), and the J1 Trace Message is part of the Path Overhead (POH). Section Overhead is part of the overall Transport Overhead (TOH). Together, the Path Overhead and the data payload form the Synchronous Payload Envelope (SPE).

In composite SONET frames, where multiple 810-byte STS-1 (OC-1) basic frames are concatenated, as in OC-3c, OC-12c, OC-48c, and OC-192c, only the set of 27 transport overhead bytes for the first STS-1 are actually providing information, while most of the remaining TOH bytes are considered undefined and are ignored in processing the frame. Therefore, even in the large OC-192c SONET frames, only the first of the J0 and J1 trace messages in the composite frame are examined. Z0 is used in place of J0 for the remaining STS-n's, and a similar substitution is used for the J1 messages. J0 bytes contain a code that identifies the sender (for example, the serial number for a piece of equipment).

There are two different SONET framing modes, SONET and SDH, and there are different rules for each type, as described in *Table:SONET Framing Mode—Rules*.

Table:SONET Framing Mode—Rules

Framing Mode	Message Type	Length	Rules
SONET	J0	1 byte	No limitations except for length. It may be any value from 00 to FF (hex).
	J1	64 bytes	(hex) The last 2 bytes should be the Carriage Return delimiter '0x0D0A'. This signals the SONET framer that it is the end of the message. NOTE J1 is not present if Channelized mode is selected for 2.5G MSM or 10G MSM boards (on General tab).
SDH	J0	16 bytes	(hex) The MSB (most significant bit) of the first byte is set high, then the framer triggers on this value, and it is treated as the Start delimiter, signaling the start of the message. For the remaining 15 bytes, the MSB is not set, so there is no confusion about the location of the start of the message.
	J1	16 bytes	(hex) Same as for J0 (SDH rules).

The controls and fields in the *J0/J1* sub-tab are described in *Table:J0/J1 Sub-Tab*.

Table:J0/J1 Sub-Tab

Byte	Operation	Field/Control	Usage
J0	Transmit	Insert J0	Check this box to enable the insertion of J0 (Section Trace) byte(s) into the SONET frame Section Overhead.
		(J0 Field)	Enter the hex value for the J0 byte(s) according to the rules stated in *Table:J0/J1 Sub-Tab*.
	Receive		If the Rules (in *Table:SONET Framing Mode—Rules*) are followed in configuring for transmission in the upper part of the sub-tab, you will see that the Trace Message is received in the message field in the lower part of the sub-tab.
J1	Transmit	Insert J1	Check this box to enable the insertion of a J1 (Path Trace) byte into the SONET frame Path overhead. NOTE J1 is not present if Channelized mode is selected for 2.5G MSM or 10G MSM boards (on General tab).
		(J1 Field)	Enter the hex value for the J1 bytes according to the rules stated in *Table:J0/J1 Sub-Tab*.
	Receive		If the Rules (in *Table:SONET Framing Mode—Rules*) are followed in configuring for trans-

Byte	Operation	Field/Control	Usage
			mission in the upper part of the sub-tab, you will see that the Trace Message is received in the message field in the lower part of the sub-tab.
		Show Hex	Check this box to display the contents of the J1 byte in hexadecimal format, for Transmit and Receive.

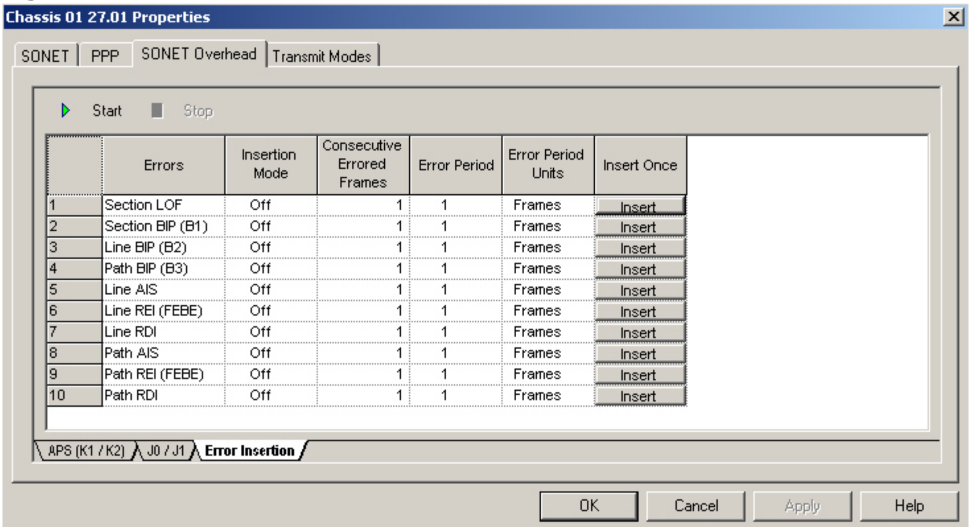
SONET Error Insertion

The SONET Overhead *Error Insertion* sub-tab contains a grid with a list of the available SONET errors which can be inserted into the data stream. The number of available error types depends on the type of POS module. The OC-48c and OC-192c POS modules have extended capability, as shown in *Figure:SONET Overhead Error Insertion Grid—OC-48c and OC-192c. The OC-12c/OC-3c POS and 10GE WAN modules are configured using the grid shown in Figure:SONET Overhead Error Insertion—OC-12c/OC-3c POS and 10GE*

This sub-tab is accessed by right-clicking a port, selecting the *Properties* options, selecting the *SONET Overhead* tab, then selecting the *Error Insertion* sub-tab.

NOTE The ATM/POS 622 has one extra error insertion option (Path LOP) not shown in the diagrams below.

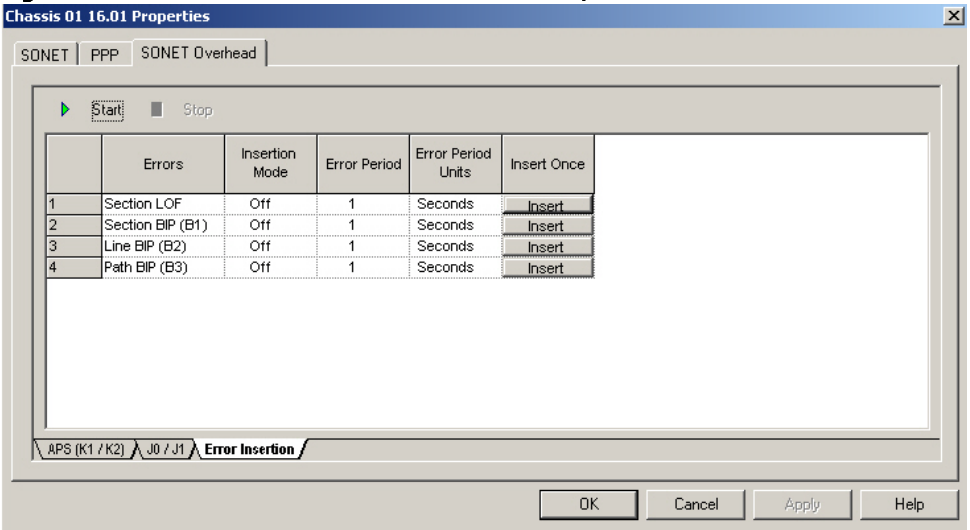
Figure:SONET Overhead Error Insertion Grid—OC-48c and OC-192c



SONET Error Insertion—Reduced Error Set

The SONET Overhead *Error Insertion* sub-tab for OC-12c/OC-3c POS (including POS 622) and 10GE WAN load modules provides a reduced set of errors that can be inserted, as shown in *Figure:SONET Overhead Error Insertion—OC-12c/OC-3c POS and 10GE WAN*

Figure:SONET Overhead Error Insertion—OC-12c/OC-3c POS and 10GE WAN



SONET Error Insertion -- Channelized Mode

The SONET Overhead *Error Insertion* sub-tab for 2.5G MSM and 10G MSM load modules (when Channelized mode is selected in Port Properties *General* tab) provides only section and line type errors that can be inserted, as shown in *Figure 19-19.SONET Overhead Error Insertion—2.5G MSM and 10G MSM (inChannelized Mode)*.

Path type errors are inserted from the SONET Overhead tab in Circuit Properties–*SONET Overhead Error Insertion*.

Figure:SONET Overhead Error Insertion—2.5G MSM and 10G MSM (in Channelized Mode)

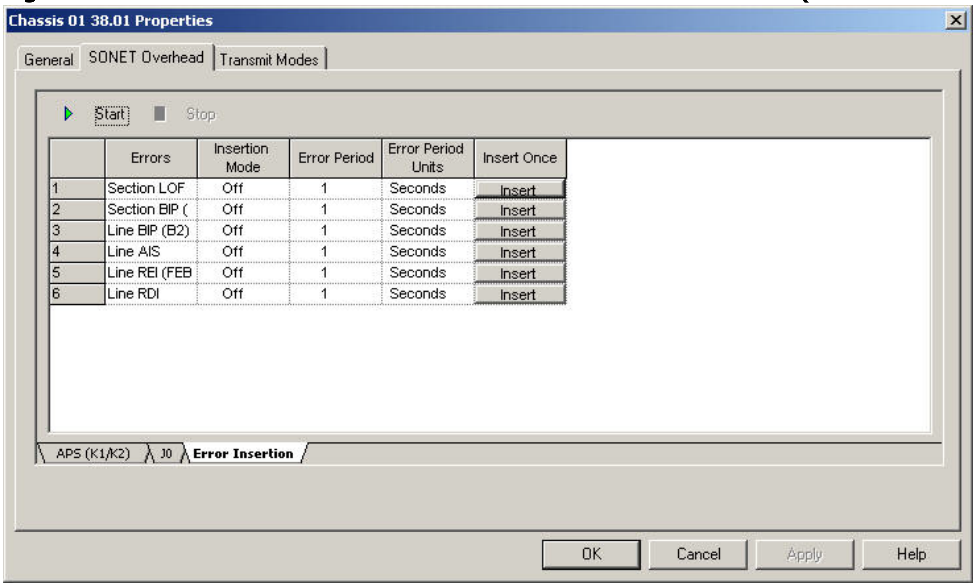
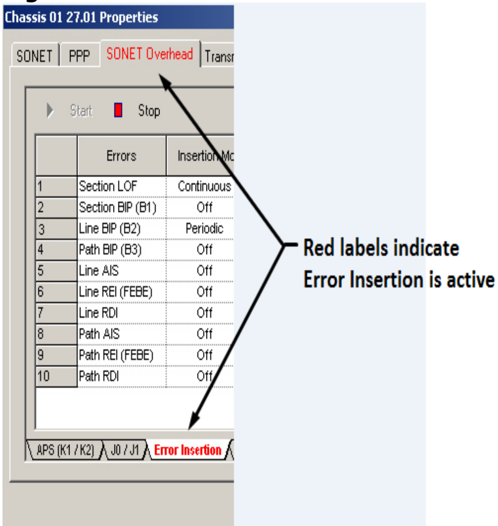


Figure:Error Insertion with Error Insertion Enabled



The columns specify how these errors are inserted into the SONET frame. The columns are described in *Table:SONET Overhead Error Insertion Sub-Tab.*

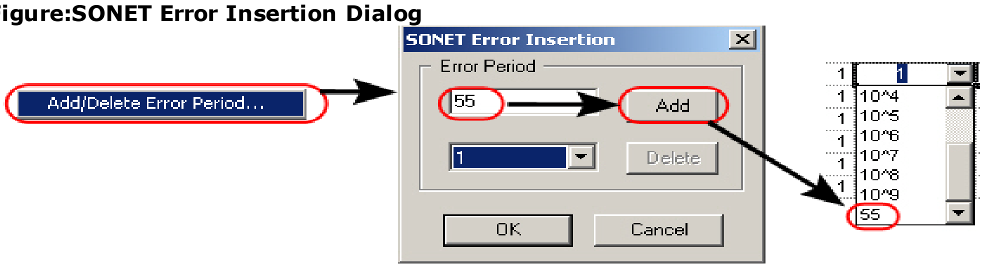
Table:SONET Overhead Error Insertion Sub-Tab

Column	Usage
Errors	List of available Errors, with one error per row: • Section LOF (Loss of Frame) • Section BIP (B1) • Line BIP (B2) • Path BIP (B3) • Line AIS (except OC-12c/OC-3c) • Line REI (except OC-12c/OC-3c) • Line RDI (except OC-12c/OC-3c) • Path AIS (except OC-12c/OC-3c) • Path REI (except OC-12c/OC-3c) • Path RDI (except OC-12c/OC-3c) • Path LOP (only ATM/POS 622)
Insertion Mode	Choose one of: • **Continuous**—this error is inserted into every SONET frame. • **Periodic**—this error is inserted at regular intervals based on a combination of the number of SONET frames in the Consecutive Errors column and the Error Period. • **Off**—no Continuous or Periodic error insertion. In this mode, the *Insert Once* button becomes available for use.
Consecutive Errored	Used for 'Periodic Insertion' mode and *Insert Once* option. Units = Frames. Choose one of: • **Periodic Insertion**—enter an integer to specify the number of SONET frames into which errors are inserted. The error insertion process is repeated at the interval specified by the Error Period.

Column	Usage
	• **Insert Once option**—enter an integer to specify the number of SONET frames with errors to be inserted once-only. (Not available for OC-12c/OC-3c and 10GE WAN.)
Error Period	Use the list or pop-up dialog to select one of the following values: • Values available when error units are in Frames: 1, 10, 10^2, 10^3, 10^4, 10^5, 10^6, 10^7, 10^8, 10^9 • Values available when error units are in Seconds: 1, 10, 10^2, 10^3, 10^4, 10^5 In combination with the Error Units, the Error Period specifies the number of frames or seconds between periodic insertions of errors. Using the pop-up dialog, custom values may be specified, as shown in *Figure:SONET Error Insertion Dialog.* For OC-12c/OC-3c POS and 10GE WAN, setting the Error Period for one error will affect all of the other errors.
Error Period Units	Choose one of: • Frames • Seconds NOTE For OC-12c/OC-3c and 10GE WAN, only the use of Seconds is supported.
Insert Once	The *Insert* button is available for use ONLY when the Insertion Mode is set to *Off*. When an *Insert* button in the *Insert Once* column is clicked, the associated error type is inserted one time. NOTE If the Insertion Mode for an error type is set to Periodic or Continuous, and the global Start button is clicked, the 'Insert' label on the corresponding button will disappear. The label will reappear when the Stop button is clicked.
	When this button is clicked, it performs a global 'Start' to turn on all of the repetitive (periodic or continuous) errors that have been configured in the grid.
	When this button is clicked, it performs a global 'Stop' to turn off all of the repetitive (periodic or continuous) errors that have been configured in the grid.

The *SONET Error Insertion* dialog is shown in *Figure:SONET Error Insertion Dialog. It is displayed by double-clicking one of the rows, or by right-clicking a row and then selecting Add/Delete Error Period....*

Figure:SONET Error Insertion Dialog



To create custom values for the Error Period, enter an integer value in the top field in the dialog. Click the *Add* button. The custom value will be displayed as the last entry in the list of values.

Transmit Modes for POS Modules

The *Transmit Modes* tab is available for OC-48c and OC-192c modules (including UNIPHY modules set to OC-192c POS) and allows to select the transmission mode for the port. It specifies the packet stream mode by default, as shown in *Figure:Transmit Modes Tab (shown for OC-192c POS/BERT)*. (This tab is not available for older OC-12c/OC-3c POS or OC-12c POS 32 MB load modules, but is available for the POS 622 (OC-12c/OC-3c POS) modules.)

NOTE

For DCC Transmit Modes
For information on the DCC feature that is displayed for some modules in the Transmit Modes section, refer to *Port Properties for DCC*.

The *Transmit Modes* tab is accessed by right-clicking a port, selecting *Properties* from the menu options, then selecting the *Transmit Modes* tab.

Figure:Transmit Modes Tab (shown for OC-192c POS/BERT)

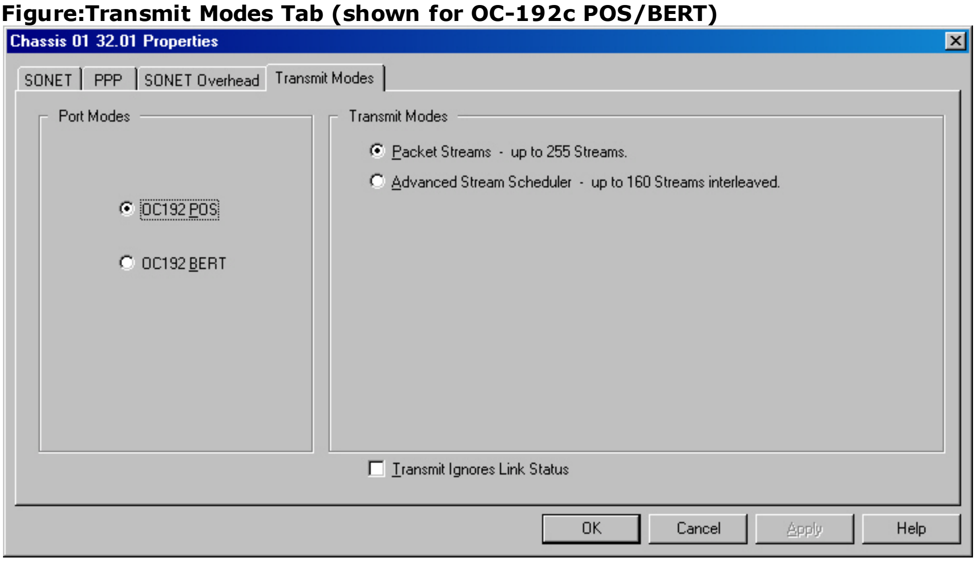


Figure:Transmit Modes Tab (shown for UNIPHY OC-192c POS)

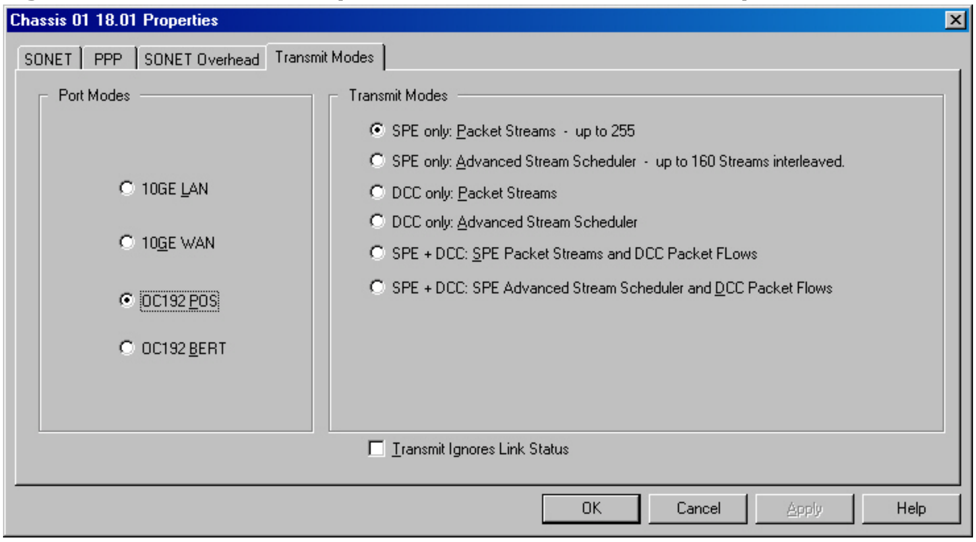
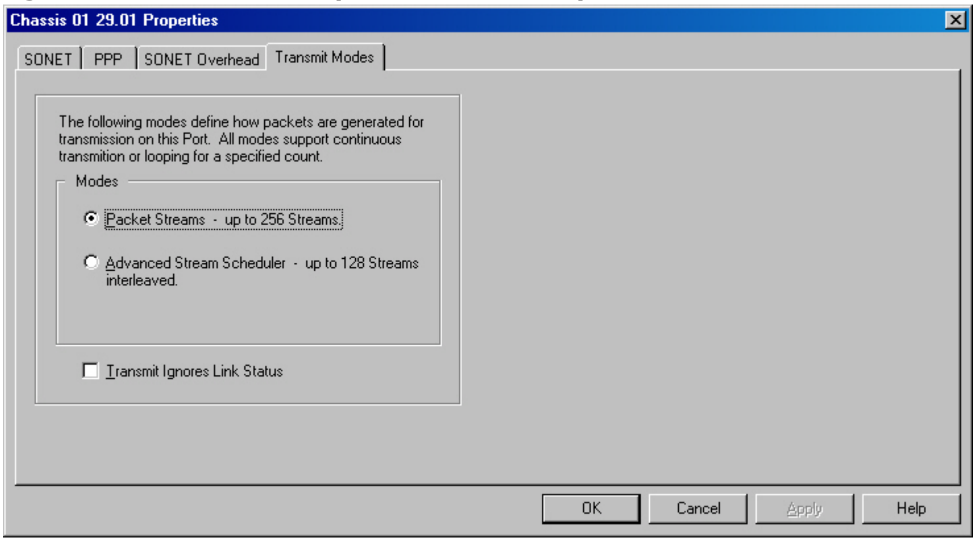


Figure:Transmit Modes Tab (shown for 622 POS)



NOTE If the Channelized mode was selected on the General tab (for 2.5G MSM and 10G MSM boards only), then the Transmit Modes tab features only the choice of modes. The transmit scheduler is available for the channelized ports under the Circuit Properties window. *Transmit Modes Circuit Properties*.

The various types of transmit modes which may be selected in the *Transmit Mode* tab are described in *Table:Transmit Modes Tab (shown for OC-192c POS/BERT/10GE WAN)*.

Table:Transmit Modes Tab (shown for OC-192c POS/BERT/10GE WAN)

Section	Mode	Description
Port Modes	10GE LAN	Selects the 10GE WAN mode of operation.*10GE LAN Port Properties*. (This option is only available on UNIPHY modules.)
	10GE WAN	Selects the 10GE WAN mode of operation. *10GE WAN Port Properties* for additional information.
	POS Operation (OC-192c POS in	Selects the OC-192c POS mode of operation.

Section	Mode	Description
	this example)	
	BERT Operation (OC-192c BERT in this example)	Selects the OC-192c BERT operating mode. *SONET-framed BERT* for additional information.
Transmit Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure up to 255 streams. For UNIPHY modules (and other modules with the DCC option) this field has 'SPE' preceding it. Refer to *Port Properties for DCC* for more information. Not available for BERT mode.
	Advanced Stream Scheduler	Sets the basic operating mode for the port to Advanced Stream Scheduler, which sets up the transmission of up to 160 interleaved packet streams on modules which support this feature. (Advanced Stream Scheduler Not available for BERT mode.) For UNIPHY modules (and other modules with the DCC option) this field has 'SPE' preceding it. Refer to *Port Properties for DCC* for more information. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Concatenated	(for OC-192c BERT mode only) *Port Properties for BERT* for additional information on BERT.
	Channelized	(for OC-192c BERT mode only) *Channelized BERT* for additional information on channelized BERT.
	SPE only: Packet Streams	This is the 'normal' packet stream mode, where streams of packets are transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 255 'normal' packet streams may be configured for the port.
	SPE only: Advanced Stream Scheduler	This is the 'normal' advanced stream scheduler mode, where up to 160 streams of packets can be interleaved and transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 160 'normal' advanced streams may be configured for the port.
	DCC only: Packet Streams	When this mode is selected, streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame.

Section	Mode	Description
		In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Packet Streams.' DCC Packet Streams and Packet Flows for additional information.
	DCC only: Advanced Stream Scheduler	When this mode is selected, interleaved streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Advanced Streams.' DCC Packet Streams and Packet Flows for additional information.
	SPE + DCC: SPE Packet Streams and DCC Packet Flows	When this mode is selected, flows of packets are transmitted over the DCC 'channel' in the SONET frame header, ***and*** 'Normal' streams of data packets are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details, 'DCC Packet Flows' are listed in addition to 'Packet Streams.' For configuring Stream Properties of the DCC Packet Flows, Stream Control is renamed to 'Frame Control.' DCC Packet Streams and Packet Flows for additional information. Protocols are not available for use with DCC packet flows.
	SPE + DCC: SPE Advanced Stream Scheduler and DCC Packet Flows	When this mode is selected, flows of packets are transmitted over the DCC 'channel' in the SONET frame header, ***and*** 'Normal' interleaved streams of data packets are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details, 'DCC Packet Flows' are listed in addition to 'Advanced Streams.' When DCC Packet Flows are selected, an additional, modified stream configuration window (and stream dialog) is presented. The DCC flow packets are created and then stored in memory

Section	Mode	Description
		until transmission is started. For configuring Stream Properties of the DCC Packet Flows, the *Stream Control* tab is renamed to *Frame Control*.DCC Packet Streams and Packet Flows for additional information. Protocols are not available for use with DCC packet flows.
	Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down.

Port Properties for BERT

Certain Ixia load modules support Bit Error Rate Testing (BERT), which is described in specifications ITU-T G.826 and CCITT O.151. The BERT feature is supported in both BERT-only load modules, as an option in combination with POS, and in 10GE XAUI and WAN modules. The OC-192c POS/BERT/10GE WAN and 10GE XAUI/BERT modules support both concatenated SONET-framed BERT and channelized BERT. Multi-rate and Single-rate Unframed BERT modules are also available.

Refer to the *Ixia Platform Reference Manual* for information about the load modules which support this feature.

The types of BERT testing available are listed below:

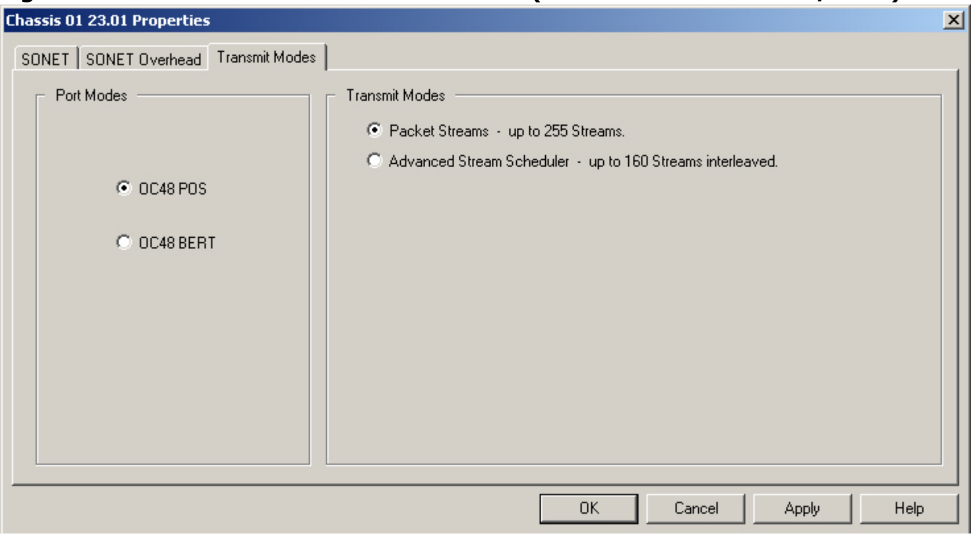
- Concatenated BERT:
  - *SONET-framed BERT*
  - *10GE XAUI and XENPAK BERT*
- *Channelized BERT*
  - *Channelized BERT*
  - *10GE XAUI/XENPAK Channelized BERT*
- *Unframed BERT*
  - *Unframed BERT—Multi-Rate*
  - *Unframed BERT—Single-Rate*

SONET-framed BERT

A *Transmit Modes* tab for a POS module with the BERT option is shown in *Figure:POS with BERT—Transmit Modes Tab (shown for OC-48c POS/BERT)*.

Transmit Modes for POS with BERT

Figure:POS with BERT—Transmit Modes Tab (shown for OC-48c POS/BERT)



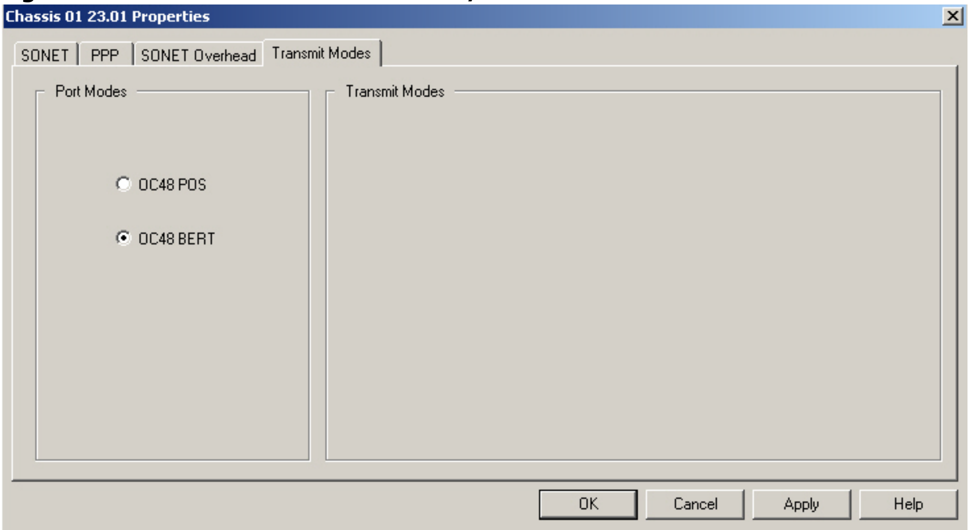
The available modes in the *Transmit Modes* tab are described in *Table:Transmit Modes Tab Controls—BERT-Capable Module*.

Table:Transmit Modes Tab Controls—BERT-Capable Module

Control	Description
OC-xx POS	Packet Over SONET mode at OC-xxc line rate.
OC-xx BERT	SONET-framed Bit Error Rate Test (BERT). Data are transmitted in patterns of bits to the receiving interface, where the data are matched to known patterns, and then monitored for mismatches to evaluate data integrity for the connection. The Pseudo-Random Binary Sequence (PRBS) is encapsulated within SONET frames.
Packet Streams	Sets the basic operating mode for the port to sequential Packet Streams. This allows to configure up to 255 streams. A stream may be programmed for continuous burst or packet generation—generating a continuous, infinite number of packets.
Advanced Stream Scheduler	Sets up the transmission of up to 160 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
BERT	Bit Error Rate Test (BERT). Data is transmitted in patterns of bits to the receiving interface, where the data are matched to known patterns, and then monitored for mismatches to evaluate data integrity for the connection.

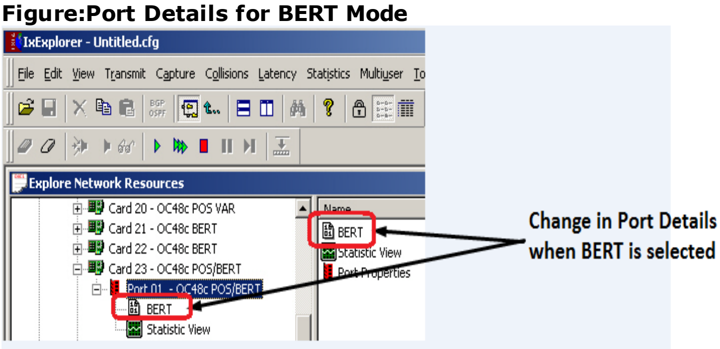
When the *OC-xx BERT* option button is selected, followed by selecting *Apply*, a new series of tabs is displayed for the Port Properties sheet, and SONET headers and CRC configuration options are unavailable. A Port Properties page for a module in BERT mode is shown in *Figure:Transmit Modes for OC-48c POS/BERT Module–with OC-48 BERT Mode Selected*.

Figure:Transmit Modes for OC-48c POS/BERT Module–with OC-48 BERT Mode Selected



When the BERT option is being used, only a subset of the standard port detail options is available in the Resources window as shown in *Figure:Port Details for BERT Mode*.

Figure:Port Details for BERT Mode



As shown above, the BERT option appears in the port details list on the right. Of the original six options in port details, only the Statistic View and Port Properties are still available for use with the BERT mode.

SONET Tab for BERT Mode

The *SONET* tab in the *Port Properties* dialog has a different format for ports in BERT mode, because many of the SONET options do not apply in this mode. The *SONET* tab for BERT mode is shown in *Figure:SONET Tab for BERT Mode (shown for OC-192c POS/BERT module with BERT selected)*. This tab is accessed by right-clicking a port, selecting *Properties* from the menu options, then selecting the *SONET* tab.

Figure:SONET Tab for BERT Mode (shown for OC-192c POS/BERT module with BERT selected)

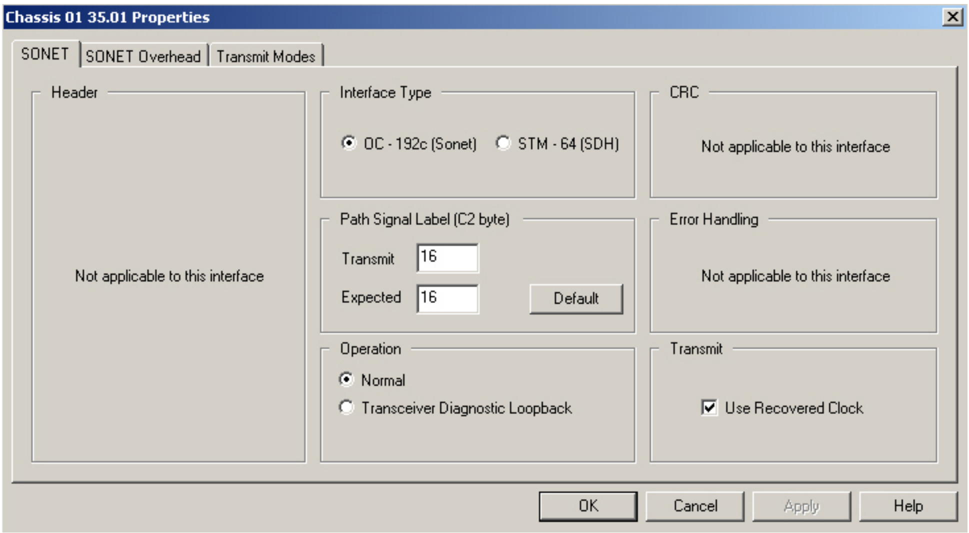
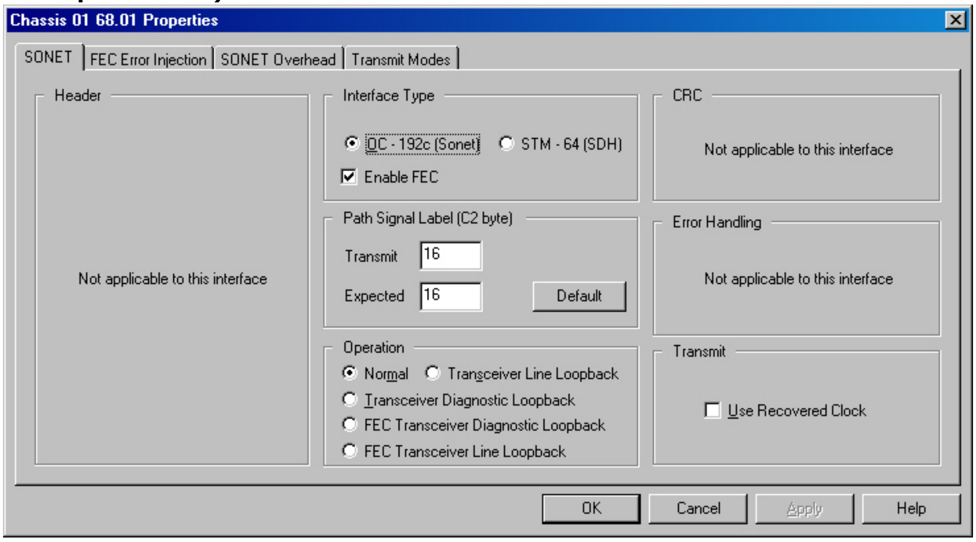


Figure:SONET Tab for BERT Mode (shown for OC-192c POS/BERT module with BERT selected and with optional FEC)



The controls in the BERT *SONET* tab are explained in *Table:Packet Over SONET (POS) with BERT—SONET Tab*.

Table:Packet Over SONET (POS) with BERT—SONET Tab

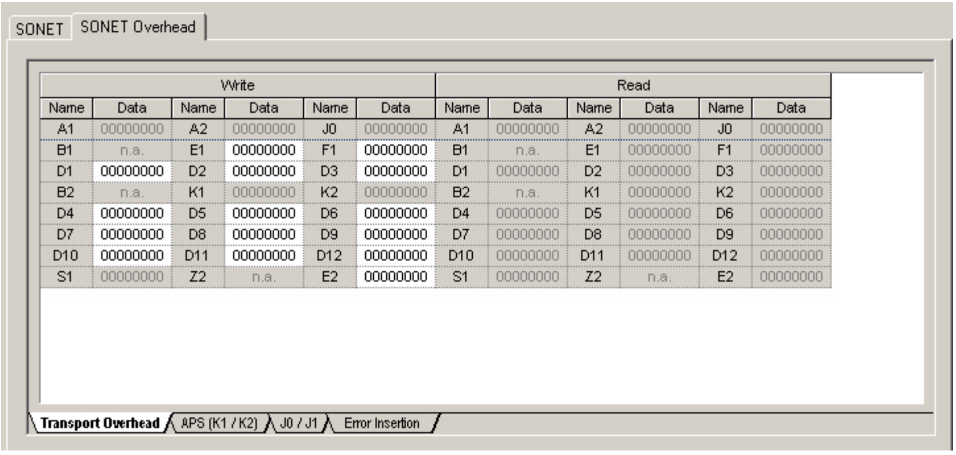
Section	Field/Control	Description
Payload Type		This section is not applicable to the BERT SONET module.
Interface Type	OC-192c (SONET)	Optical Carrier level 192 concatenated.
	STM-64 (SDH)	Synchronous transfer mode level 64.
	Enable FEC	Enables FEC information to be included with transmitted data. This also enables the features found on the *FEC Error Injections* tab page, described in *FEC Error Injection*. (Only for UNIPHY 10GE OC-192c POS/BERT with FEC options)

Section	Field/Control	Description
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted header. (Hex)
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both *Transmit* and *Expected* values to the default value (16).
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Line Loop-back	(Not available for OC-192c modules.) Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disabled if FEC is enabled.)
	FEC Transceiver Dia-gnostic Loopback	Causes the FEC information to be looped back at the transceiver. (Only for UNIPHY 10GE OC-192c POS/BERT with FEC options.)
	FEC Transceiver Line Loopback	Causes the data from the receive port to be sent out the transmit port from the FEC Framer. (Only for UNIPHY 10GE OC-192c POS/BERT with FEC options.)
CRC		This section doesn't apply to BERT POS.
Error Handling		This section doesn't apply to BERT POS.
Transmit Clock-ing	Use Recovered Clock	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal clock. Select this check box if the DUT will supply the clock signal on one of a pair of directly con-nected Ixia ports.

SONET Overhead—Transport Overhead

An additional *Transport Overhead* sub-tab for configuration of the SONET Overhead bytes for load modules running in BERT mode is shown in *Figure:Transport Overhead for BERT*. This sub-tab is accessed by right-clicking a port, selecting *Properties* from the menu options, selecting the *SONET Overhead* tab, then selecting the *Transport Overhead* sub-tab.

Figure:Transport Overhead for BERT



Write						Read					
Name	Data	Name	Data	Name	Data	Name	Data	Name	Data	Name	Data
A1	00000000	A2	00000000	J0	00000000	A1	00000000	A2	00000000	J0	00000000
B1	n.a.	E1	00000000	F1	00000000	B1	n.a.	E1	00000000	F1	00000000
D1	00000000	D2	00000000	D3	00000000	D1	00000000	D2	00000000	D3	00000000
B2	n.a.	K1	00000000	K2	00000000	B2	n.a.	K1	00000000	K2	00000000
D4	00000000	D5	00000000	D6	00000000	D4	00000000	D5	00000000	D6	00000000
D7	00000000	D8	00000000	D9	00000000	D7	00000000	D8	00000000	D9	00000000
D10	00000000	D11	00000000	D12	00000000	D10	00000000	D11	00000000	D12	00000000
S1	00000000	Z2	n.a.	E2	00000000	S1	00000000	Z2	n.a.	E2	00000000

This sub-tab allows to set the values for the D1 through D12 bytes in the Transport Overhead section of the SONET frame, by typing the values into the fields. The D1 through D3, E1, and F1 bytes are part of the Section Overhead, and the D4 through D12 bytes and E2 bytes are part of the Line Overhead.

BERT Window

NOTE For information on Channelized BERT on OC-192c POS and 10GE XAUI modules, *Channelized BERT*

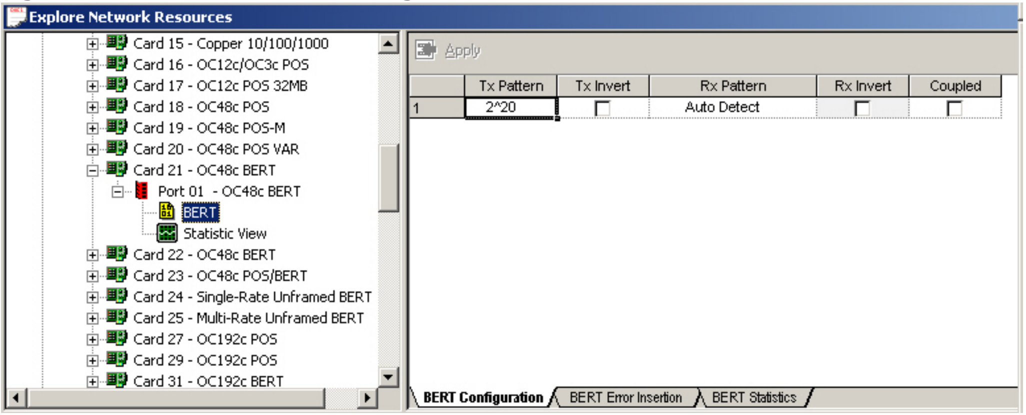
When BERT is selected in the Port Details list, the BERT window is displayed in one of the following configurations:

- For **Concatenated BERT** on OC-48c and OC-192c POS modules, and 10GE XAUI and XENPAK modules, the BERT window consists of three tab views, described in the following sections:
  - *BERT Configuration*
  - *BERT Error Insertion*
  - *BERT Statistics*
- For **Unframed BERT**, the BERT window consists of two tab views, described in the following sections:
  - *BERT Configuration*
  - *BERT Error Insertion*

BERT Configuration

The BERT properties are available for configuration in the *BERT Configuration* tab, as shown in *Figure:BERT Window—BERT Configuration*. This screen is accessed by selecting the BERT icon in the Resources window.

Figure:BERT Window—BERT Configuration



The fields on the BERT window *BERT Configuration* tab are described in *Table:BERT Window—BERT Configuration*.

Table:BERT Window—BERT Configuration

Field/Column Heading	Description
Tx Pattern	Select the pseudo-random data pattern to be transmitted. Choose one of: • 2^7 (XAUI Concatenated BERT ONLY) • 2^9 (XAUI Concatenated BERT ONLY) • 2^11 • 2^15 • 2^20 • 2^23 • 2^31 • All Zero • Alternating One/Zero • LowFreq (XAUI Concatenated BERT **ONLY**)— The Low frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.2), tests low frequency random jitter and PLL tracking error. • MixedFreq (XAUI Concatenated BERT **ONLY)** —The Mixed frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.3), tests the combination of random jitter and deterministic jitter. • Continuous Random (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CRPAT (Continuous Random Pattern), defined in IEEE 802.3 Annex 48A (48A.4). It is used to measure jitter at the component or system level—providing broad spectral content and minimal peaking. • Continuous Jitter (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CJPAT (Continuous Jitter Pattern), defined in IEEE 802.3 Annex 48A (48A.5). It is used to measure receiver jitter in

Field/Column Heading	Description
	response to large, instantaneous phase jumps.
Tx Invert	If enabled, the selected data transmission pattern is sent in inverted order.
Rx Pattern	Select the pseudo-random data pattern against which the received data will be matched. Choose one of: • 2^7 (XAUI Concatenated BERT ONLY) • 2^9 (XAUI Concatenated BERT ONLY) • 2^11 • 2^15 • 2^20 • 2^23 • 2^31 • All Zero • Alternating One/Zero • LowFreq (XAUI Concatenated BERT **ONLY**)— The Low frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.2), tests low frequency random jitter and PLL tracking error. • MixedFreq (XAUI Concatenated BERT **ONLY)** —The Mixed frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.3), tests the combination of random jitter and deterministic jitter. • Continuous Random (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CRPAT (Continuous Random Pattern), defined in IEEE 802.3 Annex 48A (48A.4). It is used to measure jitter at the component or system level—providing broad spectral content and minimal peaking. • Continuous Jitter (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CJPAT (Continuous Jitter Pattern), defined in IEEE 802.3 Annex 48A (48A.5). It is used to measure receiver jitter in response to large, instantaneous phase jumps. • Auto Detect—In Auto Detect mode, the receiving interface will attempt to match the incoming data pattern with known patterns, including those listed above and user-defined patterns.
Rx Invert	If enabled, the incoming data will be matched against the inverted form of selected receive pattern. In Auto Detect mode, this option is disabled.
Coupled	The Transmit and Receive interfaces are coupled. When this option is selected, the *Tx Pattern* field information will be automatically copied to the *Rx Pattern* field, including inverted pattern status. Any additional changes to either of these patterns (Tx or Rx) will be automatically

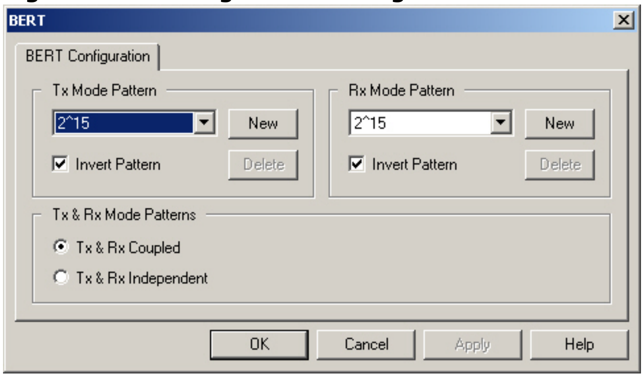
Field/Column Heading	Description
	reflected in pattern for the other interface.

Double-click in the BERT Configuration window to display the *BERT Configuration* dialog, described in *BERT Configuration Dialog*.

BERT Configuration Dialog

The *BERT Configuration* dialog is shown in *Figure:BERT Configuration Dialog*. This dialog is accessed by selecting the *BERT* icon in the Resources window, then double-clicking the BERT stream in the right side of the IxExplorer GUI.

Figure:BERT Configuration Dialog



The *BERT Configuration* dialog permits more detailed configuration of the Tx and Rx patterns. The fields and controls in this dialog are described in *Table:BERT Dialog—BERT Configuration*.

Table:BERT Dialog—BERT Configuration

Section	Field/Control	Description
Tx Mode Pattern	Pattern field	Select the pseudo-random data pattern to be transmitted. Choose one of: • 2^7 (XAUI Concatenated BERT **ONLY**) • 2^9 (XAUI Concatenated BERT **ONLY**) • 2^11 • 2^15 • 2^20 • 2^23 • 2^31 • All Zero • Alternating One/Zero • LowFreq (XAUI Concatenated BERT **ONLY**)—The Low frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.2), tests low frequency random jitter and PLL tracking error.
Tx Mode Pattern (cont'd)	Pattern field (cont'd)	• MixedFreq (XAUI Concatenated BERT **ONLY)**—The Mixed frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.3),

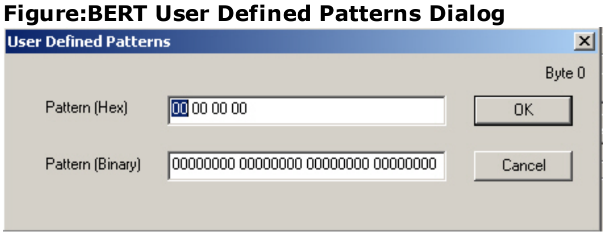
Section	Field/Control	Description
		tests the combination of random jitter and deterministic jitter. • Continuous Random (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CRPAT (Continuous Random Pattern), defined in IEEE 802.3 Annex 48A (48A.4). It is used to measure jitter at the component or system level—providing broad spectral content and minimal peaking. • Continuous Jitter (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CJPAT (Continuous Jitter Pattern), defined in IEEE 802.3 Annex 48A (48A.5). It is used to measure receiver jitter in response to large, instantaneous phase jumps.
	Invert Pattern	If enabled, the selected data transmission pattern is sent inverted.
	New	When this button is clicked, the *User Defined Patterns* dialog will open. *BERT User Defined Patterns Dialog*.
	Delete	When this button is clicked, the selected Transmit pattern will be deleted.
Rx Pattern		Select the pseudo-random data pattern against which the received data will be matched. Choose one of: • 2^7 (XAUI Concatenated BERT ONLY) • 2^9 (XAUI Concatenated BERT ONLY) • 2^11 • 2^15 • 2^20 • 2^23 • 2^31 • All Zero • Alternating One/Zero • LowFreq (XAUI Concatenated BERT **ONLY**)—The Low frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.2), tests low frequency random jitter and PLL tracking error. • MixedFreq (XAUI Concatenated BERT **ONLY)**—The Mixed frequency test pattern, defined in IEEE 802.3 Annex 48A (48A.3), tests the combination of random jitter and deterministic jitter.

Section	Field/Control	Description
		• Continuous Random (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CRPAT (Continuous Random Pattern), defined in IEEE 802.3 Annex 48A (48A.4). It is used to measure jitter at the component or system level, providing broad spectral content and minimal peaking. • Continuous Jitter (XAUI Concatenated BERT **ONLY**)—This pattern is also known as CJPAT (Continuous Jitter Pattern), defined in IEEE 802.3 Annex 48A (48A.5). It is used to measure receiver jitter in response to large, instantaneous phase jumps. • Auto Detect—In Auto Detect mode, the receiving interface will attempt to match the incoming data pattern with known patterns, including those listed above and user-defined patterns.
	Invert Pattern	If enabled, the incoming data will be matched against the inverted form of selected receive pattern. In Auto Detect mode, this option is disabled.
	New	When this button is clicked, the *User Defined Patterns* dialog will open. *BERT User Defined Patterns Dialog*.
	Delete	When this button is clicked, the selected Receive pattern will be deleted.
Tx & Rx Mode Patterns	Tx & Rx Coupled	The Transmit and Receive interfaces are coupled. When this option is selected, the *Tx Pattern* field information will be automatically copied to the *Rx Pattern* field, including inverted pattern status. Any additional changes to either of these patterns (Tx or Rx) will be automatically reflected in pattern for the other interface.
	Tx & Rx Independent	The Transmit and Receive interfaces are not coupled.

BERT User Defined Patterns Dialog

This dialog is accessed by selecting one of the *New* buttons in the *BERT* dialog.

Figure:BERT User Defined Patterns Dialog

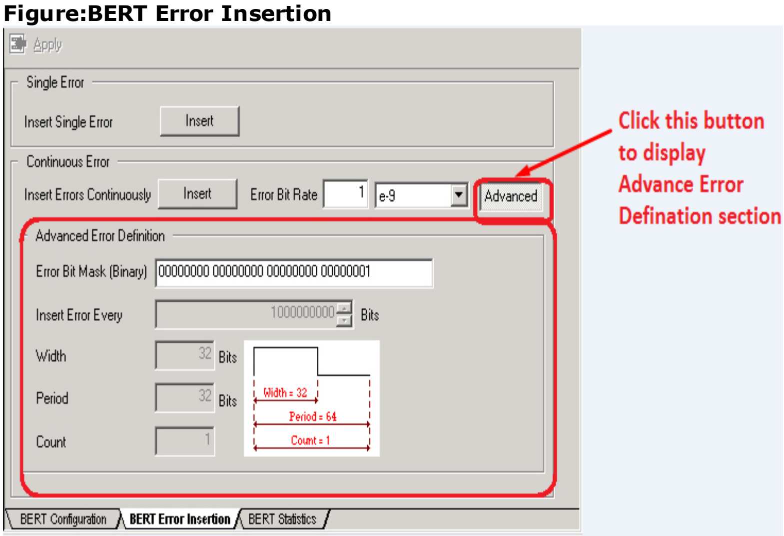


This dialog allows to create unique 32-bit data patterns, using either hexadecimal or binary format. If the Pattern is being modified in the *Pattern (Hex)* field, the current byte will be displayed in the upper right-hand corner.

BERT Error Insertion

The *BERT Error Insertion* tab of the BERT window allows for the insertion of BERT errors, as shown for an OC-48c BERT module in *Figure:BERT Error Insertion*. This tab is accessed by selecting the *BERT* icon in the Resources window, and then selecting the *BERT Error Insertion* tab.

Figure:BERT Error Insertion



This tab allows for the addition of BERT errors into the data stream, for detection by the receiving interface. The fields are described in *Table:BERT Error Insertion*.

Table:BERT Error Insertion

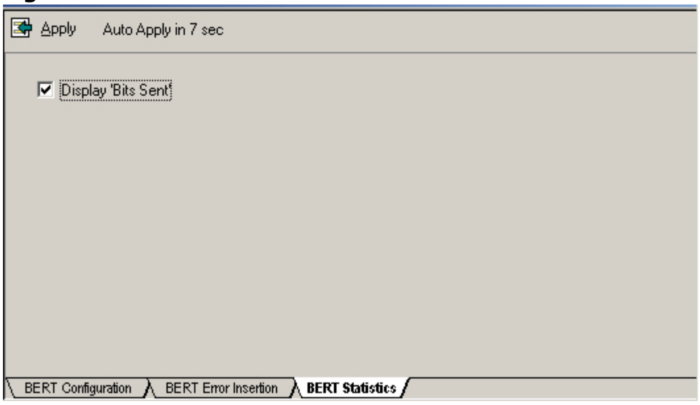
Section	Field/Control	Description
Single Error	Insert Single Error	When clicked, inserts one BERT error.
Continuous Error	Insert Errors Continuously	When clicked, inserts BERT errors continuously, at the rate selected in the *Error Bit Rate* field.
	Error Bit Rate - integer	Enter the integer portion of the error bit rate value, which will be multiplied by the selected exponential value in the list. The valid range is 1 to 32.
	Error Bit Rate - exponent	Select the exponential multiplier for the error bit rate value. One of: • e-2 (= 10^{-2}) • e-3 (= 10^{-3}) • e-4 (= 10^{-4}) • e-5 (= 10^{-5}) • e-6 (= 10^{-6}) • e-7 (= 10^{-7}) • e-8 (= 10^{-8}) • e-9 (= 10^{-9})

Section	Field/Control	Description
		• e-10 (= 10^{-10}) • e-11 (= 10^{-11}) • User Defined—when this option is selected, all of the fields in the *Advanced Error Definition* section (below) are active and can be configured.
	Advanced	Pressing this button displays the Advanced Error Definition section of this dialog.
Advanced Error Definition	Error Bit Mask (Binary)	This bit mask consists of 4 groups of 8 bits. It determines which bits in a 32-bit word are errored.
	Insert Error Every (Bits)	(Read-Only except when User-Defined Error Bit Rate is being used.) This value is directly linked to the entry in the *Error Bit Rate Multiplier* field. In User Defined mode, the value can be changed in 32-bit increments. Min. value = 32 bits.
	Width	(Read-Only except when User Defined Error Bit Rate is being used.) The width of the bit pattern.
	Period	(Read-Only except when User Defined Error Bit Rate is being used.) The length (in bits) of a period.
	Count	(Read-Only except when User Defined Error Bit Rate is being used.) The number of times the period is to be repeated.
	Diagram	Example diagram showing the relationship among the Pattern Width, Period, and Count.

BERT Statistics

The *BERT Statistics* tab is accessed by selecting the *BERT* icon in the Resources window, and then selecting the *BERT Statistics* tab.

Figure:BERT Statistics Tab



The *BERT Statistics* tab has one option available. When the *Display Bits Sent* check box is enabled, the *Bits Sent* statistics counter will be displayed in the Statistic View for this port. See *Statistic View*, for more information on the Statistic View.

Unframed BERT

Unframed BERT operates at the physical layer, Layer 1 (Physical Layer) of the OSI model, without the addition of Layer 2 encapsulation (such as Ethernet or SONET). The Pseudo-Random Binary Sequence (PRBS) is sent in raw form, output directly as a serial bit stream. The standard BERT windows for BERT configuration and BERT Error Insertion are available, with the following PRBS patterns: 2^11, 2^15, 2^20, 2^23, and Alternate One/Zero.

SONET-framed BERT uses a standard grouping of data bits called a 'Block,' and data is transmitted at a rate of 8,000 blocks per second. For OC-3c, OC-12c, and OC-48c speeds with unframed BERT, 'virtual blocks' are used for grouping receive statistics. Other rates do not collect block-level statistics. ITU G.826 statistics are collected on the received bits. The *Bits Sent* statistic is enabled by default, so no tab for this purpose is present in the BERT window.

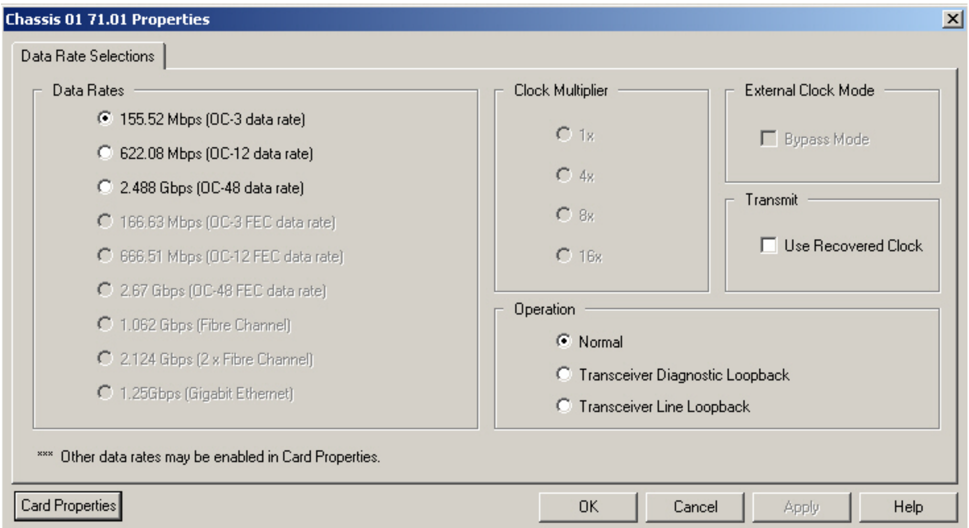
The types of Ixia unframed bit error rate testing load modules available are:

- *Unframed BERT—Multi-Rate*
- *Unframed BERT—Single-Rate*

Unframed BERT—Multi-Rate

The Multi-Rate Unframed Bert load module supports a large number of data rates. The *Port Properties* dialog allows selection of the data rate, as shown in *Figure:Unframed BERT—Multi-Rate*.

Figure:Unframed BERT—Multi-Rate



The fields and controls in this dialog are described in *Table:Unframed BERT—Multi-Rate*

Table:Unframed BERT—Multi-Rate

Section	Field/Control	Description
Data Rates	Choose one of: • 155.52 Mbps (OC-3 data rate) • 622.08 Mbps (OC-12 data rate) • 2.488 Gbps (OC-48 data rate)	Select the data rate to be used.

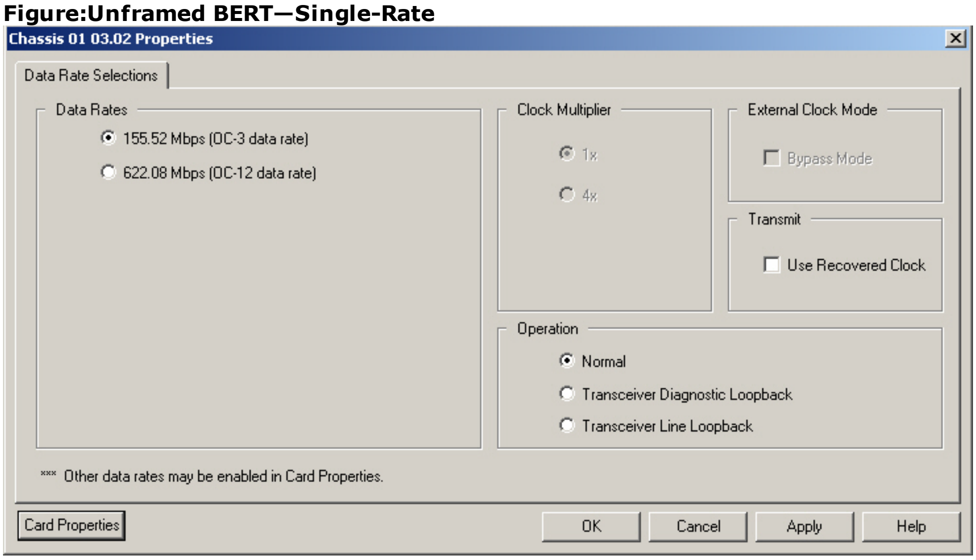
Section	Field/Control	Description
	The following options must first be selected in the Clock Options dialog: (See *Unframed BERT—Clock Options*.) 166.63 Mbps (OC-3 FEC data rate) 666.51 Mbps (OC-12 FEC data rate) 2.67 Gbps (OC-48 FEC data rate) 1.062 Gbps (Fibre Channel) 2.124 Gbps (2 x Fibre Channel) 1.25 Gbps (Gigabit Ethernet)	
	Card Properties	Press this button to display the *Clock Options* tab in the *Card Properties* dialog for this load module. See *Unframed BERT—Clock Options* for additional information.
Clock Multiplier	Select one of: • 1x • 4x	Only for use with the External Clock option which may be selected in the Card Properties–Clock Options dialog. The clock-in signal will be used to control the rate of data transmission for rates not available in the data rate dialog. The clock-in signal will be multiplied by the selected multiplier value. The Clock Multiplier option is not available in bypass mode.
External Clock Mode	Bypass Mode	Only for use with the External Clock option which may be selected in the Card Properties –Clock Options dialog. The external clock signal bypasses the transceiver, allowing a wider range for the clock input.
Transmit	Use Recovered Clock	Select this check box to enable use of the clock signal from the DUT.
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the bit stream to be looped back at the transceiver.
	Transceiver Line Loopback	Causes the bit stream received by the port to be sent back out to the sending port, creating an echo of the link partner. These bits can

Section	Field/Control	Description
		also be captured.

Unframed BERT—Single-Rate

Single-Rate unframed BERT testing operates in the same manner as multi-rate, but without the support for multiple types of data rates. The *Data Rate Selections* dialog for Single-Rate Unframed BERT is shown in *Figure:Unframed BERT—Single-Rate*.

Figure:Unframed BERT—Single-Rate



The fields and controls in this dialog are a subset of the fields included in the Unframed BERT Multi-Rate dialog and are described in *Table:Unframed BERT—Single-Rate*.

Table:Unframed BERT—Single-Rate

Section	Field/Control	Description
Data Rates	Choose one of: • 155.52 Mbps (OC-3 data rate) • 622.08 Mbps (OC-12 data rate)	Select the rate to be used.
	Card Properties	Press this button to display the *Clock Options* tab in the *Card Properties* dialog for this load module. See *Unframed BERT—Clock Options*for additional information.
Clock Multiplier	Select one of: • 1x • 4x	Only for use with the External Clock option which may be selected in the Card Properties–Clock Options dialog. The Clock Multiplier option is not available in bypass mode.
External Clock Mode	Bypass Mode	N/A
Transmit	Use Recovered Clock	Select this check box to

Section	Field/Control	Description
		enable use of the clock signal from the DUT.
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the bit stream to be looped back at the trans-ceiver.
	Transceiver Line Loopback	Causes the bit stream received by the port to be sent back out to the sending port, creating an echo of the link partner. These bits can also be captured.

Unframed BERT—Clock Options

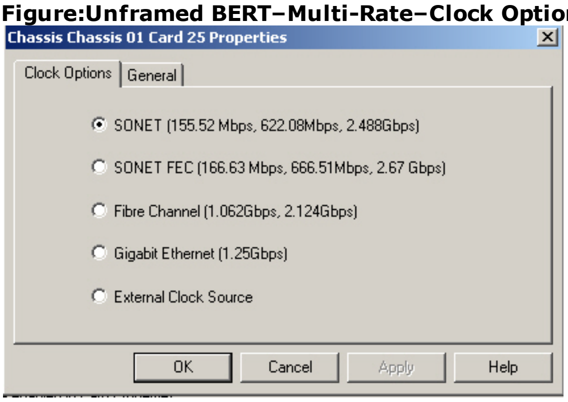
When the *Card Properties* button on the Unframed BERT Data Rate Selection page is clicked, the applicable *Clock Options* tab in the Unframed BERT *Card Properties* dialog is displayed. The two types of *Clock Options* tabs are:

- *Unframed BERT–Multi-Rate–Clock Options*
- *Unframed BERT–Single-Rate–Clock Options*

Unframed BERT–Multi-Rate–Clock Options

The Unframed BERT Multi-Rate *Clock Options* tab is shown in *Figure:Unframed BERT–Multi-Rate–Clock Options*.

Figure:Unframed BERT–Multi-Rate–Clock Options



Only one of the five option items may be selected and activated at one time. The options available in this tab are described in *Table:Unframed BERT–Multi-Rate–Clock Options*.

Table:Unframed BERT–Multi-Rate–Clock Options

Options	Description
SONET (155.52 Mbps, 622.08 Mbps, 2.488 Gbps)	Enables the SONET group of data rates in the Data Rate Selection (155.52 Mbps/OC-3c, 622.08 Mbps/OC-12c, and 2.488 Gbps/OC-48c) in the *Port Properties* dialog.
SONET FEC (166.63 Mbps, 666.51 Mbps, 2.67 Gbps)	Enables the SONET Forward Error Correction (FEC) group of data rates in the Data Rate Selection in the *Port Prop-*

Options	Description
	erties dialog. *Forward Error Correction* for additional information on FEC.)
Fibre Channel (1.062 Gbps, 2.124 Gbps)	Enables the Fibre Channel group of data rates in the Data Rate Selection in the *Port Properties* dialog: Fibre Channel base rate, and 2 times the Fibre Channel base rate. (The Fibre Channel **protocol** is not used in an unframed BERT application.)
Gigabit Ethernet (1.25 Gbps)	Enables the Gigabit Ethernet rate in the Data Rate Selection in the *Port Properties* dialog.
External Clock Source	Enables the use of an external timing source (which is connector to the module's Clock In connector). When this option is selected, only timing options may be selected in the Data Rate Selection in the *Port Properties* dialog (data rate selections are dimmed).

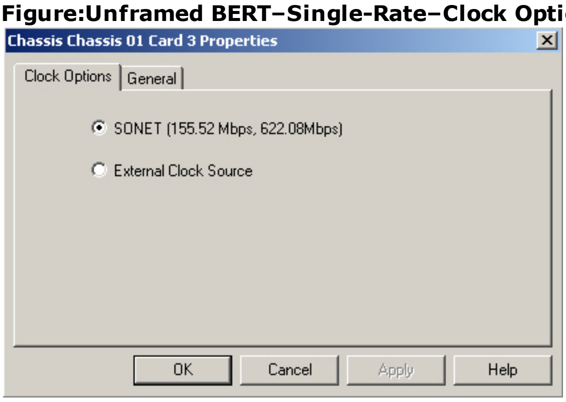
Forward Error Correction

FEC uses complex mathematical algorithms to encode data before transmission over optical circuits and decode it upon receipt. This technique is used to extend the usable (relatively error-free) distance between transmit and receive optics, without resorting to higher-powered lasers.

Unframed BERT–Single-Rate–Clock Options

When the *Card Properties* button on the Single-Rate Data Rate Selection page is clicked, the Unframed BERT *Card Properties* tab is displayed, as shown in *Figure:Unframed BERT–Single-Rate–Clock Options*.

Figure:Unframed BERT–Single-Rate–Clock Options



Only one of the two option items may be selected and activated at one time. The options available in this tab are described in *Table:Unframed BERT–Single-Rate–Clock Options*.

Table:Unframed BERT–Single-Rate–Clock Options

Options	Description
SONET (155.52 Mbps, 622.08 Mbps)	Enables the SONET group of data rates in the Data Rate Selection (OC-3c, OC-12c) in the *Port Properties* dialog.
External Clock Source	When this option is selected, only timing options may be selected in the Data Rate Selection (data rate selections

Options	Description
	are dimmed) in the *Port Properties* dialog.

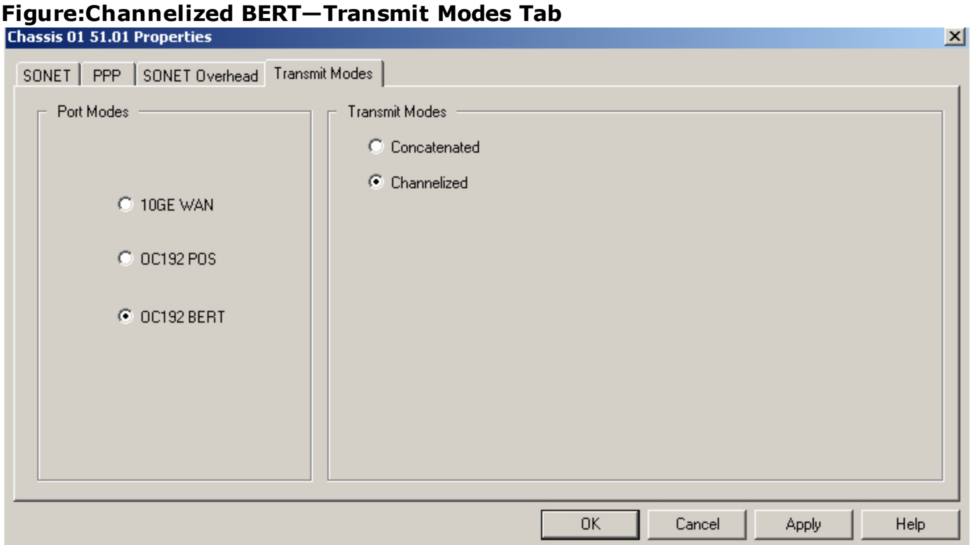
Channelized BERT

Channelized BERT is available as an option on some of the OC-192c and 10GE XAUI load modules.

The OC-192c data rate is evenly divided across four OC-48c channels. Each of the STS-48 channels may be subdivided further into four OC-12c channels, for a maximum of 16 channels. The different types of channels may be used together in combination, such as two OC-48c channels plus eight OC-12c channels.

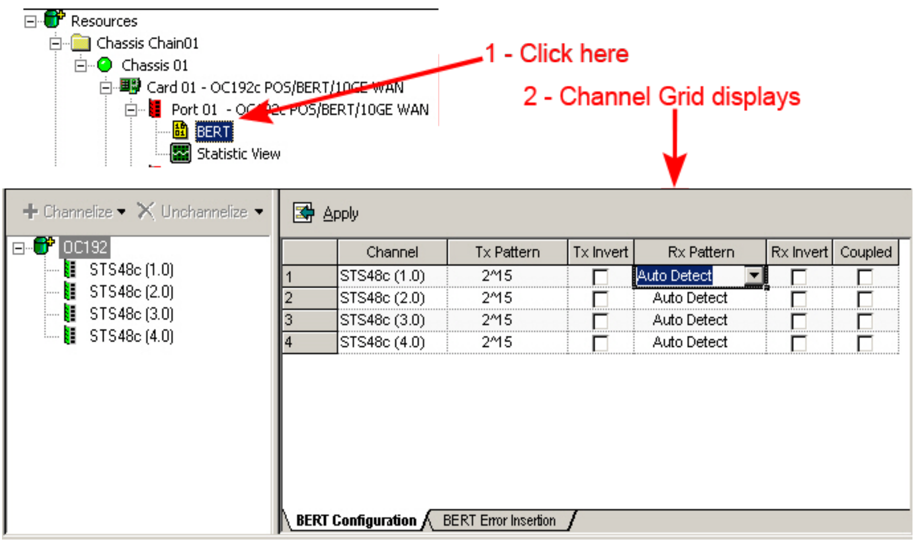
The Channelized BERT mode is selected in the *Transmit Modes* tab, as shown in *Figure:Channelized BERT—Transmit Modes Tab*.

Figure:Channelized BERT—Transmit Modes Tab



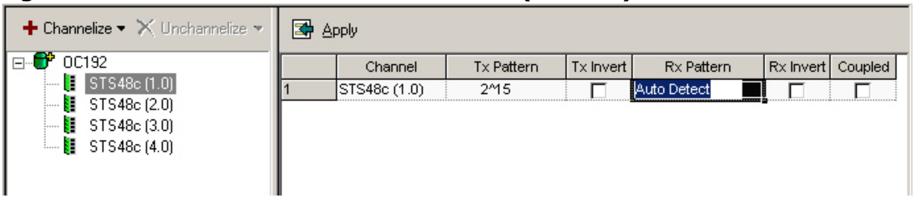
When the *OC-192c BERT* option is selected, two transmit modes are available: Concatenated, and Channelized. Select *Channelized*, and then select *BERT* under the port name in the Resources tree (left pane) or in the Port Details list (right pane). The BERT window will open as shown in *Figure:Channelized BERT Window*.

Figure:Channelized BERT Window



The OC-192c line capacity is divided into four STS48c channels, numbered 1.0 through 4.0. When one of the STS48c channels is selected in the list at the left, the grid in the far right pane displays information for only that channel, as shown in *Figure:Channel Grid View for One Channel (STS48c)*, and the *Channelize* button is active.

Figure:Channel Grid View for One Channel (STS48c)



Clicking the *Channelize* button for a selected STS48c channel causes that channel to be sub-divided into four STS12c channels, as shown in *Figure:Channelized BERT Configuration Tab (STS48c to STS12c)*.

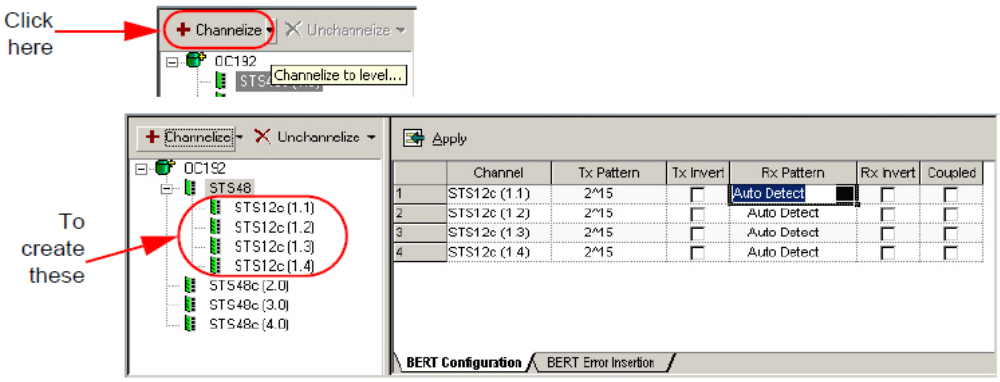
After the channels are defined, the remaining steps for setting up channelized BERT testing are:

1. *OC-192c Channelized BERT Configuration*—Configure the background BERT pattern to be transmitted.
2. *OC-192c Channelized BERT Error Insertion*—Configure the errors to be inserted into the BERT pattern.
3. *OC-192c Channelized BERT Statistics*—View the BERT statistics.

OC-192c Channelized BERT Configuration

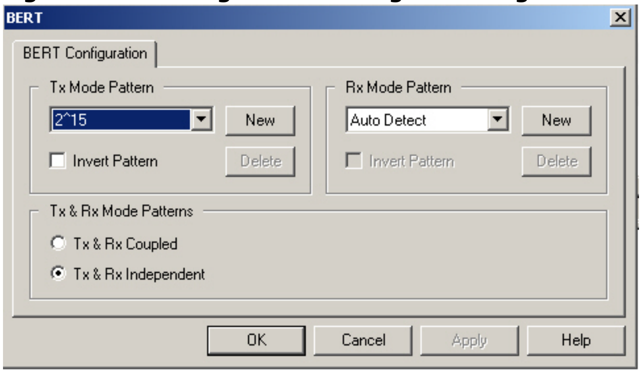
The BERT transmit and receive patterns are selected in the *BERT Configuration* tab, which is displayed in *Figure:Channelized BERT Configuration Tab (STS48c to STS12c)*.

Figure:Channelized BERT Configuration Tab (STS48c to STS12c)



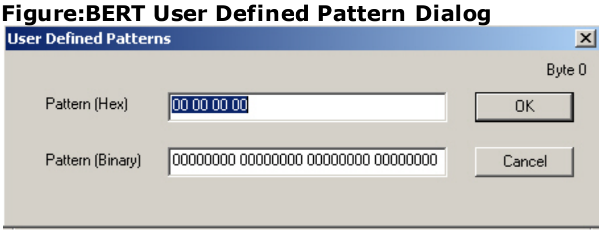
Double-clicking one of the channel rows in the grid displays the *BERT Configuration* dialog, shown in *Figure:BERT Configuration Dialog for a Single Channel*.

Figure:BERT Configuration Dialog for a Single Channel



To create a user-defined bit pattern, click the *New* button to display the *User Defined Pattern* dialog, shown in *Figure:BERT User Defined Pattern Dialog*.

Figure:BERT User Defined Pattern Dialog

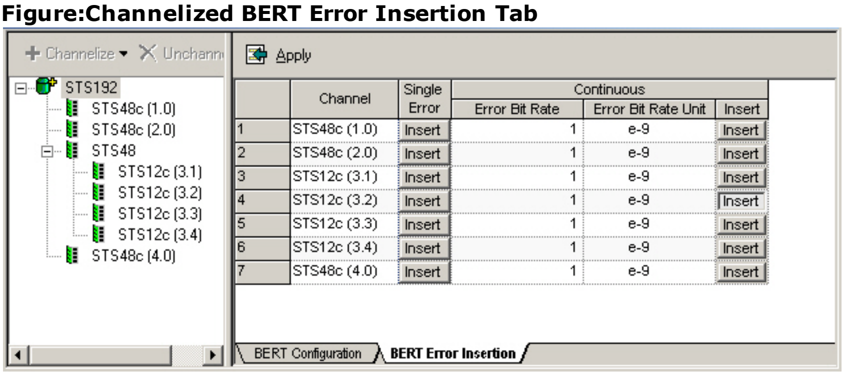


This dialog allows to create unique 32-bit data patterns, using either hexadecimal or binary format.

OC-192c Channelized BERT Error Insertion

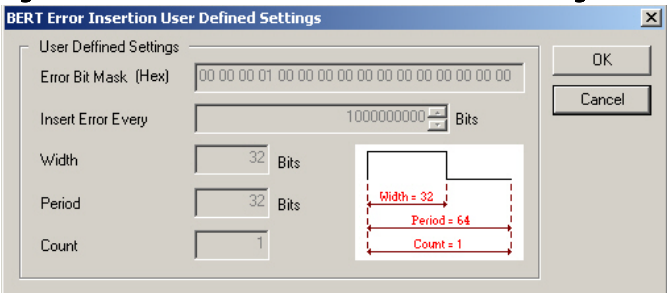
The channelized *BERT Error Insertion* tab is shown in *Figure:Channelized BERT Error Insertion Tab*.

Figure:Channelized BERT Error Insertion Tab



Double-clicking one of the channel rows in the grid displays the *BERT Error Insertion User Defined Settings* dialog, as shown in *Figure:BERT Error Insertion User Defined Settings Dialog*.

Figure:BERT Error Insertion User Defined Settings Dialog

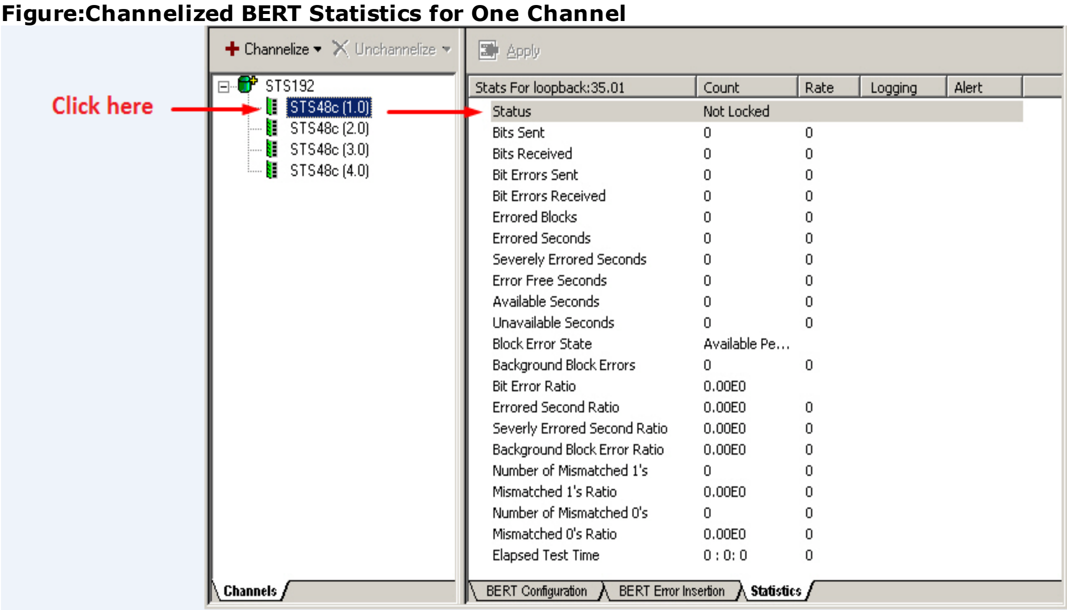


Users may specify the types of errors to be inserted for a channel, then return to the *BERT Error Insertion* tab, and press the *Insert* button for that channel.

OC-192c Channelized BERT Statistics

The statistics for each STSc channel can be displayed separately. Select the lowest level of channels in the list (STS48c in this case) to display individual statistics, as shown in *Figure:Channelized BERT Statistics for One Channel*.

Figure:Channelized BERT Statistics for One Channel



The available BERT statistics are described in *Table:Channelized BERT Statistics*. (Non-BERT statistics are listed in the normal Statistic View.) They can be displayed by clicking *Statistics* under the port name in the Resources tree, or by double-clicking *Statistics* in the Port Details list. Refer to *Statistic View—Port* for additional information on Statistic Views.

Table:Channelized BERT Statistics

Statistic	Description
Status	The status of the connection. 'Locked' when the receiving interface locks onto the data pattern.
Bits Sent - Count and Rate	The total number of bits sent, and the rate at which they are sent.
Bits Received - Count and Rate	The total number of bits received, and the rate at which they are received.

Statistic	Description
Bit Errors Sent - Count and Rate	The total number of bit errors sent, and the rate at which they are sent.
Bit Errors Received - Count and Rate	The total number of bit errors received, and the rate at which they are sent.
Errored Blocks	(EB) Number of blocks containing at least one errored second.
Errored Seconds	(ES) Number of seconds containing at least one errored block or a defect.
Severely Errored Seconds	(SES) Number of seconds with 30% or more of the errored blocks or a defect.
Error Free Seconds	(EFS) Number of seconds with no errored blocks or defects.
Available Seconds	(AS) Number of seconds which have occurred during Available Periods.
Unavailable Seconds	(UAS) Number of seconds which have occurred during Unavailable Periods.
Block Error State	Available Period or Unavailable Period, determined according to the running count and calculation of seconds in various error conditions. A minimum of 10 non-SESs must pass for the state to change from Unavailable to Available. A minimum of 10 SESs must pass for the state to change from Available to Unavailable.
Background Block Errors (BBE)	The number of errored blocks not occurring as part of a Severely Errored Second.
Bit Error Ratio (BER)	The ratio of the number of errored bits compared to the total number of bits transmitted.
Errored Second Ratio (ESR)	The ratio of Errored Seconds (ES) to the total seconds.
Severely Errored Second Ratio (SESR)	The ratio of Severely Errored Seconds (SESs) to the total seconds in available time.
Background Block Error Ratio (BBER)	The ratio of Background Block Errors (BBEs) to the total number of blocks in available time.
Number of Mismatched 1’s	The number of expected ones received as zeros.
Mismatched 1’s Ratio	The ratio of the number of expected ones received as zeros to all bits. In the following format: 0.00E0.
Number of Mismatched 0’s	The number of expected zeros received as ones.
Mismatched 0’s Ratio	The ratio of the number of expected zeros received as ones to all bits. In the following format: 0.00E0.
Elapsed Test Time	The elapsed test time, exclicked as HH : MM : SS.

Port Properties for VSR

Ixia OC-192c POS and BERT ports with Very Short Reach (VSR-1) optical transceivers support 850 nm VSR-1 parallel interfaces for intra-Point of Presence (POP) connections, with a maximum fiber length of up to 300 meters.

The OC-192c serial data stream is modified to be carried by a ribbon cable containing 12 parallel optical fibers. The data from an OC-192c POS frame is ‘byte-striped’ byte-wise across 10 channels, where the first byte is transmitted across Channel 1, the second byte across Channel 2, and so forth, with the process repeated at the 11th byte, 21st byte, and so forth. The receiver operates on a recovered clock for each channel.

Channel 11 is designated for protection switching. The ten data channels are XOR'd, and this data can be recovered if one of the data channels fails. Channel 12, called the Error Detection Channel (EDC), is for Cyclical Redundancy Checks (CRCs) from each of the 10 data channels plus the protection channel and the EDC itself. Even if these two channels are not utilized in a test configuration, the channels are still sent by the transmitter.

Test parameters for the VSR-1 interface can be configured in IxExplorer. The *VSR Statistics* dialog is accessed by clicking a OC-192c VSR POS or VSR BERT port in the Network Resources Tree and then double-clicking VSR Statistics in the port details list in the right pane.

The *VSR Statistics* dialog consists of two main sections:

- Upper section—contains six tabbed views for configuring the errors to be inserted into the stream:
  - *Options*—options to set general parameters.
  - *Section BIP*—options related to Section BIP errors.
  - *CRC Error*—options related to CRC errors.
  - *Frame Delimiter*—options related to inserting Frame Delimiter errors.
  - *Channel Skew*—options related to inserting Channel Skew errors.
  - *8b/10b Code*—options related to inserting 8b/10b Code errors.
- Lower section—contains a spreadsheet grid where VSR statistics are displayed. *VSR Statistic View*.

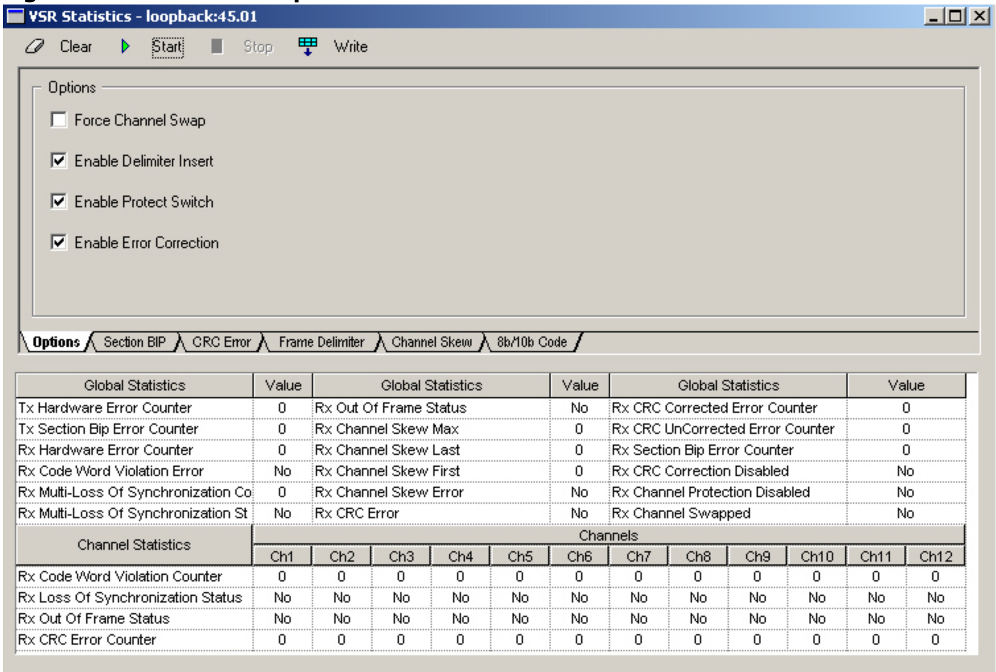
  In addition, the toolbar at the top of the window contains the following four buttons for global operations:

  - **Clear**—clears all statistics currently displayed in the grid view.
  - **Start**—starts transmission.
  - **Stop—**stops transmission.
  - **Write**—updates all of the VSR parameters and 'writes' them to IxServer, so the hardware has the same settings as the GUI.

Options

The *Options* tab view of the *VSR Statistics* dialog is shown in *Figure:VSR Statistics—Options Tab*. The statistics spreadsheet grid is common to all of the tabbed views. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, and then selecting the *Options* tab.

Figure:VSR Statistics—Options Tab



The options that can be selected in this tab are described in *Table:VSR—Options Tab*. *VSR Statistic View*, for information on the statistics displayed in the lower part of the window.

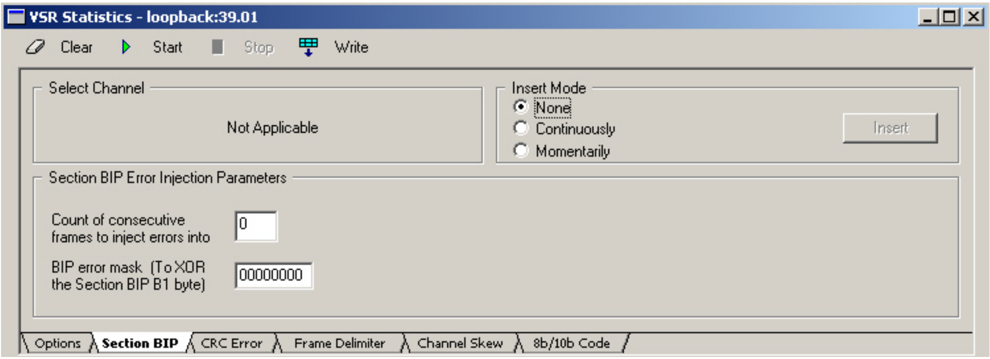
Table:VSR—Options Tab

Option	Description
Force Channel Swap	When selected, enables Channel Swapping. Channels 1-6 are swapped with Channels 7-12, to check for cable crossover.
Enable Delimiter Insert	When selected, enables the insertion of frame delimiters. Frame Delimiter Error Checking will also be enabled. *Frame Delimiter* for additional information.
Enable Protect Switch	When selected, enables the use of Protection Switching. Protection Switching is triggered when there is loss of synchronization (LOSyn) on a single data channel. The data channel can be reconstructed, based on information in the Protection Channel and the other 9 data channels. This is a feature that is always present in the transmission, but which is optionally enabled by the receiver.
Enable Error Correction	When selected, enables Error Correction.

Section BIP

The *Section BIP* tab view in the *VSR Statistics* dialog is shown in *Figure:VSR Statistics—Section BIP Tab*. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, and then selecting the *Section BIP* tab.

Figure:VSR Statistics—Section BIP Tab



The controls in this tab are described in *Table:VSR—Section BIP Tab*.

Table:VSR—Section BIP Tab

Section	Field/Control	Description
Select Channel		(Not Applicable to Section BIP Error.)
Insert Mode	One of: None Continuous Momentarily	When the *Insert* button is clicked, the Section BIP Errors will be inserted according to the mode selected. See the **Note** below for information regarding Continuous Mode.
Section BIP Error Injection Parameters	Count of consecutive frames to inject errors into	Specifies the number of consecutive frames, within a block of 256 frames, into which Section BIP Errors will be injected. The errors will repeat every 256 frames.
	BIP error mask	Allows injection of Section BIP (B1) errors into the data stream.

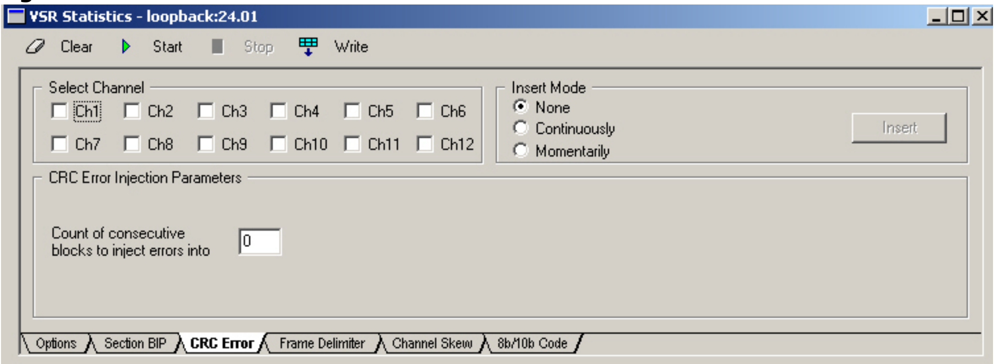
NOTE If you set the Frame Delimiter Insert Mode to Continuously and then click the Start button, the Insert function is automatically enabled and the Insert button is disabled. The Insert button remains dimmed until you click the Stop button.

CRC Error

The Error Detection Channel (Channel 12) carries 16-bit CRCs containing information to be used by the receiver to check for errors in transmission. A CRC is calculated for each virtual block of 24 bytes on a channel. CRCs are calculated for each of the 10 data channels, plus the Protection channel, and even for the EDC itself. The group of 2-byte CRCs for all 12 channels adds up to a virtual block of 24 bytes on Channel 12, which coincides with the virtual blocks on the other channels. The CCITT CRC16 polynomial is used for the calculations. This is a feature that is always present in the transmission, but which is optionally enabled by the receiver.

The *CRC Error* tab view in the *VSR Statistics* dialog is shown in *Figure:VSR Statistics—CRC Error Tab*. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, then selecting the *CRC Error* tab.

Figure:VSR Statistics—CRC Error Tab



The fields and controls in the VSR *CRC Error* tab are described in *Table:VSR—CRC Error Tab*.

Table:VSR—CRC Error Tab

Section	Field/Control	Description
Select Channel	Ch1 - Ch12	Select one or more of the data communication channels where the CRC Errors will be inserted.
Insert Mode	Choose one of: • None • Continuous • Momentarily	When the *Insert* button is clicked, the CRC Errors will be inserted according to the mode selected. See the **Note** below for information regarding Continuous Mode.
CRC Error Injection Parameters	Count of consecutive blocks to inject errors into	The number of consecutive virtual blocks to inject CRC errors into, within a group of 16 virtual blocks. The errors will be repeated every 16 blocks.

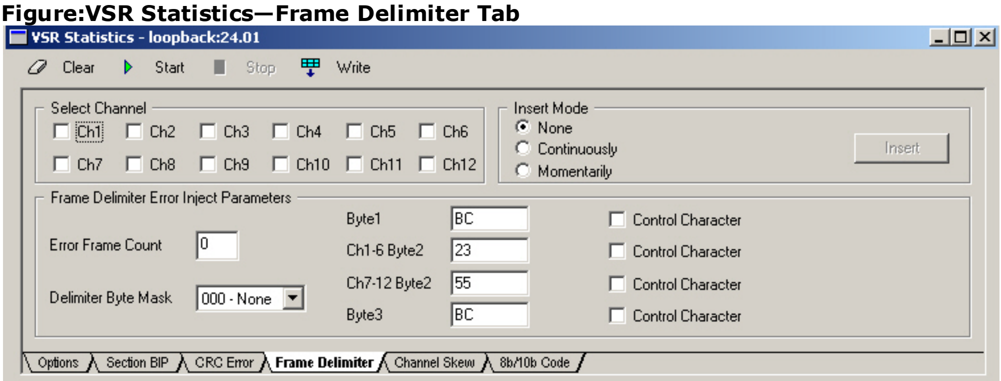
NOTE If you set the Frame Delimiter Insert Mode to Continuously and then click the Start button, the Insert function is automatically enabled and the Insert button is disabled. The Insert button remains dimmed until you press the Stop button.

Frame Delimiter

The first three bytes of the SONET frame (all ‘A1’s) are encoded in 8b/10b characters, so they serve as a Frame Delimiter which marks the start of the frame. The Frame Delimiter permits compensation for inter-channel skew, where the channels are out of alignment, time-wise. The time for transmission of a SONET frame is always 125 µs, which provides a basis for alignment. The Frame Delimiter also allows detection of crossover in the ribbon cable, and correct reordering of the data bytes at the receiving end of the connection.

The *Frame Delimiter* tab view in the *VSR Statistics* dialog is shown in F*igure:VSR Statistics—Frame Delimiter Tab*. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, and then selecting the *Frame Delimiter* tab.

Figure:VSR Statistics—Frame Delimiter Tab



The fields and controls for the VSR *Frame Delimiter* tab are described in *Table:VSR—Frame Delimiter Tab*.

Table:VSR—Frame Delimiter Tab

Section	Field/Control	Description
Select Channel	Ch1 - Ch12	Select one or more of the channels where the Frame Delimiter errors will be inserted.
Insert Mode	One of: • None • Continuously • Momentarily	The *Frame Delimiter Insert* check box on the Options page must be selected before an Insert Mode (for errors) can be selected. *Options* for additional information. When the *Insert* button is clicked, the Frame Delimiter Error will be inserted according to the mode selected (*Continuously* or *Momentarily*). See the **Note** below for information regarding Continuous Mode.
Frame Delimiter Error Inject Parameters	Error Frame Count	The number of consecutive frames to inject CRC errors into, within a block of 16 frames. The error will be repeated for each block of 16 frames. If the count = 0, frame delimiter error injection is disabled.
	Delimiter Byte Mask	Specifies the frame delimiter byte where the frame delimiter errors will be inserted.
	Byte 1	For the first delimiter byte, the 8b injected value. The value shown (hex BC) translates to Codeword K28.5.
	Control Character	If selected, the injected value is a control character.
	Ch1-6 Byte 2	For the second delimiter byte, the 8b injected value in channels 1-6. The value shown (hex 23) translates to Codeword D3.1. The delimiter for Channels 1-6 is different from that for Channels 7-12, so the polarity of the patchcord/channel order can be detected. (Cable

Section	Field/Control	Description
		crossover.)
	Control Character	If selected, the injected value is a control character.
	Ch7-12 Byte 2	For the second delimiter byte, the 8b injected value.in channels 7-12. The value shown (hex 55) translates to Codeword D21.2. The delimiter for Channels 0-5 is different from that for Channels 7-12, so the polarity of the patch-cord/channel order can be detected (cable crossover).
	Control Character	If selected, then the injected value is a control character.
	Byte 3	For the third delimiter byte, the 8b injected value. The value shown (hex BC) translates to Codeword K28.5.
	Control Character	If selected, then the injected value is a control character.

NOTE

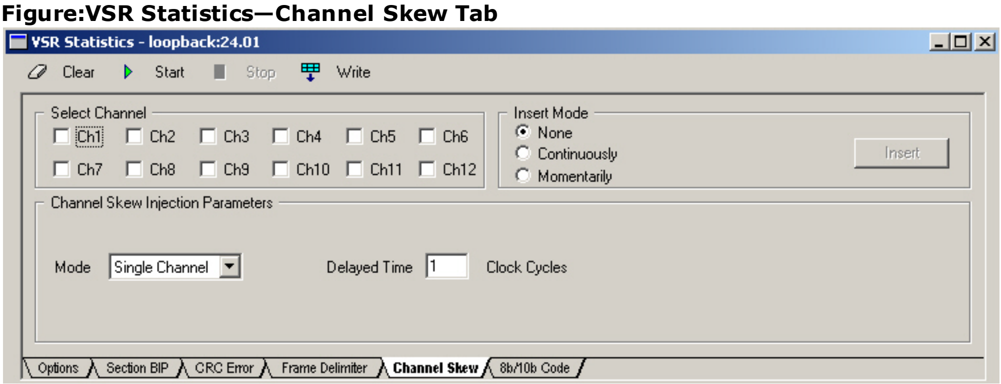
If you set the Frame Delimiter Insert Mode to Continuously and then click the Start button, the Insert function is automatically enabled and the Insert button is disabled. The Insert button remains disabled until you click the Stop button. The Insert Frame Delimiter check box on the Options page is also disabled until the Stop button is clicked.

Channel Skew

Inter-channel skew is a condition where the channels may be out of alignment, time-wise; the data may arrive at different times due to delays in transmission. Frame Delimiters can be used to realign the parallel data streams.

The *Channel Skew* tab view in the *VSR Statistics* dialog is shown in *Figure:VSR Statistics—Channel Skew Tab*. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, and then selecting the *Channel Skew* tab.

Figure:VSR Statistics—Channel Skew Tab



The fields and controls for the VSR *Channel Skew* tab are described in *Table:VSR—Channel Skew Tab*.

Table:VSR—Channel Skew Tab

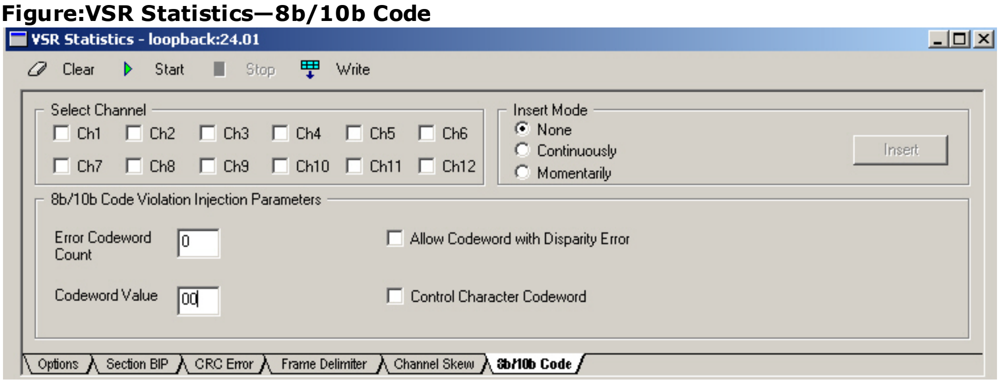
Section	Field/Control	Description
Select Channel	Ch1 - Ch12	Select one or more of the channels where the Channel Skew errors will be inserted.
Insert Mode	One of: • None • Continuous • Momentarily	When the *Insert* button is clicked, the Channel Skew Errors will be inserted according to the mode selected. See the **Note** below for information regarding Continuous Mode.
Channel Skew Injection Parameters	Mode. One of: • Multi-Channel • Single Channel	Select the skew injection mode: Multi-Channel—each and every one of the selected channels is delayed. Single Channel—just one channel is delayed.
	Delayed Time (Clock Cycles)	The specified number of clock cycles of delay to be applied to the selected channels.

NOTE If you set the Frame Delimiter Insert Mode to Continuously and then presses the Start button, the Insert function is automatically enabled and the Insert button is dimmed (unavailable). The Insert button remains dimmed until you click the Stop button.

8b/10b Code

The *8b/10b Code* tab view in the *VSR Statistics* dialog is shown in *Figure:VSR Statistics—8b/10b Code*. This tab is accessed by selecting a VSR port in the Resources window, double-clicking the *VSR Statistics* icon on the right side of the IxExplorer GUI, and then selecting the *8b/10b Code* tab.

Figure:VSR Statistics—8b/10b Code



The fields and controls in the VSR *8b/10b Code* tab are described in *Table:VSR—8b/10b Code Tab*.

Table:VSR—8b/10b Code Tab

Section	Field/Control	Description
Select Channel	Ch1 - Ch12	Select one or more of the channels where the 8b/10b Errors will be inserted.
Insert Mode	One of: • None	When the *Insert* button is clicked, the 8b/10b Errors will be inserted according to the mode selected.

Section	Field/Control	Description
	• Continuous • Momentarily	See the **Note** below for information regarding Continuous Mode.
8b/10b Code Violation Injection Parameters	Error Codeword Count	Specifies the number of consecutive codewords, per block of 16 code words, into which code violations will be injected. This pattern will be repeated for every block of 16 codewords.
	Codeword Value	Specifies the 8b value for the code word to be injected.
	Allow Codeword with Disparity Error	If this box is selected, disparity errors will be injected. Note: These disparity errors may cause codeword violations.
	Control Character Codeword	If selected, the injected code word will be a control character.

NOTE If you set the Frame Delimiter Insert Mode to Continuously and then presses the Start button, the Insert function is automatically enabled and the Insert button is dimmed (unavailable). The Insert button remains dimmed until you click the Stop button.

VSR Statistic View

The displayed VSR statistics are grouped into the two following categories:

- *Global Statistics*
- *Channel Statistics*

Global Statistics

The VSR Global Statistics are described in *Table:VSR Global Statistics*. Global statistics are cumulative for all of the channels on the port.

Table:VSR Global Statistics

Item	Value	Description
TX Hardware Error Counter	Integer	The number of hardware errors detected on the transmit side.
TX Section Bip Error Counter	Integer	The number of Section Bit Interleaved Parity (BIP) errors that have been detected on the transmit interface.
Rx Hardware Error Counter	Integer	The number of hardware errors detected on the receive side.
Rx Code Word Violation Error	Yes/No	The 8b/10b Code Word Violation error status for the receiving interface. *No* indicates no errors. *Yes* indicates one or more errors.
Rx Multi-Loss Of Synchronization Counter	Integer	Indicates the number of times that two or more data or protection channels were in the Loss of Synchronization state.

Item	Value	Description
Rx Multi-Loss of Synchronization Status	No	The status of Multiple Loss of Synchronization for the receiving interface. *No* indicates no errors. *Yes* indicates one or more errors.
Rx Out Of Frame Status	No	The Out Of Frame (OOF) status for the receiving interface. *No* indicates no errors. *Yes* indicates one or more errors.
Rx Channel Skew Max	Integer	This counter increments every time the channel skew is equal to or greater than the maximum channel skew.
Rx Channel Skew Last	Integer	Indicates the channel number of the latest channel to arrive on the receiving interface. If more than one channel arrives at the same time, Channel #1 has the highest priority, and so on.
Rx Channel Skew First	Integer	Indicates the channel number of the earliest channel to arrive on the receiving interface. If more than one channel arrives at the same time, Channel #1 has the highest priority and so on.
Rx Channel Skew Error	Yes/No	The status of the Channel Skew Error detection on the receiving interface. An error means that the Rx Channel Skew Max has been exceeded. No indicates no errors. Yes indicates one or more errors.
Rx CRC Error	Yes/No	The status of CRC Error detection on the receiving interface. *No* indicates no errors. *Yes* indicates one or more errors.
Rx CRC Corrected Error Counter	Integer	The number of corrected CRC block errors accumulated on the receiving interface.
Rx CRC UnCorrected Error Counter	Integer	The number of uncorrected CRC block errors accumulated on the receiving interface. If the CRC error correction is disabled, correctable errors are also accumulated as uncorrected errors.
Rx Section Bip Error Counter	Integer	The number of Section BIP errors detected on the receiving interface.
Rx CRC Correction Disabled	Yes/No	The status of the CRC Error Correction on the receiving interface.
Rx Channel Protection Disabled	Yes/No	The status of Channel Protection on the receiving interface.
Rx Channel Swapped	Yes/No	The Channel Swap status on the receiving interface. *No* indicates no errors. *Yes* indicates one or more errors.

Channel Statistics

The VSR Channel Statistics are described in *Table:VSR Channel Statistics*. These statistics are displayed on a per-channel basis.

Table:VSR Channel Statistics

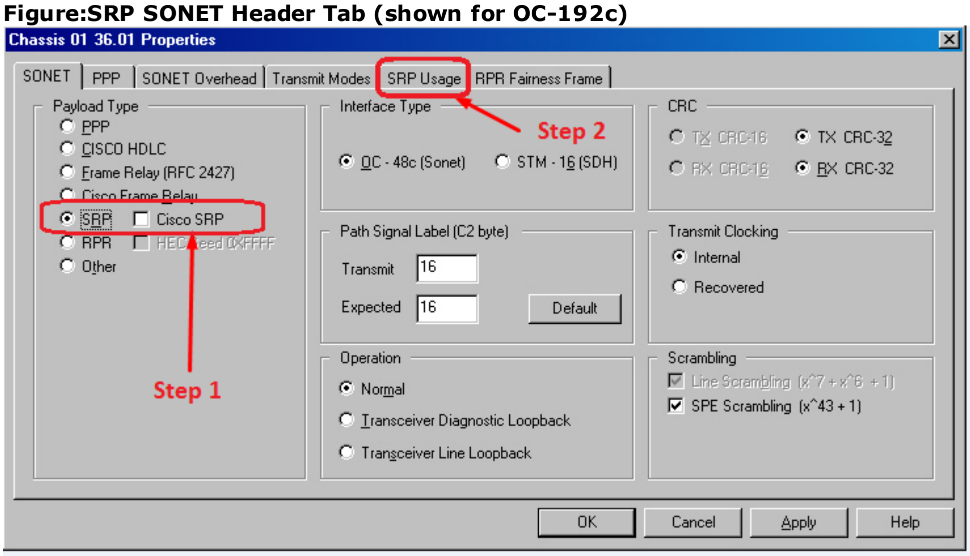
Item	Value	Description
Rx CodeWord Violation Counter	Integer	The number of codeword violations detected on the receiving channel interface. Codeword violations include running disparity errors, undefined codewords, and any control characters besides K28.5.
Rx Loss of Synchronization Status	Yes/No	The Loss of Synchronization status of the receiving interface.
Rx Out Of Frame Status	Yes/No	The Out Of Frame (OOF) status for this channel on the receiving interface.
Rx CRC Error Counter	Integer	The number of CRC errors detected on the receiving channel interface. The CRC Error counter does not accumulate errors if any channel is in LOSyn State or OOF State, or if Channel 12 has errors.

Port Properties for SRP

The optional Ixia Spatial Reuse Protocol (SRP) implementation can be used on OC-192c POS modules (including UNIPHY modules set to OC-192c POS). To enable this feature, set the SONET header to *SRP* in the *SONET* tab of the *Port Properties* dialog, as shown in *Figure:SRP SONET Header Tab (shown for OC-192c)*.

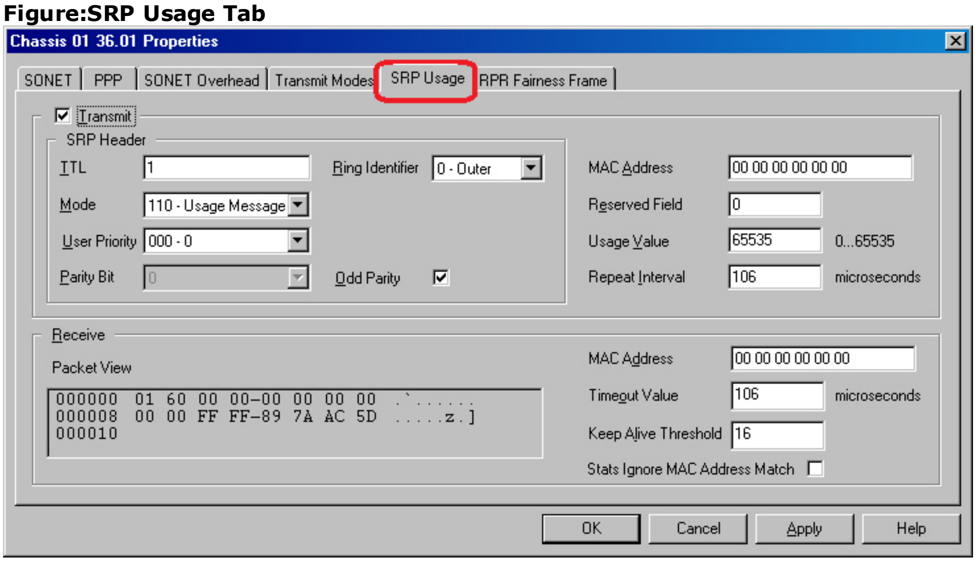
Note that an option is available for using the Cisco SRP format, where the 6-byte Originator MAC address is included in the calculation for the Length field of the Topology Discovery frames.SRP Topology Discovery Dialog and SRP Topology Discovery Packet 'Length Calculations' for additional information. The SRP type used (Cisco SRP or non-Cisco SRP) for Topology Discovery frames must be the same for the transmitting port AND the receiving port. If the SRP type does not match, the frames will be decoded incorrectly upon receipt.

Figure:SRP SONET Header Tab (shown for OC-192c)



Click the *SRP Usage* tab to display the SRP configuration options, as shown in *Figure:SRP Usage Tab*.

Figure:SRP Usage Tab



NOTE For SRP Frame Data:

Frame Data for SRP for information on configuring SRP frame headers.

The fields and controls in this tab are described in *Table:SRP Usage Tab*.

Table:SRP Usage Tab

Section	Field/Control	Description
Transmit NOTE Transmit can be enabled and dis-abled to simulate link up and link down.	MAC Address	The 6-byte MAC address that is inserted into the transmitted Usage frames to notify the receiver that this node is alive.
	Repeat Interval	(in microseconds) The length of the time inter-val between transmission of SRP Usage frames.
	Usage Value	Enter an integer value between 0 and 65535.
	Reserved Field	(Reserved)
SRP Header		The fields in this section are included in the header for the SRP Usage frames.
	TTL	Time-To-Live (TTL). This 8-bit node hop count is decremented by each node as it forwards the packet. When the TTL reaches 0, the packet is stripped from the ring. TTL is set to 1 (default) for Usage frames, because Usage frames are one-hop only.

Section	Field/Control	Description
	Ring Identifier	Specifies which ring the SRP packet will be sent on. Choose one of: • 0 - Outer • 1 - Inner
	Mode	The 3-bit field for the packet type. Choose one of: • 000 - Reserved • 001 - Reserved • 010 - Reserved • 011 - ATM cell • 100 - Control (pass)–Control Message (Pass to host). • 101 - Control (local)–Control Message (Locally Buffered for host). • 110 - Usage Message • 111 - Packet Data
	User Priority	The SRP User Priority (**not** IP TOS priority). Higher values have higher priorities. Choose one of: • 000 - 0 • 001 - 1 • 010 - 2 • 011 - 3 • 100 - 4 • 101 - 5 • 110 - 6 • 111 - 7
	Parity Bit	(Read only) The *Parity Bit* field, used for data integrity over the preceding 15 bits of the SRP Usage frame header. It is automatically set to 1 or 0, if the *Odd Parity* option is enabled (selected).
	Odd Parity	If selected, odd parity will be used as a check on the SRP Usage frame header. The Parity bit will be forced to the value (1 or 0) that will be added to the value of the 15 preceding bits to create an odd value.
Receive	MAC Address	The 6-byte MAC address in the received SRP Usage frames (the MAC address of the DUT). Received Usage frames will be counted only if the Usage Frame MAC address matches this value.

Section	Field/Control	Description
	Timeout Value	(in microseconds) The time interval between SRP Usage packets, which serve a KeepAlive function, approximately every 106 micro-seconds.
	Keep Alive Threshold	The KeepAlive timeout interval. The number of timeout values that can pass before the sending interface will be considered down. The value should be defaulted to 16.
	Stats Ignore MAC Address Match	When selected, this check box allows the statistics counter to ignore the MAC address when counting Usage Frames. All Usage Frames regardless of the MAC address are counted.
Packet View		Displays the hexadecimal and ASCII interpretation of the packet.

Port Properties for RPR

Ixia's optional Resilient Packet Ring (RPR) implementation is available on the OC-48c and OC-192c POS load modules (including UNIPHY modules set to OC-192c POS). RPR is a proposed industry standard for MAC Control on Metropolitan Area Networks (MANs), defined by IEEE P802.17/D2.1. This feature provides a cost-effective method to optimize the transport of bursty traffic, such as IP, over existing ring topologies.

Note that there is an additional option for setting the CRC for the 16 byte header to either all 0s (0000) or all 1s (FFFF). This is an addition to the original proposal that allows for changing the value of the starting calculation (originally all 0s).

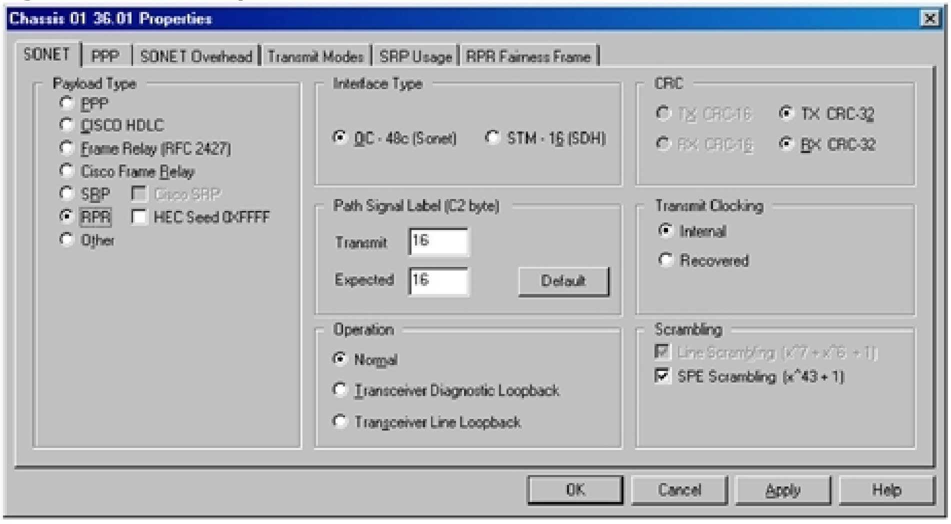
For more information on RPR, see the RPR—Resilient Packet Ring section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

RPR SONET Dialog

The Port Properties *SONET* tab with the RPR option is shown in *Figure:RPR Port Properties—SONET Tab*. The RPR feature is enabled by selecting *RPR* in the Header section of this dialog, and then clicking the *Apply* button. Then proceed to the *RPR Fairness Frame* tab, described in *RPR Fairness Frame Tab*.

The 32-bit CRC is calculated for all types of RPR frames: Data, Fairness, and Control frames.

Figure:RPR Port Properties—SONET Tab



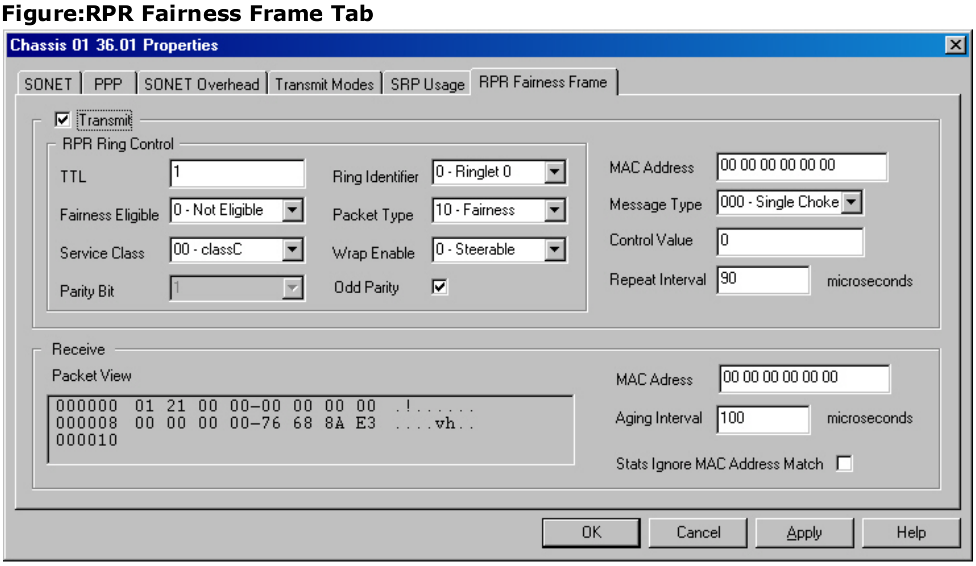
RPR Fairness Frame Tab

The RPR Fairness Algorithm (FA) is used to manage congestion on the ringlets in an RPR network. Fairness frames are sent periodically to advertise bandwidth usage parameters to other nodes in the network to maintain weighted fair share distributions of bandwidth. The messages are sent in the direction opposite to the data flow, and therefore, on the other ringlet.

For more information on RPR Fairness Frame, see the RPR—Resilient Packet Ring section in the 'Theory of Operation: General' chapter of the Ixia Platform Reference Manual.

The Port Properties *RPR Fairness Frame* tab allows to configure the fields and the frequency of transmission for Fairness frames, as shown in *Figure:RPR Fairness Frame Tab*. (The overview of RPR is presented in *Port Properties for RPR*.)

Figure:RPR Fairness Frame Tab



The fields and controls in this tab are described in *Table:RPR Fairness Frame Tab*.

Table:RPR Fairness Frame Tab

Section	Field/Control	Description
Transmit	Transmit	If selected, the transmission of RPR Fairness Control Messages (FCMs) is enabled. They will be sent at the repeat interval specified below, until the transmit option is disabled (unse- lected).
	MAC Address	The 6-byte MAC Source address (for the trans- mitting node/station).
	Message Type	The type of RPR fairness control message (FCM), used for congestion control. Choose one of: • 000 = Single Choke—sent once per advert- isement interval for implementing the Fair- ness Algorithm. Contains information on the congestion level for the ringlet. • 001 = Multi Choke—sent every 10 advert- isement intervals, for multi-choke imple- mentations. • 010 through 111 = Reserved
	Control Value	(16 bits) The normalized fair rate (advertised fair rate). FULL RATE (All ones) = full line rate.
	Repeat Interval	(in microseconds) The time interval between transmissions of Fairness frames. The range is from 10 to 65,000 microseconds.
RPR Ring Control		An RPR frame header contains 2 bytes for Ring Control: the TTL field and baseRingControl field. The following tab entry fields configure the contents of the ring control fields.
	TTL	(8-bit - TTL field) The first octet in an RPR frame header is the Time to Live hop count. The user indicates the maximum number of hops to the destination to prevent an endless loop around the ring. In a Fairness Control Message, the originator sets the TTL to 255. When a single-choke FCM changes the SA to the local SA, it will also reset the TTL to 255.
	Fairness Eligible	(1 bit - FE field) Indicates RPR fairness eli- gibility status. • 0 - Not Eligible for fairness algorithm (FA) NOTE ClassA service is not eligible for FA • 1 - Eligible for fairness algorithm
	Service Class	(2 bits - SC field) The MAC service class for the

Section	Field/Control	Description
		frame. Choose one of: • 00 - classC • 01- classB • 10 - classA1 • 11 - classA0 **ClassA** is the highest service level, providing an allocated and guaranteed data rate, plus low delay and jitter (Committed Information Rate/CIR). It is not eligible for the Fairness Algorithm. There are two subclasses (invisible to the MAC Client): • **ClassA0**—may not be reclaimed (reused) by ClassB or ClassC traffic if not in use. • **ClassA1**—may be reclaimed (reused) by ClassB or ClassC traffic if not in use. **ClassB** is the next highest service level - with an allocated and guaranteed data rate for a portion of the traffic, plus low delay and jitter (CIR). The additional traffic with no guaranteed data rate (Excess Information Rate/EIR) is eligible for the Fairness Algorithm. **ClassC** is the lowest level of traffic service—best-effort. None of the traffic has a guaranteed data rate, and no limits are placed on delay and jitter. NOTE *RPR MAC Service Classes* for additional information on MAC service classes.
	Parity Bit	(1 bit - P field) (Read-only) Used for parity check of the ring control header, since there is no HEC field in an RPR Fairness Frame. The setting for this field is controlled by the *Odd Parity* check box at the right.
	Odd Parity	If selected, then the Parity Bit in the field to the left is *Odd Parity*. Odd parity means that the total of '1' bits in the 'ttl' field and the 'baseRingControl' field is an **odd** number (including the parity bit itself). If this option is selected, the value of the Parity bit will be forced to a '1' or a '0', depending on the total number of '1' bits—to make the num-

Section	Field/Control	Description
		ber odd. If unselected, an odd number of 1 bits will not be required for header checking.
	Ring Identifier	(1 bit - RI field) The Ringlet Identifier (RI). The ringlet where the RPR frame was first transmitted. • 0 - Ringlet 0 • 1 - Ringlet 1
	Packet Type	(2 bits - PT field) Corresponds to the RPR frame type (FT) field—the type of RPR packet being transmitted. • 01 - Control (except fairness frame) • 11 - Data
	Wrap Enable	(1 bit - WE field) Used to specify that the frame may be wrapped, if necessary. • 0 - Steerable (only) • 1 - Wrap Eligible
Receive	Packet View	Displays the hexadecimal and ASCII interpretation of the packet.
	MAC Address	The 6-byte MAC Address from which the packet was sent.
	Aging Interval	(In microseconds) This is a keepalive timeout interval after which the connection is considered down if no RPR message has been received.
	Stats Ignore Mac Address Match	When selected, this check box allows the statistics counter to ignore the MAC address when counting Usage Frames. All Usage Frames regardless of the MAC address are counted.

RPR MAC Service Classes

The following table, based on IEEE P802.17, illustrates the characteristics of the three main MAC service classes used for RPR traffic—*Table:MAC Service Classes for RPR Traffic*.

Table:MAC Service Classes for RPR Traffic

Name	Bandwidth	Delay & Jitter	Use (example)
ClassA	Allocated (CIR)	Low	Real Time
ClassB	Allocated	Bounded	Near Real Time
	Opportunistic	Unbounded	
ClassC	Opportunistic		Best Effort

RPR—Additional Information

See the following sections for additional information on RPR configuration and use in testing:

- *Frame Data for RPR*—to configure the contents of RPR packets to be transmitted.
- *Pattern Match Tabs*—to select RPR-specific filter patterns for received traffic.
- *Statistics Tab*—to enable the option for adding RPR statistics to the Statistic View for the port.

Port Properties for GFP

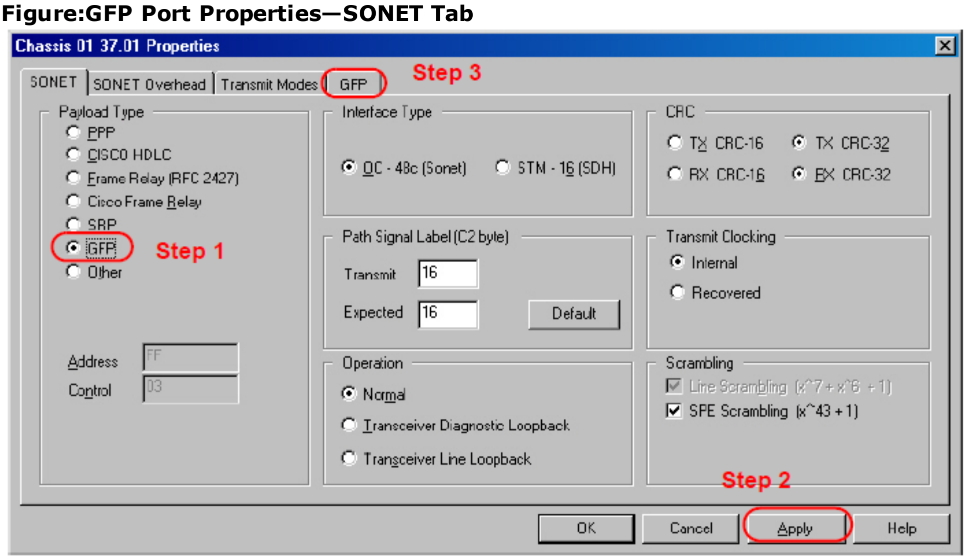
Generic Framing Procedure (GFP) provides a generic mechanism to adapt traffic from higher-layer client signals over a transport network. Two kinds of GFP frames are defined: GFP client frames and GFP control frames. GFP also supports a flexible (payload) header extension mechanism to facilitate the adaptation of GFP for use with diverse transport mechanisms.

For more information on GFP, see the GFP—Generic Framing Procedure section in the 'Theory of Operation: General' chapter of the Ixia Platform Reference Manual.

GFP SONET Tab Option

The Port Properties *SONET* tab with the GFP option is shown in *Figure:GFP Port Properties—SONET Tab*. The GFP feature is enabled by selecting *GFP* in the Header section, and then clicking the *Apply* button. Then proceed to the *GFP* tab, described in *GFP Tab*..

Figure:GFP Port Properties—SONET Tab

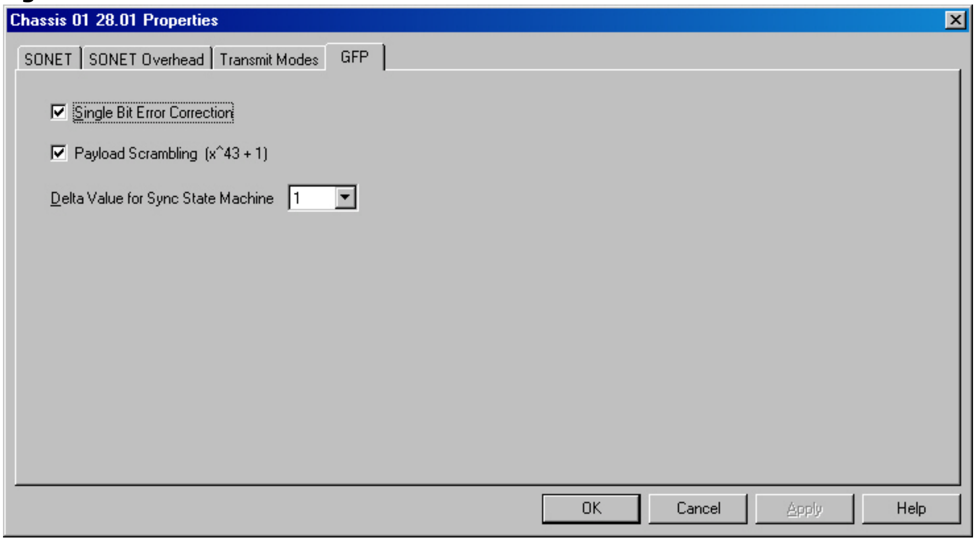


Activating GFP allows the *GFP* tab to display in the Stream Queue grid, as described in *Stream Grid–GFP Tab*.

GFP Tab

The Port Properties *GFP* tab allows to configure the Error checking level, Payload Scrambling, and delineation Delta value, as shown in *Figure:GFP Frame Tab*.

Figure:GFP Frame Tab



The fields and controls in this tab are described in *Table:GFP Frame Tab*.

Table:GFP Frame Tab

Field/Control	Description
Single Bit Error Correction	When this is check box is selected, Single Bit Error Correction is used. No error correction is performed otherwise.
Payload Scrambling (x^43+1)	Selecting this check box enables payload scrambling using the listed algorithm.
Delta Value for Sync State Machine	The value set is the number of cHEC matches needed to move the state machine from the HUNT state to the SYNC state.

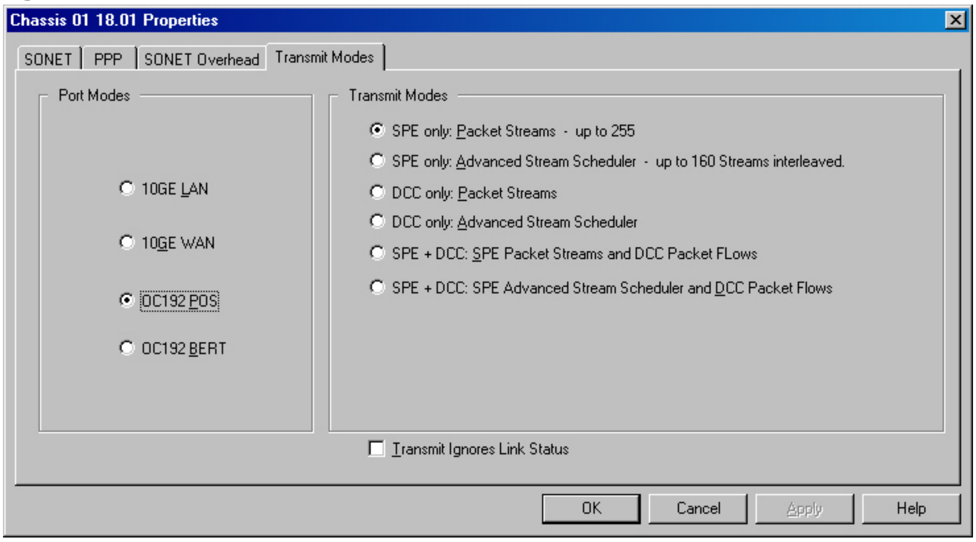
Port Properties for DCC

The optional Ixia SONET Data Communication Channel (DCC) implementation can be used on OC-192c POS modules (including UNIPHY modules set to OC-192c POS). The Ixia implementation is based on the Bellcore (now Telcordia) GRE-253-CORE guidelines. Section DCC (SDCC) uses the D1 through D3 bytes of the Section Overhead within the SONET frame for communication with network equipment. Line DCC (LDCC) uses the D4 through D12 bytes of the Line Overhead.

To enable the DCC feature, choose the appropriate DCC transmit mode from the *Transmit Modes* tab in the *Port Properties* dialog. The *Transmit Modes* tab for the OC-192c POS module, as modified for use with the DCC feature, is shown in *Figure:Transmit Modes for DCC*.

NOTE: The 10G MSM load module, when set to OC-192c mode, only has one option for SPE and DCC. They are located on the SONET tab.

Figure:Transmit Modes for DCC



Note that the DCC feature is available only for OC-192c POS Port Mode. The Transmit Modes available in this tab are described in *Table:Transmit Modes for DCC*.

Table:Transmit Modes for DCC

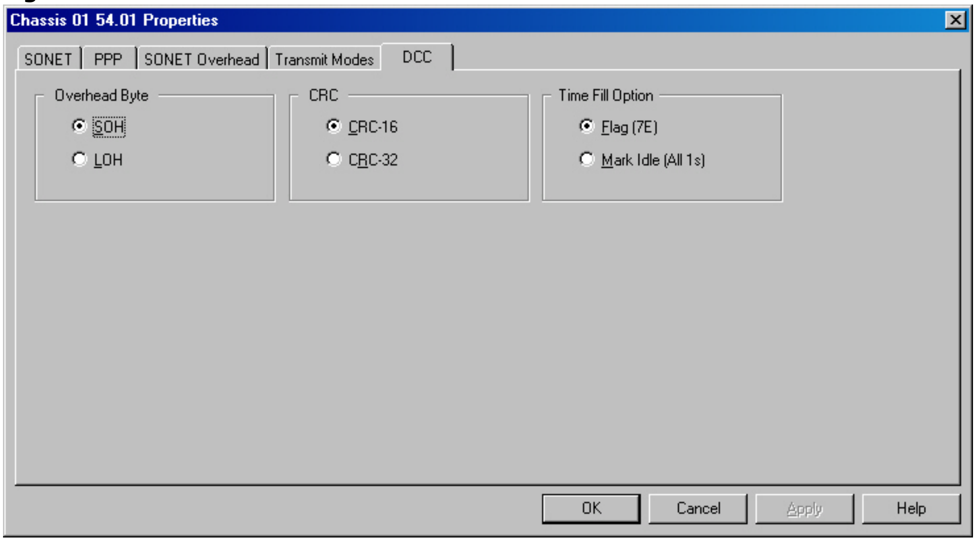
Transmit Modes	Description
SPE only: Packet Streams	This is the 'normal' packet stream mode, where streams of packets are transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 255 'normal' packet streams may be configured for the port.
SPE only: Advanced Stream Scheduler	This is the 'normal' advanced stream scheduler mode, where up to streams of packets can be interleaved and transmitted as part of the Synchronous Payload Envelope (SPE) of the SONET frame. Up to 160 'normal' advanced streams may be configured for the port.
DCC only: Packet Streams	When this mode is selected, streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Packet Streams.' DCC Packet Streams and Packet Flows for additional information.
DCC only: Advanced Stream Scheduler	When this mode is selected, interleaved streams of packets are transmitted ONLY over the DCC 'channel' in the SONET frame header. No data, just 'idle bytes' (7E), are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details list, see 'DCC Advanced Streams.' DCC Packet Streams and Packet Flows for additional information.

Transmit Modes	Description
SPE + DCC: SPE Packet Streams and DCC Packet Flows	When this mode is selected, flows of packets are transmitted over the DCC 'channel' in the SONET frame header, ***and*** 'Normal' streams of data packets are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details, 'DCC Packet Flows' are listed in addition to 'Packet Streams.' For configuring Stream Properties of the DCC Packet Flows, Stream Control is renamed to 'Frame Control.' DCC Packet Streams and Packet Flows for additional information. Protocols are not available for use with DCC packet flows.
SPE + DCC: SPE Advanced Stream Scheduler and DCC Packet Flows	When this mode is selected, flows of packets are transmitted over the DCC 'channel' in the SONET frame header, ***and*** 'Normal' interleaved streams of data packets are transmitted in the SPE payload of the SONET frame. In the list under the Port in the Resources tree, and in the Port Details, 'DCC Packet Flows' are listed in addition to 'Advanced Streams.' When DCC Packet Flows are selected, an additional, modified stream configuration window (and stream dialog) is presented. The DCC flow packets are created and then stored in memory until transmission is started. For configuring Stream Properties of the DCC Packet Flows, the *Stream Control* tab is renamed to *Frame Control*. DCC Packet Streams and Packet Flows for additional information. Protocols are not available for use with DCC packet flows.
Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down.

SONET Overhead for DCC

The SONET Overhead for DCC, as shown in *Figure:DCC SONET Overhead* can be used to send information over the SOH or LOH of the SONET frame. Refer to SONET Levels for additional information on SONET levels and network equipment.

Figure:DCC SONET Overhead



The controls in this tab are described in *Table:DCC SONET Overhead Tab.*

Table:DCC SONET Overhead Tab

Section	Field/Control	Description
Overhead Byte	(choose one type)	Choose the type of Overhead bytes to be used for transmitting the DCC packet streams or flows.
	SOH	Select for Section OverHead (SOH). The D1, D2, and D3 bytes of the Section Overhead are used to create a single data communications 'channel.' The 3-byte SOH DCC channel can be used for all SONET equipment along a network path, including signal regenerators. It is used for the Section-level Operations, Administration, Maintenance, and Provisioning (OAM&P) functions. Information transmitted in this channel includes alarms, administration data, signal control information, and maintenance messages.
	LOH	Select for Line OverHead (LOH). The D4 through D12 bytes of the Line Overhead are used to create a single data communications 'channel.' The 9-byte LOH DCC channel can be used for all SONET equipment along a network path. It is used for the Line-level Operations, Administration, Maintenance, and Provisioning (OAM&P) functions. Information transmitted in this channel includes alarms, administration data, and maintenance messages.
CRC	(choose one	This option is enabled only after a DCC Transmit

Section	Field/Control	Description
	type)	Mode has been selected.
	CRC-16	Select for 16-bit DCC CRC. *CRC Modes with DCC* for additional information.
	CRC-32	Select for 32-bit DCC CRC. *CRC Modes with DCC* for additional information.
Time Fill Option		Chose the type of bytes used to fill the gap between DCC frames.
	Flag (7E)	Fills the gap between DCC frames with hex 7E bytes.
	Mark Idle (all 1s)	Fills the gap between DCC frames with all ones.

CRC Modes with DCC

The CRC mode to use varies with the transmit mode, as shown in *Table:CRC Selection*.

Table:CRC Selection

Mode	CRCs to Use
SPE Packet Streams	Uses TX CRC option from SONET page.
SPE Advanced Stream Scheduler	Uses TX CRC option from SONET page.
DCC Packet Streams	Uses DCC CRC option in the *DCC* tab.
DCC Advanced Stream Scheduler	Uses DCC CRC option in the *DCC* tab.
DCC Packet Flows and SPE Packet Streams	For DCC Packet Flows—uses DCC CRC option in the *DCC* tab. For SPE Packet Streams—uses TX CRC option in the *SONET* tab.
DCC Packet Flows and SPE Advanced Stream Scheduler	For DCC Packet Flows—uses DCC CRC option in the *DCC* tab. For SPE Advanced Stream Scheduler—uses TX CRC option in the *SONET* tab.

ATM/POS 622 Modules

Asynchronous Transfer Mode (ATM) is supported by the Ixia ATM/POS 622 Multi-Rate load module (LM622MR). This module allows Ethernet traffic to be transmitted over ATM over SONET. In addition, the LM622MR module supports OC-12c/OC-3c Packet over SONET (POS), with expanded capabilities compared to earlier OC-12c/OC-3c POS modules. The complete specifications for the ATM/POS 622 Multi-Rate modules can be found in the *Ixia Platform Reference Manual*.

The two modes of operation, OC-12c/OC-3c POS and ATM are described in the following sections:

- *OC-12c/OC-3c POS Operation*
- *ATM Operation*

OC-12c/OC-3c POS Operation

The new OC-12c/OC-3c POS ports in the LM622-MR module feature enhanced capabilities that are described in the following sections.

Port Properties Dialog for POS 622

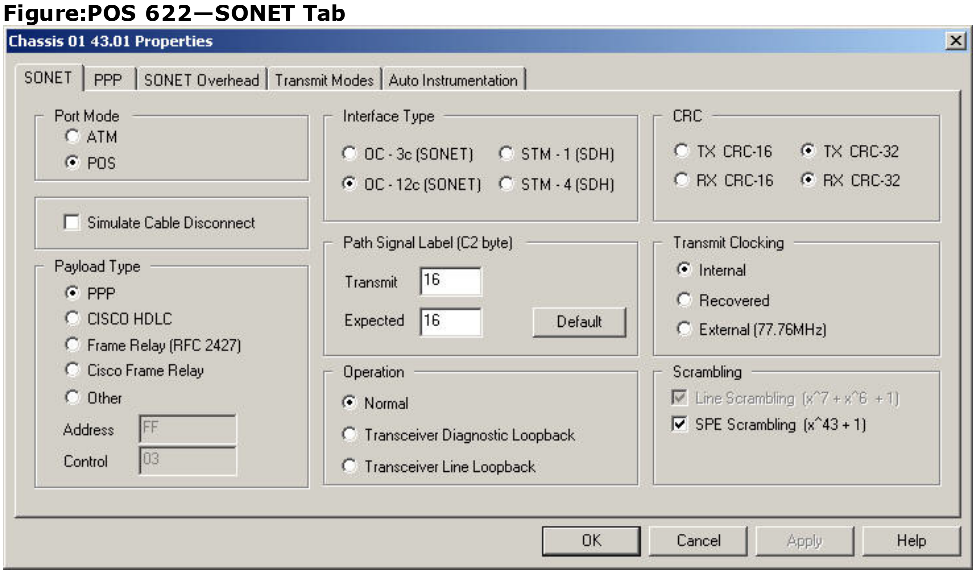
The set of tabs in the *Port Properties* dialog for the LM622MR, in OC-12c/OC-3c POS mode, are described in the following sections:

- *SONET Tab for POS 622*
- *PPP Properties*
    - *PPP Negotiation*
    - *PPP Link Control Protocol*
    - *PPP Network Control Protocols*
- *SONET Overhead*
    - *APS K1/K2 Sub-Tab*
    - *J0/J1 Sub-Tab*
    - *SONET Error Insertion—Reduced Error Set*
- *Transmit Modes for POS Modules*
- Auto Instrumentation tab,*Auto Instrumentation Tab for Ethernet Modules* (Chapter 18)

SONET Tab for POS 622

The Port Properties *SONET* tab for the LM622MR module in OC-12c/OC-3c POS mode is shown in *Figure:POS 622—SONET Tab*.

Figure:POS 622—SONET Tab



The fields and controls in this tab are described in *Table:LM622MR Module (OC-12c/OC-3c POS Mode)—SONET Tab*.

Table:LM622MR Module (OC-12c/OC-3c POS Mode)—SONET Tab

Section	Field/Control	Description
Port Mode	ATM	(N/A for POS mode.)
	POS	Select for OC-12c/OC-3c POS mode.
	Simulate Cable Dis-connect	If this is selected, then the port acts as if the cable has been disconnected.
Payload Type		NOTE Available for POS mode only.
	PPP	Selects fixed PPP address, control, and protocol header values.
	CISCO HDLC	Selects Cisco proprietary address, control, and protocol header values. HDLC = High-level Data Link Control, a data link layer protocol.
	Frame Relay (RFC 2427)	Selects Frame Relay address, control, and pro-tocol header values.
	Cisco Frame Relay	Selects Cisco proprietary Frame Relay address, control, and protocol header values.
	Other	Allows to select values for Address and Control as described in the next two rows.
	Address	When *Other* header is selected, allows the set-ting of the values for the SONET header address field; otherwise, reflects the fixed val-ues associated with the header choice.
	Control	When *Other* header is selected, allows the set-ting of the values for the SONET header control field; otherwise, reflects the fixed values asso-ciated with the header choice.
Interface Type	OC-12c (SONET)	Optical Carrier level 12 concatenated.
	STM-4 (SDH)	Synchronous transfer mode level 4.
	OC-3c (SONET)	Optical Carrier level 3 concatenated.
	STM-1 (SDH)	Synchronous transfer mode level 1.
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted header. (Hex) The default is 16.
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex) The default is 16.
	Default	Use of this button forces both *Transmit* and *Expected* values to the default value (16).
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver.
	Transceiver Line Loop-back	Causes the SONET frames received by the port to be sent back out to the sending port, cre-ating an echo of the link partner. These frames

Section	Field/Control	Description
		can also be captured.
CRC	TX CRC-16	Selects transmission with a 16-bit CRC.
	RX CRC-16	Selects reception with a 16-bit CRC.
	TX CRC-32	Selects transmission with a 32-bit CRC.
	RX CRC-32	Selects reception with a 32-bit CRC.
Transmit Clocking	Internal	If enabled, the transmit clock is derived from the internal clock.
	Recovered	If enabled, the transmit clock is derived from the recovered (received) clock. Enable this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
	External	If enabled, an External clock source will be used. The clock-in signal will be used to control the rate of data transmission.
Scrambling	Line Scrambling	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling	If enabled, data is scrambled with the $x^{43} + 1$ polynomial.
(Footer)	OK	Applies the changes to the port configuration and closes the GUI window.
	Cancel	Press this button to exit the *Port Properties* dialog without changing the port's properties.
	Apply	Applies the changes to the port configuration, but does not close the GUI window.
	Help	Press this button to display the Help page describing this dialog.

Additional Information for POS 622 Modules

For information on the additional features of the POS 622 module in OC-12c/OC-3c POS mode, see the following sections:

- *Stream Control for POS 622 Modules*
- *POS 622 Frame Data*
- *SONET Extended Statistics*

ATM Operation

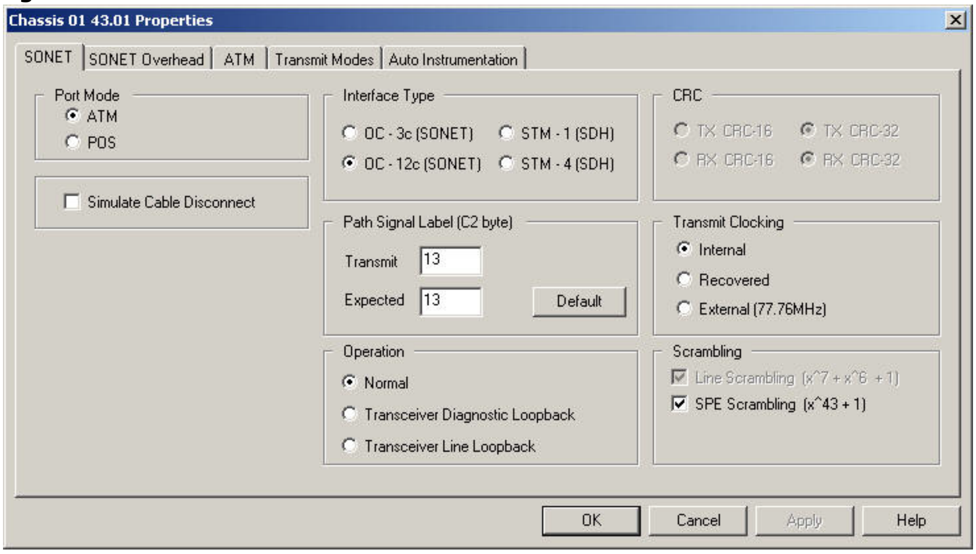
ATM is a point-to-point, connection-oriented protocol that carries traffic over 'virtual connections/circuits' (VCs), in contrast to Ethernet connectionless LAN traffic. ATM traffic is segmented into 53-byte cells (with a 48-byte payload), and allows traffic from different Virtual Circuits to be interleaved (multiplexed). Ixia's ATM module allows up to 4096 transmit streams per port, shared across up to 15 interleaved VCs.

For more information about ATM, see the ATM section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

Port Properties Dialog for ATM

The *SONET* tab for the ATM 622 load module is shown in *Figure:ATM 622 SONET Header Tab*. Only the ATM header type is available in this tab. Note that the *Path Signal Label* value for both Transmit and Receive is '13' for ATM, and that the CRC fields in this tab do not apply to ATM functions.

Figure:ATM 622 SONET Header Tab



The fields and controls in this tab is described in *Table:ATM 622 SONET Header Tab*.

Table:ATM 622 SONET Header Tab

Section	Field/Control	Description
Port Mode	ATM/POS	Asynchronous Transfer Mode or Packets over SONET. If POS is selected, the layout and options for the *SONET* tab change; a new tab, *PPP*, also becomes available for configuration. For more information on the POS options, *Port Properties Dialog for POS 622*.
Interface Type	OC - 3c (SONET)	Optical Carrier level 3 concatenated.
	STM - 1 (SDH)	Synchronous transfer mode level 1.
	OC - 12c (SONET)	Optical Carrier level 12 concatenated.
	STM - 4 (SDH)	Synchronous transfer mode level 4.
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted path overhead. For ATM, the transmitted value is '13' (Hex).
	Expected	The expected value of the C2 byte in the received path overhead. Typically, this will match the value in the *Transmit* field. For ATM, the expected value is '13' (Hex).
	Default	Use of this button forces both *Transmit* and *Expected* values to the default value '13' (Hex).
Operation	Normal	Full Duplex Tx and Rx paths.
	Transceiver Diagnostic	Causes the SONET frames to be looped back

Section	Field/Control	Description
	Loopback	from transmit to receive internally.
	Transceiver Line Loop-back	Causes the SONET frames received by the port to be transmitted back out to the sending port, creating an echo of the link partner. These frames can also be captured.
	Enable Path Error Hand-ling	Reserved for future use.
Transmit Clock-ing	Internal	Use the chassis internal clock.
	Recovered	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal clock. Enable this check box if the DUT will supply the clock signal on one of a pair of directly con-nected Ixia ports.
	External (77.76 MHz)	If enabled, the transmit clock is derived from an external clock source.
Scrambling	Line Scrambling	(Always enabled.) Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling	If enabled, data is scrambled with the $x^{43} + 1$ polynomial. NOTE The ATM cell header is not scrambled.

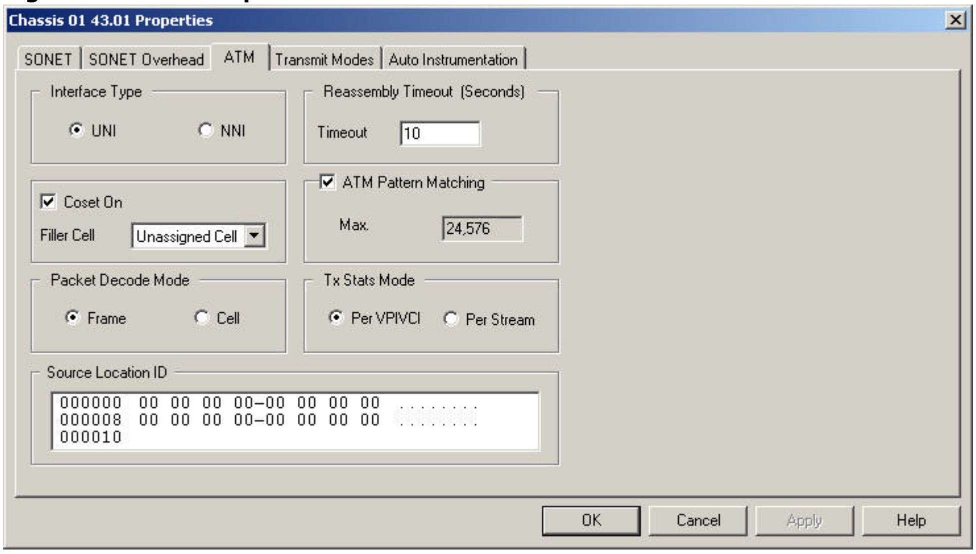
ATM Tab

The Port Properties *ATM* tab allows to choose the main ATM characteristics. The Interface Type can be set to UNI (User-to-Network Interface) format or NNI (Network-to-Node Interface aka Network-to-Network Interface) format.

ATM/POS 622 Modules for additional information. For more information about ATM, see the ATM section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The Port Properties *ATM* tab is shown in *Figure:ATM Port Properties—ATM Tab*.

Figure:ATM Port Properties—ATM Tab



The fields and controls in this tab are described in *Table:ATM Port Properties—ATM Tab*.

Table:ATM Port Properties—ATM Tab

Section	Field/Control	Description
Interface Type		Choose one of: • UNI—The ATM Forum-defined User-to-Network- Interface. • NNI—The ATM Forum-defined Network-to-Node-Interface.
Coset On		The *Coset On* check box allows the user to add/enable the Coset algorithm to be used with the Header Error Control (HEC). The code used for HEC is a cyclic code with generating polynomial x^8 + x^2 + x + 1. If Coset is turned on, the result of this polynomial is XOR'd with 0x55 (Coset Leader). Choose one of: • selected–Enabled/On • Unselected–Disabled/Off
Filler Cell		SONET frame transmission is continuous even when data or control messages are not being transmitted. Choose the cell type to be transmitted during those intervals: • Idle Cell (VPI/VCI = 0 and CLP = 1) • Unassigned Cell (VPI/VCI = 0 and CLP = 0)
Packet Decode Mode	Frame or Cell	Sets the mode for the display in Packet View. Choose one of: • Frame (AAL5) • Cell (53-byte ATM cells)

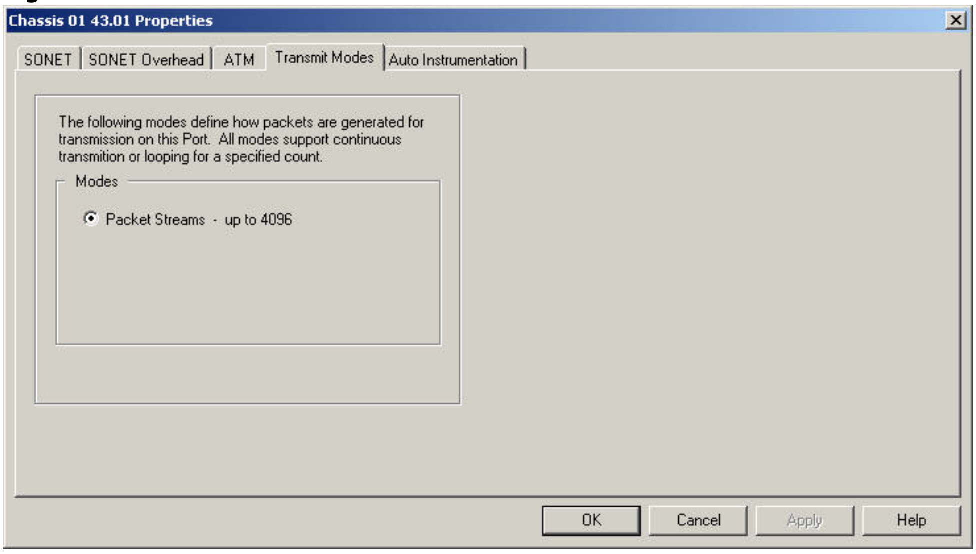
Section	Field/Control	Description
Reassembly Timeout (Seconds)	Timeout	(hex value) Sets the value for the Reassembly Timeout. It is the period of time that the receive side will wait for another cell on that channel–for reassembly of cells into a CPCS PDU (packet). If no cell is received within that period, the timer will expire.
ATM Pattern Match-ing		This check box is used to enable capture/filter values for use with ATM ports. When selected, the frame data from one or more VPI/VCIs may be used as capture trigger or capture filter option. This check box also enables the *ATM* tab in the *Filter Properties* tab page, as described in *ATM Filter Properties*.
	Max VCCs	The maximum number of Virtual Channel Con-nections for this port. It will be 12288 if *ATM Pat-tern Matching* is enabled, and 16383 if not.
	Tx Stats Mode	Select the type of Transmit Stats to collect: Per VPIVCI–*Per VPIVCI Statistic View* Per Stream–*Per Stream Statistic View*
Source Location		A 16 byte field that is used to identify the location of the ATM node for loopback, AIS, and RDI OAM cells.

ATM Transmit Modes Tab

The *Transmit Mode* tab controls the type of stream to generate. For the ATM/POS 622 in ATM mode, the only option available is Packet Streams. This tab is reached by opening the *Port Properties* dialog, setting the port to ATM, and selecting the *Transmit Mode* tab.

The ATM *Transmit Mode* tab is shown in *Figure:ATM Transmit Mode Tab*.

Figure:ATM Transmit Mode Tab



The controls in this tab page are described in *Table:ATM Transmit Modes Controls*.

Table:ATM Transmit Modes Controls

Control	Description
Packet Streams	Sets the basic operating mode for the port to Packet Stream-s.This allows the hardware to generate up to 4096 streams.
Transmit Ignores Link Status	If checked, then it will allow transmission of packets even if the link is down.

ATM VPI/VCI Statistic View

For a more granular evaluation of the ATM VC traffic, an additional VPI/VCI Statistic View window is available, as shown in *Figure:ATM VPI/VCI Statistic View—Receive* and in *Fig-ure:ATM VPI/VCI Statistic View—Transmit*

It displays Receive, Transmit, and OAM statistics per VPI/VCI address. A maximum of 4096 VPI/VCI entries can be monitored for statistics.

Figure:ATM VPI/VCI Statistic View—Receive

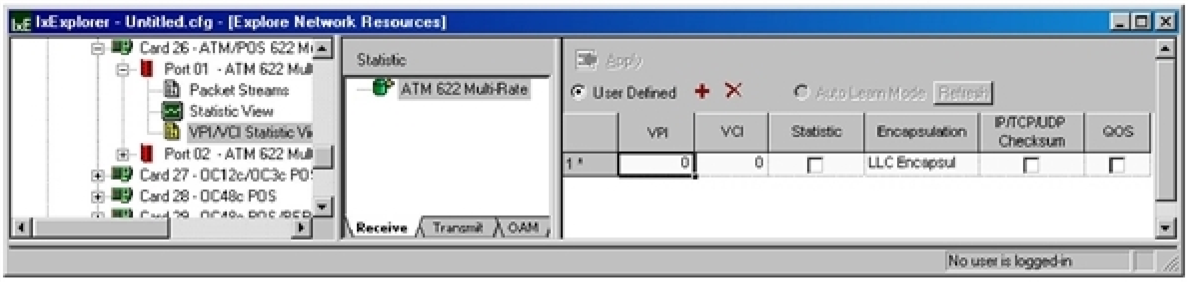


Figure:ATM VPI/VCI Statistic View—Transmit

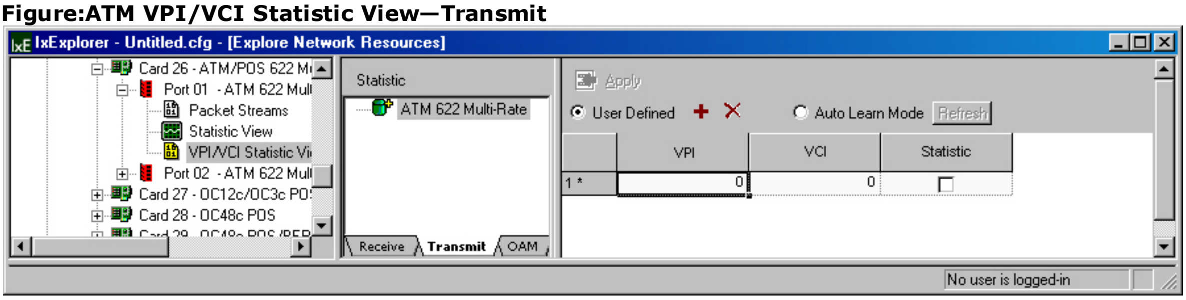
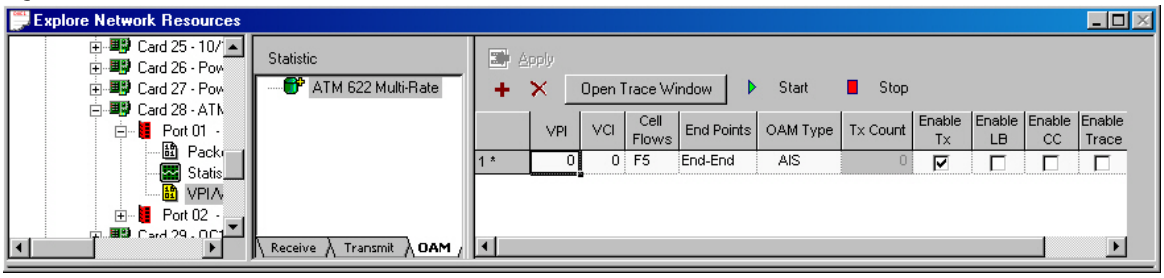


Figure:ATM VPI/VCI Statistic View—OAM



The fields and controls in these views are described in *Table:ATM VPI/VCI Statistic View*.

Table:ATM VPI/VCI Statistic View

Section/View	Field/Control	Description
Window Header	User Defined	If this option is selected, you create the VCs that will be received on this ATM interface.
	Auto Learn Mode	(**For Transmit ONLY**) If this option is selected, the **first** VPI/VCI configured per transmit stream queue is auto-learned.
		(For use with Auto Learn Mode ONLY.) When this button is clicked, the auto-learned VPI/VCI information is updated.
		Add an entry.
		Deleted selected entry(ies).
		Press this button to apply the changes that have been made in the window. **NOTE** If this button is not clicked after changes are made, the Auto-Apply timer applies the changes automatically after 10 seconds have passed.
Receive View		This view displays information about the received VCs.
	VPI	Virtual Path Identifier for the VC over which information is being received.
	VCI	Virtual Channel Identifier for the VC over which

Section/View	Field/Control	Description
		information is being received.
	Statistic	If an entry is selected, statistics are collected for that VC.
	Encapsulation (Available only when Packet Group Mode is enabled in the *Receive Mode* tab– *Receive Mode Tab*	If Packet Group Mode has been enabled in the *Receive Mode* tab, the Receive encapsulation type can be selected from the following types: ■ LLC/Snap Routed Protocol ■ LLC Bridged Ethernet/802.3 ■ LLC Bridged Ethernet/802.3 no FCS ■ LLC Encapsulated PPP ■ LLC Multiplexed PPP ■ VC Mux Routed Protocol IPv4/IPv6/MPLS ■ VC Mux Bridged Ethernet/802.3 ■ VC Mux Bridged Ethernet/802.3 no FCS NOTE These ATM encapsulation types are described in more detail in the following section: • *ATM Frame Data*
	IP/TCP/UDP Checksum	If this check box is selected, the IP/TCP/UDP Checksum statistics are counted and shown for this VPI/VCI.
	QOS	If this check box is selected, the QoS statistics are counted and shown for this VPI/VCI.
Transmit View		This view displays information about the VCs over which cells are being transmitted.
	VPI	Virtual Path Identifier for the VC being used for transmission.
	VCI	Virtual Channel Identifier for the VC being used for transmission.
	Statistic	If an entry is selected, statistics will be collected for that VC.
OAM View		This view displays information about the OAM cells being transmitted and received, and allows to configure OAM cells. OAM cells can be configured using the stream grid (described below), or by double-clicking the stream grid and opening a configuration dialog, described in *ATM OAM Tx Cell Configuration*.
		Opens the trace window for OAM cells. *ATM OAM Trace Window* for more information.

Section/View	Field/Control	Description
		Starts ATM OAM cell transmission.
		Stops ATM OAM cell transmission.
	VPI	Virtual Path Identifier for the VC being used for transmission.
	VCI	Virtual Channel Identifier for the VC being used for transmission.
	Cell Flows	Selects the maintenance level that is transmitted. The options are *F4* or *F5*. Note that the options set here, in conjunction with the options set in the *End Points* field, determines the VCI setting and PTI setting. The combinations are: • F4/End-to-End—VCI column is dimmed with a value of 4. • F4/Segment—VCI column is dimmed with a value of 3. • F5/End-to-End—The PTI bit in the ATM header is set to 101. • F5/Segment—The PTI bit in the ATM Header is set to 100.
	End Points	Selects the type of connection, either *End-to-End* or *Segment*. Note that the options set here, in conjunction with the options set in the *Cell Flows* field, determines the VCI setting and PTI setting. The combinations are: • F4/End-to-End—VCI column is dimmed with a value of 4. • F4/Segment—VCI column is dimmed with a value of 3. • F5/End-to-End—The PTI bit in the ATM header is set to 101. • F5/Segment—The PTI bit in the ATM Header is set to 100.
	OAM Type	Selects what type of OAM cell to send. Options are: • AIS • RDI • Fault Management CC • Fault Management LB • Activation/Deactivation CC

Section/View	Field/Control	Description
	Tx Count	The number of OAM cells that are transmitted. If gray, then the transmit is continuous. This field can only be modified in the *ATM OAM Tx Cell Configuration* dialog. *ATM OAM Tx Cell Configuration* for more information.
	Enable Tx	Enable the transmission of OAM cells.
	Enable LB	Enables the processing of incoming loopback OAM cells. If this option is not selected, incoming LB cells will be discarded after incrementing the receive statistics counters.
	Enable CC	Enables OAM Continuity Check cells, which provide continuous monitoring of a connection at a segment or end-to-end basis.
	Enable Trace	Enables the trace function for OAM cells. *ATM OAM Trace Window* for more information.

ATM OAM Statistics Control

OAM cells are used for operation, administration, and maintenance of ATM networks. They operate on ATM's physical layer and are not recognized by higher layers. Operation, Administration, and Maintenance (OAM) performs standard loopback (end-to-end or segment) and fault detection and notification Alarm Indication Signal (AIS) and Remote Defect Identification (RDI) for each connection. It also maintains a group of timers for the OAM functions. When there is an OAM state change such as loopback failure, OAM software notifies the connection management software.

ATM OAM Tx Cell Configuration

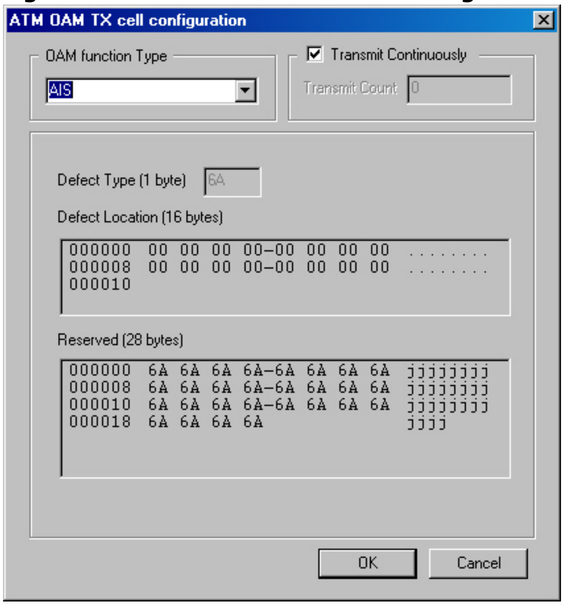
The ATM OAM Tx Cell Configuration dialog allows to set the types of OAM cells to transmit. Depending on the type of OAM cell being created, the dialog displays different controls. The sets of controls for each type are described below:

- *AIS/RDI OAM Cells*
- *Fault Management CC OAM Cells*
- *Fault Management LB OAM Cells*
- *Activation/Deactivation CC OAM Cells*

AIS/RDI OAM Cells

AIS and RDI OAM cells can be configured using the ATM OAM Tx Cell Configuration dialog box, as shown in *Figure:AIS or RDI ATM OAM Cell Configuration*. The OAM function Type setting must be set to either *AIS* or *RDI* for the controls shown in *Figure:AIS or RDI ATM OAM Cell Configuration* to appear.

Figure:AIS or RDI ATM OAM Cell Configuration



The configurations options are explained in *Table:AIS/RDI OAM Cell Configuration Options*.

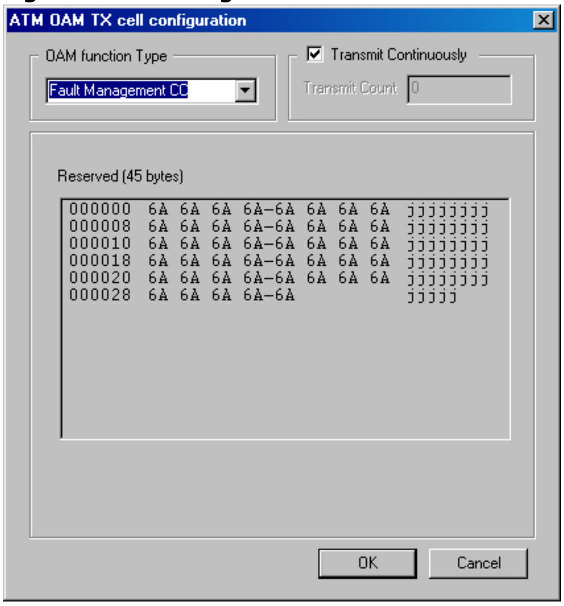
Table:AIS/RDI OAM Cell Configuration Options

Control	Description
OAM function Type	The pull-down menu allows you to select the type of ATM OAM cell to be transmitted. *AIS* or *RDI* must be selected to display the dialog options shown in *Figure:AIS or RDI ATM OAM Cell Configuration*.
Transmit Continuously	Selecting this check box means the configured OAM cells are continuously transmitted, until manually stopped using the *Stop Transmit* button. When unselected, you can specify the number of OAM cells to transmit using the *Transmit Count* field.
Defect Type (1 byte)	The Hex representation of the defect type. Selecting an OAM cell type changes this field.
Defect Location (16 bytes)	Displays the location of the defect type information in the cell data.
Reserved (28 bytes)	The data in the Reserved portion of the OAM cell.

Fault Management CC OAM Cells

Fault Management CC cells can be configured using the ATM OAM Tx Cell Configuration dialog box, as shown in *Figure:Fault Management CC ATM OAM Cell Configuration*. The OAM function Type setting must be set to either *Fault Management CC* for the controls shown in *Figure:Fault Management CC ATM OAM Cell Configuration* to appear.

Figure:Fault Management CC ATM OAM Cell Configuration



The configurations options are explained in *Table:Fault Management CC ATM OAM Cell Configuration Options*

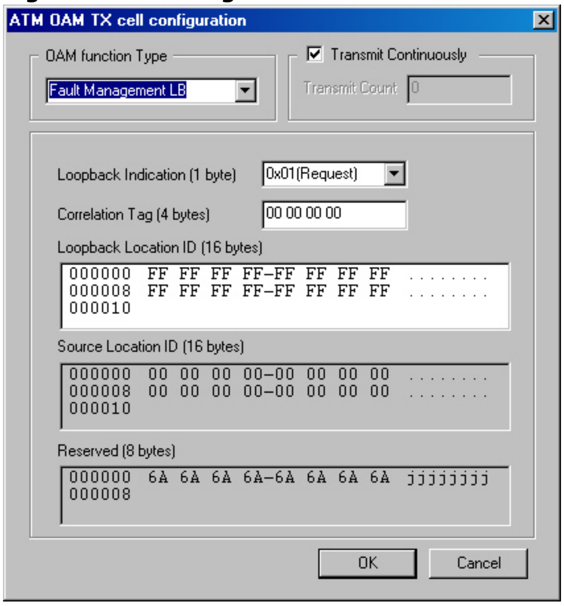
Table:Fault Management CC ATM OAM Cell Configuration Options

Control	Description
OAM function Type	The pull-down menu allows you to select the type of ATM OAM cell to be transmitted. *Fault Management CC* must be selected to display the dialog options shown in *Figure:Fault Management CC ATM OAM Cell Configuration*.
Transmit Continuously	Selecting this check box means the configured OAM cells are continuously transmitted, until manually stopped using the *Stop Transmit* button. When cleared, you can specify the number of OAM cells to transmit using the *Transmit Count* field.
Reserved (28 bytes)	The data in the Reserved portion of the OAM cell.

Fault Management LB OAM Cells

Fault Management LB cells can be configured using the ATM OAM Tx Cell Configuration dialog box, as shown in *Figure:Fault Management LB ATM OAM Cell Configuration*. The OAM function Type setting must be set to either *Fault Management CC* for the controls shown in *Figure:Fault Management LB ATM OAM Cell Configuration* to appear.

Figure:Fault Management LB ATM OAM Cell Configuration



The configurations options are explained in *Table:Fault Management LB ATM OAM Cell Configuration Options*.

Table:Fault Management LB ATM OAM Cell Configuration Options

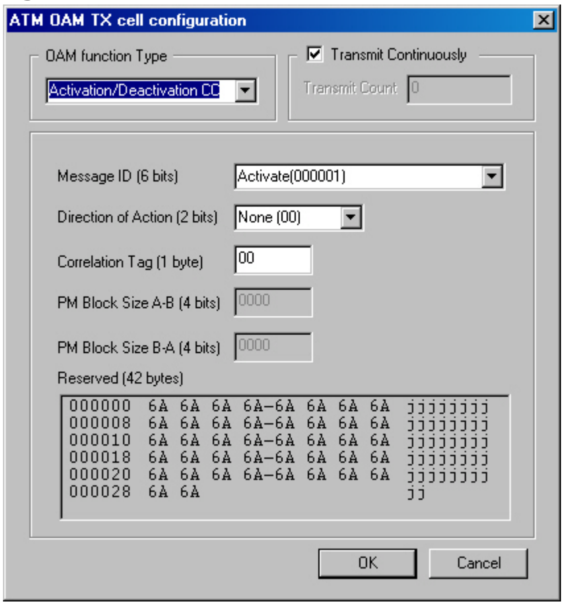
Control	Description
OAM function Type	The list allows you to select the type of ATM OAM cell to be transmitted. *Fault Management LB* must be selected to display the dialog options shown in *Figure:Fault Management LB ATM OAM Cell Configuration*.
Transmit Continuously	Selecting this check box means the configured OAM cells are continuously transmitted, until manually stopped using the *Stop Transmit* button. When cleared, you can specify the number of OAM cells to transmit using the *Transmit Count* field.
Loopback Indication (1 byte)	Indicates the direction of the loopback, either forward or backward. Options are: • 0x01 (Request)–Forward • 0x00 (Reply)–Backward
Correlation Tag (4 bytes)	A consecutive number value that allows received loopback cells to be matched to the sent cell.
Loopback Location ID (16 bytes)	Indicates the ATM node where the loopback is to occur, or the ID of the ATM node at which the loopback occurred.
Source Location ID (16 byte)	Indicates the ID of the originating ATM node.
Reserved (28 bytes)	The data in the Reserved portion of the OAM cell.

Activation/Deactivation CC OAM Cells

Fault Management LB cells can be configured using the ATM OAM Tx Cell Configuration dialog box, as shown in *Figure:Activation/Deactivation CC ATM OAM Cell Configuration*. The

OAM function Type setting must be set to either *Fault Management CC* for the controls shown in *Figure:Activation/Deactivation CC ATM OAM Cell Configuration* to appear.

Figure:Activation/Deactivation CC ATM OAM Cell Configuration



The configurations options are explained in *Table:Activation/Deactivation CC ATM OAM Cell Configuration Options*.

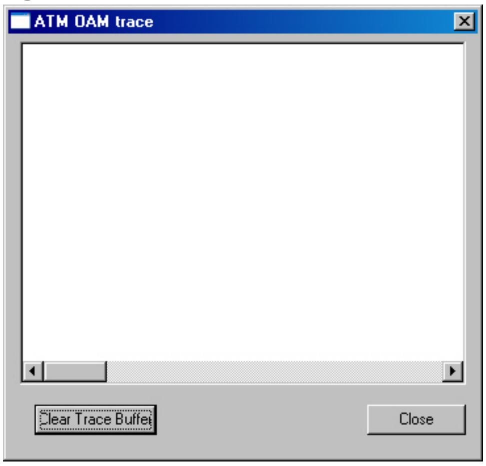
Table:Activation/Deactivation CC ATM OAM Cell Configuration Options

Control	Description
OAM function Type	The pull-down menu allows you to select the type of ATM OAM cell to be transmitted. *Activation/Deactivation CC* must be selected to display the dialog options shown in *Figure:Activation/Deactivation CC ATM OAM Cell Configuration*.
Transmit Continuously	Selecting this check box means the configured OAM cells are continuously transmitted, until manually stopped using the *Stop Transmit* button. When cleared, you can specify the number of OAM cells to transmit using the *Transmit Count* field.
Message ID (6 bits)	
Direction of Action (2 bits)	Identifies the direction of transmission to activate or deactivate the OAM function. Options are: • None • B-A • A-B • Two way
Correlation Tag (1 byte)	A consecutive number value that allows received loopback cells to be matched to the sent cell.
PM Block Size A-B (4 bits)	N/A
PM Block Size B-A (4 bits)	N/A
Reserved (28 bytes)	The data in the Reserved portion of the OAM cell.

ATM OAM Trace Window

To help with processing incoming ATM OAM cells, you can select the OAM cell header to be traced by selecting the *Enable Trace* check box. By selecting the *Open Trace Window* button, a trace window is opened for all VCCs that have tracing enabled, shown in *Figure:ATM OAM Trace Window*.

Figure:ATM OAM Trace Window



The OAM processor checks the cell header and calls back whenever the OAM cell with the matched header is transmitted and received.

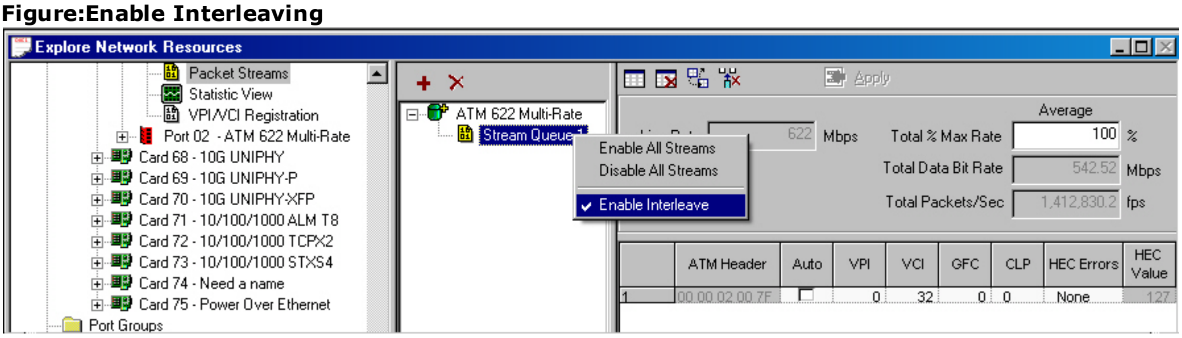
Use the *Clear Trace Buffer* button to clear previous trace information.

ATM Interleaving Blocking

Normally, flows from different stream queues interleave during transit, meaning that the cells from various streams are weaved together during transmit, and reassembled at the far end in correct sequence and stream.

It is possible to prevent certain stream queues from interleaving using the Enable Interleaving function in the ATM stream control window. *Figure:Enable Interleaving* shows the Enable Interleaving function.

Figure:Enable Interleaving



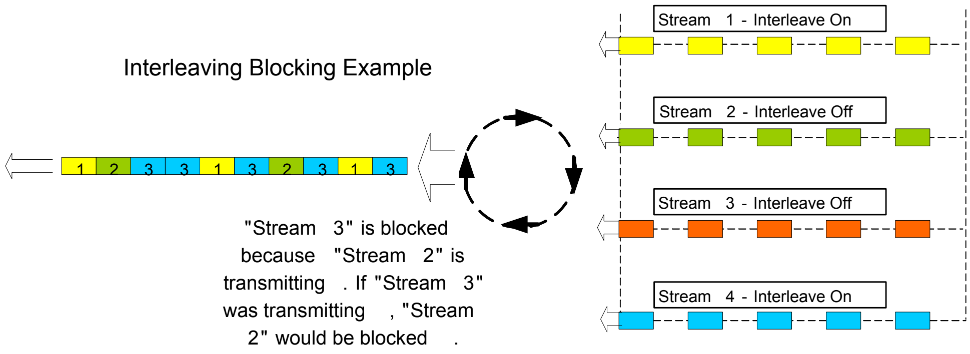
When Enable Interleave is selected (not blocked), stream queues will interleave normally. When Enable Interleave is selected (blocked) stream queues will not interleave with other blocked stream queues.

For example, assume that four stream queues exist, the second and third of which have interleaving off (blocked). The following scenario exists:

- Stream Queue 1 (Enable Interleave on)—cells are not blocked and interleave with queue 2, 3, and 4.
- Stream Queue 2 (Enable Interleave off)—cells are blocked when queue 3 is transmitting, cells interleave with queue 1 and 4.
- Stream Queue 3 (Enable Interleave off)—cells are blocked when queue 2 is transmitting, cells interleave with queue 1 and 4.
- Stream Queue 4 (Enable Interleave on)—cells are not blocked and interleave with queue 2, 3, and 4.

Figure:ATM Interleaving Blocking demonstrates the scenario described above.

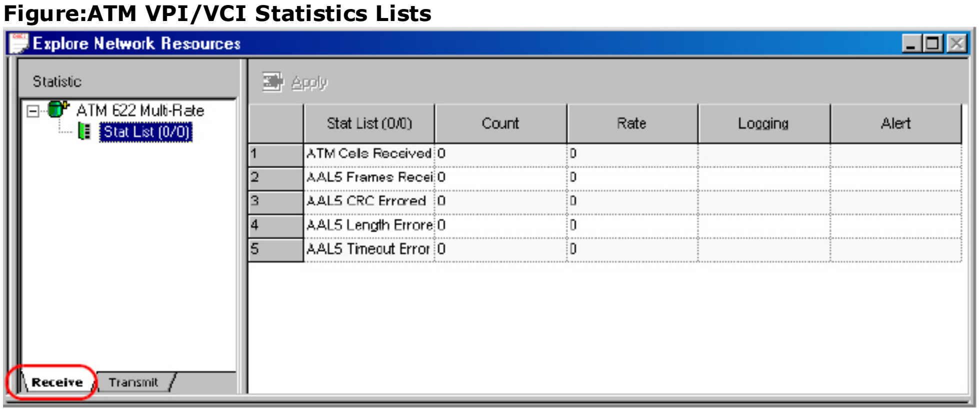
Figure:ATM Interleaving Blocking

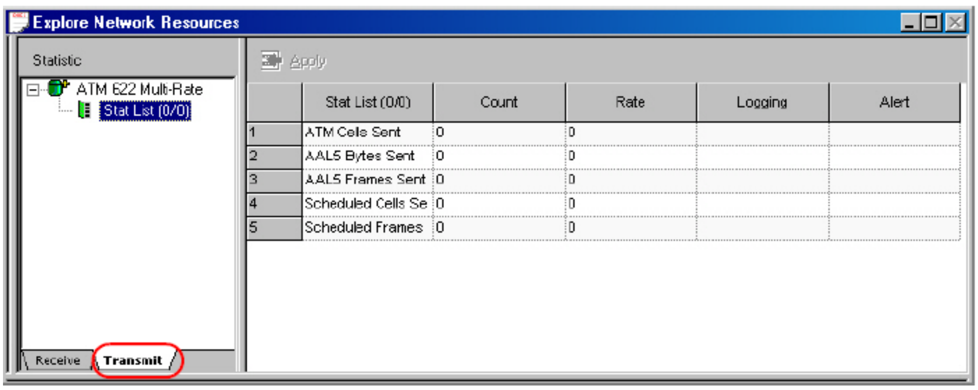


ATM VPI/VCI Stat Lists

When the *Stats* check box is selected for a received VC (in the Receive view), a named stat list is created, as shown in *Figure:ATM VPI/VCI Statistics Lists*.

Figure:ATM VPI/VCI Statistics Lists





ATM Statistics

Statistics are added to the Statistic View to provide information on the transmitted and received ATM traffic:

- **Receive Statistics**: ATM Cells Received, AAL5 Frames Received, AAL5 CRC Errored Frames Received, AAL5 Length Errored Frames Received, AAL5 Timeout Errored Frames Received.
- **Transmit Statistics**: ATM Cells Sent, AAL5 Bytes Sent, AAL5 Frames Sent, Scheduled Cells Sent, Scheduled Frames Sent.

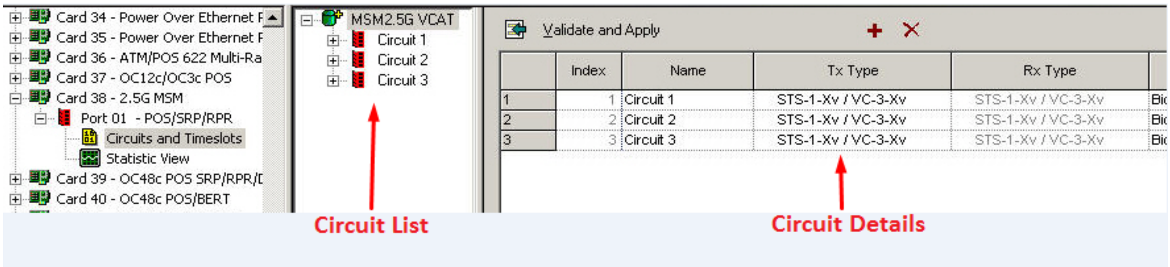
VCAT Circuit Properties

When configuring Port Properties on 2.5G MSM and 10G MSM boards (only), the Channelized mode can be selected on the *General* tab. Channelized mode permits to create a mix of virtually concatenated (VCAT) and Channelized circuits. Selecting Channelized mode automatically creates one VCAT circuit.

When Channelized mode is selected, the Port Properties window refreshes and two of its tabs disappear (SONET and PPP). The Port Properties differences have been discussed elsewhere in this chapter (*Figure:5G MSM OC-48c with Channelized Port Mode Option* for selecting Channelized mode; *J0/J1 Sub-Tab*, *SONET Error Insertion -- Channelized Mode*, and *Transmit Modes for POS Modules*). Some parameters that formerly were configured on the Port Properties pages are now configured on the Circuit Properties pages.

Circuits are arranged under the port. Selecting *Circuits and Timeslots* in the Resources tree will open a two-panel display of circuit information (for the current port), as shown in *Figure:Circuit List View and Circuit Detail View*. One panel is the circuit list, which is described in *Circuit List View*. The other panel to the right is the circuit detail panel, providing detailed configuration information for each circuit and enabling to add and delete circuits. *Circuit Detail View* for details.

Figure:Circuit List View and Circuit Detail View



Circuit List View

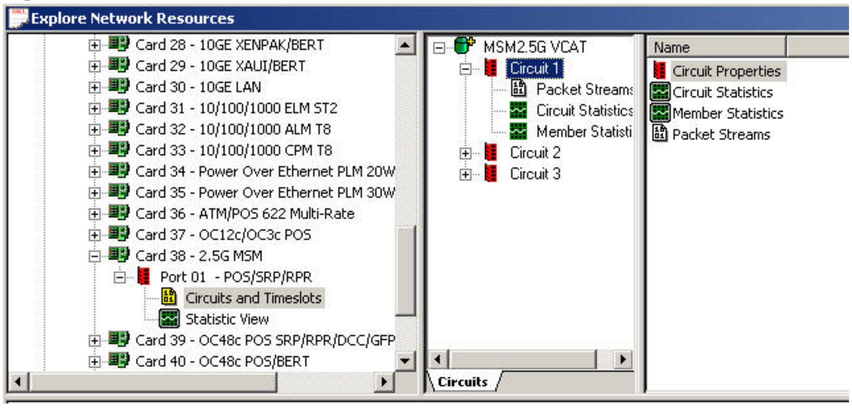
When a circuit is selected from the list, several options display which provide configuration capabilities or statistics collection/reporting for the selected circuit. *Figure:Circuit List View* shows a typical example. The options presented include:

- Circuit Properties (listed in the detail panel)–*Circuit Properties Overview*.
- Packet Streams–this grid has several tabs, depending on Payload Type (set in the Circuit Properties configuration):

- GFP Data–these parameters are defined in *Table:GFP Data Tab Display*.
- Frame/Stream Data–these parameters are defined in *Table:ATM Stream Queue Grid*.
- Gap/Rate Control–these parameters are defined in *Table:Stream Edit Available Fields*.
- DA/SA Data–these parameters are defined in *Table:ATM Stream Queue Grid*.
- Data Link & IP–these parameters are defined in *Table:ATM Stream Queue Grid*.

- *Circuit Statistics*
- *Member Statistics*

Figure:Circuit List View



Right-clicking a circuit in the list opens an options menu that includes:

- Clear All Statistics–clears per-circuit and member statistics.
- IxRouter–Opens the IxRouter window. For more information on IxRouter window function for IxExplorer, *IxRouter Window*. For more information on Protocols available, see the IxNetwork User Guide.
- Generate Tcl Script–Activates the ScriptGen feature and allows for the generation of Tcl configuration script. ScriptGen for details.
- Run Tcl Script–opens a sub-menu,Run Tcl Script...
- Properties–circuit properties, *Circuit Properties Overview*.

Right-clicking Packet Streams under a circuit opens a sub-menu of options similar to that for Streams (*Table:Stream Editing Pop-Up Menu Choices*). Start/Stop/Step Transmit and Start/Stop Capture are greyed out because transmission cannot be controlled on a per-circuit basis.

Right-clicking a statistics view also has the transmit and capture buttons greyed out, for the same reason.

Circuit Statistics

Circuit level statistics are shown per-circuit and displays only if the circuit is a VCAT group. Port level statistics are shown under the port.

Member Statistics

Member level statistics are shown per-member under a circuit. This is similar to the statview for multiple ports. This does not have traffic generation information. Member stats display VCAT/SONET path level information.

Circuit Detail View

The Circuit Detail View displays configuration details for each circuit and enables the adding and removal of circuits from the port. The circuit view panel has three tabs:

- *Circuit Setup Grid*
- *Circuit Properties Grid*
- *PPP Grid*

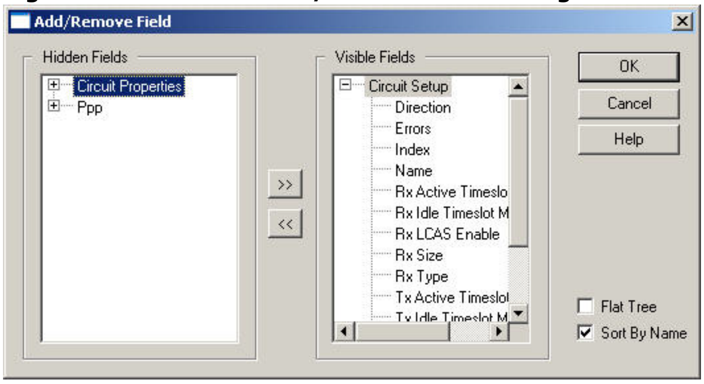
With the cursor placed anywhere on any of the circuit rows, right-click to display the options menu:

- New Circuit(s)–to add a new circuit (row) to the listing
- Copy Circuit(s)–to copy a circuit
- Paste Circuit(s)–to paste a copied circuit (you will be prompted to enter a quantity)
- Delete Circuit(s)–to delete selected circuit(s)
- Duplicate Circuit(s)–to duplicate selected circuit(s)
- Increment/Decrement–opens a sub-menu: Increment, Increment by, Decrement, Decrement by, and Same
- View Options–opens sub-menu to change the display: Add/Remove Field or Change View Order (of columns)–*Circuit Detail Add or Remove Field*.

Circuit Detail Add or Remove Field

To create or modify a customized spreadsheet view, use the >> arrow to move a *Hidden Field* to the *Visible Fields* list and << to move a *Visible Field* to the *Hidden Fields* list. The columns in a view may be moved by selecting a column in the spreadsheet and moving it to its new location (using the mouse click-and-drag method). A red line indicates where it will be placed when the mouse button is released.

Figure:Circuit Detail—Add/Remove Field Dialog

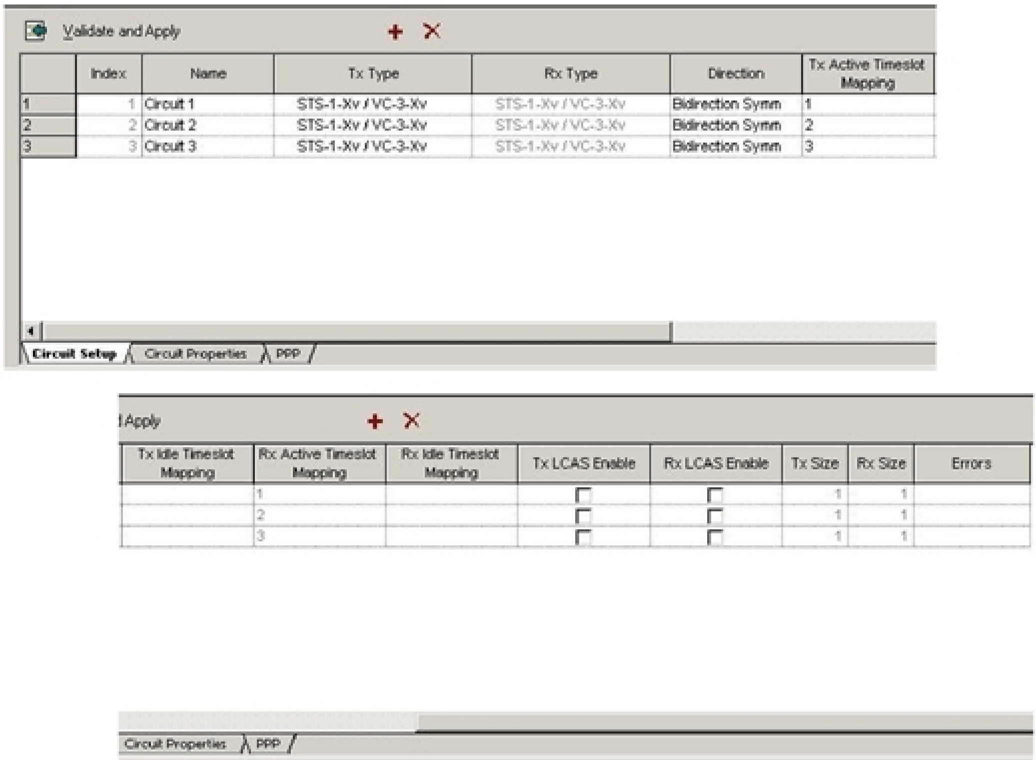


Three views are pre-programmed. These views are shown in *Figure:Circuit Setup Grid (in two segments)* and described in *Table:Circuit Setup Fields and Controls.*

Circuit Setup Grid

The Circuit Setup tab is shown in *Figure:Circuit Setup Grid (in two segments)*; it has been segmented to fit on the page.

Figure:Circuit Setup Grid (in two segments)



Definitions of the Circuit Setup grid elements are provided in *Table:Circuit Setup Fields and Controls.*

Table:Circuit Setup Fields and Controls

Field or Control	Description
Add New Circuit	Click button to add a new circuit. Inserts a new row for each new circuit. The new row displays a background color different from the validated rows.
Delete Circuit	Click button to delete the highlighted circuit.
Validate and Apply	Click to validate an added or changed circuit and apply changes to the port. All circuits entered by you will be validated top to bottom. Invalid circuits will have the corresponding rows displaying a different background color. (Invalid circuits have an Error field on the far right end of the row, which specifies why the circuit cannot be validated.) A pop-up message informs that not all circuits are valid. When all circuits are valid, clicking the Apply button sends commands to the server and applies current configurations.
Index	Read-only. Circuit index.
Name	Circuit name.
Tx Type	Select from pulldown: • STS-1/VC-3 • STS-3c/VC-4

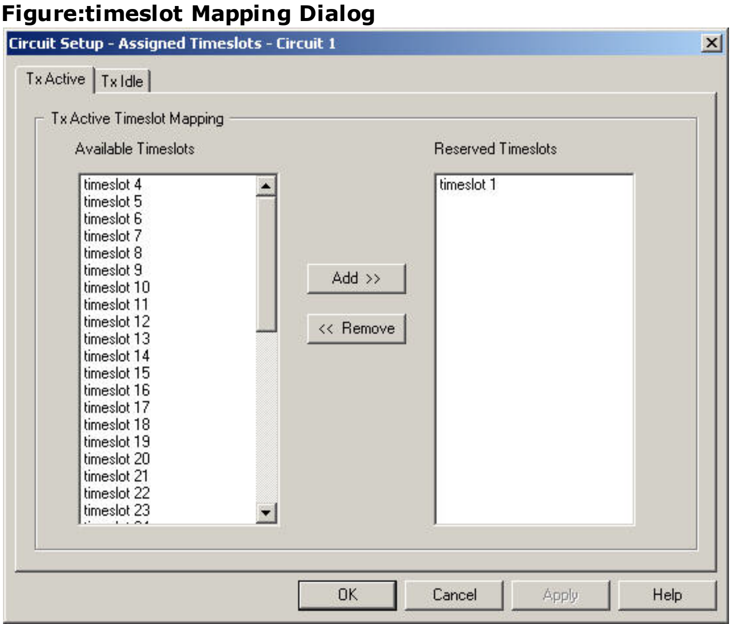
Field or Control	Description
	• STS-12c/VC-4-4c • STM-0 • STM-16 • STS-1-Xv • STS-3c-Xv • VC-3-Xv • VC-4-Xv • STS-48c/VC-4-16c (addition for MSM 10G only)
Rx Type	Select from pulldown: • STS-1/VC-3 • STS-3c/VC-4 • STS-12c/VC-4-4c • STM-0 • STM-16 • STS-1-Xv • STS-3c-Xv • VC-3-Xv • VC-4-Xv • STS-48c/VC-4-16c (addition for MSM 10G only)
Direction	Select from pulldown: Unidirection Tx Unidirection Rx Bidirection Symmetrical Bidirection Asymmetrical NOTE if Circuit Type is not a VCAT group, Direction must be Bidirectional Symmetrical.
Tx Active Timeslot Mapping	The starting slot number. When Direction is Unidirectional Tx, Receive Mappings are grayed out. When Direction is Unidirectional Rx, Transmit Mappings are grayed out. When Direction is Bidirectional Asymmetrical, both are available. When Direction is Bidirectional Symmetrical, only the Transmits are editable, and the Receives copy the values. Double-click this value to open the *Timeslot Mapping Dialog* for active and idle timeslots.
Tx Idle Timeslot Mapping	See TxActive Timeslot Mapping, above. Double-click this value to open the *Timeslot Mapping Dialog* for active and idle timeslots.
Rx Active Timeslot Mapping	See TxActive Timeslot Mapping, above. Double-click this value to open the *Timeslot Mapping Dialog* for active and idle timeslots.

Field or Control	Description
Rx Idle Timeslot Mapping	See TxActive Timeslot Mapping, above. Double-click this value to open the *Timeslot Mapping Dialog* for active and idle timeslots.
Tx LCAS Enable	Enable or disable. Grayed out if selected Circuit Type (Tx Type and Rx Type) is not a VCAT group.
Rx LCAS Enable	Enable or disable. Grayed out if selected Circuit Type (Tx Type and Rx Type) is not a VCAT group.
Tx Size	Read-only.
Rx Size	Read-only.
Errors	Errors that are generated when Validate fails.

Timeslot Mapping Dialog

Use the timeslot mapping dialog to make a list of timeslots that are to be used by the circuit that is being configured. Select one or more of the Available Timeslots (free timeslots) and assign them to the map (Reserved Timeslots). To open this dialog, double-click any of the timeslot mapping fields in the Circuit Setup grid. The timeslot mapping dialog is shown in *Figure:timeslot Mapping Dialog*. It has two tabs, Active and Idle, for configuring both active and idle (backup) timeslots.

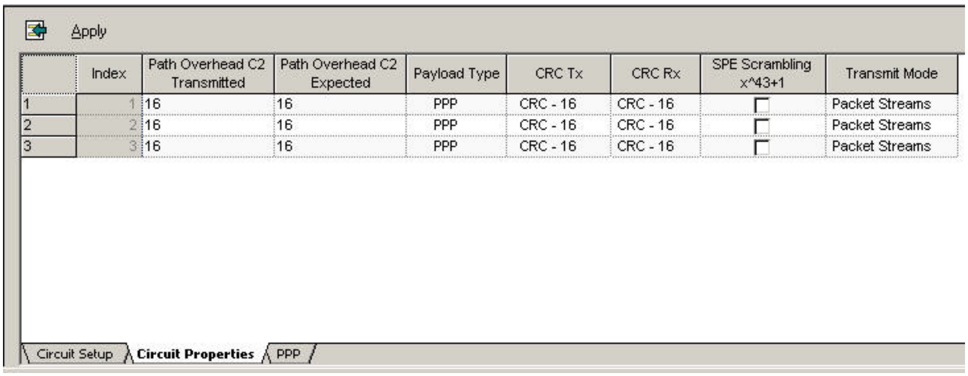
Figure:timeslot Mapping Dialog



Circuit Properties Grid

The Circuit Properties grid displays values that are configured on the Circuit Properties–SONET page. *SONET Circuit Properties* for details. *Figure:Circuit Properties Grid* shows the Circuit Properties grid.

Figure:Circuit Properties Grid



The Circuit Properties grid elements are described in *Table:Circuit Properties Fields and Controls*.

Table:Circuit Properties Fields and Controls

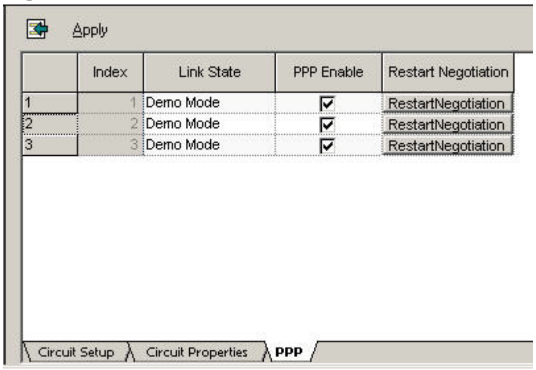
Field or Control	Description
Apply	Click button to apply changes to port. Sends commands to the server and applies current configurations.
Index	Read-only. Circuit index.
Path Overhead C2 Transmitted	The value of the C2 byte in the transmitted header. (Hex) To set this value, double-click this value to open the Circuit Properties–SONET tab.
Path Overhead C2 Expected	The expected value of the link partner’s C2 byte. Typically, this will match the value in the *Transmit* field. (Hex) To set this value, double-click this value to open the Circuit Properties–SONET tab.
Payload Type	Select from pulldown: • PPP • Cisco HDLC • Frame Relay (RFC 2427) • Cisco Frame Relay • GFP • Other • Double-click this value to open the Circuit Properties–SONET tab.
CRC Tx	Select transmission from pulldown: • CRC-16 • CRC-32 Double-click this value to open the Circuit Properties–SONET tab.
CRC Rx	Select reception from pulldown: • CRC-16 • CRC-32

Field or Control	Description
	Double-click this value to open the Circuit Properties–SONET tab.
SPE Scrambling x^43+1	Click to enable. If enabled, data is scrambled with the $x^{43} + 1$ polynomial. Double-click this value to open the Circuit Properties–SONET tab.
Transmit Mode	Select from pulldown: • Packet Streams • Advanced Scheduler For details, *Table:Transmit Modes Tab (shown for OC-192c POS/BERT/10GE WAN).* Double-click this value to open the Circuit Properties–Transmit Modes tab.

PPP Grid

The PPP grid displays values that are configured in the Circuit Properties–PPP page. *PPP Circuit Properties* for details. The PPP grid is shown in *Figure:PPP Grid*.

Figure:PPP Grid



The fields and controls in this tab are identical to those on the Port Properties–PPP–Negotiation tab, described in *Table:PPP Negotiation Tab*.

Circuit Properties Overview

Each circuit can be a single timeslot (STS-1/STS-3c/STS-12c/STS-48c, and so on) or a group of VCAT timeslots. Properties that are applicable to the entire port are configured at the port level (using Port Properties) while properties that are applicable to the circuit are configured at the circuit level using Circuit Properties. Each circuit has its own stream engine and statistics.

Each Circuit Properties window has individual tabs for:

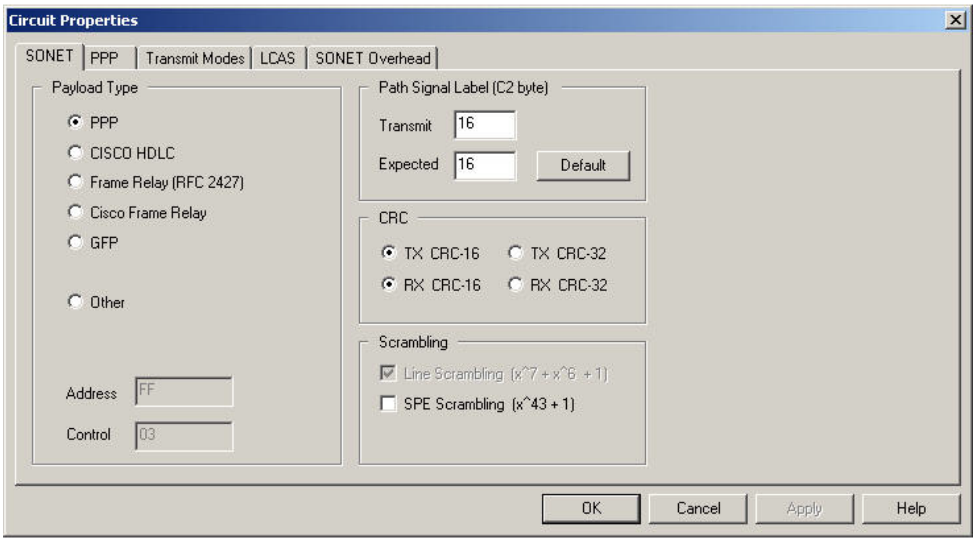
- *SONET Circuit Properties*
- *PPP Circuit Properties*
- *Transmit Modes Circuit Properties*
- *LCAS Circuit Properties*

- *SONET Overhead Circuit Properties*
- GFP Circuit Properties

SONET Circuit Properties

The *SONET* tab is accessed by right-clicking a circuit in the Circuits window, selecting the *Properties* menu option, then selecting the *SONET* tab, which is shown in *Figure:Circuit Properties–SONET*.

Figure:Circuit Properties–SONET



The fields and controls in these tabs are described in *Table:Circuit Properties–SONET Tab*.

Table:Circuit Properties–SONET Tab

Section	Field/Control	Description
Payload Type		NOTE The choice of Payload Type in this tab is reflected in the Stream Properties/Frame Data/Protocols dialogs.
	PPP	Selects fixed PPP address, control, and protocol header values.
	CISCO HDLC	Selects Cisco proprietary address, control, and protocol header values. HDLC = High-level Data Link Control, a data link layer protocol.
	Frame Relay (RFC 2427)	Selects Frame Relay address, control, and protocol header values.
	Cisco Frame Relay	Selects Cisco proprietary Frame Relay address, control, and protocol header values.
	GFP	Selects Generic Framing Procedure (GFP). If selected, the GFP tab will appear (after clicking Apply). *GFP Circuit Properties*.
	Other	Allows to select values for Address and Control as described in the next two rows.
	Address	When *Other* header is selected, allows the setting of the values for the SONET header address field; otherwise, reflects the fixed values asso-

Section	Field/Control	Description
		ciated with the header choice.
	Control	When *Other* header is selected, allows the setting of the values for the SONET header control field; otherwise, reflects the fixed values associated with the header choice.
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted header. (Hex)
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both Transmit and Expected values to the default value corresponding to the payload type selected. (Example: PPP = 16.)
CRC	TX CRC-16	Selects transmission with 16-bit CRC.
	RX CRC-16	Selects reception with 16-bit CRC.
	TX CRC-32	Selects transmission with 32-bit CRC.
	RX CRC-32	Selects reception with 32-bit CRC.
Scrambling	Line Scrambling (x^7 + x^6 + 1)	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling (x^43 + 1)	If enabled, data is scrambled with the $x^{43} + 1$ polynomial.

PPP Circuit Properties

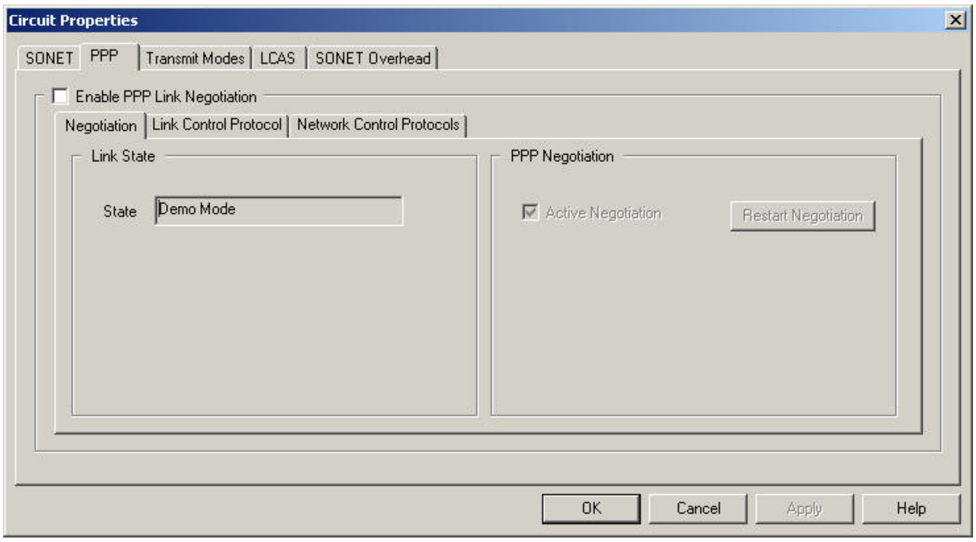
Point to Point Protocol (PPP) properties for Packet over SONET modules are configured using the *PPP* tab, which has three sub-tabs, described in the following sections:

- *PPP Negotiation*
- *PPP Link Control Protocol*
- *PPP Network Control Protocols*

PPP Negotiation

The PPP *Negotiation* sub-tab is shown in *Figure:Circuit Properties–PPP–Negotiation Tab*. This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* option, selecting the *PPP* tab, then selecting the *Negotiation* sub-tab (which is the default).

Figure:Circuit Properties–PPP–Negotiation Tab

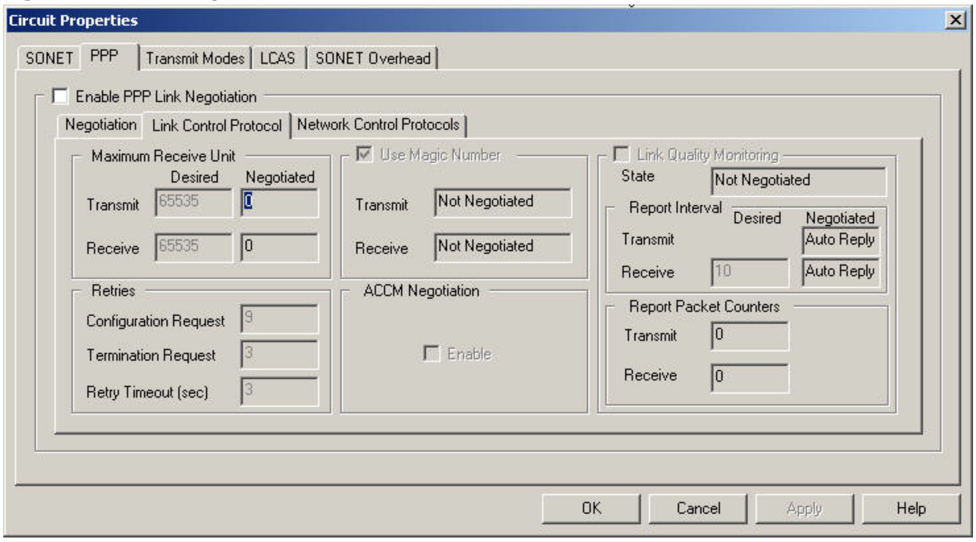


The fields and controls in this tab are identical to those on the Port Properties–PPP–Negotiation tab, described in *Table 19-3. PPP Negotiation Tab*.

PPP Link Control Protocol

The PPP *Link Control Protocol* sub-tab is shown in *Figure:Circuit Properties–PPP–Negotiation Tab*. This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* option, selecting the *PPP* tab, then selecting the *Link Control Protocol* sub-tab.

Figure:Circuit Properties–PPP–Link Control Protocol Tab



The fields and controls in this tab are identical to those on the Port Properties–PPP–Link Control Protocol tab, described in *Table:PPP Link Control Protocol Sub-Tab*.

PPP Network Control Protocols

PPP Network Control Protocols (NCP) are designed to assign and manage network layer addresses and configuration on Point-to-Point links. PPP allows self-configuration by providing numerous options that can be negotiated with the other peer on the link. Each of the peers describes its capabilities and requirements. NCP packets cannot be exchanged until the PPP negotiation has completed the Link Control Protocol phase, optional authentication phase, and reached the Network-Layer Protocol phase. Exactly one NCP packet can be carried in the Information field of a PPP Data Link Layer frame, with the Protocol Type field set to the corresponding value.

The PPP *Network Control Protocols* sub-tab shows the different network protocols that can be negotiated in the IxExplorer GUI. There are individual configuration sub-tabs for each of the protocols, described in the following sections:

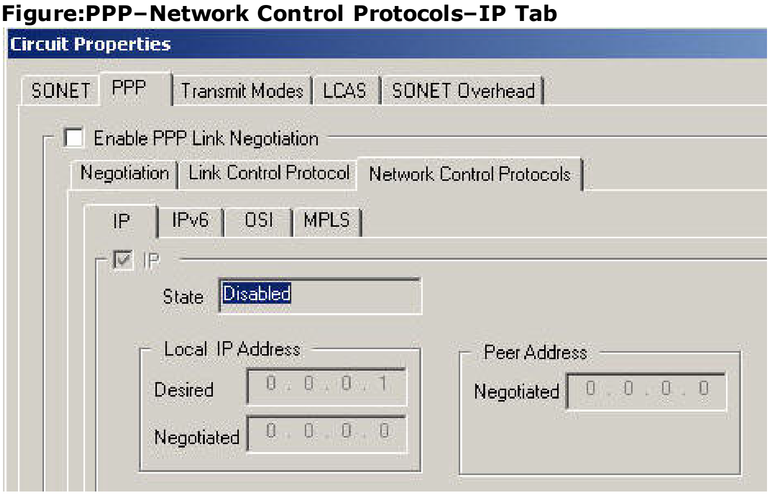
- *Network Control Protocols–IP*
- *Network Control Protocols–IPv6*
- *Network Control Protocols–OSI*
- *Network Control Protocols–MPLS*

Network Control Protocols–IP

The PPP Network Control Protocols *IP* sub-tab is shown in *Figure:PPP Network Control Protocols–IPv6*. This sub-tab is used to configure the Internet Protocol Control Protocol (IPCP) on the link. IPv4 data packets may be exchanged only after the IPv4 control protocol has reached the Opened state.

This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocols* sub-tab, then selecting the *IP* sub-tab (which is the default).

Figure:PPP–Network Control Protocols–IP Tab



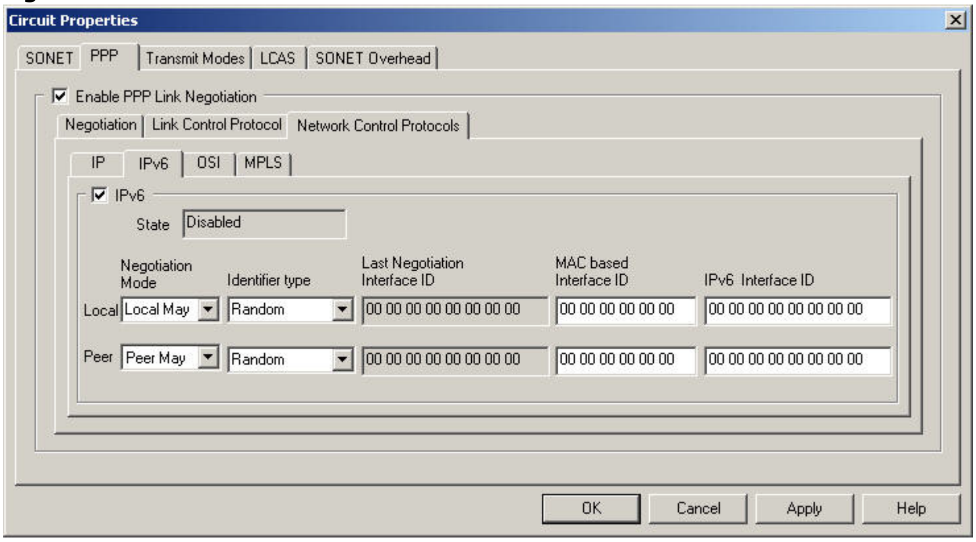
The fields and controls in this tab are identical to those on the Port Properties–PPP–Network Control Protocols–IP sub-tab, described in *Table:PPP Network Control Protocols—IP*.

Network Control Protocols–IPv6

The PPP Network Control Protocols *IPv6* sub-tab is shown in *Figure:PPP Network Control Protocols–IPv6*. This sub-tab is used to configure the Internet Protocol Version 6 Control Protocol (IPv6CP), defined in RFC 2472.

IPv6 data packets may be exchanged only after the IPv6 control protocol has reached the Opened state. This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, then selecting the *IPv6* sub-tab.

Figure:PPP Network Control Protocols–IPv6



For further information on IPv6 and a diagram of the IPv6 Interface ID, see the NCP—Network Control Protocols section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The fields and controls in this tab are identical to those on the Port Properties–PPP–Network Control Protocols–IPv6 sub-tab, described in *Table:PPP Network Control Protocols—IPv6*.

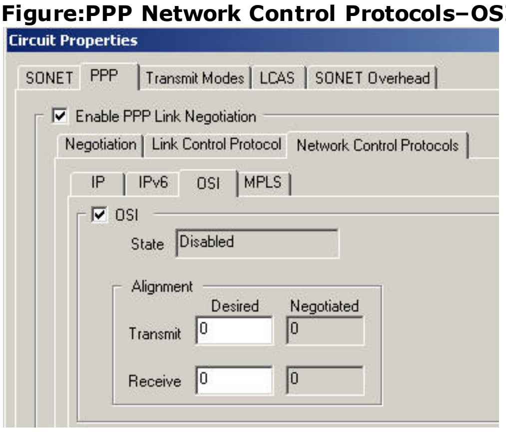
Network Control Protocols–OSI

The PPP Network Control Protocols *OSI* sub-tab is shown in *Figure:PPP Network Control Protocols–OSI.* This tab is used to configure the OSI Network Layer Control Protocol (OSINLCP) Configuration Options, as specified in RFC 1377. OSI data packets may be exchanged only after the OSI control protocol has reached the Opened state.

This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, then selecting the *OSI* sub-tab.

This configuration option is identical to that described in detail at *PPP Network Control Protocols—OSI*.

Figure:PPP Network Control Protocols–OSI



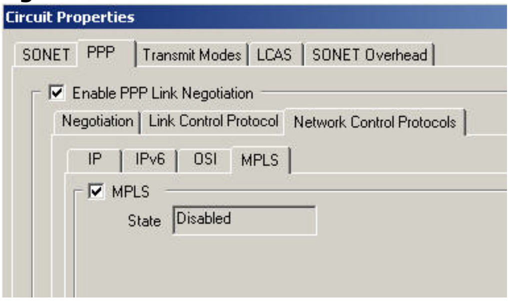
The fields and controls in this tab are identical to those on the Port Properties–PPP–Network Control Protocols–OSI sub-tab, described in *Table:PPP Network Control Protocols—OSI*.

Network Control Protocols–MPLS

The PPP Network Control Protocols *MPLS* sub-tab is shown in *Figure:PPP Network Control Protocols–MPLS .* A node that sends an MPLS configuration request is advertising to its peer that it supports MPLS on that link.

This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *PPP* tab, selecting the *Network Control Protocol* sub-tab, and then selecting the *MPLS* sub-tab.

Figure:PPP Network Control Protocols–MPLS



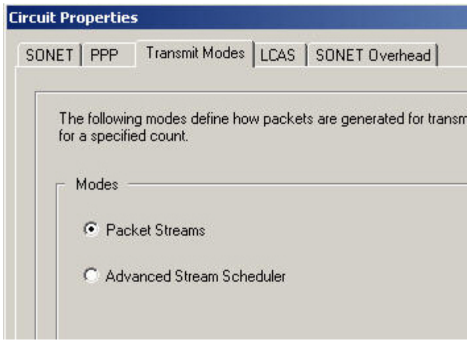
The fields and controls in this tab are identical to those on the Port Properties–PPP–Network Control Protocols–MPLS sub-tab, described in *Table:PPP Network Control Protocols—MPLS*.

Transmit Modes Circuit Properties

The *Transmit Modes* tab is available for for 2.5G MSM and 10G MSM load modules and allows to select the transmission mode for the circuit. The *Transmit Modes* tab is accessed by right-clicking a circuit, selecting *Properties* from the menu options, then selecting the *Transmit Modes* tab.

It specifies the packet stream mode by default, as shown in *Table:PPP Network Control Protocols—MPLS*.

Figure:Circuit Properties–Transmit Modes



The various types of transmit modes which may be selected in the *Transmit Mode* tab are described in *Figure:Circuit Properties–Transmit Modes*.

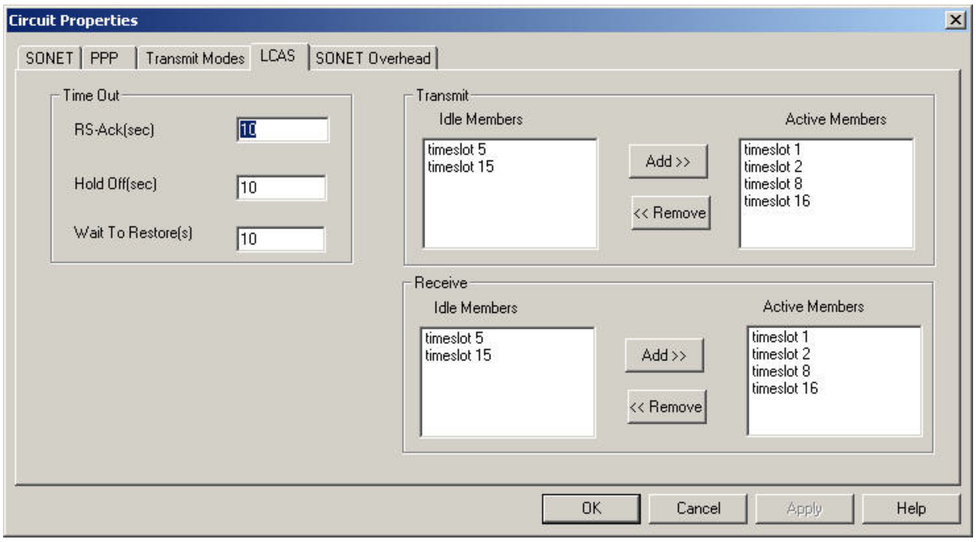
LCAS Circuit Properties

The Circuit Properties–LCAS tab is used to set LCAS configuration parameters and create LCAS commands.

The following parameters are configured per-circuit on the LCAS page.

- Rs-Ack Time Out value (sec)
- HoldOff Time Out value (sec)
- Wait to Restore Time Out value (sec)

Figure:Circuit Properties–LCAS



The ADD and REMOVE buttons will move members from the Idle Members list to the Active Members list (for ADD), and from the Active list to the Idle list (for REMOVE).

SONET Overhead Circuit Properties

The SONET Overhead is configured using the following set of sub-tabs found in the *SONET Overhead* tab:

- *SONET Overhead J1 Sub-Tab*
- *SONET Overhead Error Insertion*

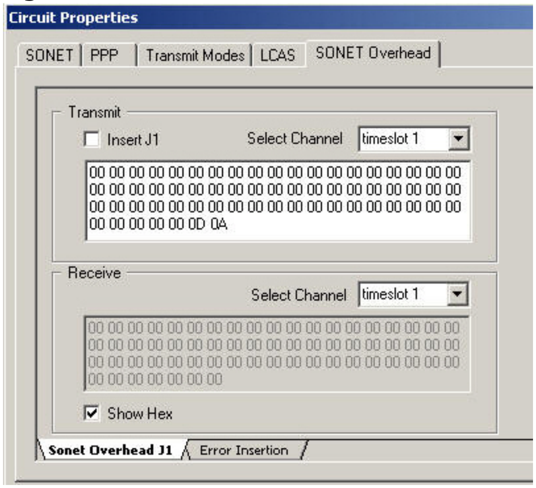
This tab is accessed by right-clicking a circuit, selecting the *Properties* options and then selecting the *SONET Overhead* tab.

SONET Overhead J1 Sub-Tab

The *J1* sub-tab allows to configure and insert J1 trace messages into the overhead for the SONET frames. The SONET Overhead *J1* sub-tab is shown in *Figure:SONET Overhead–J1*.

This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *SONET Overhead* tab, then selecting the *J1* sub-tab (the default).

Figure:SONET Overhead–J1



The controls and fields in the *J1* sub-tab are described in *Table:J1 Sub-Tab*.

Table:J1 Sub-Tab

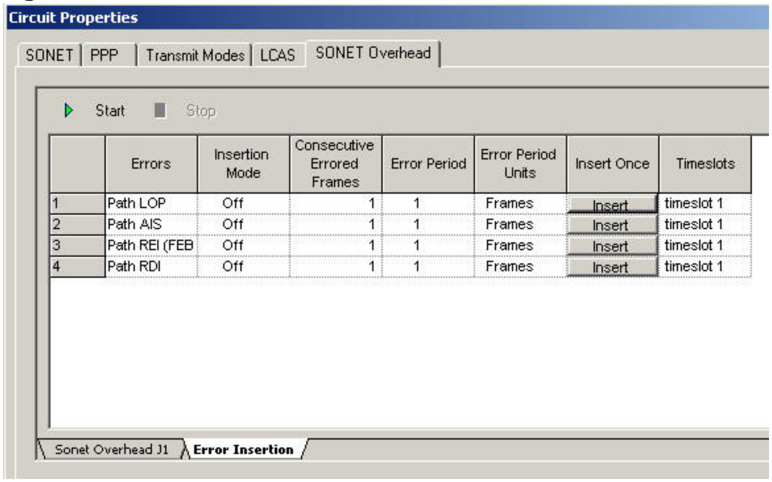
Byte	Operation	Field/Control	Usage
J1	Transmit	Insert J1	Check this box to enable the insertion of a J1 (Path Trace) byte into the SONET frame Path overhead. **NOTE** When Channelized mode is selected for 2.5G MSM or 10G MSM boards (on the General tab), J1 moves from Port Properties to this location–the SONET Overhead tab in Crcuit Properties.
		(J1 Field)	Enter the hex value for the J1 bytes according to the rules stated in *Table:SONET Framing Mode—Rules*.
	Receive		If the Rules (in *Table:SONET Framing Mode—Rules*) are followed in configuring for transmission in the upper part of the sub-tab, you will see that the Trace Message is received in the message field in the lower part of the sub-tab.
		Show Hex	Check this box to display the contents of the J1 byte in hexadecimal format, for Transmit and Receive.

SONET Overhead Error Insertion

SONET Error Insertion -- Channelized Mode

The *Circuit Properties* SONET Overhead *Error Insertion* sub-tab for 2.5G MSM and 10G MSM load modules provides only path type errors that can be inserted, as shown in *Figure:SONET Overhead–Error Insertion*. Section and line type errors are inserted from SONET Overhead tab in *Port Properties–SONET Error Insertion -- Channelized Mode*.

Figure:SONET Overhead–Error Insertion



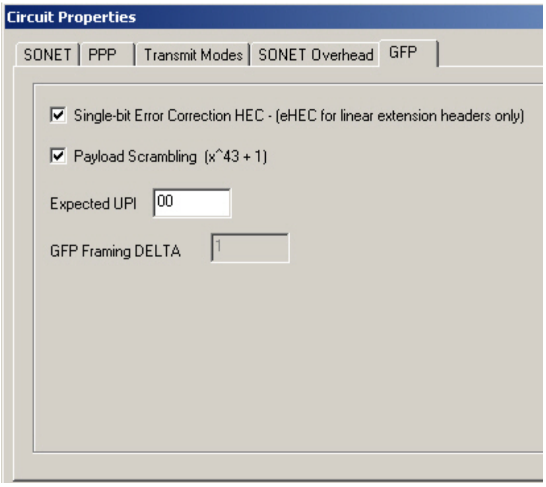
The grid specifies how these errors are inserted into the SONET frame. The grid is described in *Table:SONET Overhead Error Insertion Sub-Tab*.

This sub-tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *SONET Overhead* tab, then selecting the *Error Insertion* sub-tab.]

GFP Circuit Properties

The *GFP* tab is accessed by right-clicking a circuit, selecting the *Properties* options, selecting the *GFP* tab. The *GFP* tab is only present when, in the *SONET* tab, the payload type **GFP** is selected.

Figure:GFP Circuit Properties



The controls and fields defined in *Table:GFP Circuit Properties* are configured per-circuit on the GFP tab.

Table:GFP Circuit Properties

Field/Control	Usage
Single-bit error correction HEC	(eHEC for linear extension headers only) When this is check box is selected, single-bit error correction is used. No error correction is performed otherwise.
Payload Scrambling	Selecting this check box enables payload scrambling using the

Field/Control	Usage
(x^43+1)	listed algorithm.
Expected UPI	User Payload Identifier. *Table:GFP Payload Header Configuration* for details.
GFP Framing DELTA	(grayed-out) Controls state machine transitions. The number of cHEC matches needed (+1) to move the state machine from the *hunt* state to the *sync* state.

Chapter 20 - Port Properties–10 GE and UNIPHY Families

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog is a display that corresponds to the module type. The following sections describe the functions and configuration of the 10 Gigabit Ethernet and UNIPHY family of module port properties.

Port properties differ for the various module types, and are described in the following sections.

- *Port Properties for 10 Gigabit Modules*(including the 10GE LSM)
- *Port Properties for UNIPHY Modules* (including the 10GE MSM)
- *Channelized BERT*

NOTE BERT, VSR, SRP, RPR, and DCC are also available on some 10 Gigabit Ethernet and UNIPHY modules. See Chapter 19, *Port Properties–POS and ATM Families* for more information.

For NGY port properties, see Chapter 22, *Port Properties– NGY Family*.

For FCM port properties, see Chapter 23, *Port Properties– FCM Family*.

For Xcellon-Flex port properties, see Chapter 24, *Port Properties– Xcellon-Flex Family*.

Port Properties for 10 Gigabit Modules

The 10 Gigabit Ethernet *Port Properties* dialog is accessed by right-clicking a 10 Gigabit Ethernet port in the Resources pane, then selecting the *Properties* menu option.

The complete specification for the 10 Gigabit type boards can be found in the *Ixia Platform Reference Manual*.

- 10 Gigabit Load Module Specifications

  Ixia 10 Gigabit Ethernet (10GE) modules support speeds of 10 gigabits per second (10,000 Mbps). There are two general families of these modules:

- **10 GE LAN** (including XAUI and XENPAK) Modules—*10GE LAN Port Properties*.
- **10 GE WAN** Modules—*10GE WAN Port Properties*.

Port Properties for BERT for additional information on Bit Error Rate Testing (BERT).

The 10 Gigabit characteristics are defined in the IEEE 802.3ae standard. For more information about this standard and 10 Gigabit architecture, see the 10GE section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

10GE LAN Port Properties

NOTE For information on 10GE WAN modules, *10GE WAN Port Properties*.For NGY port properties, *Port Properties–NGY Family*.

There are three general types of 10GE LAN modules: 10GE XAUI and XENPAK modules, 10GE LAN modules, and 10GE LSM modules. BERT capabilities are available for the XAUI and XENPAK modules.

- 10GE XAUI and XENPAK Modules:
  - The following port property tabs are available for 10GE XAUI, and 10GE XENPAK and XENPAK-M modules without BERT enabled:
    - *10GE Port Properties–Preamble*
    - *10GE Port Properties—General*
    - *10GE XENPAK or 10GBASE-T Port Properties–LASI* (XENPAK Only)
    - *10GE Port Properties–Flow Control*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–Advanced MII*
    - *10GE Port Properties—SerDes*
    - *10GE Port Properties–Link Fault Signaling*
    - *10GE Port Properties—Lane Skew*
  - The following port property tabs are available for 10GE XAUI and 10GE XENPAK modules with BERT enabled:
    - *10GE Port Properties—General*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–Advanced MII*
    - *10GE Port Properties—SerDes*
    - *10GE Port Properties–Link Fault Signaling*
    - *10GE Port Properties—Lane Skew* (not available for XAUI channelized BERT)
  - **10GE LAN Modules—**The following port property tabs are available for 10GE LAN (and 10GE LAN-M) modules:
    - *10GE Port Properties–Preamble*
    - *10GE Port Properties–Flow Control*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–Link Fault Signaling*
  - **10GE LSM Modules**
    - The following port properties are available for 10GE LSM modules using the XENPAK carrier card.
      - *10GE Port Properties—General*
      - *10GE LSM Port Properties–Xenpak*
      - *10GE Port Properties–Transmit Modes*
      - *10GE Port Properties–Preamble*
      - *10GE Port Properties–Flow Control*
      - *10GE Port Properties—Lane Skew*
      - *10GE Port Properties–Link Fault Signaling*
      - Auto Instrumentation tab, *Auto Instrumentation Tab for Ethernet Modules* (Chapter 18)

- The following port properties are available for 10GE LSM modules using the XFP carrier card.
    - *10GE Port Properties—General*
    - *10GE Port Properties–Preamble*
    - *10GE Port Properties–Link Fault Signaling*
    - *10GE Port Properties–Flow Control*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–XFP*
    - *10GE Port Properties–OAM*
    - Auto Instrumentation tab, *Auto Instrumentation Tab for Ethernet Modules* (Chapter 18)
- The following port properties are available for 10GE LSM modules using the 10GBASE-T adapter module.
    - *10GE LSM with 10GBASE-T Adapter—General Port Properties*
    - *10GE XENPAK or 10GBASE-T Port Properties–LASI*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–Preamble*
    - *10GE Port Properties–Flow Control*
    - Auto Instrumentation tab, *Auto Instrumentation Tab for Ethernet Modules* (Chapter 18)
- The following port properties are available for 10GE LSM MACSec module.
    - *10GE LSM XENPAK/XFP–General Port Properties*
    - *10GE Port Properties–Preamble*
    - *10GE Port Properties–Link Fault Signaling*
    - *10GE Port Properties–Flow Control*
    - *10GE Port Properties–Transmit Modes*
    - *10GE Port Properties–XFP*
    - *10GE Port Properties–OAM*
    - *10GE Port Properties–MACSec Tx/Rx Tabs*
    - *Auto Instrumentation for MACSec Load Modules*

10GE Port Properties—General

The *General* tab in the *Port Properties* dialog differs between XAUI, XENPAK, and 10GE LSM XENPAK load modules. The versions are:

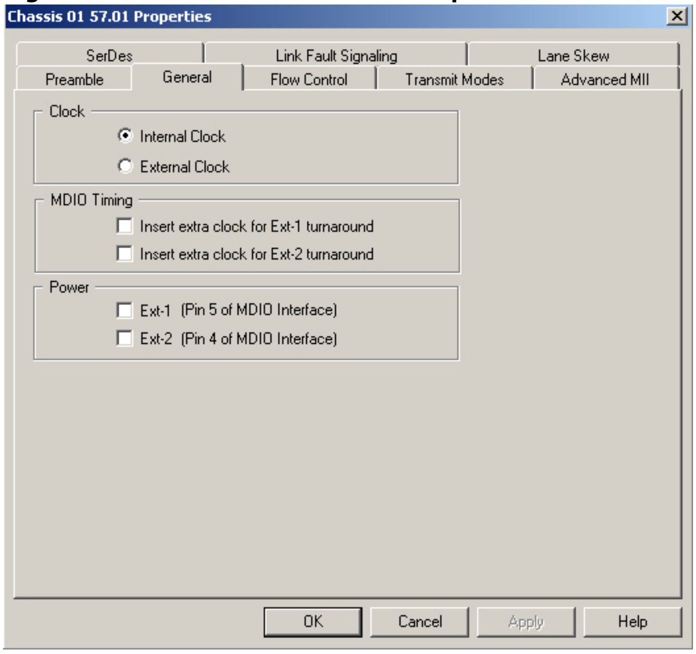
- *10 GE XAUI—General Port Properties*
- *10GE XENPAK—General Port Properties*
- *10GE LSM XENPAK/XFP–General Port Properties*
- *10GE LSM LAN/WAN—General Port Properties*
- *10GE LSM with 10GBASE-T Adapter—General Port Properties*
- *10GE Port Properties for Uniphy Modules—General Tab*

The *General* tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu options, then selecting the *General* tab.

10 GE XAUI—General Port Properties

The 10 GE XAUI Port Properties *General* tab is shown in *Figure:10 GE XAUI—General Port Properties*.

Figure:10 GE XAUI—General Port Properties



The fields and controls for this tab are described in *Figure:10GE XAUI—General Port Properties*.

Table:10GE XAUI—General Port Properties

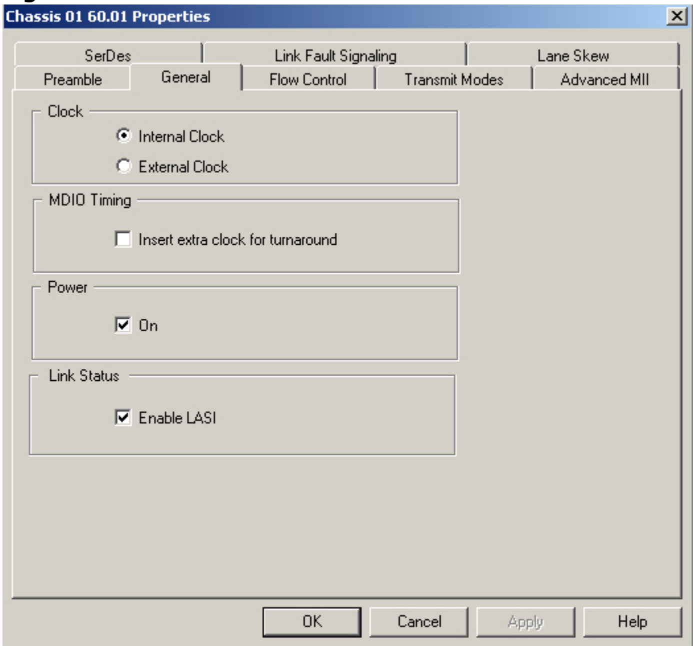
Section	Choices	Description
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from an external device connected to the Clock IN connector on the front panel of the module.
MDIO Timing	Insert extra clock for Ext-1 turnaround	Reserved for future use.
	Insert extra clock for Ext-2 turnaround	This option is used to aid in turnaround timing adjustments for a user's MII interface. When selected, the module provides 2-1/2 clocks of turnaround before clocking in MII data. When cleared, the module provides 1-1/2 clocks of turnaround before clocking in MII data.
Power	Ext-1 (Pin 5 of MDIO Interface)	Selecting this option applies 5V power, limited to 500ma current at Pin 5 of the D15 MDIO connector on the front panel. (Pins 9 through 15 of the MDIO connector are ground pins.)
	Ext-2 (Pin 4 of MDIO	(If an Ixia pod is not present, this power can be

Section	Choices	Description
	Interface)	utilized by the User, also.) Selecting this option applies 5V power, limited to 500ma current, at Pin 4 of the D15 MDIO connector on the front panel. (Pins 9 through 15 of the MDIO connector are ground pins.)

10GE XENPAK—General Port Properties

The 10 GE XENPAK Port Properties *General* tab is shown in *Figure:10GE XENPAK—General Tab*.

Figure:10GE XENPAK—General Tab



The fields and controls in this tab are described in *Table:10GE XENPAK Port Properties—General*.

Table:10GE XENPAK Port Properties—General

Section	Field/Control	Description
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from external device connected to the Clock IN connector on the front panel of the module.
MDIO Timing	Insert extra clock for turnaround	This option is used to aid in turnaround timing adjustments for a user's MII interface. When selected, the module provides 2-1/2 clocks of turnaround before clocking in MII data. When cleared, the module provides 1-1/2 clocks of turnaround before clocking in MII data
Power	On	A toggle to turn the power on or off.

Section	Field/Control	Description
Link Status	Enable LASI	If the box is selected, link status is detected through the SerDes lock, PMD, and Link Alarm Status Interrupt (LASI) line (output pin 9 from the XENPAK module). If the box is cleared, the link status is detected through the SerDes lock, and PMD.

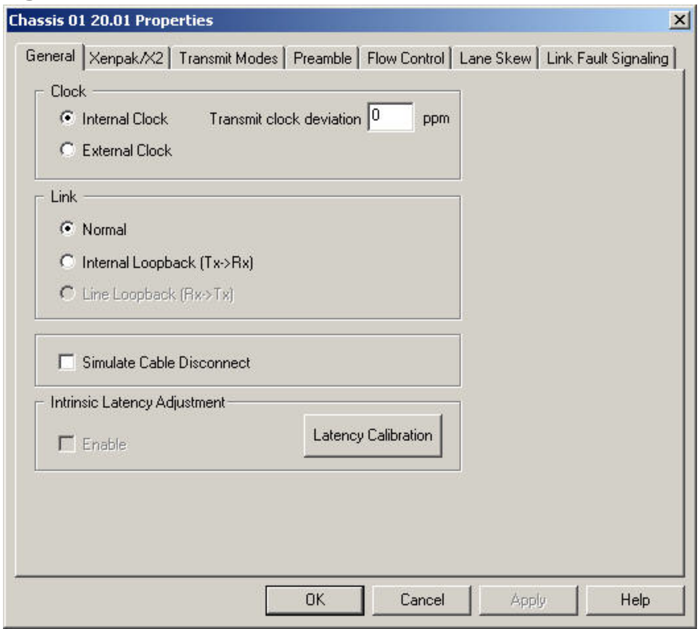
10GE LSM XENPAK/XFP–General Port Properties

For NGY modules, see *NGY Port Properties—General*.

For Xcellon-Flex modules, see *Flex Port Properties—General*.

The 10 GE XENPAK and XFP Port Properties *General* tab is shown in *Figure:10GE LSM XENPAK/XFP—General Tab*.

Figure:10GE LSM XENPAK/XFP—General Tab



The controls for the *General* tab configuration are described in *Table:10GE LSM XENPAK/XFP General Tab Configuration*.

Table:10GE LSM XENPAK/XFP General Tab Configuration

Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from an external device connected to the Clock IN connector on the front panel of the module.
	Transmit Clock Deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port.

Section	Control/Field	Usage
		10 GE LSM cards can be adjusted from -128 to +127 ppm from the initial rate.
Link	Normal	Normal operation
	Enable Internal Loopback (Tx -> Rx)	Check this box to enable/turn on the Internal Loopback—Transmit to Receive.
	Enable Line Loop-back (Rx -> Tx)	Check this box to enable/turn on the Line Loop-back—Receive to Transmit.
Simulate Cable Dis-connect		If this is selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific trans-ceiver. It is available if a value exists (in the .xml file). For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
	Latency Calibration	Click to run a Tcl script that measures intrinsic latency and stores the value in an .xml file. The button is only enabled for cards with trans-ceivers that have not been pre-measured for intrinisic latency by Ixia. The button will be grayed-out if any one of the following con-ditions are present: • there is no carrier • there is no transceiver • the transceiver is XFP or XAUI (which do not need to be calibrated) • the transceiver is XENPAK or X2 and a value is found for it in the list of pre-cal-ibrated values.

10GE LSM LAN/WAN—General Port Properties

The 10GE LSM LAN/WAN Port Properties *General* tab with WAN mode set is shown in *Fig-ure:10 GE LSM LAN/WAN—General Tab: WAN Mode*, and with LAN mode set is shown in *Fig-ure:10GE LSM LAN/WAN—General Tab: LAN Mode*. The 10GE LSM MACSec module is included in this grouping.

Figure:10 GE LSM LAN/WAN—General Tab: WAN Mode

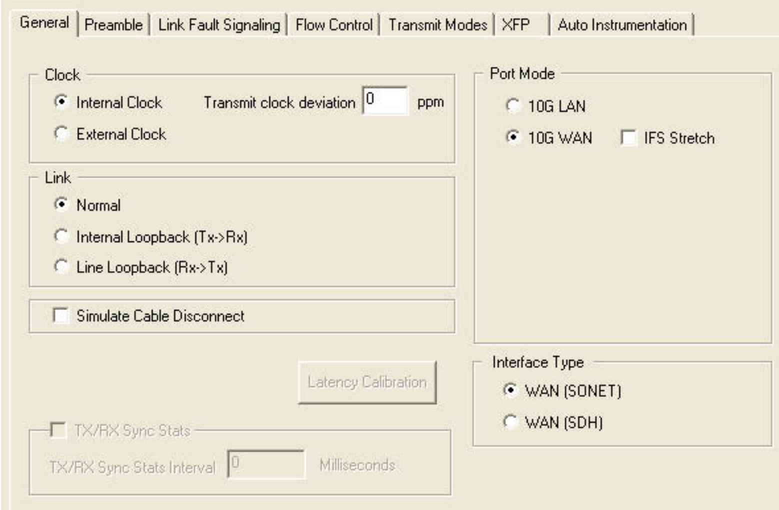
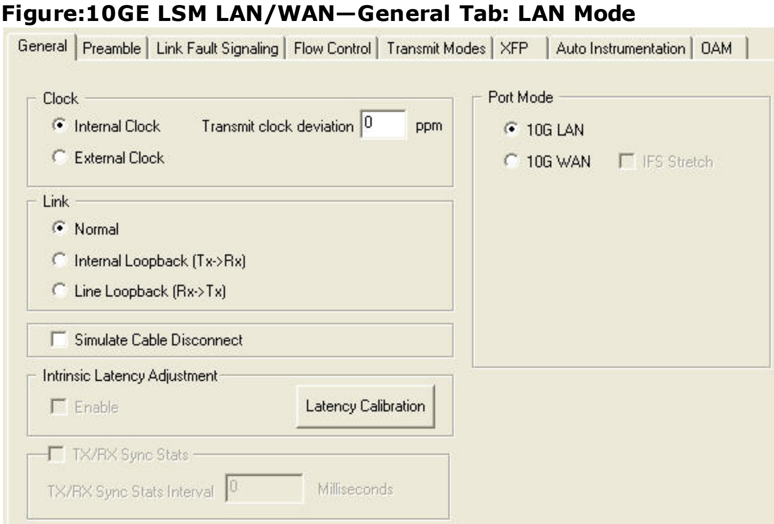


Figure:10GE LSM LAN/WAN—General Tab: LAN Mode



The controls for the *General* tab configuration are described in *Table:10GE LSM LAN/WAN General Tab Configuration*.

Table:10GE LSM LAN/WAN General Tab Configuration

Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from an external device connected to the Clock IN connector on the front panel of the module.
	Transmit Clock Deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port. 10 GE LSM cards can be adjusted from: • -127 to +128 ppm from the initial rate (LAN

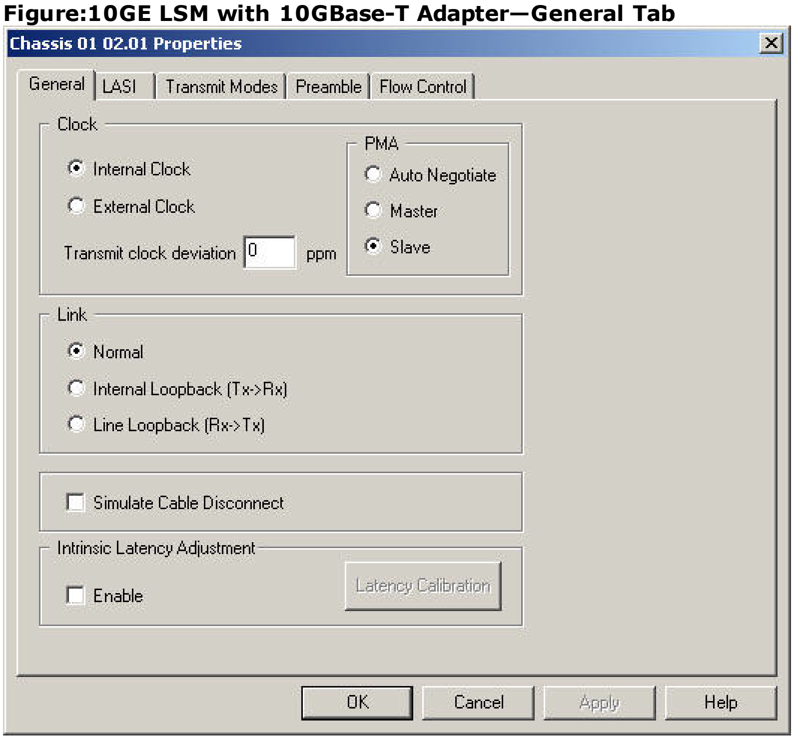
Section	Control/Field	Usage
		mode). • -127 to +128 (WAN mode).
Link	Normal	Normal operation
	Enable Internal Loopback (Tx -> Rx)	Check this box to enable/turn on the Internal Loopback–Transmit to Receive.
	Enable Line Loop-back (Rx -> Tx)	Check this box to enable/turn on the Line Loop-back–Receive to Transmit.
Port Mode	10G LAN	Sets the port to 10GE LAN mode (normal mode, only visible when the 10GE LSM is using a LAN/WAN XFP carrier card, set to LAN).
	10G WAN	Sets the port to 10GE WAN mode (only visible when the 10GE LSM is using a LAN/WAN XFP carrier card, set to WAN). When set to WAN mode, IFS Stretch becomes selectable.
	IFS Stretch	(WAN mode only) check box to enable WAN Interframe Spacing Stretch. Using this method, the frame rate is slightly lowered by adding additional IPG. In Packet Streams or Advanced Streams view with IFS Stretch mode enabled, the Line Rate will be 9,286 Mbps instead of 9,294 Mbps. And in Statistic View, the Line Speed will be characterized as 10GE WAN with IFSS. For details, see *IFS Stretch* in Chapter 18 of the *Ixia Hardware & Reference Manual*.
Interface Type	WAN (SONET)	Selects the SONET interface type (only visible when the 10GE LSM is using a LAN/WAN XFP carrier card, set to WAN).
	WAN (SDH)	Selects the SDH interface type (only visible when the 10GE LSM is using a LAN/WAN XFP carrier card, set to WAN).
Simulate Cable Dis-connect		If this is selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	LAN mode only. Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific trans-ceiver. It is available if a value exists (in the .xml file). For details, *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
	Latency Calibration	LAN mode only.

Section	Control/Field	Usage
		Click to run a Tcl script that measures intrinsic latency and stores the value in an .xml file. The button is only enabled for cards with transceivers that have not been pre-measured for intrinisic latency by Ixia. The button will be grayed-out if any one of the following conditions are present: • there is no carrier • there is no transceiver • the transceiver is XFP or XAUI (which do not need to be calibrated) • the transceiver is XENPAK or X2 and a value is found for it in the list of pre-calibrated values.

10GE LSM with 10GBASE-T Adapter—General Port Properties

The Port Properties *General* tab for the 10GE LSM with 10GBASE-T Adapter is shown in *Figure:10GE LSM with 10GBase-T Adapter—General Tab*.

Figure:10GE LSM with 10GBase-T Adapter—General Tab



The controls for the *General* tab configuration are described in *Table:10GE LSM with 10GBase-T Adapter General Tab Configuration*.

Table:10GE LSM with 10GBase-T Adapter General Tab Configuration

Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from an external device connected to the Clock IN connector on the front panel of the module.
	Transmit Clock Deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port. 10 GE LSM cards can be adjusted from: • -127 to +128 ppm from the initial rate (LAN mode). • -127 to +128 (WAN mode).
PMA	Auto Negotiate	If selected, determining which port is Master or Slave is performed **automatically**. (Enabling this check box disables the manual option for selecting Master or Slave.
	Master	If selected, port is configured as Master.
	Slave	If selected, port is configured as Slave.
Link	Normal	Normal operation
	Internal Loopback (Tx -> Rx)	Check this box to enable/turn on the Internal Loopback–Transmit to Receive.
	Line Loopback (Rx -> Tx)	(Disabled) Enable this check box to enable the Line Loopback–Receive to Transmit.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	LAN mode only. Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific transceiver. It is available if a value exists (in the .xml file). For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
	Latency Calibration	LAN mode only. Click to run a Tcl script that measures intrinsic latency and stores the value in an .xml file. The button is only enabled for cards with transceivers that have not been pre-measured for intrinisic latency by Ixia. The button will be

Section	Control/Field	Usage
		grayed-out if any one of the following conditions are present: • there is no carrier • there is no transceiver • the transceiver is XFP or XAUI (which do not need to be calibrated) • the transceiver is XENPAK or X2 and a value is found for it in the list of pre-calibrated values.

10GE XENPAK or 10GBASE-T Port Properties–LASI

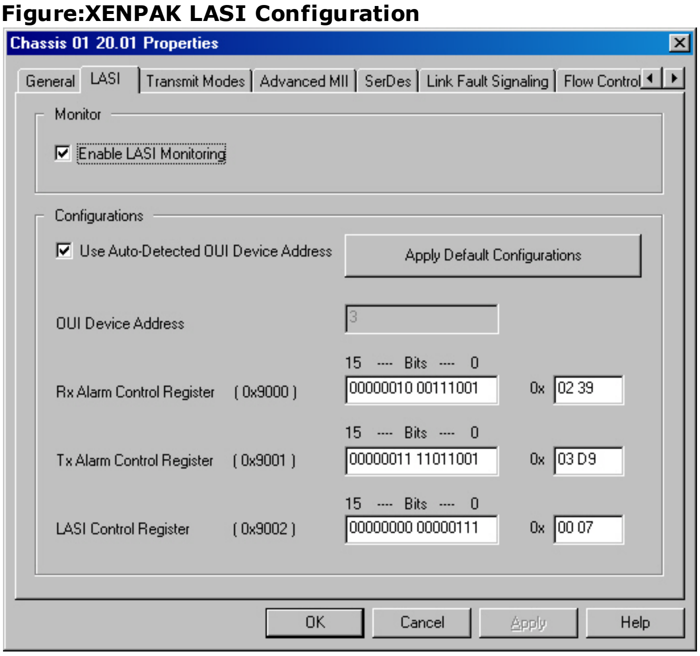
For NGY10GBASE-T module, *NGY 10GBASE-T Port Properties–LASI*.

The Link Alarm Status Interrupt (LASI) is an active-low output from the XENPAK module (or from the 10GBASE-T adapter) that indicates a link fault condition has been asserted or has been cleared. Control registers are provided so that LASI may be programmed to assert only for specific fault conditions.

For more detailed information on LASI, see the Link Alarm Status Interrupt (LASI) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The *LASI* tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu options, then selecting the *LASI* tab. The *LASI* tab page is shown in *Figure:XENPAK LASI Configuration*.

Figure:XENPAK LASI Configuration



The controls for LASI configuration are described in *Table:LASI Configuration*.

Table:LASI Configuration

Section	Control/Field	Usage
Monitor		Activates the LASI monitoring feature.
	Enable LASI Monitoring	Selecting this check box enables LASI monitoring.
Configurations		Controls LASI configuration.
	Use Auto-Detected OUI Device Address	Selecting this check box sets the OUI address to the detected address. If this is selected, then the OUI *Device Address* field is disabled.
	Apply Default Configuration	Selecting this button resets the LASI values to their default settings.
	OUI Device Address	The Organizationally Unique Identifier (OUI) device address, which signifies the device where the LASI control/status registers are located.
	Rx Alarm Control Register	Controls the register written at offset 0x9000, and indicates what type of receive path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	Tx Alarm Control Register	Controls the register written at offset 0x9001, and indicates what type of transmit path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	LASI Control Register	Controls the register written at offset 0x9002, and indicates what type of alarms are enabled. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.

10GE LSM Port Properties–Xenpak

The 10GE LSM *Xenpak* tab controls three options:

- Carrier power and laser power
- Link Alarm Status Interrupt (LASI)
- Transmit Pre-Emphasis

Carrier and laser power can be shut on or off through the controls on this tab. LASI is an active-low output from the XENPAK module that indicates a link fault condition has been asserted or has been cleared. Control registers are provided so that LASI may be programmed to assert only for specific fault conditions.

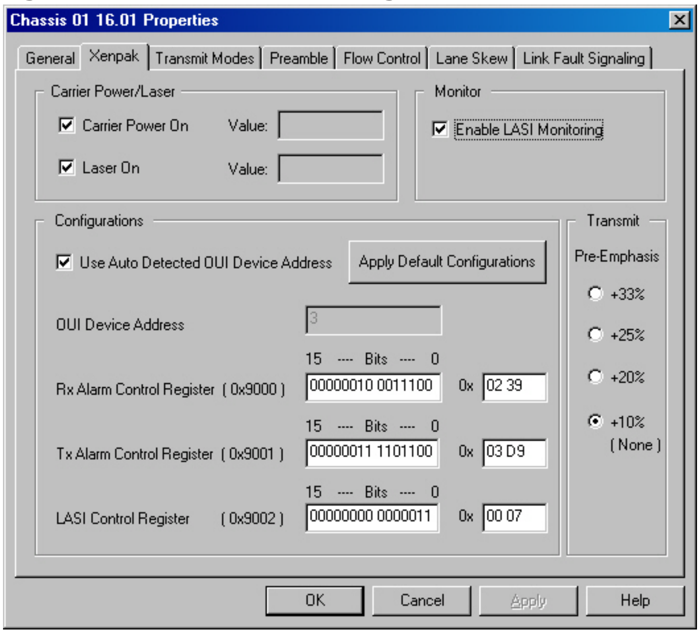
For more detailed information on LASI, see the Link Alarm Status Interrupt (LASI) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

Transmit pre-emphasis is used to boost the signal during transmission. The energy in the high frequency portion of the spectrum is boosted at the time of transmission. Since higher frequency components are attenuated more than lower frequency components, an equalized eye results at the destination.

The *Xenpak* tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu options, then selecting the *Xenpak* tab.

The *Xenpak* tab page is shown in *Figure:10GE LSM XENPAK Configuration*.

Figure:10GE LSM XENPAK Configuration



The controls for XENPAK configuration are described in *Table:XENPAK Configuration*.

Table:XENPAK Configuration

Section	Control/Field	Usage
Carrier Power/Laser		Allows to turn off the carrier or laser power.
	Carrier Power On	Select this check box to enable the carrier power. Note that the actual reading will be displayed in the *Value* field.
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the *Value* field.
Monitor		Activates the LASI monitoring feature.
	Enable LASI Monitoring	Selecting this check box enables LASI monitoring.
Configurations		Controls LASI configuration.
	Use Auto-Detected OUI Device Address	Selecting this check box sets the OUI address to the detected address. If this is selected, then the OUI *Device Address* field is disabled.
	Apply Default Configuration	Selecting this button resets the LASI values to their default settings.
	OUI Device Address	The Organizationally Unique Identifier (OUI)

Section	Control/Field	Usage
		device address, which signifies the device where the LASI control/status registers are located.
	Rx Alarm Control Register	Controls the register written at offset 0x9000, and indicates what type of receive path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	Tx Alarm Control Register	Controls the register written at offset 0x9001, and indicates what type of transmit path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	LASI Control Register	Controls the register written at offset 0x9002, and indicates what type of alarms are enabled. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
Transmit		Allows for creating pre-emphasis on transmitted signals.
	Pre-Emphasis	Selects the increase in percentage of signal strength for pre-emphasis.

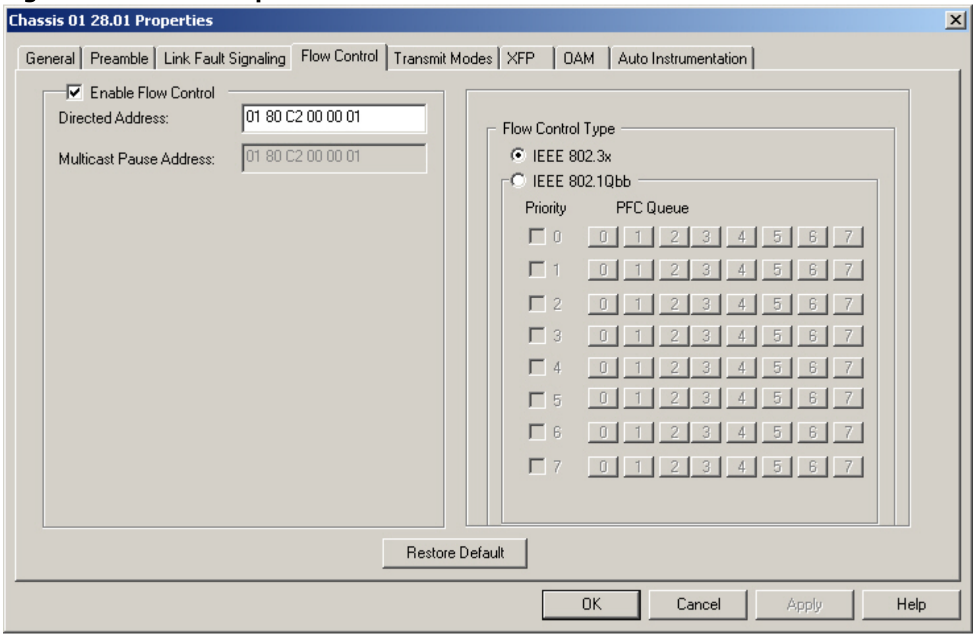
10GE Port Properties–Flow Control

For NGY modules, see *NGY–Flow Control tab*.

When a port is receiving data at a faster rate than it can handle from another, directly connected port, the receiving port can send a MAC control PAUSE frame to the sending port to temporarily halt transmission of frames. The PAUSE function is defined in IEEE 802.3. Pause Control Dialog for details.

The *Flow Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The *Flow Control* tab is shown in *Figure:10GE Port Properties—Flow Control*.

Figure:10GE Port Properties—Flow Control



The fields and controls in this tab are described in *Table:10GE—Flow Control Tab*.

Table:10GE—Flow Control Tab

Section	Field/Control	Description
Enable Flow Control		Enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type		Pause Control Dialog for details.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

10GE Port Properties–Transmit Modes

NOTE For NGY modules, see *NGY Transmit Modes Configuration*.

For FC modules, see *FCM Port Properties—Transmit Modes*.

For Flex modules, see *Flex Port Properties—Transmit Modes*.

For XDM10G32S modules, see *XDM10G32S Port Properties—Transmit Modes*.

The *Transmit Modes* tab for 10GE load modules is accessed by double-clicking a port in Resources pane, or by right-clicking a port and selecting the *Properties* menu option. Then select the *Transmit Modes* tab.

- For 10GE LAN/XAUI/XENPAK load modules, *Figure:10GE LAN/XAUI/XENPAK–Transmit Modes (shown for 10GE XAUI)*

- For the 10GE XENPAK-M and LAN-M *Transmit Modes* tab, *Figure:10GE LAN-M/XENPAK-M–Transmit Modes (shown for 10GEXENPAK-M)*.
- For 10GE LSM modules (including 10GE LSM MACSec), *Figure:10GE LSM—Transmit Modes*.
- For 10G MSM modules, *Figure:10GE LSM and MSM—Transmit Modes*.
- For 10GE LSM 10GBASE-T modules, *Figure:10GE LSM 10GBASE-T—Transmit Modes*.

For additional information on 10GE XAUI/BERT load modules, *10GE XAUI and XENPAK BERT*.

Figure:10GE LAN/XAUI/XENPAK–Transmit Modes (shown for 10GE XAUI)

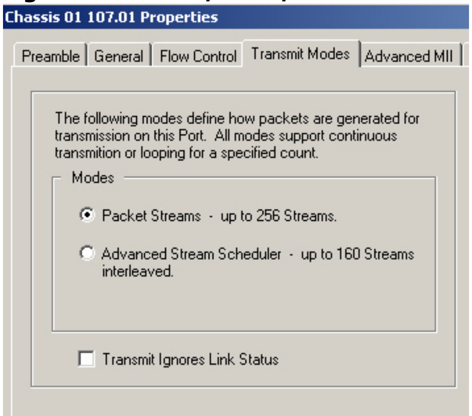


Figure:10GE LAN-M/XENPAK-M–Transmit Modes (shown for 10GE XENPAK-M)

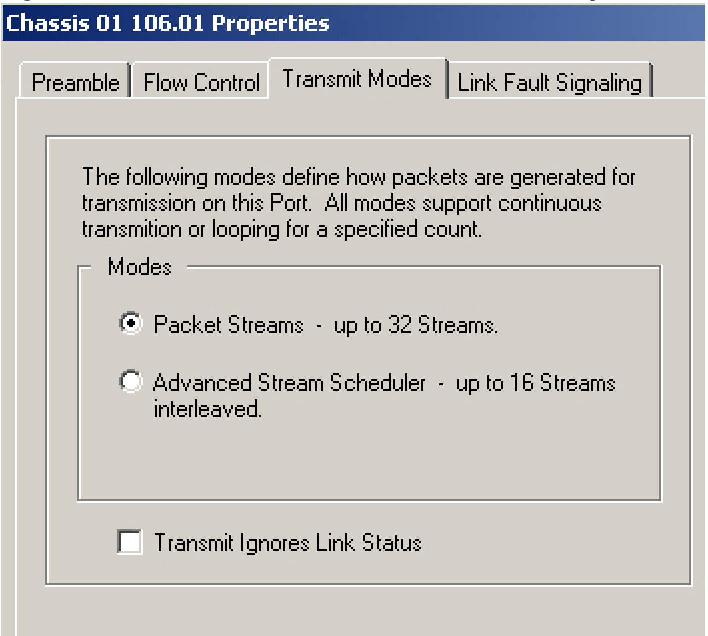


Figure:10GE LSM—Transmit Modes

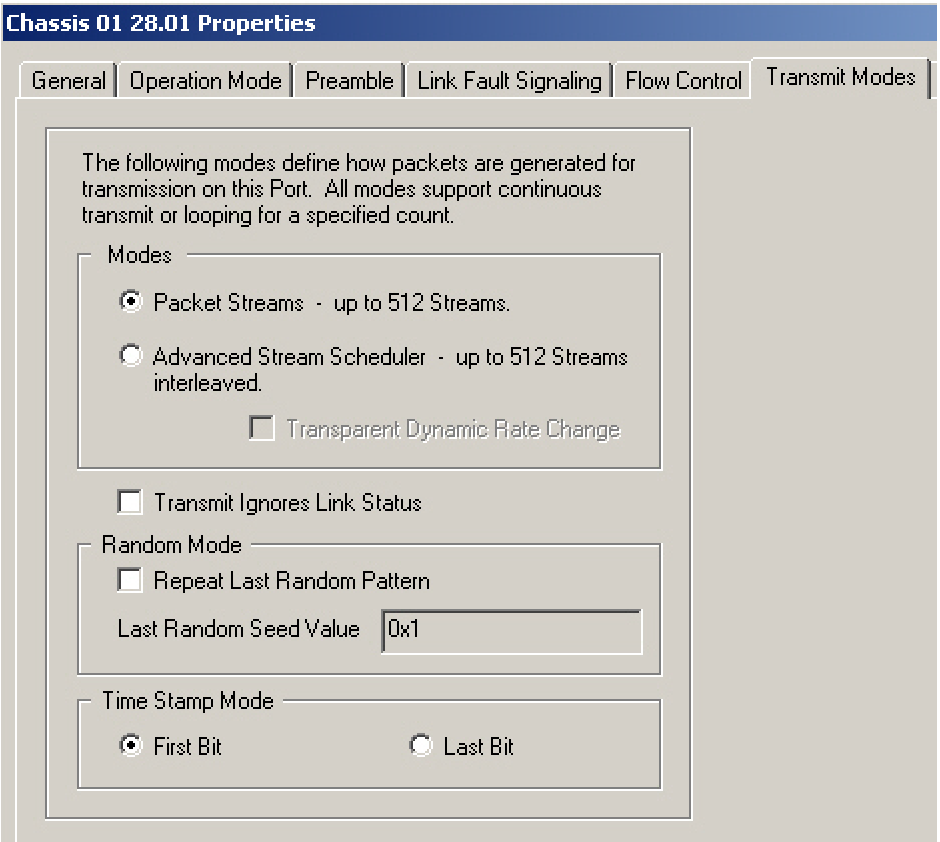


Figure:10GE LSM and MSM—Transmit Modes

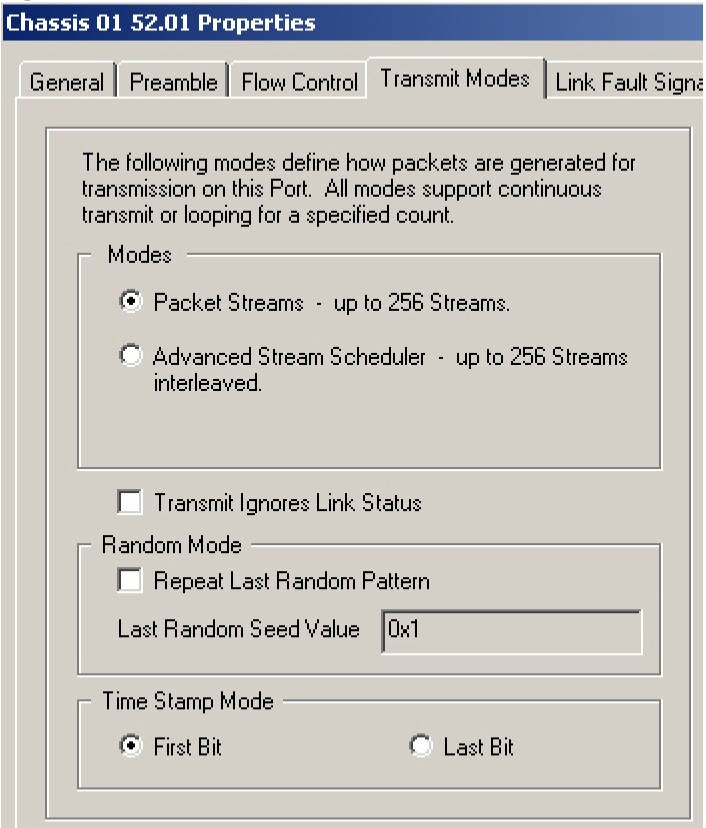


Figure:10GE LSM 10GBASE-T—Transmit Modes

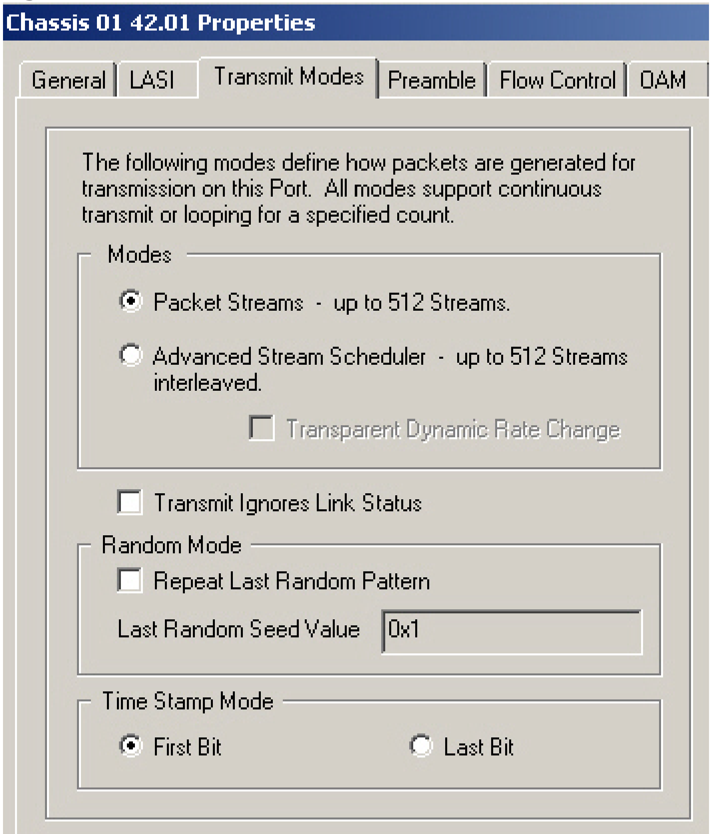
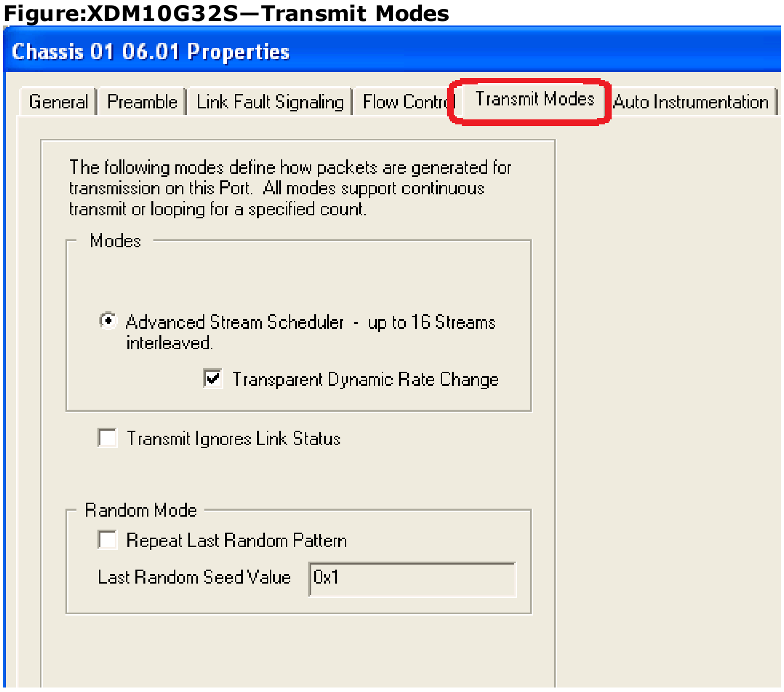


Figure:XDM10G32S—Transmit Modes



The fields and controls for the Transmit Modes tab are described in *Table:10GE LSM Transmit Modes Configuration*.

Table:10GE LSM Transmit Modes Configuration

Section	Field/Control	Description
Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 256 streams. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets up the transmission of up to 256 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams. NOTE XDM10G32S load module transmits up to 16 streams of interleaved packet streams.
	Transparent Dynamic Rate Change (for XDM10G32S load module)	If selected, the dynamic rate control will allow rate change across counters, for this port.
	Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Time Stamp Mode	First Bit	Store and Forward latency mode uses first bit time stamp mode
	Last Bit	Store and Forward latency mode uses last bit time stamp mode

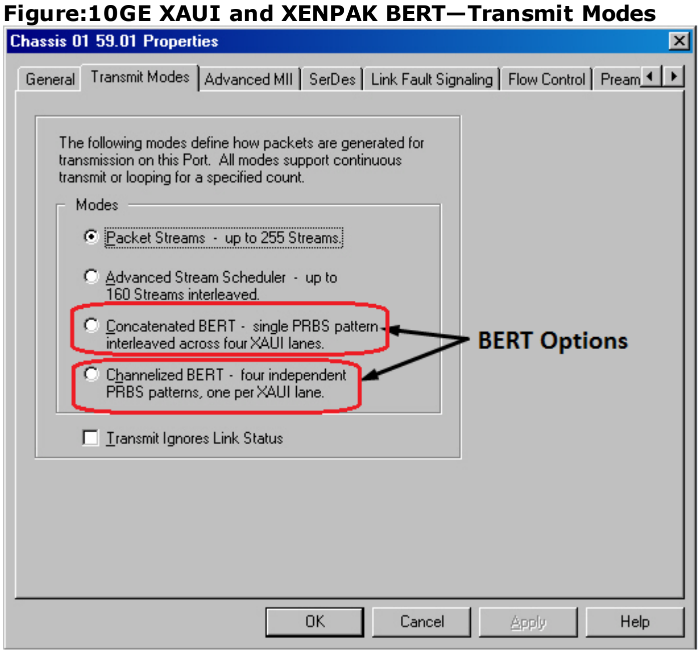
10GE XAUI and XENPAK BERT

BERT options for use with the 10GE XAUI and 10GE XENPAK modules are selected in the Port Properties *Transmit Modes* tab, which is shown in *Figure:10GE XAUI and XENPAK*

BERT—Transmit Modes. It is accessed by double-clicking a port in Resources pane, or by right-clicking a port and selecting the *Properties* menu option. Then select the *Transmit Modes* tab.

The example tabs shown here are for combination XAUI/BERT and XENPAK/BERT modules.

Figure:10GE XAUI and XENPAK BERT—Transmit Modes



The 10GE XAUI and XENPAK BERT Transmit Modes options are described in *Table:10GE XAUI and XENPAK BERT—Transmit Modes*.

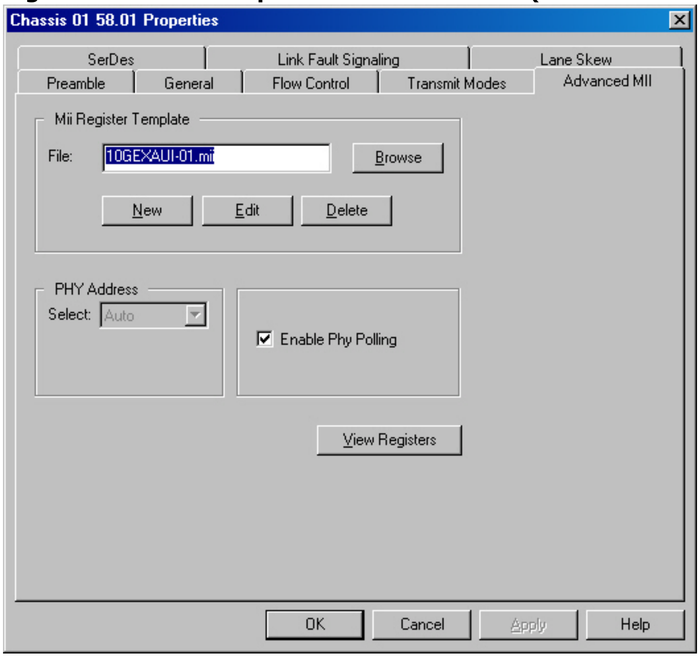
Table:10GE XAUI and XENPAK BERT—Transmit Modes

Modes	Description
Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 255 streams. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
Advanced Stream Scheduler	Sets up the transmission of up to 160 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
Concatenated BERT	A Single Pseudo-Random Binary Sequence (PRBS) pattern can be interleaved across all four of the XAUI lanes.BERT Window for additional information on how to configure concatenated XAUI BERT.
Channelized BERT	Four independent PRBS patterns can be transmitted, one over each of the four XAUI lanes.*10GE XAUI/XENPAK Channelized BERT* for additional information.
Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down. This options is not available when either BERT option is selected.

10GE Port Properties–Advanced MII

The *Advanced MII* tab for the 10GE XAUI and XENPAK modules is similar to those for the 10/100 modules. It is accessed by double-clicking a port in Resources pane, or by right-clicking a port and selecting the *Properties* menu option. Then select the *Advanced MII* tab. For detailed information refer to *MII Register Files*.

Figure:10GE Port Properties–Advanced MII (shown for 10GE XAUI)

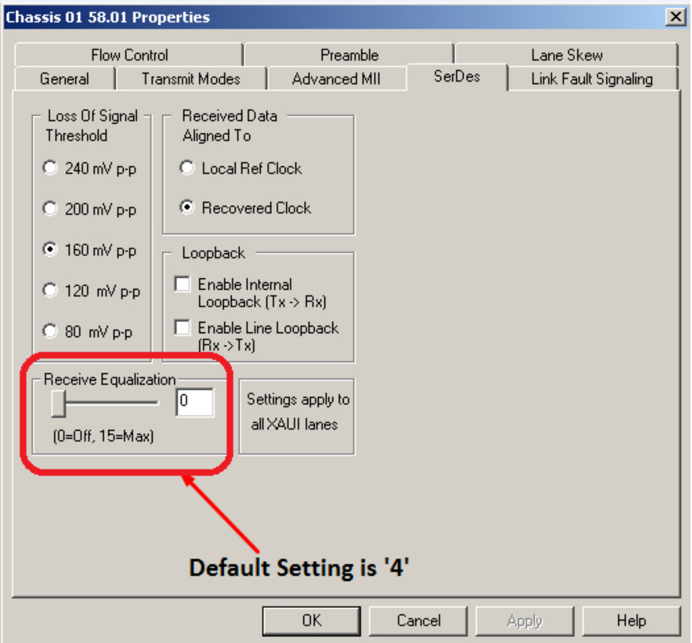


10GE Port Properties—SerDes

The *SerDes* tab (Serialization/De-serialization) provides a convenient way for you to adjust functions for the XAUI interface. The SerDes is an internal Serialization/Deserialization device.

It is accessed by double-clicking a port in Resources pane, or by right-clicking a port and selecting the *Properties* menu option. Then select the *SerDes* tab. The *SerDes* tab for the 10GE XAUI and XENPAK modules is shown in *Figure:10GE Port Properties—SerDes*.

Figure:10GE Port Properties—SerDes



The options available in the *SerDes* tab are described in *Table:XAUI/XENPAK SerDes Tab*.

Table:XAUI/XENPAK SerDes Tab

Section	Field/Control	Description
Loss of Signal Threshold	Choose one of: • s240mV p-p • 200 mV p-p • 160 mV p-p • 120 mV p-p • 80 mV p-p	The Loss of Signal Threshold is the value below which the signal is considered to be 'lost.' The units are milli-Volts point-to-point.
Receive Equal-ization	Slider Bar: (0 to 15)	(Hex value) The range of Receive Equalization values is 0 to 15. Max. is 15. 0 = OFF. NOTE The factory default setting is '4,' which corresponds to an equalization setting of approximately 25%.
Received Data Aligned To	Choose one of: • Local Ref Clock • Recovered Clock	Sets the Receive Clock Mode. The Local Refer-ence Clock is derived from the internal system clock. The Recovered Clock is derived from the received data.
LoopBack	Enable Internal Loop-back (Tx -> Rx)	Check this box to enable/turn ON the XAUI **Internal** Loopback—Transmit to Receive.
	Enable Line Loopback (Rx -> Tx)	Check this box to enable/turn ON the Line Loop-back—Receive to Transmit.
	Apply	Pressing this button writes the changes to the MII registers without closing the *SerDes* tab.

Section	Field/Control	Description
	OK button	Pressing this button writes the changes to the MII registers and closes the *SerDes* tab.

NOTE The Serialization/Deserialization settings that are made in this tab apply to all four of the XAUI lanes.

10GE Port Properties–Link Fault Signaling

NOTE For NGY module, see *NGY Port Properties–Link Fault Signaling*.

For Fibre Channel modules, see *FCM Port Properties—Link Fault Signaling*.

For Xcellon-Flex modules, see *Flex Port Properties—Link Fault Signaling*.

For XDM10G32S modules, see *XDM10G32S Port Properties—Link Fault Signaling*.

For Xcellon-Multis modules, see *Xcellon-Multis Port Properties—Link Fault Signaling*.

For Novus modules, see *Novus Port Properties—Link Fault Signaling*.

Link Fault Signaling is defined in Section 46 of the IEEE 802.3ae specification for 10 Gigabit Ethernet. When the feature is enabled, four statistics will be added to the list in Statistic View for the port. One is for monitoring the Link Fault State. Two provide a count of the Local Faults and Remote Faults. The last one is for indicating the state of error insertion, whether or not it is ongoing.

Link Fault Signaling for originates with the PHY sending an indication of a local fault condition in the link being used as a path for MAC data. In the typical scenario, the Reconciliation Sublayer (RS) that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

For the 10GE LAN and LAN-M serial modules, the Physical Coding Sublayer (PCS) of the PHY handles the transition from 64 bits to 66 bit 'Blocks.' The 64 bits of data are scrambled, and then a 2-bit synchronization (sync) header is attached before transmission. This process is reversed by the PHY at the receiving end.

Link Fault Signaling for the 10GE XAUI/XENPAK is handled differently across the four-lane XAUI optional XGMII extender layer, which uses 8B/10B encoding.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab. The 10GE *Link Fault Signaling* tab for most 10GE modules is shown in *Figure:10GE Link Fault Signaling—Shown for a 10GE LAN Module*. The 10GE *Link Fault Signaling* tab for 10GE LSM modules using XFP (and 10GE LSM MACSec modules) is shown in *Figure:10 GE LSM XFP Link Fault Signaling*. The *Link Fault Signaling* tab for XDM10G32S load module is shown in *XDM10G32S Port Properties—Link Fault Signaling*

Figure:10GE Link Fault Signaling—Shown for a 10GE LAN Module

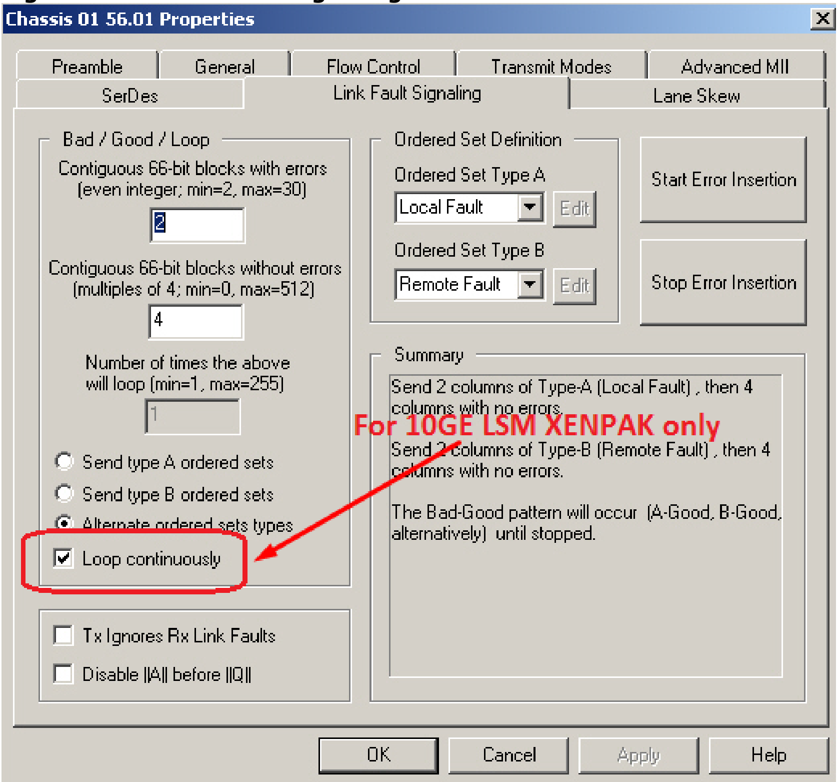
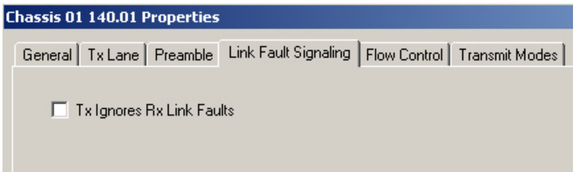
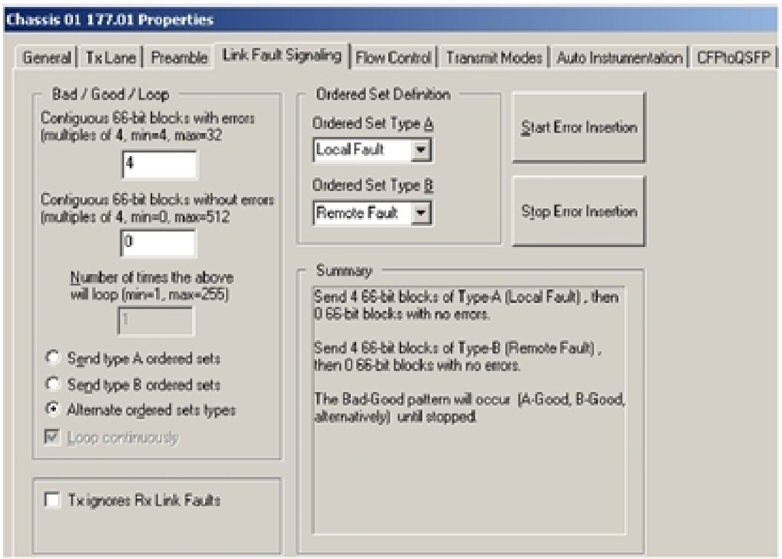


Figure:10 GE LSM XFP Link Fault Signaling



The Link Fault Signaling tab for HSE 100GE load module is shown in the following figure:

Figure:Link Fault Signaling—Shown for HSE 100GE Module



The fields and controls in the **Link Fault Signaling** tab for HSE 100GE load module is described in the following table:

Table:HSE 100GE Link Fault Signaling

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets-A and B-are defined in the Ordered Set Definition box in this tab.) This pattern will be combined with the Good blocks/Bad blocks pattern for transmission. • Type A only • Type B only • Alternate Type A and Type B
	Loop continuously	If selected, the loop defined by the combination of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the Stop Error Insertion button is clicked.
Ordered Set Definition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault
Start Error Insertion		To start the transmission of the configured error patterns.
Stop Error Insertion		To stop the transmission of the configured error patterns.
Tx Ignores Rx Link Faults		If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.
Summary (Window)		(Read-only) Displays descriptions of the patterns that will be transmitted.

The Link Fault Signaling tab allows to set up different configurations of error patterns to be sent with Local Fault an Remote Fault (or custom-defined) Sequence ordered sets. The options available in the *Link Fault Signaling* tab are described in *Table:10GE Link Fault Signaling Tab*. Also, see the Examples of Link Fault Signaling Error Insertion section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for an example of error patterns.

Table:10GE Link Fault Signaling Tab

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (even integer; min = 2, max = 30)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern. This value must be an even integer. The allowed minimum and maximum are 2 blocks and 30 blocks, respectively. NOTE The minimum and maximum values for a 10GE LSM and 10GE MSM modules are slightly different. There is no even integer limitations, and the min./max. is 0 to 1,024.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 0, max = 512)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The allowed minimum and maximum are 0 blocks and 512 blocks, respectively. NOTE The minimum and maximum values for a 10GE LSM and 10GE MSM modules are slightly different. There is no even integer limitations, and the min./max. is 1 to 512.
	Number of times the above will loop (min = 1, max = 255)	This field is available only when the *Loop continuously* check box is **NOT** selected. It is the number of times that the combination of Bad/Good and Type patterns will be repeated. After all of the 66-bit blocks have been sent, the transmission will automatically stop.
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets—A and B—are defined in the *Ordered Set Definition* box in this tab.) This pattern will be combined with the Good blocks/Bad blocks pattern for transmission. • Type A only • Type B only • Alternate Type A and Type B.
	Loop continuously	If selected, the loop defined by the combination

Section	Field/Control	Description
		of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the *Stop Error Insertion* button is clicked. NOTE If fixed loop count is selected, and Send type A or Send type B is selected, one loop iteration will consist of Error-Good pattern; if the Alternate ordered set types option is selected, one loop iteration will consist of Error-Good-Error-Good pattern.
Ordered Set Definition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault • Custom —this option allows to define the contents for the ordered set. Press the *Edit* button to edit the content. *10GE Custom Ordered Set Definition Dialogs* for additional information.
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault • Custom—this option allows to define the contents for the ordered set. Press the *Edit* button to edit the content. See *10GE Custom Ordered Set Definition Dialogs* for additional information.
(Additional Options)	Tx Ignores Rx Link Faults	If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.
	Disable ||A|| before ||Q||	(FOR XAUI & XENPAK ONLY) The /Q/ symbol represents the Sequence ordered_set control character. The /A/ symbol can be used to represent Idle characters for XAUI. (It has 'Reserved' status for XGMII.)
Summary (Window)		(Read-only) Displays descriptions of the patterns that will be transmitted.
Start Error Insertion		Press this button to start the transmission of the configured error patterns.
Stop Error Insertion		(Available only for use with the *Loop continuously* option.) Press this button to stop the transmission of the configured error patterns.

10GE Custom Ordered Set Definition Dialogs

There are two *Custom Ordered Set Definition* dialogs:

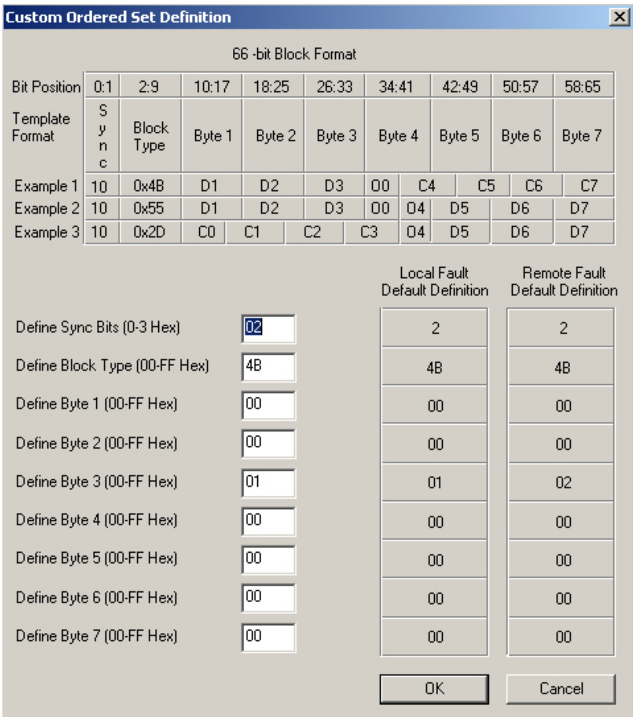
- *10GE LAN Custom Ordered Set Definition Dialog*
- *10GE XAUI/XENPAK Custom Ordered Set Definition Dialog*

10GE Custom Ordered Set Definition Dialogs

The *Custom Ordered Set Definition* dialog is accessed from the *Link Fault Signaling* tab. Select the *Custom* option in either *Ordered Set A* or *B*, then select the *Edit* button.

The *Custom Ordered Set Definition* dialog for the 10GE LAN and LAN-M modules is shown in *Table:10GE LAN Custom Ordered Set Definition Dialog*.

Table:10GE LAN Custom Ordered Set Definition Dialog



The default values for Local Fault status and Remote Fault status, as defined in IEEE 802.3ae, are displayed as read-only information. The fields and controls in this dialog are described in *Table:10GE LAN Custom Ordered Set Definition Dialog*.

Table:10GE LAN Custom Ordered Set Definition Dialog

Section	Field/Control	Description
66-bit Block Format	Bit Position	Lists the groups of bits for each segment of the 66-bit Block Format.
	Template Format	Shows the format template for the segments of the 66-bit Block Format.
	Examples	Shows the general format of the contents of the 66-bit Blocks for: • Example 1: Block Type = 0x4B (for Local or Remote Fault message • Example 2: Block Type = 0x55

Section	Field/Control	Description
		• Example 3: Block Type = 2D
Define Bit-s/Bytes	Define Sync Bits (0-3 Hex)	Enter the desired hex value for the two sync bits (0:1) at the beginning of the 66-bit Block. This value can only be: • 01 (= 1 hex)–for data, or • 10 (= 2 hex)–for control. NOTE In the examples at the top of the dialog, the sync values are exclicked in binary format. For configuration purposes, however, the value is entered as a hex value. For example, a Sync value of 10 (binary), is entered as 02 (hex).
	Define Block Type (00-FF Hex)	Bits 2 through 9 of the 66-bit block are used to configure the Block Type. Block Type: • 0x4B • 0x55 • 0x2D
	Define Bytes 1 through 7 (00-FF Hex)	Define each of the next 7 bytes of the 66-bit block. The bytes may contain different types of bit sequences, depending on the Block Type. • D1 through D7—Data (Data units are 8 bits long) • C1 through C7—Control info (Control units are 7 bits long) • O0—'O' code (O code units are 4 bits long) NOTE For Block Type 4B, for Local or Remote Default Definition, the value of Byte 3 indicates Local or Remote. • 01 = Local Fault • 02 = Remote Fault
Local Fault Definition		Shows the default contents (in hex) of the 66-bit Block for 'Local Fault.'
Remote Fault Definition		Shows the default contents (in hex) of the 66-bit Block for 'Remote Fault.'

10GE XAUI/XENPAK Custom Ordered Set Definition Dialog

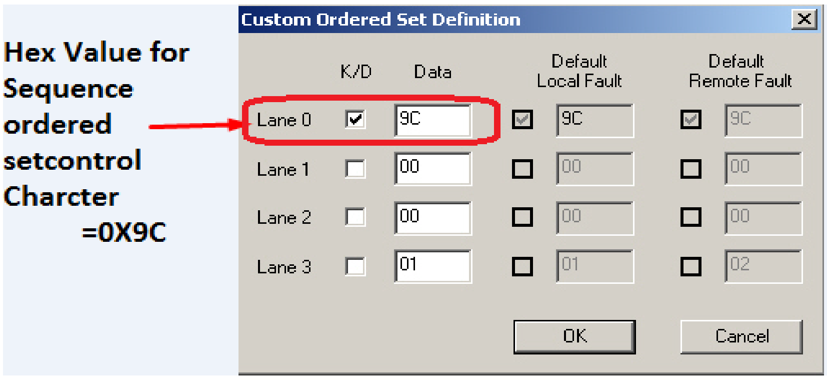
For 10GE XAUI and 10GE XENPAK modules, a Status message contains a 4-byte ordered set with a Sequence control character plus three data characters (in hex), distributed across the four lanes. Four Sequence ordered sets are defined in IEEE 802.3ae, but only two of these—Local Fault and Remote Fault—are currently in use; the other two are reserved for future use.

See the 10GE section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual* for more information on XAUI/XENPAK status messages.

The *Custom Ordered Set Definition* dialog is accessed from the *Link Fault Signaling* tab. Select the *Custom* option in either *Ordered Set A* or *B*, then select the *Edit* button.

The *Custom Ordered Set* dialog for the 10GE XAUI and XENPAK modules is shown in *Figure:10GE XAUI/XENPAK Custom Ordered Set Definition Dialog*.

Figure:10GE XAUI/XENPAK Custom Ordered Set Definition Dialog



This dialog allows to define custom values (in hex) for all four bytes of a ordered set for the 10GE XAUI interface. The default values for *Local Fault* and *Remote Fault* status, as defined in IEEE 802.3ae, are displayed as read-only information in the right side of the dialog.

The hex value for Sequence ordered_set is 0x9C, which is shown in this dialog. In general, ordered sets are used for sending status information, such as the *Local* and *Remote Faults*, and control information. Additional ordered sets may be created by entering a control character for the first character, plus three data characters.

The fields and controls in this dialog are described in *Table:10GE XAUI/XENPAK Custom Ordered Set Definition Dialog*.

Table:10GE XAUI/XENPAK Custom Ordered Set Definition Dialog

Section	Field/Control	Description
Configuration Fields (R/D)	Lane 0	If *R/D* is selected, then the value entered in the *Data* field will be used. The default setting is *R/D* selected, with a value of '0x9C,' which is the hex value for *Sequence ordered_set*.
	Lane 1	If *R/D* is selected, then the value entered in the *Data* field will be used.
	Lane 2	If *R/D* is selected, then the value entered in the *Data* field will be used.

Section	Field/Control	Description
	Lane 3	If *R/D* is selected, then the value entered in the *Data* field will be used. **NOTE** For Local or Remote Default Definition, the value of Lane 3 indicates Local or Remote. • 01 = Local Fault • 02 = Remote Fault
Default Local Fault		The default values for Local Fault status are displayed, as defined in IEEE 802.3ae.
Default Remote Fault		The default values for Remote Fault status are displayed, as defined in IEEE 802.3ae.

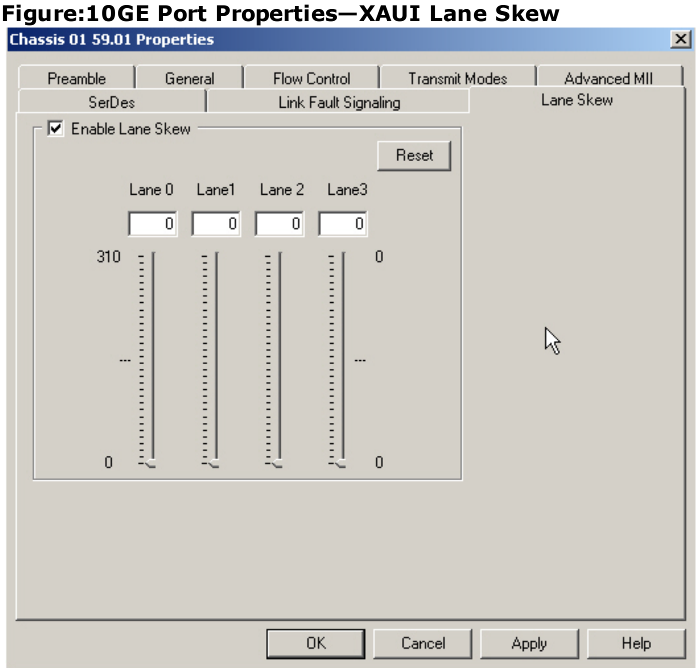
10GE Port Properties—Lane Skew

The *Lane Skew* tab allows a XAUI lane to be skewed by as much as 310 UI with respect to the other three lanes. When skewing is enabled, the four lanes mimic the settings in this dialog. The skew is displayed in a relative fashion, from one lane to another. To effectively use this feature, the four lanes should be set to different skew values. Setting all four lanes to zero is equivalent to setting all four lanes to 310 UI. In both cases, the lanes are synchronous and there is no lane skew. When lane skewing is enabled, /A/, /K/, and /R/ codes are inserted into the data stream BEFORE the lanes are skewed.

For more information on Lane Skewing, see the Lane Skew section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

This tab is accessed by right-clicking a port in the Resource Window, selecting the *Properties* menu option, then selecting the *Lane Skew* tab. The *Lane Skew* tab for the 10GE XAUI and XENPAK modules is shown in *Figure:10GE Port Properties—XAUI Lane Skew.*

Figure:10GE Port Properties—XAUI Lane Skew



The options available in the *Lane Skew* tab are described in *Table:10GE XAUI/XENPAK Lane Skew*.

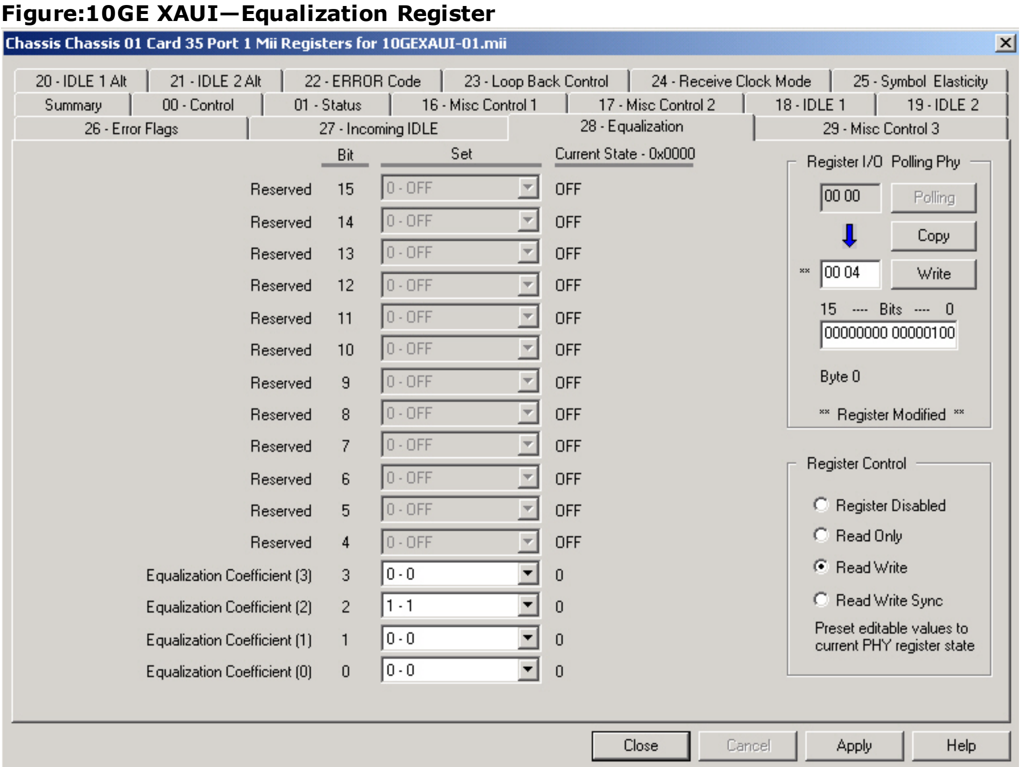
Table:10GE XAUI/XENPAK Lane Skew

Field/Control	Description
Enable Lane Skew	If selected, then the Lane Skew feature is enabled.
Lane 0, Lane 1, etc.	These fields correspond to the four XAUI lanes–0 through 3. The values set with the slider bars below are displayed in these fields. The values may also be set in these fields by entering the value and then pressing the *Apply* button.
Slider Bar (for each lane) (0 to 310)	The range of skew values is 0 to 310. Set the skew value for each of the lanes by placing the cursor on the slide indicator and moving it to the desired value on the scale. Max. is 310. 0 = OFF.
Reset	Pressing this button sets the lane skew values for all four of the lanes to ‘0.’

10GE XAUI Receive Equalization Register

Receive-side equalization may be adjusted by using the *MII Registers for 10GEXAUI* dialog, shown in *Figure:10GE Port Properties–Advanced MII (shown for 10GE XAUI)*, to directly access the Equalization register. Press the *View Registers* button in the *Advanced MII* tab (shown in *10GE Port Properties–Advanced MII*) to display the default MII template - *10GEXAUI-01.mii*. Select the tab for the register labeled: *28 - Equalization*, which is shown in *Figure:10GE XAUI—Equalization Register*. For additional information on the use of the Advanced MII Registers, refer to *MII Control Tab*.

Figure:10GE XAUI—Equalization Register



In the 10GE XAUI *28–Equalization* register, shown in *Figure:10GE XAUI—Equalization Register*, the first four bits (0 through 3) are assigned for the *Equalization Coefficient*. (Bits 4 through 15 are not used.)

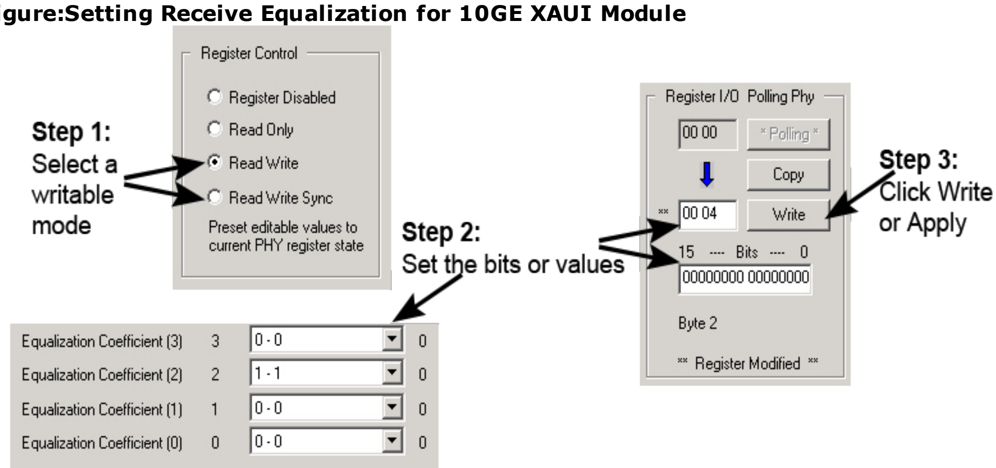
Each of the four bits can be set to 1 or 0, to specify the binary value. There are 16 possible settings, from 00 00 (Equalization = 0%/Off) to 00 0F (Equalization = 100%/Maximum).

Figure:10GE XAUI—Equalization Register shows the default setting of '4' (00 04 hex), which corresponds to an equalization level of approximately 25%.

For longer cable or backplane lengths, the equalization may need to be increased above the default setting. In the case where the Device Under Test (DUT) has Transmit pre-emphasis capability, it may be necessary to either lower the pre-emphasis level, or reduce the equalization level for the XAUI load module.

To set the equalization level, the *Register Control* must be set to *Write* or *Read Write Sync*, as shown in *Figure:Setting Receive Equalization for 10GE XAUI Module*. Select '1' or '0' in the dialog table for each of the four equalization coefficient bits, as necessary, and the corresponding values will automatically be applied to the hex and binary fields in the *Register I/O Polling* section of the dialog. An alternate method is to enter the hex or binary value in the polling fields, and then press the *Write* button to apply that value to the other polling field and the bit settings in the table.

Figure:Setting Receive Equalization for 10GE XAUI Module



10GE XAUI and 10GE XENPAK Load Modules

The 10 Gigabit XAUI interface has been defined in the IEEE draft specification P802.3ae by the 10 Gigabit Ethernet Task Force (10GEA). XAUI stands for 'X' (the Roman Numeral for 10, as in '10 Gigabit'), plus 'AUI' or Attachment Unit Interface originally defined for Ethernet.

The 10 Gigabit Ethernet XENPAK Load Modules accept XENPAK-compliant front panel hot pluggable optical transceivers. The XENPAK Load Module implements the latest draft of the XENPAK Multi-Source Agreement (MSA), and supports IEEE 802.3ae-approved interfaces through an industry standard electrical 70-pin connector. It can be used to validate XENPAK transceivers and 10GE optical switches and routers.

10GE XAUI and XENPAK MII Templates

The 10GE XAUI and XENPAK modules have an additional configuration capability for a set of unique MII Templates. See 10GE Module MII Lists for additional information on these MII templates.

10GE Port Properties–SFP

NOTE For FC modules, see *FCM Port Properties—SFP+*.

For Xcellon-Flex modules, see *Flex Port Properties—SFP+*.

The following load modules can support SFP+ interfaces.

- LSM10G1-01(M) and LSM10GL1-01 LSM10GR1-01

This tab allows to set the carrier and laser power settings, the transceiver type, and the monitor options. The *SFP+* tab is shown in *Figure:10GE LSM—SFP+ Tab*.

Figure:10GE LSM—SFP+ Tab

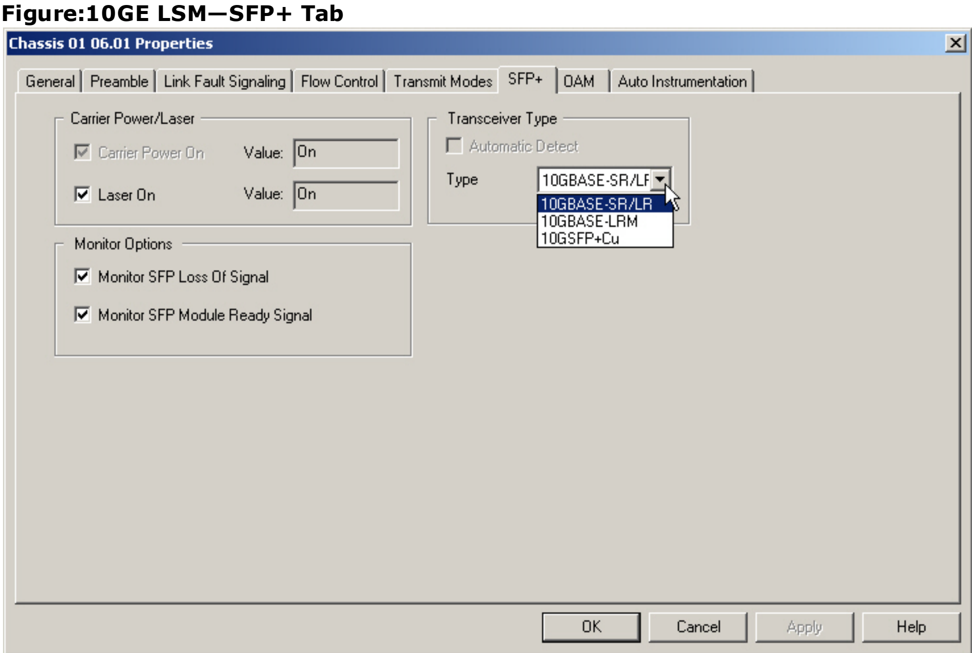


Table:SFP Tab Page Usage explains the configuration options of the *SFP* tab.

Table:SFP Tab Page Usage

Heading	Field	Usage
Carrier Power/Laser	Carrier Power On	Select this check box to enable the carrier power. Note that the actual reading will be displayed in the *Value* field.
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the *Value* field.
Monitor Options	Monitor SFP Loss of Signal	When selected, indicates the interface will conform to SFP specifications and require the absence of a Loss of Signal for transmitting and receiving.
	Monitor SFP Module Ready Signal	When selected, indicates the interface will conform to SFP specifications and require the detection of a Module Ready signal for transmitting and receiving.
Tranceiver Type	Automatic Detect	(For future use) Not available

Heading	Field	Usage
	Type	Select from pull-down: • 10GBASE-SR/LR • 10GBASE-LRM (does not support WAN mode) • 10GSFP+Cu

10GE Port Properties–OAM

For NGY modules,*NGY Port Properties–OAM*.

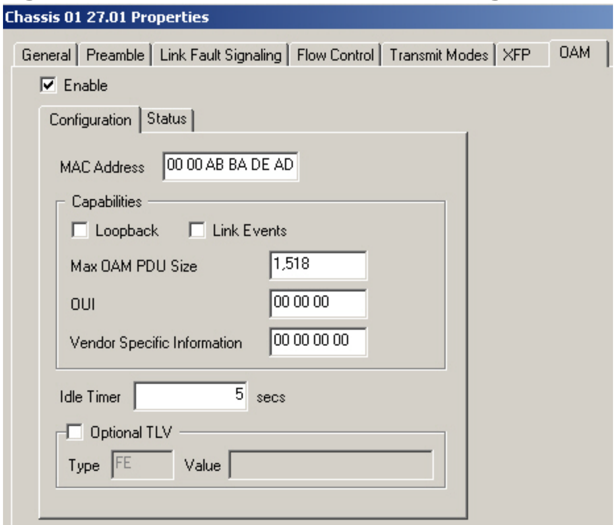
For Flex modules,*Flex Port Properties—OAM*.

The *OAM* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *OAM* tab. The *OAM* tab for 10GE load modules allows to configure local stateful OAM Data Terminating Entities (DTE) and view the status of both local and remote OAM PDUs.

OAM Configuration

The OAM Configuration tab is shown in *Figure:OAM Tab for 10GE Modules, Configuration*.

Figure:OAM Tab for 10GE Modules, Configuration



The Operations, Administration, and Maintenance (OAM) sublayer provides mechanisms useful for monitoring link operation such as remote fault indication and remote loopback control. In general, OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAM PDUs). OAM PDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links.

The fields and controls in this tab are in *Table:OAM Configuration Tab for 10GE Modules*.

After making configuration changes, click **Apply** to send the changes to the chassis without leaving the tab. Click **OK** to send changes and close the Properties window.

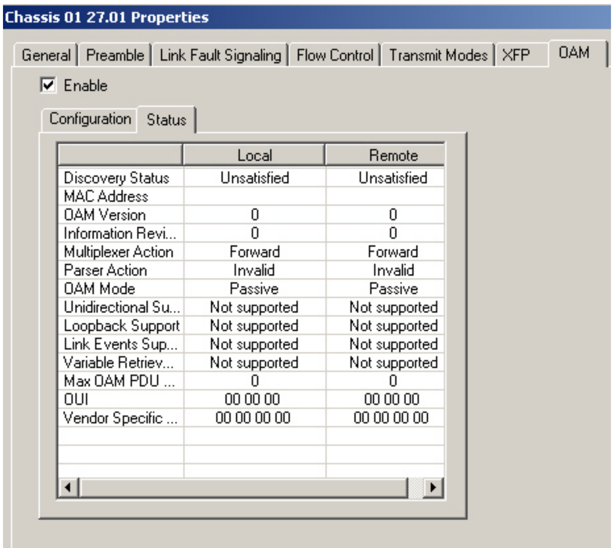
Table:OAM Configuration Tab for 10GE Modules

Section	Field/Control	Description
	Enable	Enables and starts OAM state machine configuration
MAC Address		The individual source MAC address of the Ixia port acting as DTE (through which the OAM PDU is transmitted)
Capabilities	Loopback	Advertises OAM remote loopback capability
	Link Events	Advertises link event capability
	Max OAM PDU Size	11-bit field which represents the largest OAM PDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.
	OUI	24-bit 3-octet field, Organizationally Unique Identifier. Example: 00 00 00
	Vendor Specific Information	4-octet field, 32-bit identifier that may be used to differentiate a vendor's product models/versions.
Idle Timer		local_lost_link_timer Timer used to reset the Discovery state. Duration: 5 sec ± 10%.
Optional TLV	Type	This is any Information TLV that you want to send. This one-octet field indicates the nature of the data carried in this TLV-tuple. • 0x00 End of TLV marker • 0x01 Local Information • 0x02 Remote Information • 0x03-0xFD Reserved - shall not be transmitted, should be ignored on reception by OAM client • 0xFE Organization Specific Information • 0xFF Reserved - shall not be transmitted, should be ignored on reception by OAM client
	Value	This field indicates the value of the Information TLV. This field's length and contents are unspecified.

OAM Status

The OAM Status tab is shown in *Figure:OAM Tab for 10GE Modules, Status*.

Figure:OAM Tab for 10GE Modules, Status



The fields and controls in the Status tab are described in *Table:OAM Status Tab*. for each category, there is both a Local and a Remote status indicator.

Table:OAM Status Tab

Field/Control	Description
Discovery Status	Detects the presence of an OAM sublayer at the remote DTE
MAC Address	Defined in *Table:OAM Configuration Tab for 10GE Modules*
OAM Version	This one-octet field indicates the version supported by the DTE. This field always contains the value 0x01.
Information Revision	This two-octet field indicates the current revision of the Inform-ation TLV. The value of this field shall start at zero and be incre-mented each time something in the Information TLV changes.
Multiplexer Action	Forward (0) = Device is forwarding non-OAMPDUs to the lower sub-layer (local_mux_action = FWD). Discard (1) = Device is discarding non-OAMPDUs (local_mux_action = DISCARD).
Parser Action	00 = Device is forwarding non-OAMPDUs to higher sublayer (local_par_action = FWD). 01 = Device is looping back non-OAMPDUs to the lower sublayer (local_par_action = LB). 10 = Device is discarding non-OAMPDUs (local_par_action = DISCARD). 11 = Reserved. In Local Information TLVs, this value shall not be sent. If the value 11 is received, it should be ignored and not change the last received value.
OAM Mode	1 = DTE configured in Active mode. 0 = DTE configured in Passive mode.
Unidirectional Sup-	1 = DTE is capable of sending OAMPDUs when the receive path is

Field/Control	Description
port	non-operational. 0 = DTE is not capable of sending OAMPDUs when the receive path is non-operational.
Loopback Support	Defined in *Table:OAM Configuration Tab for 10GE Modules*
Link Events Support	Defined in *Table:OAM Configuration Tab for 10GE Modules*
Variable Retrieval Support	1 = DTE supports sending Variable Response OAMPDUs. 0 = DTE does not support sending Variable Response OAMPDUs.
Max OAM PDU Size	Defined in *Table:OAM Configuration Tab for 10GE Modules*
OUI	Defined in *Table:OAM Configuration Tab for 10GE Modules*
Vendor Specific Information	Defined in *Table:OAM Configuration Tab for 10GE Modules*

10GE Port Properties–MACSec Tx/Rx Tabs

The MACSec Tx and MACSec Rx pages are used to set up transmit and receive channel values. These will be used in the *MACSec Header Information Editor* and *MACSec Table* (Chapter 6: Frame Data–Protocol Control).

The MACSec Tx and MACSec Rx pages are virtually identical. The slight differences are identified in the field definitions *Table:MACSec Tx /Rx Page Usage*.

Figure:10GE LSM–MACSec Tx Tab

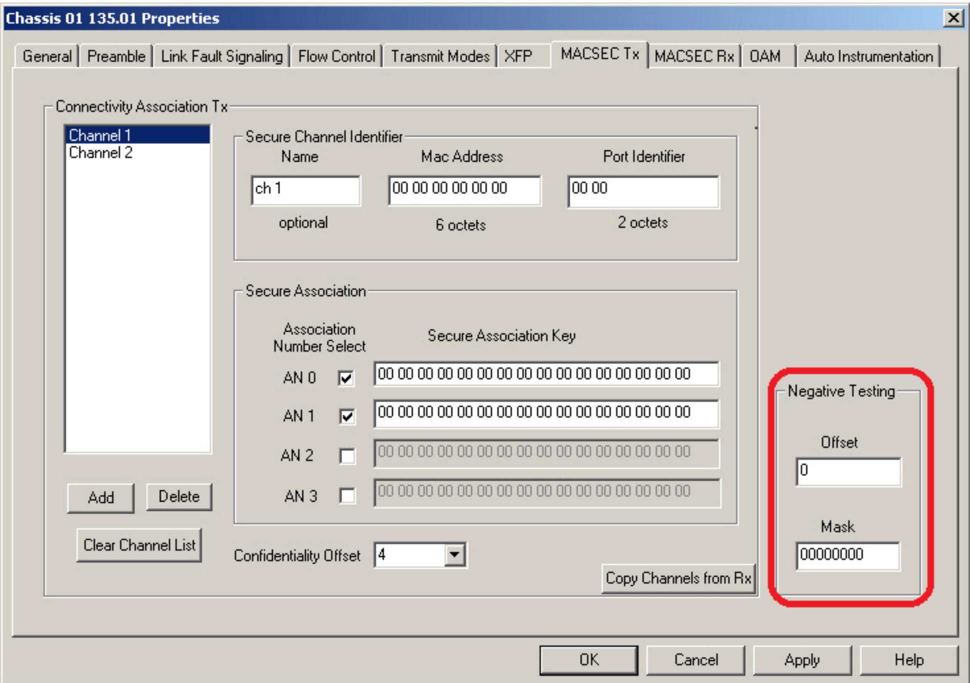


Table:MACSec Tx /Rx Page Usage explains the configuration options of the *MACSec Tx* page.

Table:MACSec Tx /Rx Page Usage

Heading	Field	Usage
Connectivity Asso-		Add

Heading	Field	Usage
ciation Tx (Rx)		Max 256 key entries–each channel can have up to 4 keys, so the limits are 64 channels with 4 keys each, up to 256 channels with 1 key each. Delete Clear Channel List
Secure Channel identifier	Name	(optional) A meaningful name for this channel (like 'Channel A')
	Mac Address	6 octets, a globally unique MAC address uniquely associated with the transmitting security entity. This corresponds to the MAC Address in Stream Properties, MACSec Header Information screen.
	Port Identifier	2 octets, the Port Identifier. This corresponds to the Port Identifier in Stream Properties, MACSec Header Information screen.
Secure Association	Association Number Select	AN 0 through AN 3 Select one or more.
	Secure Association Key	When Association Number is selected, the Key becomes active.
Negative Testing		*Negative Testing*.
Confidentiality Offset		Select an offset of 0, 4, 30, or 50 This is the byte offset from the end of the MACSec Tag.
Copy Channels from Tx (Rx)		Copies the channel setup from the other page (Rx to Tx or Tx to Rx)

Negative Testing

Negative testing allows a user-specified byte in the frame to be corrupted with a bit-mask. The byte offset and bit-mask will be set at the port level, while the enabling mechanism for actually corrupting the frame will be at the stream level. The byte will be corrupted following the MACSec encryption, to corrupt an intact MACSec frame (that is, setting the SCI to indicate that an SCI exists, when none actually does exist).

NOTE The CRC cannot be corrupted using this feature.

The Negative Testing dialog is part of the Port Properties MACSec TX page, as shown in the following figure.

Figure:MACSecTx page with Negative Testing Dialog

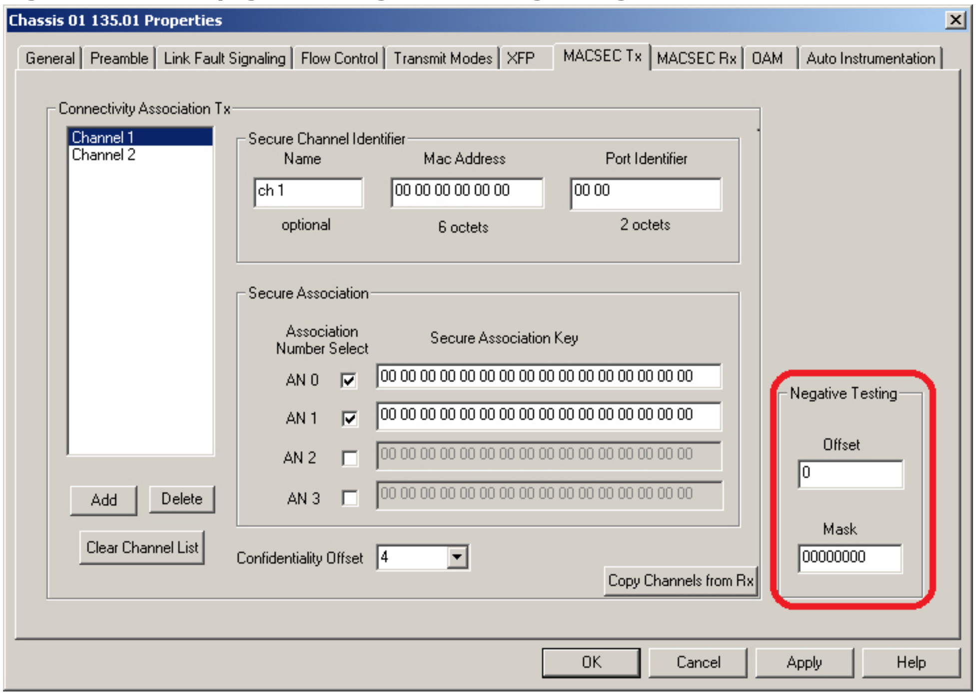
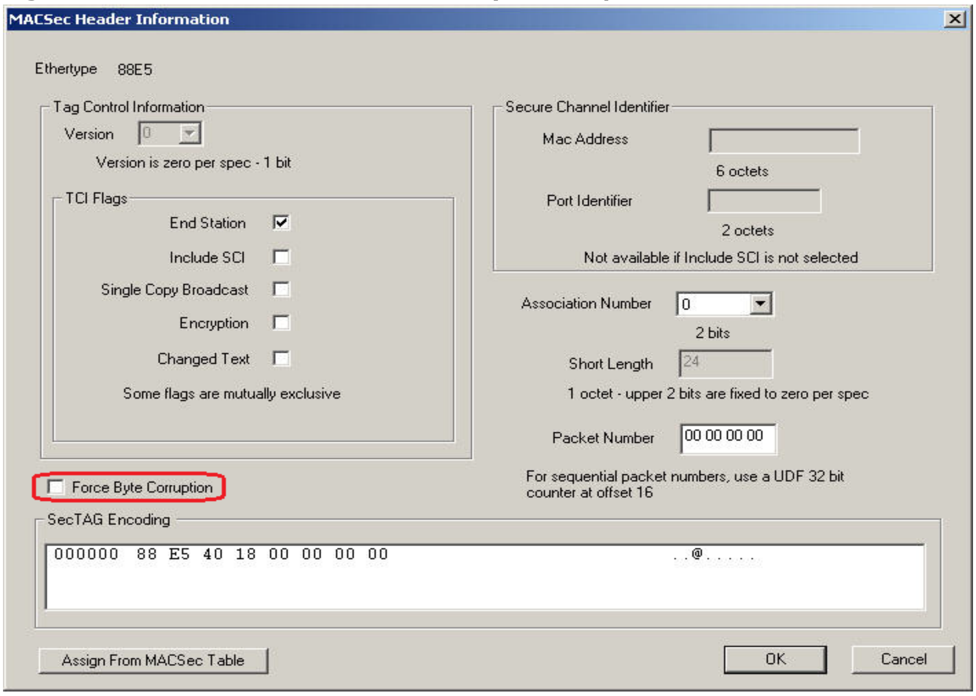


Table:Negative Testing Dialog

Field	Description
Offset	(default = 0) 16-bit Corruption Offset. This is a byte offset from the first DA byte of the frame. This first DA byte corresponds to an offset of 0000.
Mask	8-bit CorruptionMask (default = 00000000) 1 = Bit value will be flipped. 0 = Bit is masked (unchanged). For example, a mask of 'F0' means bits of upper nibble will be flipped.

On a packet level, byte corruption is enabled through a check box in the MACSec Header Information dialog as shown in Figure:MACSec Header Info with Force Byte Corruption. This screen is accessed by opening Stream Properties, Frame Data tab, then enabling and clicking the MACSec button. (See Protocol Control for 10GE LSM MACSec Modules.)

Figure:MACSec Header Info with Force Byte Corruption



Any stream that has this Force Byte Corruption selected (enabled) will result in that stream being corrupted, unless corruption offset is located in the packet CRC or beyond.

Auto Instrumentation for MACSec Load Modules

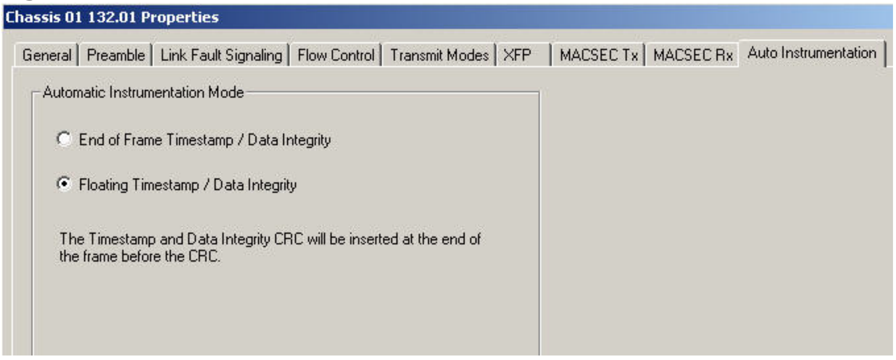
For TXS load modules (*Auto Instrumentation Tab for Ethernet Modules*, Auto Timestamp is an option that allows those ports to handle time-stamps for MAC in MAC frames, but otherwise, it is an enhanced version of Timestamp.

For MACSec load modules (LSM10GMS-01), Auto Timestamp is the **only** way that Timestamp can be added to MACSec frames. Legacy Timestamp is always placed just before CRC. But MACSec frames place ICV at that location, so the only way to make a timestamp work is to allow it to ‘float’.

The following rules apply for MACSec.

- If MACSec protocol is **not** enabled:
  - Then legacy Timestamp and Auto Instrumentation with Timestamp are both available. (*Auto Instrumentation Tab for Ethernet Modules*.)
  - If legacy Timestamp is **enabled** (and MACSec is **not** enabled), and you subsequently enables MACSec, the application will force legacy Timestamp to be unselected and grayed out.
- If MACSec protocol is **enabled**:
  - then legacy Timestamp is not selectable.
- A warning will alert if Floating Timestamp ever overlaps with MACSec ICV.

Figure:MACSec Auto Instrumentation Tab



10GE WAN Port Properties

The port properties for 10 Gigabit WAN modules are based, in part, on SONET frame properties, per the IEEE P802.3ae WAN Interface Sublayer (WIS), an optional PHY sublayer defined for 10GBASE-W equipment. This PHY is compatible with the ANSI-defined SONET STS-192c, and the ITU Synchronous Digital Hierarchy (SDH) VC-4-64c without the requirement for MAC or higher-layer processing. Since the 10GBASE-W is not intended to interoperate directly with SONET or SDH interfaces, they can interoperate only with a like interface.

For NGY port properties, see *Port Properties–NGY Family*.

The tabs which make up the 10GE WAN Port Properties are described in the following sections:

- *10GE WAN Port Properties—Preamble*
- *10GE WAN Port Properties—SONET Tab*
- *10GE Port Properties–Flow Control*
- *10GE WAN Port Properties—SONET Overhead*
- *10GE WAN Port Properties—J0/J1*
- *10GE WAN Port Properties—Transmit Modes*
- *10GE WAN Port Properties—Link Fault Signaling*

10GE WAN Port Properties—Preamble

The *Preamble* tab allows to adjust the contents of the preamble in 10 GE frames. This tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu option, and then selecting the *Preamble* tab. The 10GE WAN Port Properties *Preamble* tab is shown in *Figure:10GE WAN—Preamble Tab*. The 10G MSM WAN Preamble tab is shown in *Figure:10GE WAN—Preamble Tab*

Figure:10GE WAN—Preamble Tab

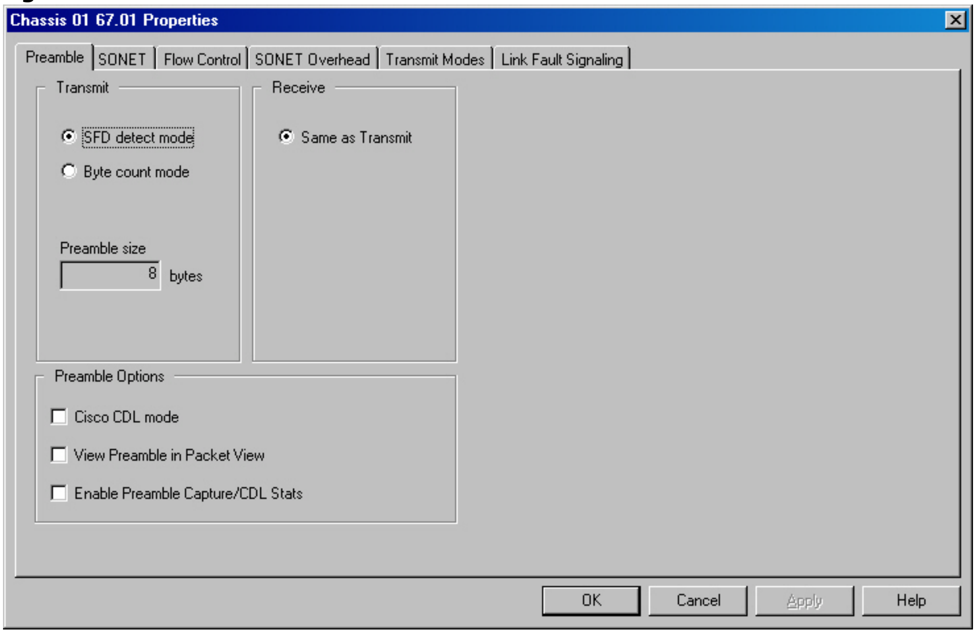
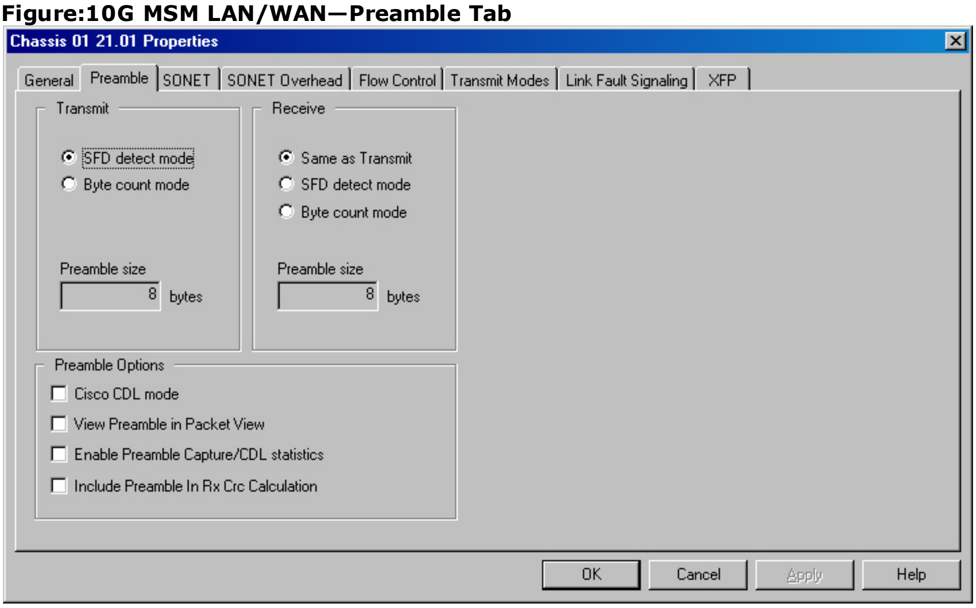


Figure:10G MSM LAN/WAN—Preamble Tab



The fields and controls in this tab are described in *Table:10GE Port Properties—Preamble*.

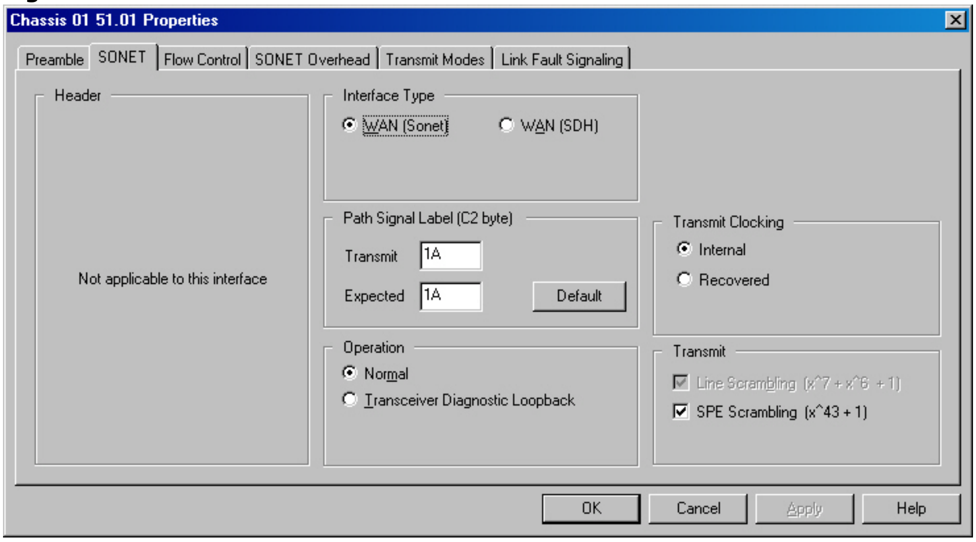
Table:10GE Port Properties—Preamble

Section	Choices	Description
Transmit	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8

Section	Choices	Description
		bytes in this case), and considers the next byte (9th) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the *Frame Data* tab in the *Stream Properties* dialog. This value is currently fixed at 8 bytes (the default).
Receive	Same as Transmit	The Receive side will accept the same choices/entries that were made for the Transmit side.
	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case), and considers the next byte (9th byte) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the *Frame Data* tab in the *Stream Properties* dialog. This value is currently fixed at 8 bytes (the default).
Preamble Options	Cisco CDL Mode	Enables the use of Cisco’s Converged Data Link (CDL) packets, which substitutes the six preamble bytes and the SFD byte with a specific seven byte CDL header (does not apply to UNIPHY modules in 10GE LAN Mode). Selecting this disables the Transmit SFD detect mode.
	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side) (does not apply to UNIPHY modules in 10GE LAN Mode).
	Enable Preamble Capture/CDL Stats	When this check box is selected, the preamble is included for all packets captured through capture engine and will enable passing preamble data through Rx engine in order for CDL statistics to function (does not apply to UNIPHY modules in 10GE LAN Mode).
	Include Preamble In Rx CRC Calculation	When this check box is selected, the CRC calculation takes into account the preamble length.

10GE WAN Port Properties—SONET Tab

Figure:10GE WAN—SONET Tab



For UNIPHY 10GE WAN Port Properties SONET information, *UNIPHY 10GE WAN—SONET Tab*.

The fields in this tab and their usage are described in .

Table:10GE WAN—SONET Tab

Section	Field/Control	Description
Header		(Not applicable to this interface.)
Interface Type	WAN (SONET)	WAN (Optical Carrier level 64 concatenated)
	WAN (SDH)	Synchronous transfer mode level 64 (SDH)
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted stream. (Hex)
	Expected	The expected value of the link partner's C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both *Transmit* and *Expected* values to '1A.'
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the 10GE WAN frames to be looped back at the transceiver.
Error Handling		(Not applicable to this interface.)
Transmit Clocking	Internal	Use the chassis internal clock.
	Recovered	If enabled, the transmit clock is derived from the recovered (received) clock. If not enabled, the transmit clock is derived from the internal clock. Select this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
Transmit	Line Scrambling	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.

Section	Field/Control	Description
	SPE Scrambling	If enabled, data is scrambled with the x^{43} + 1 polynomial.
	Use Recovered Clock	If enabled, the transmit clock is derived from the recovered (received) clock, or from the internal clock otherwise. Enable this check box if the DUT will supply the clock signal or on one of a pair of directly connected Ixia ports.

10GE WAN Port Properties—SONET Overhead

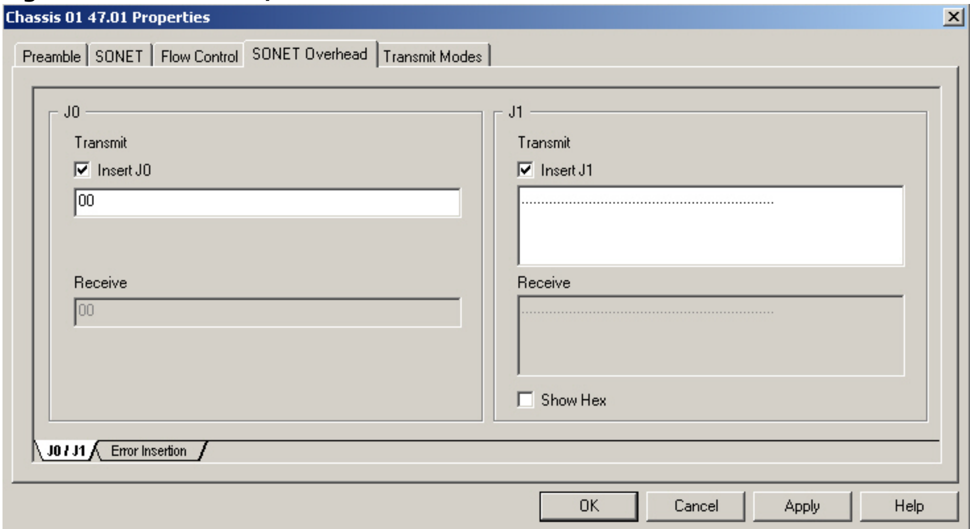
The *SONET Overhead* tab consists of two sub-tab, described in the following sections:

- *10GE WAN Port Properties—J0/J1*
- *10GE WAN Port Properties—Error Insertion*

10GE WAN Port Properties—J0/J1

The 10GE WAN Port Properties *J0/J1* sub-tab is shown in *Figure:10GE WAN—J0/J1*. Refer to *J0/J1 Sub-Tab* for information on the fields in this tab.

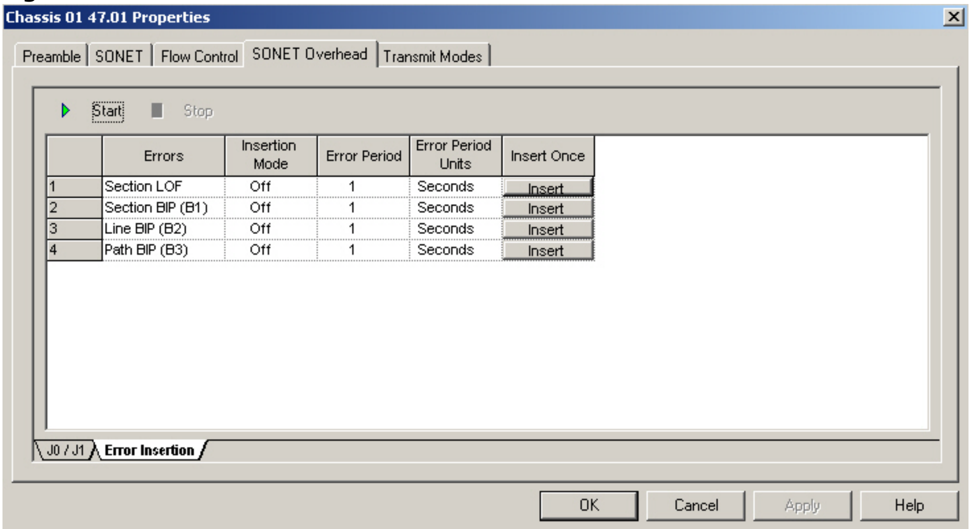
Figure:10GE WAN—J0/J1



10GE WAN Port Properties—Error Insertion

The 10GE WAN Port Properties *Error Insertion* sub-tab is shown in *Figure:10GE WAN—Error Insertion*. Refer to *SONET Error Insertion—Reduced Error Set* for information on the fields in this sub-tab.

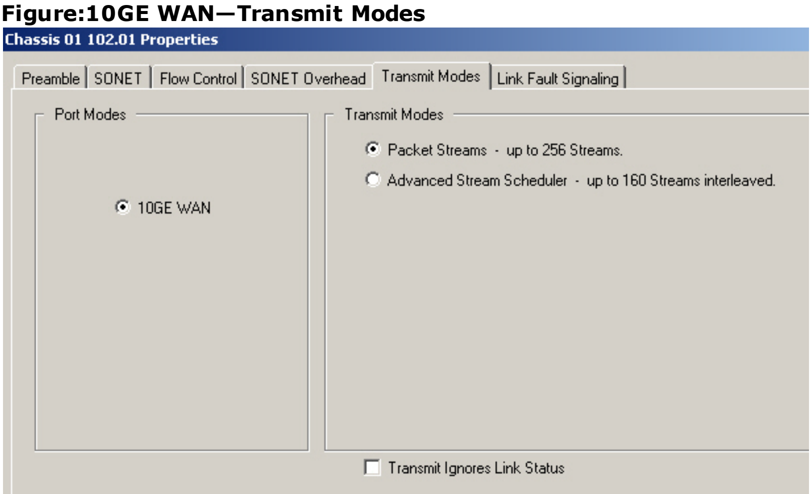
Figure:10GE WAN—Error Insertion



10GE WAN Port Properties—Transmit Modes

The 10GE WAN Port Properties *Transmit Modes* tab is shown in *10GE WAN—Transmit Modes*.

Figure:10GE WAN—Transmit Modes



The *Transmit Modes* tab for the 10GE WAN modules allows to select packet streams or advanced streams. The options are described in *Table:10GE WAN—Transmit Modes Tab*.

Table:10GE WAN—Transmit Modes Tab

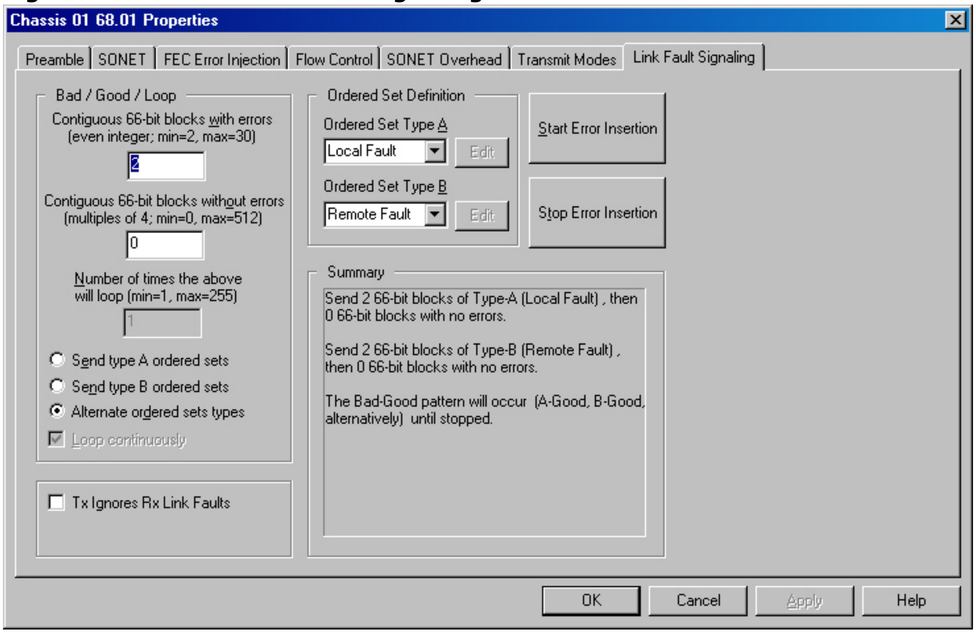
Section	Field/Control	Description
Port Modes	10GE WAN	Sets the module to the 10GE WAN mode.
Transmit Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 256 streams; each stream may contain 16 million bursts, each containing up to 16 million packets. A stream may be programmed for continuous burst or packet generation— generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets up the transmission of up to 160 interleaved

Section	Field/Control	Description
		packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
Transmit Ignores Link Status	(check box)	If selected, will allow transmission of packets even if the link is down.
	BERT (optional feature)	Bit Error Rate Test (BERT). Data are transmitted in patterns of bits to the receiving interface, where the data are matched to known patterns, and then monitored for mismatches to evaluate data integrity for the connection. *Port Properties for BERT* for additional information on 10GE WAN BERT.

10GE WAN Port Properties—Link Fault Signaling

The 10GE WAN Port Properties *Link Fault Signaling* tab is shown in *Figure:10GE WAN—Link Fault Signaling*. Refer to *10GE Port Properties–Link Fault Signaling* for information on this tab.

Figure:10GE WAN—Link Fault Signaling



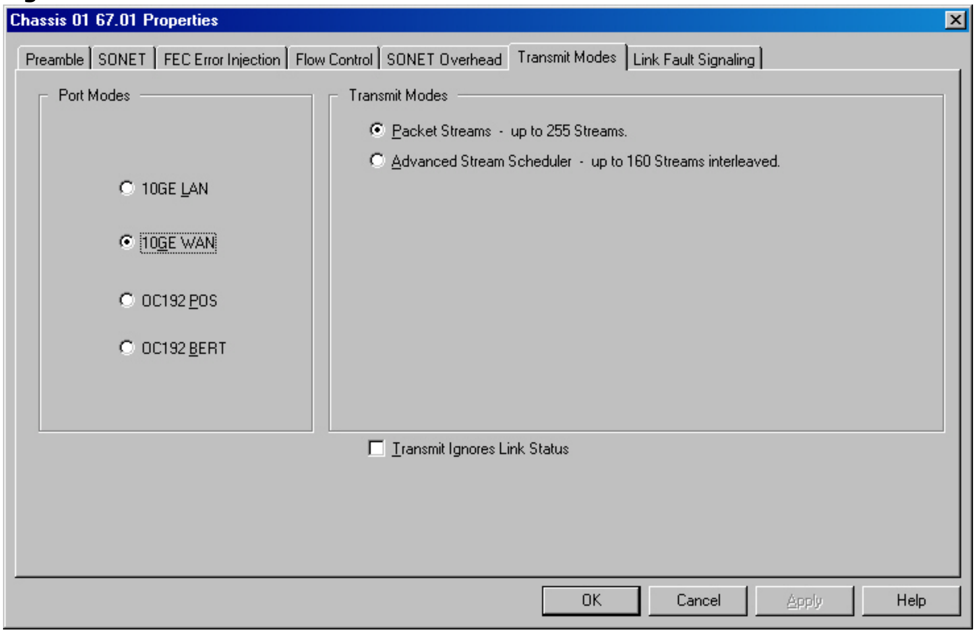
Port Properties for UNIPHY Modules

The UNIPHY module offers a choice of four modes of operation: 10GE LAN or WAN, or OC-192c POS or BERT.

The complete specifications for the UNIPHY modules can be found in the *Ixia Platform Reference Manual.*

The UNIPHY Port Properties *Transmit Modes* tab is shown in *Figure:UNIPHY Transmit Modes Tab*.

Figure:UNIPHY Transmit Modes Tab



The set of Port Properties tabs displayed depends on the Port Mode selection in the Transmit Modes page. The tabs available for each mode are described in the following sections:

- **Port Properties for 10GE LAN**:
  - *10GE Port Properties for Uniphy Modules—General Tab*
  - *10GE Port Properties–Preamble*
  - *UNIPHY 10GE Port Properties—SONET/LINK*
  - *SONET Properties*(10G MSM only)
  - *FEC Error Injection*
  - *10GE Port Properties–Flow Control*
  - *10GE Port Properties–Transmit Modes*
- **Port Properties for 10GE WAN**:
  - *10GE Port Properties for Uniphy Modules—General Tab*(10GE MSM only)
  - *10GE WAN Port Properties—Preamble*
  - *UNIPHY 10GE WAN—SONET Tab*
  - *SONET Properties*(10G MSM only)
  - *FEC Error Injection*
  - *10GE Port Properties–Flow Control*
  - *10GE WAN Port Properties—SONET Overhead*
  - *10GE WAN Port Properties—J0/J1*
  - *10GE WAN Port Properties—Transmit Modes*
  - *10GE WAN Port Properties—Link Fault Signaling*
- **Port Properties for OC-192c POS:**
  - *10GE Port Properties for Uniphy Modules—General Tab* (10GE MSM only)
  - *SONET Properties*
  - *FEC Error Injection*
  - *PPP Properties*

  - *SONET Overhead*
    - *APS K1/K2 Sub-Tab*
    - *J0/J1 Sub-Tab*
    - *SONET Error Insertion*
  - *Transmit Modes for POS Modules*
- **Port Properties for OC-192c BERT**:
  - *SONET Tab for BERT Mode*
  - *FEC Error Injection*
  - *SONET Overhead*
    - *APS K1/K2 Sub-Tab*
    - *J0/J1 Sub-Tab*
    - *SONET Error Insertion*
    - *SONET Overhead—Transport Overhead*
- **Port Properties for UNIPHY-XFP**:

  (Note that UNIPHY-XFP only differ with the addition of the XFP tab page. All other tabs are identical to the selected Transmit Mode partner.)

  - *UNIPHY—XFP Interface*

10GE Port Properties for Uniphy Modules—General Tab

The appearance of the General tab for 10GE load modules depends upon the setting in the Port Mode section. Below are the three possible configurations:

- *Figure:10G LAN Mode General Tab* is LAN mode
- *Figure:10G WAN Mode General Tab* is WAN mode
- *Figure:10G OC-192c Mode General Tab* is OC-192c mode

The *General* tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu option, and then selecting the *General* tab.

FigureL:10G LAN Mode General Tab

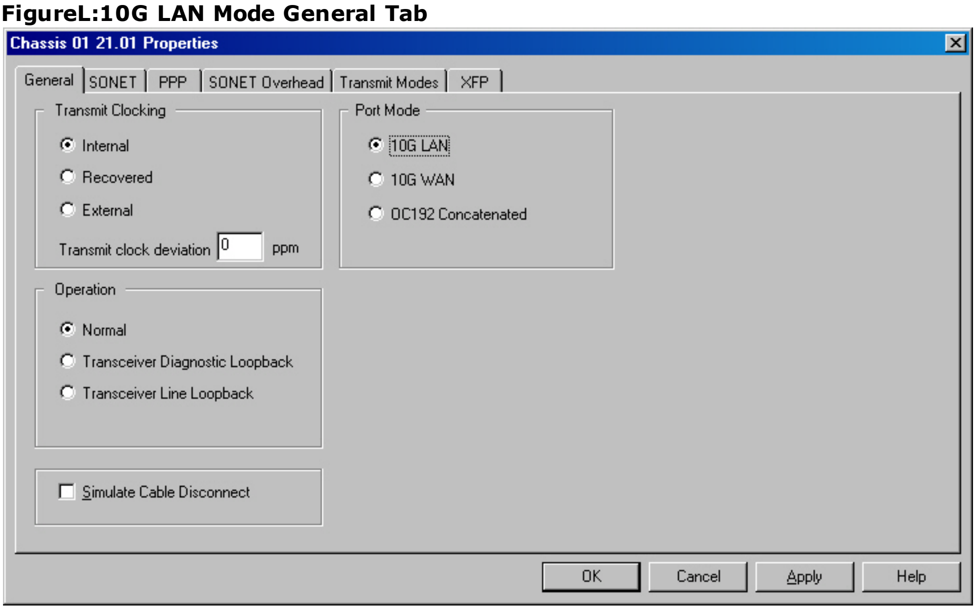


Figure:10G WAN Mode General Tab

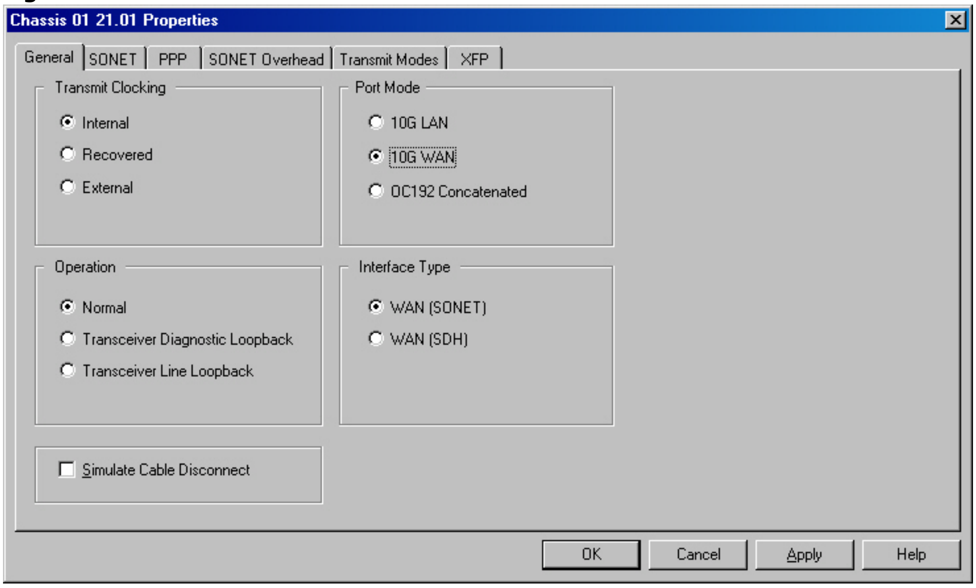


Figure:10G OC-192c Mode General Tab

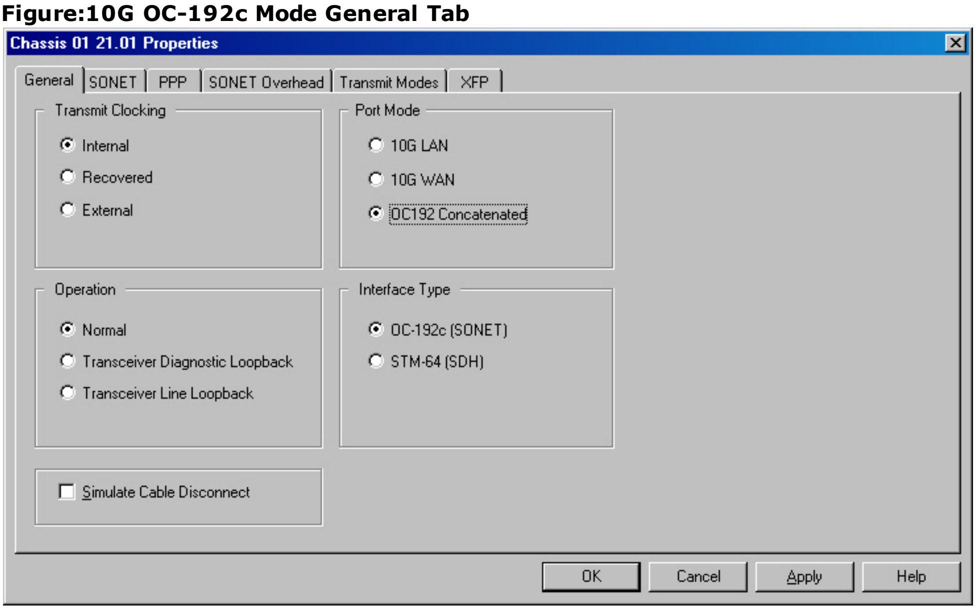


Table:General Tab Configuration Options explains the configuration options of the *General* tab.

Table:General Tab Configuration Options

Section	Field/Control	Description
Transmit Clocking	Internal	Use the chassis internal clock.
	Recovered	If enabled, then the transmit clock is derived from the recovered (received) clock. If not enabled, then the transmit clock is derived from the internal clock. Select this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
	External	If enabled, then an external clock source is

Section	Field/Control	Description
		used.
	Transmit Clock Deviation ppm	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port. 10 GE MSM cards can be adjusted from -128 to +127 ppm from the initial rate.
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disabled if FEC is enabled.)
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
Port Mode	10G LAN	Sets the transmit mode to 10G LAN.
	10G WAN	Sets the transmit mode to 10G WAN.
	OC-192c	Sets the transmit mode to OC-192c.
Interface Type	WAN (SONET)	WAN SONET option (10G WAN mode only).
	WAN (SDH)	WAN SDH option (10G WAN mode only).
	OC-192c (SONET)	Optical Carrier level 192 concatenated (OC-192c mode only).
	STM-64 (SDH)	Synchronous transfer mode level 64 (OC-192c mode only).
Simulate Cable Disconnect		If this is selected, then the port acts as if the cable has been disconnected.

UNIPHY 10GE Port Properties—SONET/LINK

After selecting the 10GE LAN option for a UNIPHY load module (as described in *Port Properties for UNIPHY Modules*) the SONET/LINK tab appears. The *SONET/Link* tab is shown in *Figure:SONET/LINK Tab for UNIPHY 10 GE LAN Modules* below.

Figure:SONET/LINK Tab for UNIPHY 10 GE LAN Modules

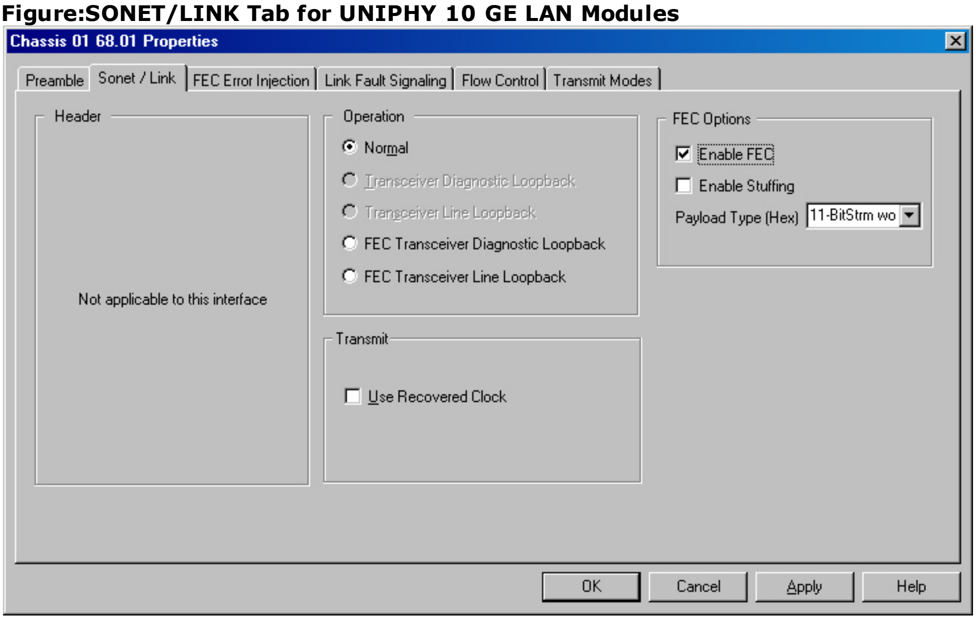


Table:SONET/LINK Configurable Parameters describes the configurable fields in the tab above.

Table:SONET/LINK Configurable Parameters

Group	Field	Usage
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Diagnostic Loopback	Causes the SONET frames to be looped back at the transceiver. (This option button is disable if FEC is enabled.)
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disabled if FEC is enabled.)
	FEC Transceiver Diagnostic Loopback	(Only available with FEC modules.) Causes the FEC data to be looped back at the transceiver.
	FEC Transceiver Line Loopback	(Only available with FEC modules.) Causes the data from the receive port to be sent out the transmit port from the FEC Framer.
Transmit	Use Recovered Clock	If enabled, then the transmit clock is derived from the recovered (received) clock. If not enabled, then the transmit clock is derived from the internal clock. Enable this check box if the DUT will supply the clock signal on one of a pair of directly connected Ixia ports.
FEC Options (Only available with FEC modules.)	Enable FEC	Enables FEC information to be included with transmitted data. This also enables the features found on the FEC Error Injections Tab page, described in *FEC Error Injection*.

Group	Field	Usage
	Enable Stuffing	Enables the FEC fixed stuff bytes field in the overhead. This check box is only visible when the *Enable FEC* check box is selected.
	Payload Type	Allows for the selection of the FEC payload type, from the following list: • 02-asy STM-N • 03-bit syn STM-N • 04-ATM • 05-GFP • 10-bit str w o.t. • 11-bit str wo o.t. • FE-PRBS This list defines what data type is being simulated in the payload area of the SONET frame. This list is only visible when the *Enable FEC* check box is selected.

FEC Error Injection

Forward Error Correction (FEC) is a method of communicating data that corrects errors in transmission on the receiving end. Prior to transmission, the data is put through a predetermined algorithm that adds extra bits specifically for error correction to any character or code block. If the transmission is received in error, the correction bits are used to check and repair the data.

The FEC Error Injection tab allows to inject FEC errors into transmitted data, and is shown in *Figure:FEC Error Injection Tab Page*

Figure:FEC Error Injection Tab Page

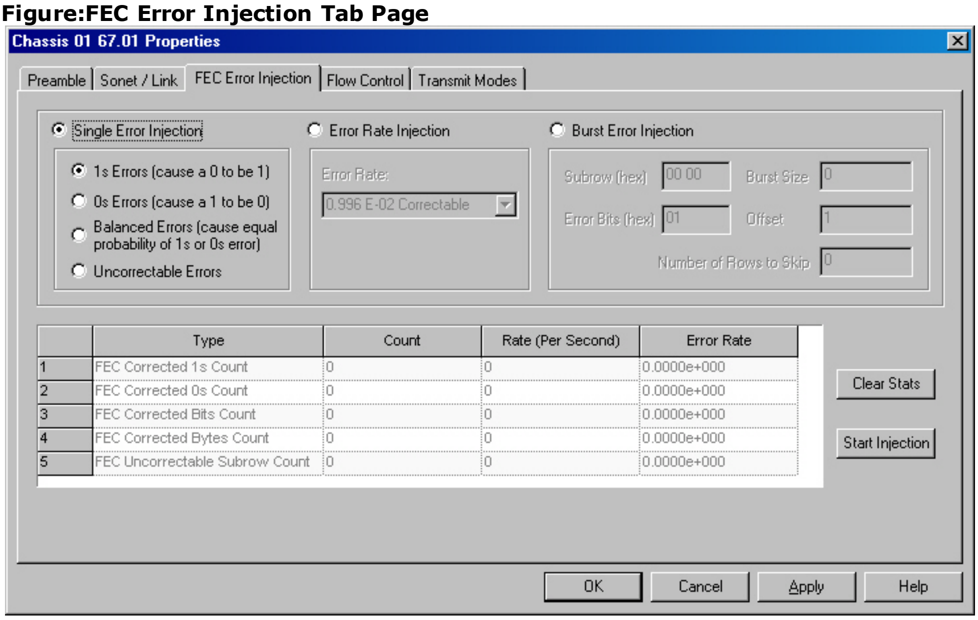


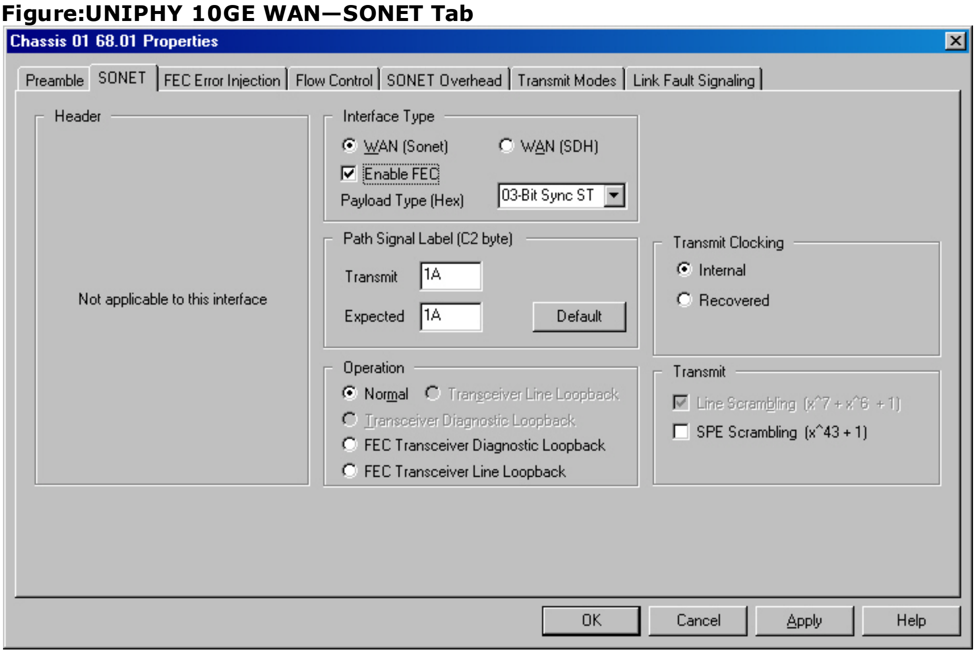
Table:FEC Tab Configuration

Section	Field	Usage
Single Error Injection		This is single shot error injection mode. Every click of *Start Injection* button generates a single error.
	1s Errors	Selecting this option button causes an error that replaces a 0 with a 1.
	0s Errors	Selecting this option button causes an error that replaces a 1 with a 0.
	Balanced Errors	Selecting this option button causes an errors which could be either a 0 or 1 replacement.
	Uncorrectable Errors	Selecting this option button creates uncorrectable errors. The FEC process will not be able to fix these errors.
Error Rate Injection		This is continuous error injection mode. The pull-down menu allows to select the error type.
	Error Rate	Eleven correctable error rates (from 0.996E-2 to 1.000E-12) and 9 uncorrectable error rates (from 0.996E-2 to 1.000E-10) are currently supported.
Burst Error Injection		(For Advanced User Only) This is continuous error injection. Click of *Start Injection* button starts the error injection.
	Subrow (Hex)	Which sub-row(s) to corrupt out of the 16 interleaved sub-rows. Each bit position represents one sub-row. Thus if Subrow = 0xFFFF, then all sub-rows have errors on them. Default Subrow = 0x0000, meaning all sub-rows are disabled.
	Error bits (Hex)	Which bits in a byte should be corrupted. Default is 01 hex, meaning only the least significant bit of the byte is corrupted when corruption is enabled.
	Burst Size	The number of consecutive bytes (up to 15) after the 1st corrupted byte in each 255-byte sub-row to also be corrupted. Thus if Burst Size = 15, then 16 bytes will be corrupted in each selected sub-row. Default Burst Size = 0, meaning only 1 byte will be corrupted. (Tips: programming burst size not less than 8, get uncorrectable errors)
	Offset	Inject errors starting at a programmable offset into the sub-row. Default is 01 hex, meaning the first byte after the OH byte will be corrupted when corruption is enabled.
	Number of Rows to Skip	How many rows to skip before the next corruption. Default is 0, meaning no rows are skipped between corruptions.

Section	Field	Usage
Type		The type of error recorded.
Count		The number of time a particular error type occurred.
Rate (Per Second)		The line rate of the port.
Error Rate		The rate of errors in the data stream.
Clear Stats		Selecting this button clears the recorded statistics.
Start Injection		Selecting this button begins the error insertion process.

UNIPHY 10GE WAN—SONET Tab

Figure:UNIPHY 10GE WAN—SONET Tab



For information on standard 10GE WAN Port Properties (non UNIPHY) for SONET, *10GE WAN Port Properties—SONET Tab*.

The fields in this tab and their usage are described in *Table:UNIPHY SONET Tab Configuration*.

Table:UNIPHY SONET Tab Configuration

Section	Field	Usage
Header		(Not applicable to this interface.)
Interface Type	WAN (SONET)	WAN (Optical Carrier level 64 concatenated)
	WAN (SDH)	Synchronous transfer mode level 64 (SDH)
	Enable FEC	(Only for FEC modules.) Enables insertion of FEC information into transmitted data. This also enables the feature found on the *FEC Error Injection* tab page, described in *FEC Error Injection*.
	Payload Type (Hex)	(Only for FEC modules.)

Section	Field	Usage
		Allows for the selection of the FEC payload type, from the following list: • 02-asy STM-N • 03-bit syn STM-N • 04-ATM • 05-GFP • 10-bit str w o.t. • 11-bit str wo o.t. • FE-PRBS This list defines what data type is being simulated in the payload area of the SONET frame. This list is only visible when the *Enable FEC* check box is selected.
Path Signal Label (C2 byte)	Transmit	The value of the C2 byte in the transmitted stream. (Hex)
	Expected	The expected value of the link partner’s C2 byte. Typically, this will match the value in the *Transmit* field. (Hex)
	Default	Use of this button forces both *Transmit* and *Expected* values to ‘1A.’
Operation	Normal	Uses standard Tx and Rx paths.
	Transceiver Line Loopback	Causes the SONET frames received by the port to be sent back out to the sending port, creating an echo of the link partner. These frames can also be captured. (This option button is disable if FEC is enabled.)
	Transceiver Diagnostic Loopback	Causes the 10GE WAN frames to be looped back at the transceiver. (This option button is disable if FEC is enabled.)
	FEC Transceiver Diagnostic Loopback	(Only for FEC modules.) Causes the 10GE WAN FEC information to be looped back at the transceiver.
	FEC Transceiver Line Loopback	(Only for FEC modules.) Causes the data from the receive port to be sent out the transmit port from the FEC Framer.
Transmit Clocking	Internal	Use the chassis internal clock.
	Recovered	If enabled, then the transmit clock is derived from the recovered (received) clock. If not enabled, then the transmit clock is derived from the internal clock. Enable this check box if the DUT will supply the clock signal on one of a pair of directly con-

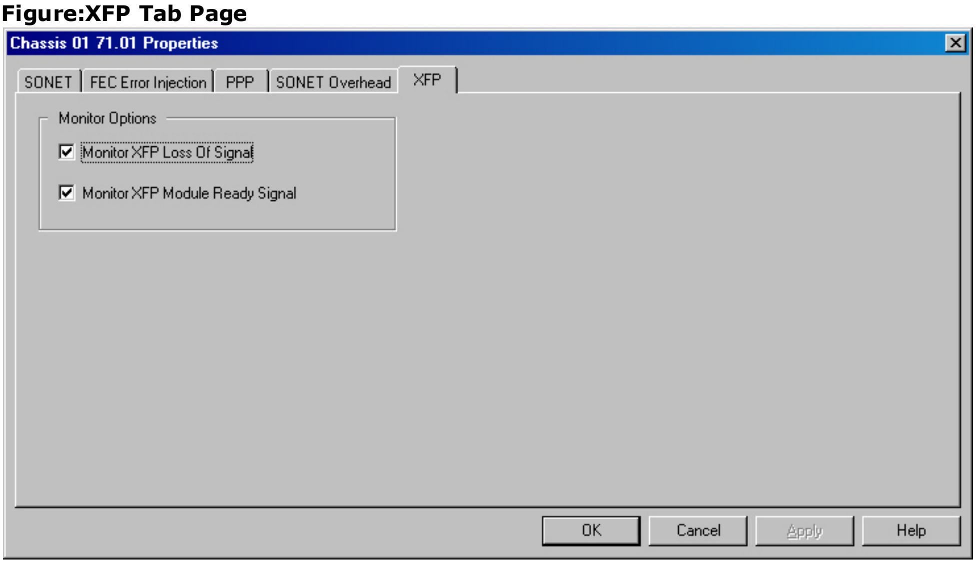
Section	Field	Usage
		nected Ixia ports.
Transmit	Line Scrambling	Standard line scrambling using the $x^7 + x^6 + 1$ polynomial.
	SPE Scrambling	If enabled, then data are scrambled with the $x^{43} + 1$ polynomial.
	Use Recovered Clock	If enabled, then the transmit clock is derived from the recovered (received) clock, or from the internal clock otherwise. Enable this check box if the DUT will supply the clock signal or on one of a pair of directly connected Ixia ports.

UNIPHY—XFP Interface

Special UNIPHY load modules can support XFP interfaces. The XFP is a hot pluggable small footprint serial-to-serial data-agnostic multi-rate optical transceiver, intended to support Telecom (SONET OC-192 and G.709 'OTU-2') and Datacom applications (10 Gb/s Ethernet and 10 Gb/s Fibre Channel).

When UNIPHY modules are equipped with an XFP interface, an extra tab is available in the *Port Properties* dialog. The *XFP* tab is shown in *Figure:XFP Tab Page*.

Figure:XFP Tab Page



The fields in this tab page are described in *Table:XFP Tab Page Usage*.

Table:XFP Tab Page Usage

Field	Usage
Monitor XFP Loss of Signal	When selected, indicates the interface will conform to XFP specifications and require the absence of a Loss of Signal for transmitting and receiving.
Monitor XFP Module Ready Signal	When selected, indicates the interface will conform to XFP specifications and require the detection of a Module Ready signal for transmitting and receiving.

Channelized BERT

Channelized BERT is available as an option on some of the OC-192c and 10GE XAUI load modules.

- *10GE XAUI/XENPAK Channelized BERT*.

10GE XAUI/XENPAK Channelized BERT

The 10GE XAUI or 10GE XENPAK Channelized BERT feature operates in a manner similar to OC-192c Channelized BERT, but with an individual PRBS data pattern transmitted on each of the four 'Lanes,' rather than in 'Channels,' as in OC-192c.

When the channelized BERT option is selected in the XAUI or XENPAK/BERT *Transmit Modes* tab, the BERT option in the Port Details list displays the XAUI/XENPAK Channelized BERT window, as shown in *Figure:Channelized BERT Window—Shown for 10GE XAUI Module*.

Figure:Channelized BERT Window—Shown for 10GE XAUI Module

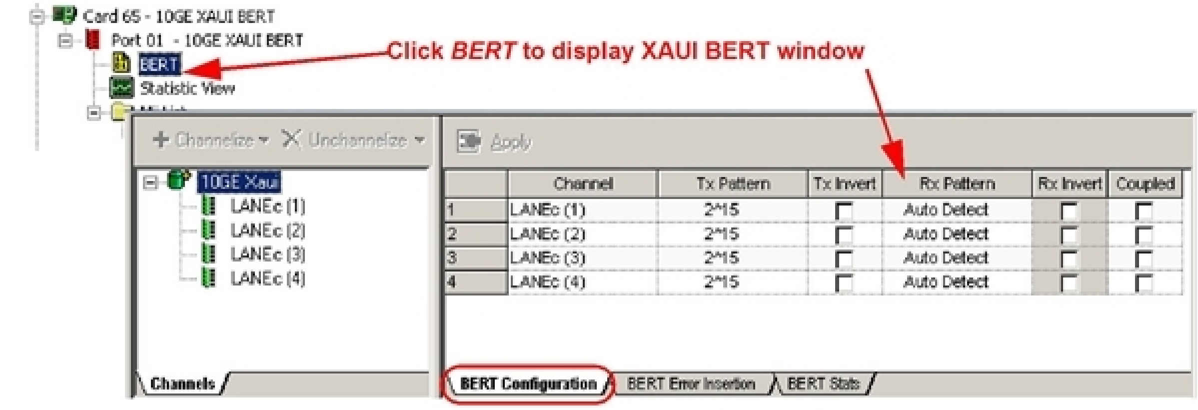
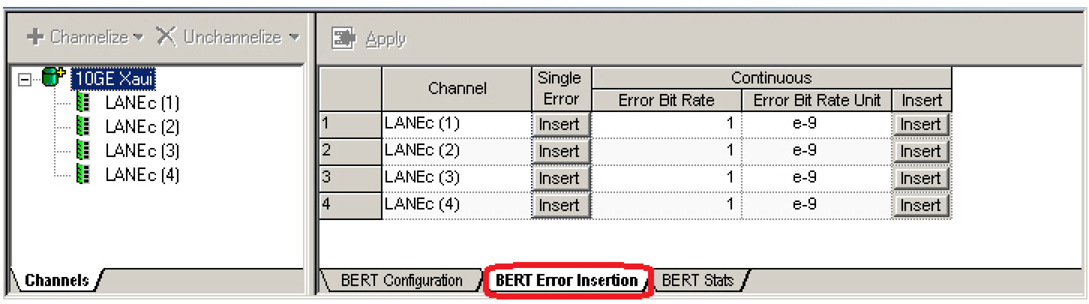
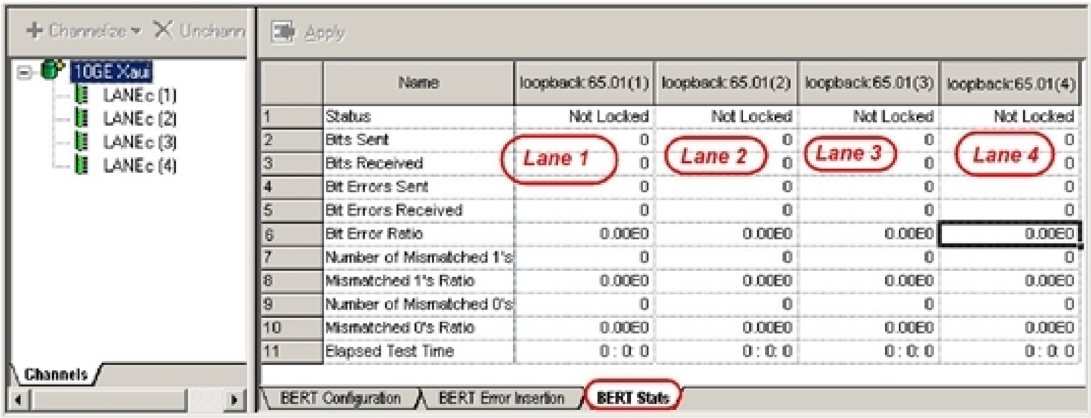


Figure:Bert Error Insertion—Shown for 10GE XAUI Module



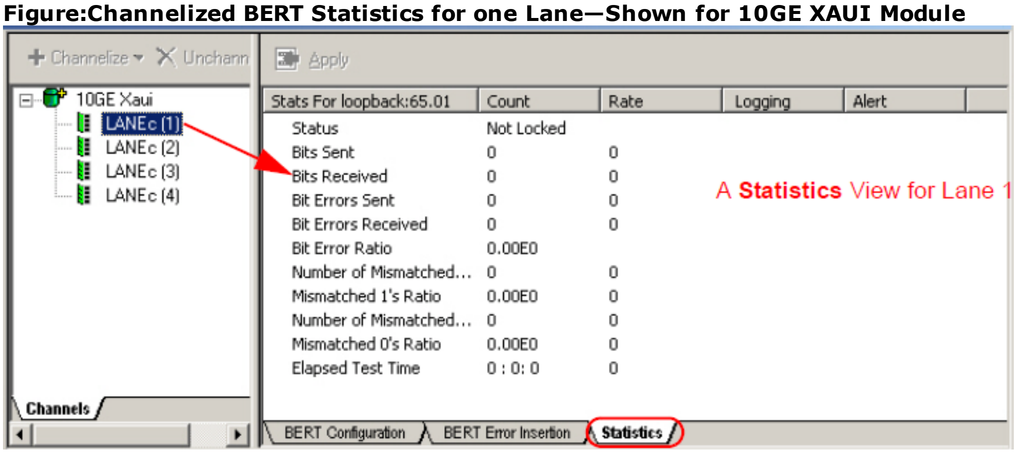
The *BERT Stats* tab displays the information fields for all four of the XAUI/XENPAK lanes, as shown in *Figure:Channelized BERT Statistics—Shown for 10GE XAUI Module*. Channelized BERT for detailed information on channelized OC-192c BERT configuration.

Figure:Channelized BERT Statistics—Shown for 10GE XAUI Module



When the *BERT Stats* tab is displayed, and one of the XAUI/XENPAK Lanes is selected in the list in the left pane, an individual Statistic View for that particular lane is then displayed in the right pane, as shown in *Figure:Channelized BERT Statistics for one Lane—Shown for 10GE XAUI Module*. *Table:Channelized BERT Statistics* for descriptions of the displayed statistics.

Figure:Channelized BERT Statistics for one Lane—Shown for 10GE XAUI Module



Note that BERT ratios are exclicked as an exponential value in the format 0.00E0 (for example, 2.82E-5). The statistics for both types of statistics displays are described in *Table:Channelized BERT Statistics*.

Table:Channelized BERT Statistics

Statistic	Description
Status	The status of the connection. 'Locked' when the receiving interface locks onto the data pattern.
Bits Sent - Count and Rate	The total number of bits sent, and the rate at which they are sent.
Bits Received - Count and Rate	The total number of bits received, and the rate at which they are received.
Bit Errors Sent - Count and Rate	The total number of bit errors sent, and the rate at which they are sent.
Bit Errors Received - Count and Rate	The total number of bit errors received, and the rate at which they are sent.
Bit Error Ratio	(BER) the ratio of the number of errored bits compared to the total number of bits transmitted. In the following format:

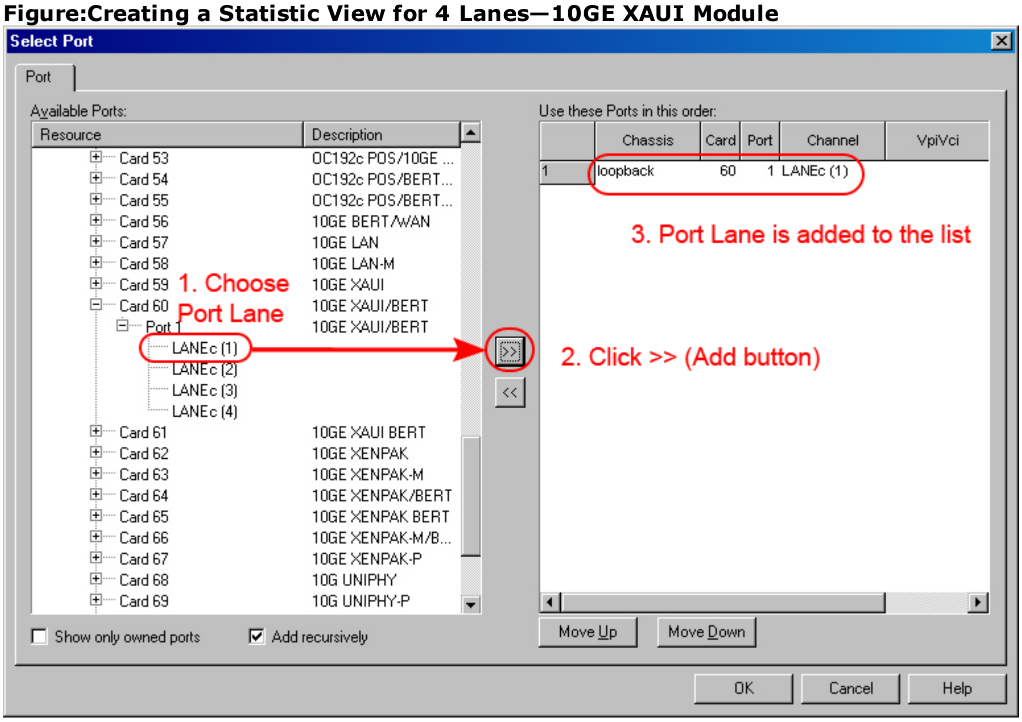
Statistic	Description
	0.00E0.
Number of Mismatched 1's - Count and Rate	The number of expected ones received as zeros.
Mismatched 1's Ratio	The ratio of the number of expected ones received as zeroes to all bits. In the following format: 0.00E0.
Number of Mismatched 0's - Count and Rate	The number of expected zeros received as ones.
Mismatched 0's Ratio	The ratio of the number of expected zeros received as ones to all bits. In the following format: 0.00E0.
Elapsed Test Time	The elapsed test time, exclicked as HH : MM : SS.

Statistic View for Multiple Lanes or Channels

A customized, spreadsheet-style Statistic View can be created which displays BERT statistics for all four Lanes of a XAUI/XENPAK BERT module. Or, the view may be created for channels of a OC-192c Channelized BERT module.

To create the view, go to *Statistic View* at the bottom of the Network Resources tree. Right-click *Statistic View*, then select *New*. The *Select Port* dialog will be displayed, as shown in *Figure:Creating a Statistic View for 4 Lanes—10GE XAUI Module*.

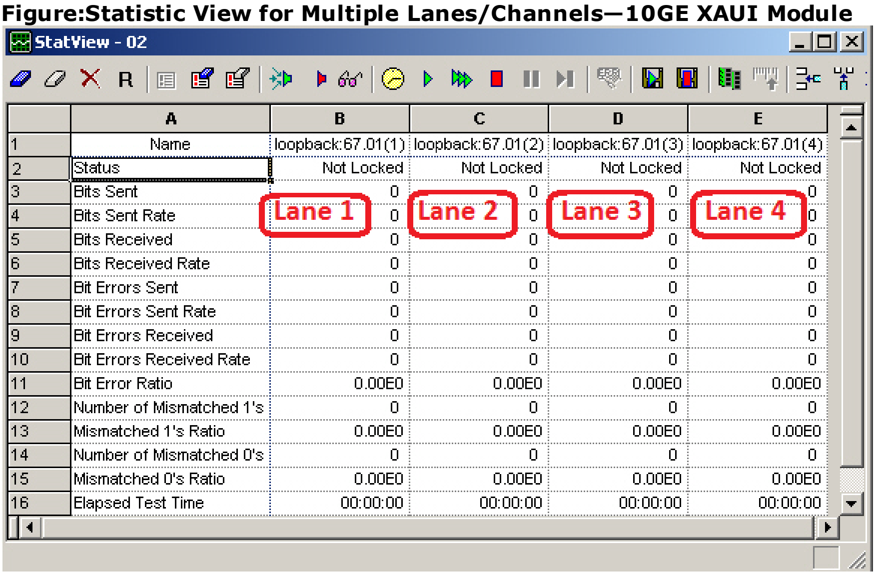
Figure:Creating a Statistic View for 4 Lanes—10GE XAUI Module



Keep adding lanes or channels as shown above, and then click *OK*. The new Statistic View will be displayed, as shown in the example for four lanes of XAUI/XENPAK BERT statistics in *Figure:Statistic View for Multiple Lanes/Channels—10GE XAUI Module*. The displayed BERT statistics are described in *Table:Channelized BERT Statistics*.

NOTE For a description of the Select Port dialog,Select Port Dialog.

Figure:Statistic View for Multiple Lanes/Channels—10GE XAUI Module



	A	B	C	D	E
1	Name	loopback:67.01(1)	loopback:67.01(2)	loopback:67.01(3)	loopback:67.01(4)
2	Status	Not Locked	Not Locked	Not Locked	Not Locked
3	Bits Sent	0	0	0	0
4	Bits Sent Rate	0	0	0	0
5	Bits Received	0	0	0	0
6	Bits Received Rate	0	0	0	0
7	Bit Errors Sent	0	0	0	0
8	Bit Errors Sent Rate	0	0	0	0
9	Bit Errors Received	0	0	0	0
10	Bit Errors Received Rate	0	0	0	0
11	Bit Error Ratio	0.00E0	0.00E0	0.00E0	0.00E0
12	Number of Mismatched 1's	0	0	0	0
13	Mismatched 1's Ratio	0.00E0	0.00E0	0.00E0	0.00E0
14	Number of Mismatched 0's	0	0	0	0
15	Mismatched 0's Ratio	0.00E0	0.00E0	0.00E0	0.00E0
16	Elapsed Test Time	00:00:00	00:00:00	00:00:00	00:00:00

[This page intentionally left blank]

Chapter 21 - Port Properties–40/100 GE Family

The *Port Properties* dialog controls a number of properties related to the port’s operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the 40/100 Gigabit Ethernet module family port properties.

Port Properties for 40/100 Gigabit Modules

The *Port Properties* dialog is accessed by right-clicking a port in the Resources window, then selecting the *Properties* menu option.

The complete specification for the 40/100 Gigabit type boards can be found in the *Ixia Platform Reference Manual*.

The 40/100 Gigabit characteristics are defined in the IEEE 802.3ba standard. For more information about this standard and 100 Gigabit architecture, see the *40GE and 100GE* subsection under *Port Hardware / Types of Ports*, in the ‘Theory of Operation: General’ chapter of the *Ixia Platform Reference Manual*.

The following port property tabs are available for 40/100GE LAN modules:

- *40/100GE Port Properties— General*
- *40/100GE Port Properties—TX Lane*
- *40/100GE Port Properties–Preamble*
- *40/100GE Port Properties–Link Fault Signaling*
- *40/100GE Port Properties–Flow Control*
- *40/100GE Port Properties–Transmit Modes*

40/100GE Port Properties— General

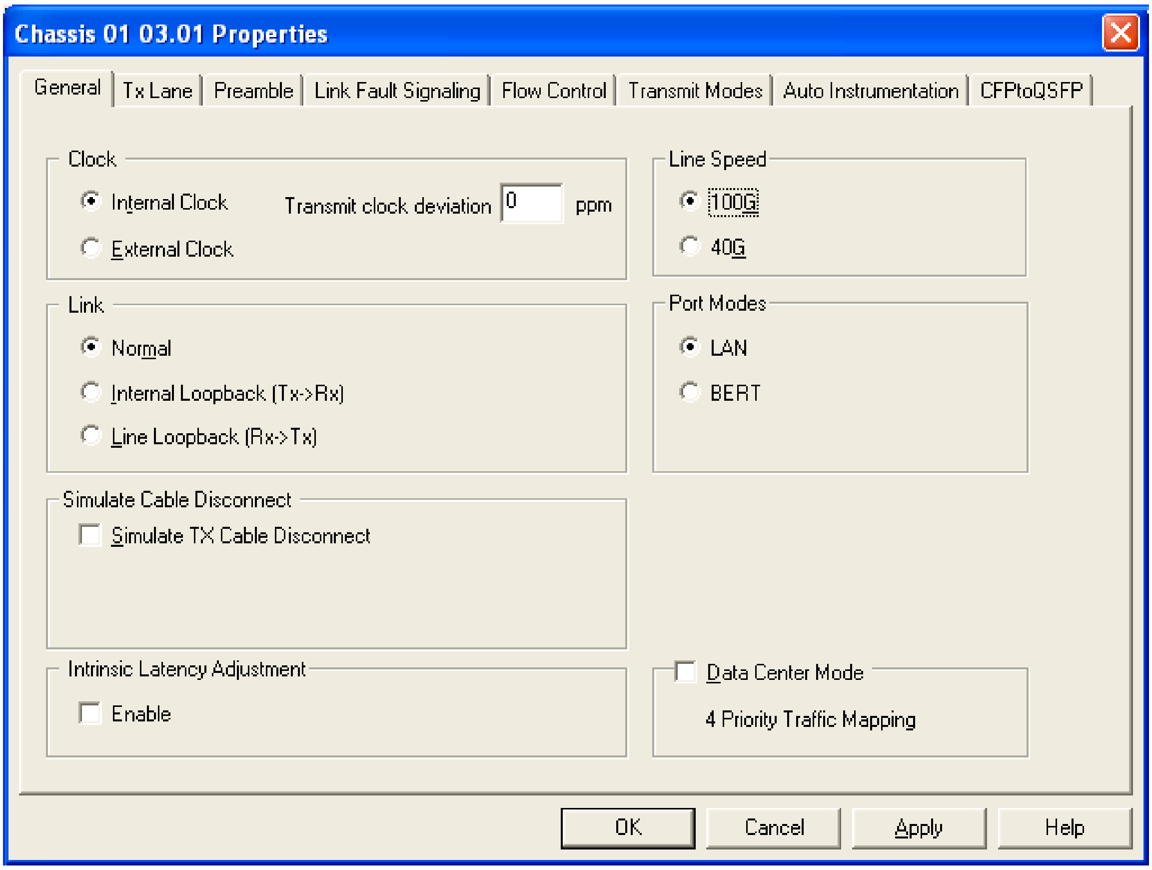
NOTE For Xcellon-Multis module, see *Xcellon-Multis Port Properties—General*.

For Novus module, see *Novus Port Properties—General.*

The **General** tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu options, then selecting the *General* tab.

The 40/100 GE Port Properties *General* tab is shown in the following figure:

Figure:40/100 GE–General Tab



The controls for the *General* tab configuration are described in the following table:

Table:40/100 GE General Tab Configuration

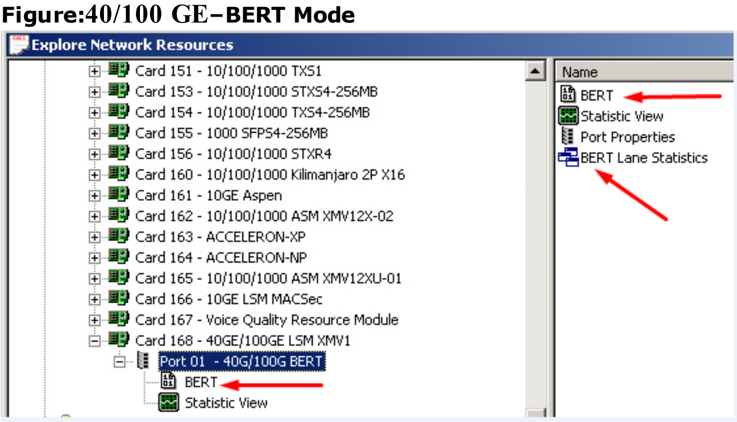
Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	External Clock	If selected, the timing for the SerDes reference clock comes from an external device connected to the Clock IN connector on the front panel of the module.
	Transmit Clock Deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port. 40/100 GE LSM cards can be adjusted from -100 to +100 ppm from the initial rate.
Link	Normal	Normal operation
	Internal Loopback (Tx -> Rx)	Enable/disable the Internal Loopback—Transmit to Receive.
	Line Loopback (Rx -> Tx)	Enable/disable the Line Loopback—Receive to Transmit.
Simulate Tx Cable		If selected, the port acts as if the cable has

Section	Control/Field	Usage
Disconnect		been disconnected.
Intrinsic Latency Adjustment	Enable	Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific transceiver. It is available if a value exists (in the .xml file). For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
	Latency Calibration	Click to run a Tcl script that measures intrinsic latency and stores the value in an .xml file. The button is only enabled for cards with transceivers that have not been pre-measured for intrinisic latency by Ixia. The button will be grayed-out or absent if any one of the following conditions are present: • there is no transceiver • the transceiver is CFP and a value is found for it in the list of pre-calibrated values.
Line Speed		Select 100G or 40G
Port Modes		Select LAN or BERT. If BERT is selected, all the Port Properties tabs except *General* will disappear.*BERT Mode*.
Data Center Mode		Frame Data for FCoE Support.

BERT Mode

If BERT is the selected Port Mode, the Port Properties dialog will have only the *General* tab. The tree view of port resources, on the left, and the detail view on the right now feature BERT and BERT Lane Statistics entries, as shown in the following figure:

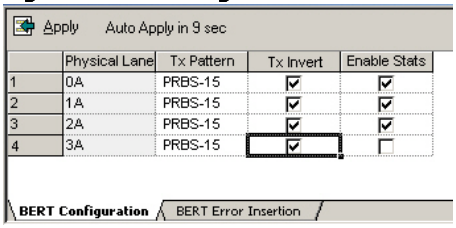
Figure:40/100 GE–BERT Mode



If the BERT entry is selected from either location above, a configuration and error insertion grid will display as shown in the following figure:

BERT Configuration

Figure:BERT Configuration



The fields in the *BERT Configuration* tab are described in the following table:

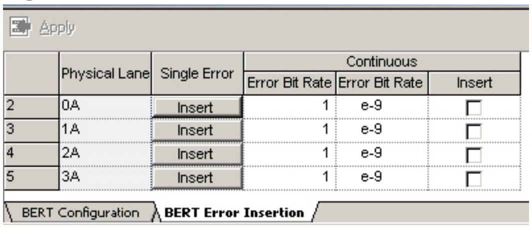
Table:BERT Configuration

Field/Control	Description
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
Tx Pattern	Select the pseudo-random data pattern to be transmitted. Choose one of: • All 1's • PRBS-31 • PRBS-23 • PRBS-20 • PRBS-15 • PRBS-11 • PRBS-9 • PRBS-7
Tx Invert	If enabled, the selected data transmission pattern is sent inverted.
Enable Stats	When selected, BERT Lane Statistics will be enabled.

BERT Error Insertion

The BERT error insertion grid is shown in the following figure:

Figure:BERT Error Insertion



The fields in the *BERT Error Insertion* tab are described in the following table:

Table:BERT Error Insertion

Section	Field/Control	Description
	Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
	Single Error (Insert)	When clicked, inserts one BERT error.

Section	Field/Control	Description
Continuous	Error Bit Rate - Integer	Enter the integer portion of the error bit rate value, which will be multiplied by the selected exponential value in the list. The valid range is 1 to 32.
	Error Bit Rate - Exponent	Select the exponential multiplier for the error bit rate value. One of: • e-2 (= 10^{-2}) • e-3 (= 10^{-3}) • e-4 (= 10^{-4}) • e-5 (= 10^{-5}) • e-6 (= 10^{-6}) • e-7 (= 10^{-7}) • e-8 (= 10^{-8}) • e-9 (= 10^{-9}) • e-10 (= 10^{-10}) • e-11 (= 10^{-11})
	Insert	check box–when selected, inserts errors con-tinuously.

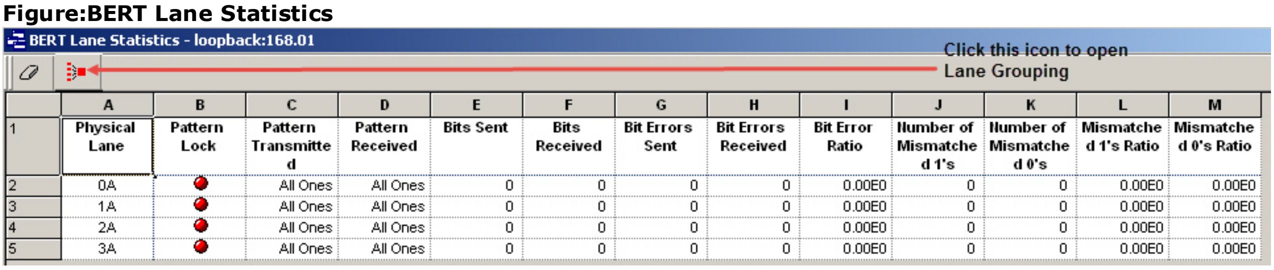
BERT Lane Statistics

If the BERT Lane Statistics entry is selected in the IxExplorer port detail window, a grid will display as shown in the following figure:

For HSE 100GE load module, FlexAP1040SQ - 40GE mode and FlexFE40QP, Lava load mod-ule Lava AP40/100GE 2P and Lava AP40/100GE 2RP load modules, you can view the fol-lowing:

- Statistics for the configured PCS lanes. For more information, *PCS Lane Statistics*.
- PCS lane error generation. For more information, *PCS Lane Error Generation*.

Figure:BERT Lane Statistics



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Physical Lane	Pattern Lock	Pattern Transmitted	Pattern Received	Bits Sent	Bits Received	Bit Errors Sent	Bit Errors Received	Bit Error Ratio	Number of Mismatched 1's	Number of Mismatched 0's	Mismatched 1's Ratio	Mismatched 0's Ratio
2	0A		All Ones	All Ones	0	0	0	0	0.00E0	0	0	0.00E0	0.00E0
3	1A		All Ones	All Ones	0	0	0	0	0.00E0	0	0	0.00E0	0.00E0
4	2A		All Ones	All Ones	0	0	0	0	0.00E0	0	0	0.00E0	0.00E0
5	3A		All Ones	All Ones	0	0	0	0	0.00E0	0	0	0.00E0	0.00E0

The fields (columns) of statistics are described in the following table:

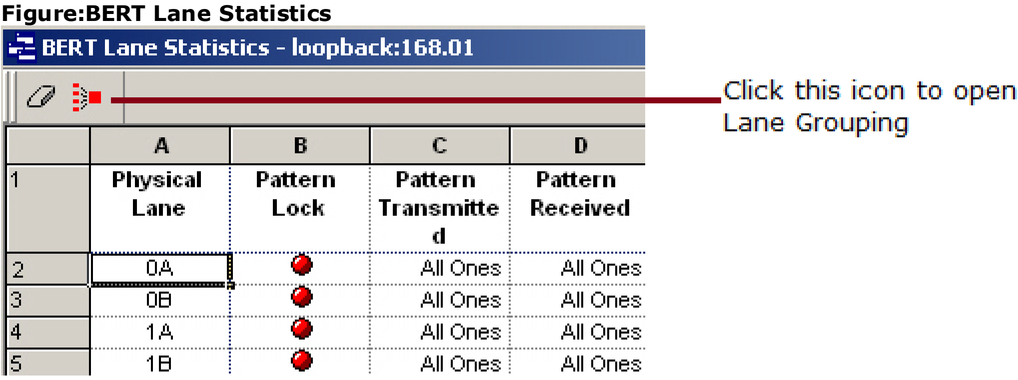
Table:BERT Lane Statistics

Field/Control	Description
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
Pattern Lock	Indicates whether the receive side is locked to a particular pattern. Green indicates success; red indicates failure.
Pattern Transmitted	The pseudo-random data pattern that was transmitted.
Pattern Received	The pseudo-random data pattern that was received.
Bits Sent	The total number of bits sent.
Bits Received	The total number of bits received.
Bit Errors Sent	The total number of bit errors sent.
Bit Errors Received	The total number of bit errors received.
Bit Error Ratio	(BER) the ratio of the number of errored bits compared to the total number of bits transmitted. In the following format: 0.00E0.
Number of Mismatched 1's	The number of expected ones received as zeroes.
Number of Mismatched 0's	The number of expected zeroes received as ones.
Mismatched 1's Ratio	The ratio of the number of expected ones received as zeroes to all bits. In the following format: 0.00E0.
Mismatched 0's Ratio	The ratio of the number of expected zeroes received as ones to all bits. In the following format: 0.00E0.

Lane Stats Grouping

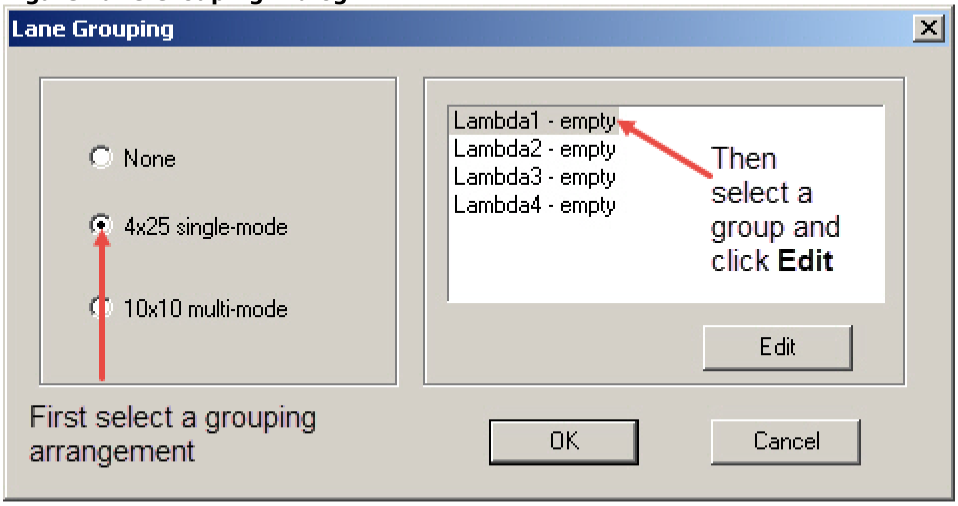
Lane stat grouping aggregates the stats from multiple lanes into a new stat. Click the icon (upper left corner) in the grid (shown in the following figure) to open the Lane Grouping dialog box.

Figure:BERT Lane Statistics



The Lane Grouping dialog will open, as shown in the following figure:

Figure:Lane Grouping Dialog

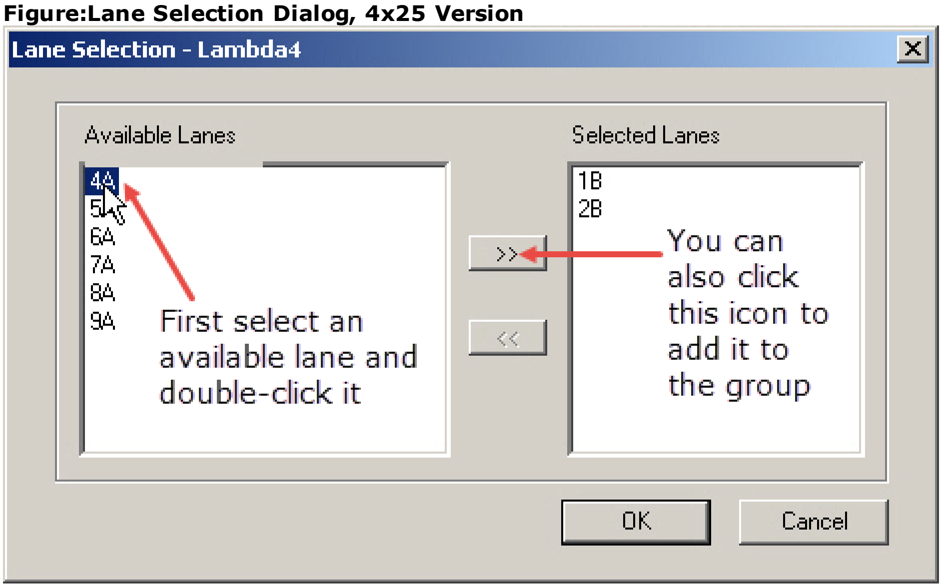


- Select a grouping approach:
  - 4x25 single-mode (4 groups of 5 lanes)-user-selectable lanes, or
  - 10x10 (10 groups of 2 lanes) multi-mode grouping-fixed configuration (0A+0B, 1A+1B, and so on).

In the example above, 4x25 has been selected. The four groups on the right are currently empty. (If 10x10 had been selected, there would be no need for the next step, since the configuration is not user-selectable.)

- Then select a group (such as Lambda1) and click **Edit**. The Lane Selection dialog box opens as shown in the following figure, for configuring the selected group.

Figure:Lane Selection Dialog, 4x25 Version

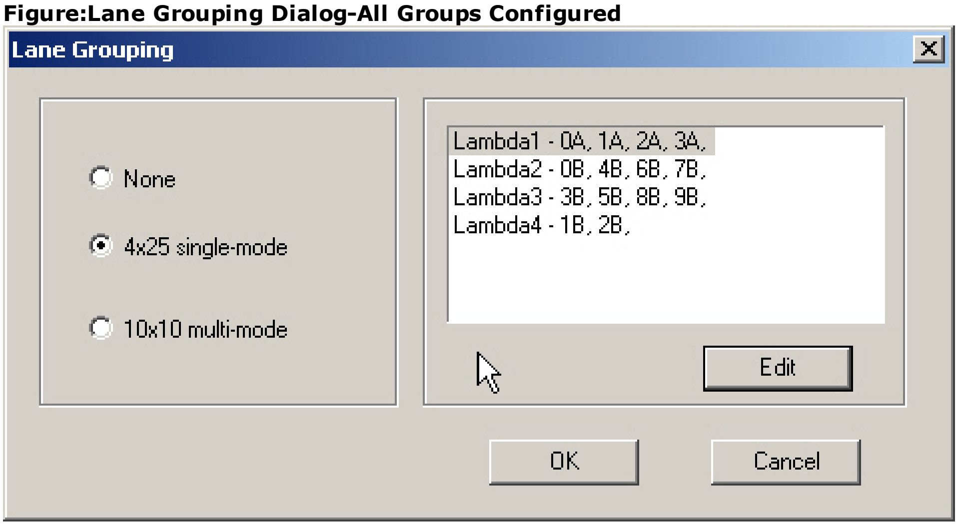


The left panel lists available lanes, and the right panel lists lanes you have selected to assign to the group (in this example, Lambda4).

- Select an available lane (or lanes) then click >> to add to the group. You can also double-click an available lane to add it to the group.

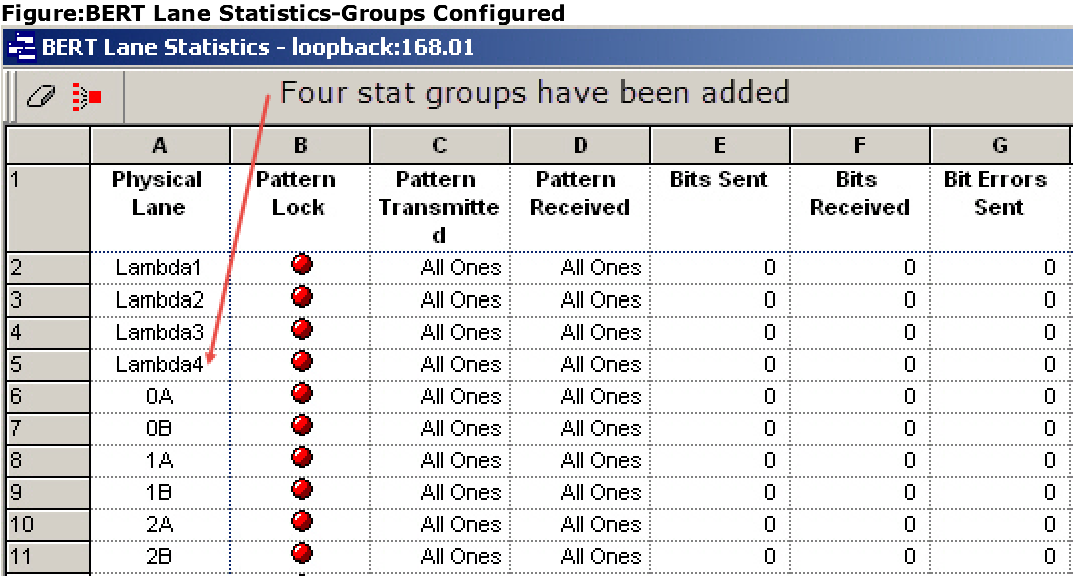
- To delete a lane from the group, select it and click <<.
- When finished selecting lanes for the group, click **OK**. The Lane Grouping dialog will display again, as shown in the following figure:

Figure:Lane Grouping Dialog-All Groups Configured



When all groups have been configured, click **OK** to close the dialog and save your changes. The BERT Lane Statistics grid will display your changes, as shown in the following figure:

Figure:BERT Lane Statistics-Groups Configured



	A	B	C	D	E	F	G
1	Physical Lane	Pattern Lock	Pattern Transmitted	Pattern Received	Bits Sent	Bits Received	Bit Errors Sent
2	Lambda1		All Ones	All Ones	0	0	0
3	Lambda2		All Ones	All Ones	0	0	0
4	Lambda3		All Ones	All Ones	0	0	0
5	Lambda4		All Ones	All Ones	0	0	0
6	0A		All Ones	All Ones	0	0	0
7	0B		All Ones	All Ones	0	0	0
8	1A		All Ones	All Ones	0	0	0
9	1B		All Ones	All Ones	0	0	0
10	2A		All Ones	All Ones	0	0	0
11	2B		All Ones	All Ones	0	0	0

40/100GE Port Properties—TX Lane

NOTE For Xcellon-Multis module, see *Xcellon-Multis Port Properties—TX-Lane*.

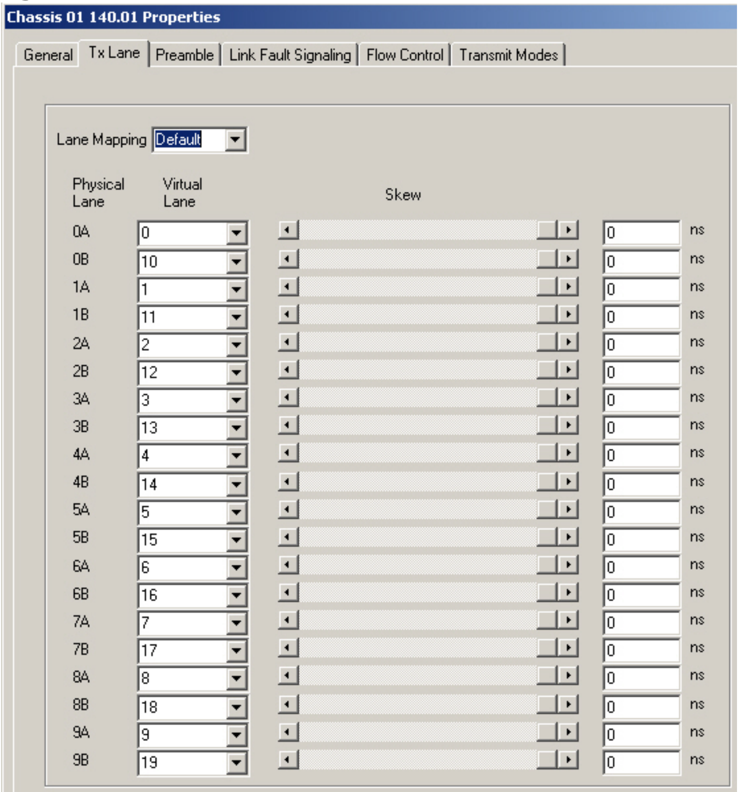
For Novus module, see *Novus Port Properties—TX-Lane.*

The *Tx Lane* tab allows to control the PCS lane order and skew rate for each lane.

For more information on Lane Skewing, see the Lane Skew topic in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*. The Lane Skew topic is located under 'Types of Ports' / '10GE'.

The 40/100 GE Port Properties *Tx Lane* tab is shown in the following figure:

Figure:40/100 GE–Tx Lane Tab



The controls for the *Tx Lane* tab configuration are described in the following table:

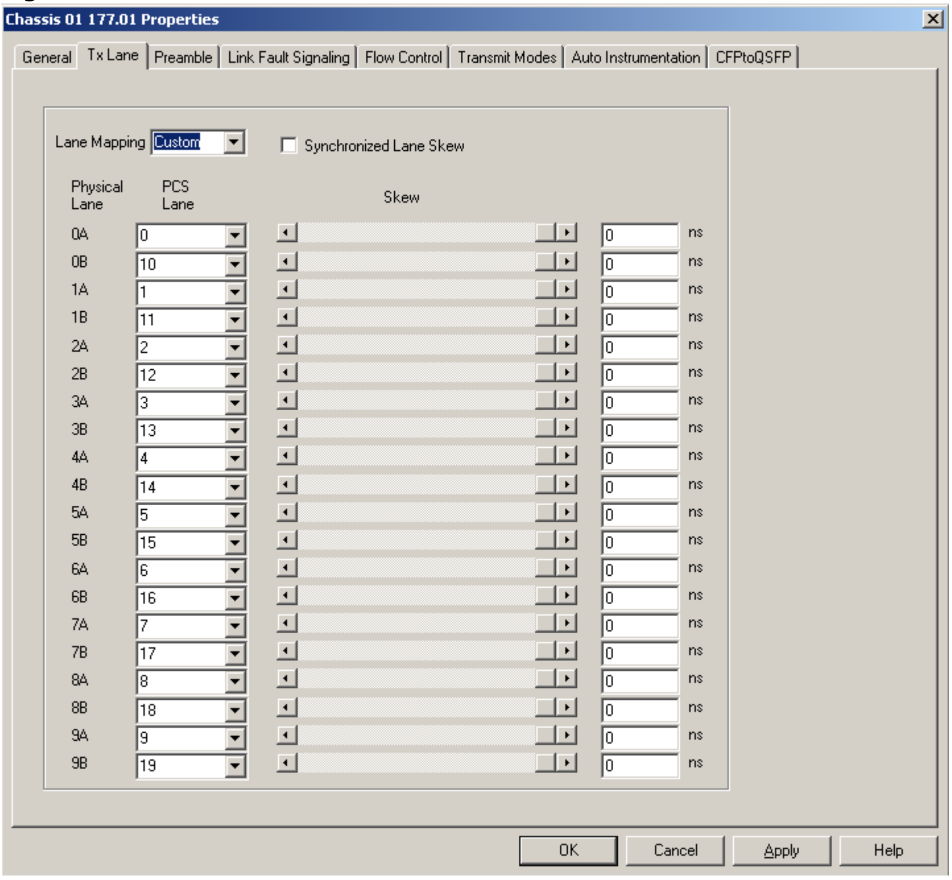
Table:Tx Lane Tab Configuration, 40/100 GE

Field	Description
Lane Mapping	Allows you to select a PCS lane ordering method. There are four options: • Default–the default ordering method. The default order is each physical port corresponds to 2 PCS lanes that are n and n+10, where n = physical lane number. • Increment–orders the lanes from 0 to 19, straight down the list. • Decrement–orders the lanes from 19 to 0, straight down the list. • Custom–allows to put the lanes in any order by manually entering the numbers in the fields. The starting order is the last selected mapping.
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
PCS Lane	A number identifier for the PCS lane. The PCS lane is paired with a corresponding physical lane.
Skew	The skew slider is used to set a skew value for the PCS lane, in nanoseconds, on the transmit side. Lane Skew is the ability to independently delay one or more of the 20 PCS lanes. When the slider is moved, the nanoseconds field is correspondingly

Field	Description
	adjusted. You can also enter a nano second value directly into this field. When the slider is fully pushed to the right, the skew injected into the transmit stream is 0 (minimum). When the slider is pushed all the way to the left. the skew injected into the transmit stream is 3 uS (maximum).

The HSE 100GE Port Properties-TX Lane is shown in the following figure:

Figure:HSE 100GE–Tx Lane Tab



The controls for the *Tx Lane* tab configuration for HSE 100GE load module are described in the following table:

Table:Tx Lane Tab Configuration, HSE 100GE

Field	Description
Lane Mapping	Allows to select a PCS lane ordering method. There are five options: • Default–the default ordering method. The default order is each physical port corresponds to 2 PCS lanes that are n and n+10, where n = physical lane number. • Increment–orders the lanes from 0 to 19, straight down the list. • Decrement–orders the lanes from 19 to 0, straight down the

Field	Description
	list. • Custom–allows to put the lanes in any order by manually entering the numbers in the fields. The starting order is the last selected mapping. • Random–PCS lanes are randomly mapped.
Synchronized Lane Skew	If selected, enables to synchronize the skewing or delaying of one or more PCS lanes.
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
PCS Lane	A number identifier for the PCS lane. The PCS lane is paired with a corresponding physical lane.
Skew	The skew slider is used to set a skew value for the PCS lane, in nanoseconds, on the transmit side. Lane Skew is the ability to independently delay one or more of the 20 PCS lanes. When the slider is moved, the nanoseconds field is correspondingly adjusted. You can also enter a nano second value directly into this field. When the slider is fully pushed to the right, the skew injected into the transmit stream is 0 (minimum). When the slider is pushed all the way to the left. the skew injected into the transmit stream is 3 uS (maximum).

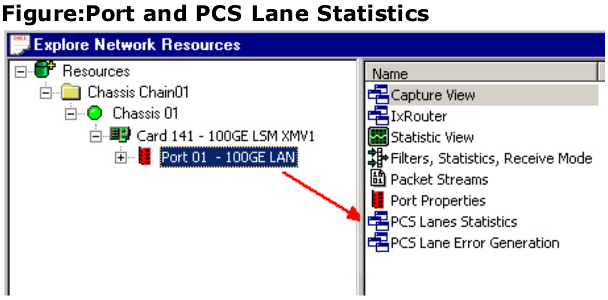
PCS Lane Statistics

The PCS Lane Statistics table allows you to view the statistics for the configured PCS lanes. It is part of the Port Properties for the module.

To open the PCS Lane Statistics table:

1. Select the HSE 100GE load module, 40 or 100GE LSM XMV1, FlexAP1040SQ - 40GE mode or FlexFE40QP, Lava Load module Lava AP40/100GE 2Pand Lava AP40/100GE 2RP module in the left pane of the IxExplorer window.
2. Expand the node, and select the Port object. In the right window pane, double-click the PCS Lane Statistics object as shown in the following figure:

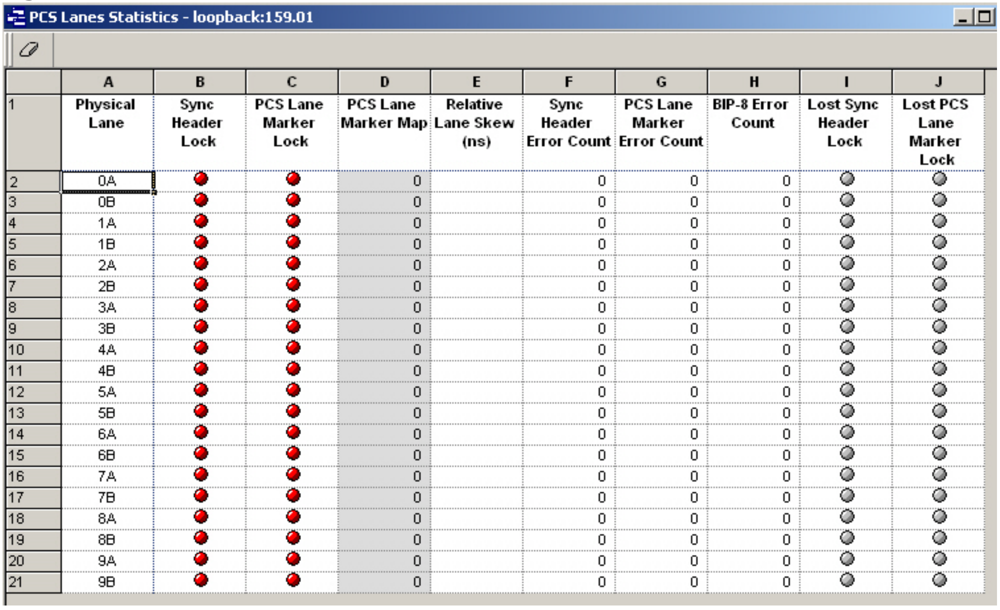
Figure:Port and PCS Lane Statistics



3. The PCS Lane Statistics table opens. Use this table to view the PCS lane statistics for each lane. The statistics are for the **receive** side.

The PCS Lane Statistics table is shown in the following figure:

Figure:PCS Lane Statistics



PCS Lanes Statistics - loopback:159.01

	A	B	C	D	E	F	G	H	I	J
1	Physical Lane	Sync Header Lock	PCS Lane Marker Lock	PCS Lane Marker Map	Relative Lane Skew (ns)	Sync Header Error Count	PCS Lane Marker Error Count	BIP-8 Error Count	Lost Sync Header Lock	Lost PCS Lane Marker Lock
2	0A			0		0	0	0		
3	0B			0		0	0	0		
4	1A			0		0	0	0		
5	1B			0		0	0	0		
6	2A			0		0	0	0		
7	2B			0		0	0	0		
8	3A			0		0	0	0		
9	3B			0		0	0	0		
10	4A			0		0	0	0		
11	4B			0		0	0	0		
12	5A			0		0	0	0		
13	5B			0		0	0	0		
14	6A			0		0	0	0		
15	6B			0		0	0	0		
16	7A			0		0	0	0		
17	7B			0		0	0	0		
18	8A			0		0	0	0		
19	8B			0		0	0	0		
20	9A			0		0	0	0		
21	9B			0		0	0	0		

The following table explains the entries in the PCS Lane Statistics table:

Table:PCS Lane Statistics Data

Field	Description
Physical Lane	The identifier for the Receive physical lane. This is a tag / fixed label to ID each lane.
Sync Header Lock	Indicates if the received PCS lane achieved sync-bit lock. Green indicates success, red indicates failure.
PCS Lane Marker Lock	Indicates if the received PCS lane has achieved alignment marker lock. Green indicates success, red indicates failure.
PCS Lane Marker Map	The VL number identified by the alignment marker. This is only valid when VL Lock is green.
Relative Lane Skew (ns)	Shows the actual skew in nanoseconds. Skew measurements are valid only when all lanes are locked with 20 unique lane markers. The first VL markers to arrive have skew of 0. All other lane skews are relative to them.
Sync Header Error Count	The number of synchronization bit errors received.
PCS Lane Marker Error Count	The number of incorrect PCS lane markers received while in PCS lane lock state.
BIP-8 Error Count	The number of BIP-8 errors for a PCS lane. BIP-8 = Bit-Interleaved Parity with eight bit errors (BIP-8). Each bit in the BIP field is an even parity calculation over all previous selected bits of a PCS lane.
Lost Sync Header Lock	When lit, indicates the loss of sync header lock since the last statistic was read. If colored gray, there is no error. If colored red, an

Field	Description
	error has occurred.
Lost PCS Lane Marker Lock	When lit, indicates the loss of PCS lane marker lock since the last statistic was read. If colored gray, there is no error. If colored red, an error has occurred.

PCS Lane Error Generation

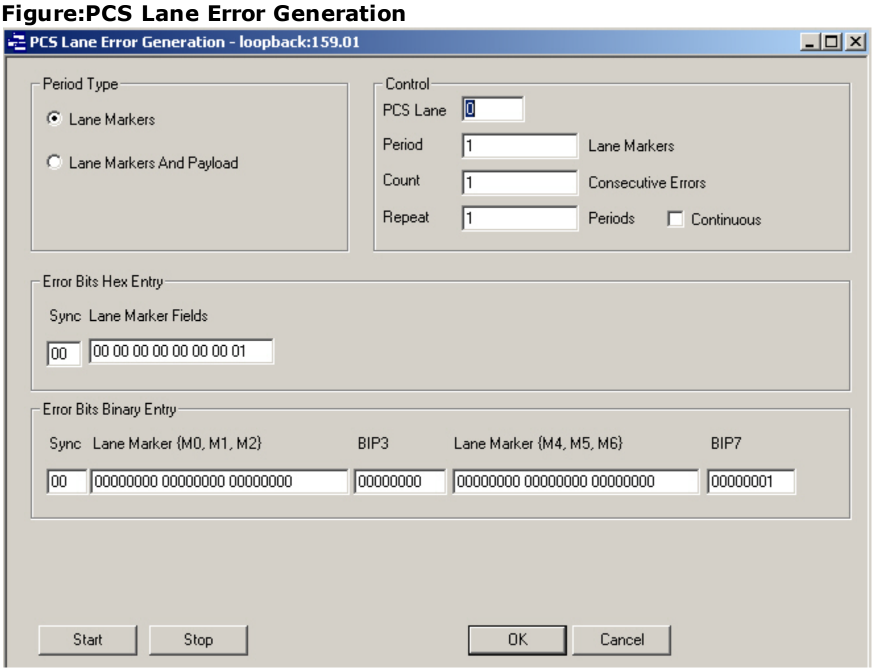
The HSE 100GE load module, Lava load module and other 40/100 GE load modules can generate errors in the BIP-8 field, or anywhere in the 40/100 GE lane markers or in the payload.

PCS Lane (virtual lane) selection is 0-19 for 100G and 0-3 for 40G.

Errors can be inserted either in only the Lane Marker fields or in both Lane Markers and Payload. The Period Type makes this choice and the Error Bits Binary Entry units change based on the selected period type, either Lane Markers or 64/66 Bit Words.

Starting and stopping errors is independent of stream transmit. Errors can be inserted when transmit is idle or active.

Figure:PCS Lane Error Generation



The following table describes the fields of the **PCS Lane Error Generation** dialog:

Table:PCS Lane Error Generation

Section	Field	Description
Period Type	Lane Markers	Insert errors only in the Lane Marker fields.
	Lane Markers and Payload	Insert errors in both Lane Markers and Payload fields.
Control	PCS Lane	Specify which lane to insert errors. 0-19 for 100G and 0-3 for 40G

Section	Field	Description
	Period	(Number) Lane Markers or 64/66 Bit Words (depending on Period Type) Define the period by the number of consecutive Lane Markers or 64/66 Bit Words.
	Count	(Number) Consecutive Errors Define the number of consecutive Lane Markers or 64/66 Bit Words containing defined errors.
	Repeat	(Number) Periods Define the number of periods to repeat the error pattern.
		Continuous (check box)–if selected, the Repeat __ Periods field is disabled, and errors are inserted continuously.
Error Bits Hex Entry	Sync / Lane Marker Fields (or) Lane Markers and Payloads	Defines which bits to error, in hex format.
Error Bits Binary Entry		Defines which bits to error, in binary format. Depending on the selected Period Type, the Error Bits Binary Entry units change, either Lane Markers or 64/66 Bit Words.
	If Lane Markers is selected as Period Type	Sync Lane Marker (M0, M1, M2) BIP 3 Lane Marker (M4, M5, M6) BIP 7
	If Lane Markers and Payload is selected as Period Type	Sync Byte 0 through Byte 7

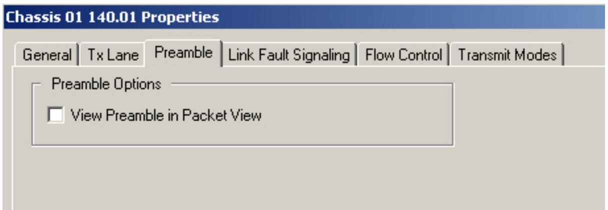
40/100GE Port Properties–Preamble

NOTE For Xcellon-Multis module, see *Xcellon-Multis Port Properties—Preamble*.

For Novus module, see *Novus Port Properties—Preamble.*

The 40/100GE *Preamble* tab allows to choose to view the preamble in Packet View. The Preamble tab for a 100GE LSM XMV LAN module is shown in the following figure:

Figure:100GE LSM XMV LAN Port Properties—Preamble



The fields and controls in this tab are described in the following table:

Table:100GE LSM XMV LAN Port Properties—Preamble

Section	Choices	Description
Preamble Options	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side).

40/100GE Port Properties–Link Fault Signaling

Link Fault Signaling is a simple method to indicate certain types of faults between Ethernet stations. The Reconciliation Sublayer (RS) controls whether the MAC is allowed to transmit. In the typical scenario, the RS that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

In the 40/100GE configuration, then you can select the option to have the transmitting RS ignore link faults from the receiving RS.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab. The 100GE *Link Fault Signaling* tab is shown in the following figure:

Figure:40/100 GE Link Fault Signaling

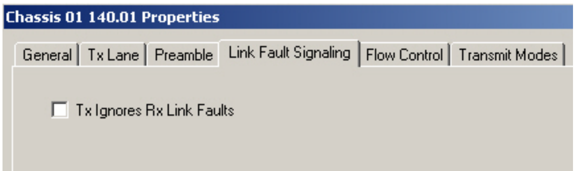


Table:40/100 GE Link Fault Signaling Tab

Field/Control	Description
Tx Ignores Rx Link Faults	If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.

40/100GE Port Properties–Flow Control

When a port is receiving data at a faster rate than it can handle from another, directly connected port, the receiving port can send a MAC control PAUSE frame to the sending port to temporarily halt transmission of frames. The PAUSE function is defined in IEEE 802.3.

The *Flow Control* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The *Flow Control* tab is shown in the following figure:

Figure:40/100 GE (non Data Center mode)Port Properties—Flow Control

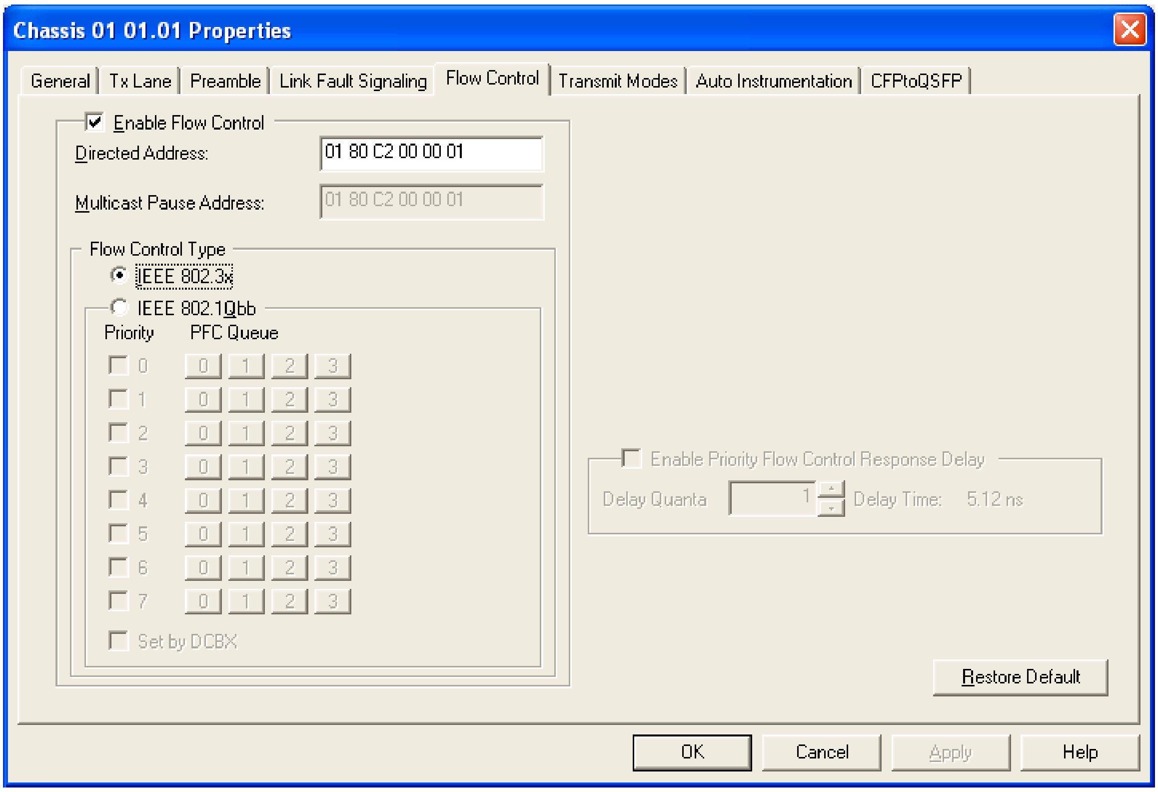
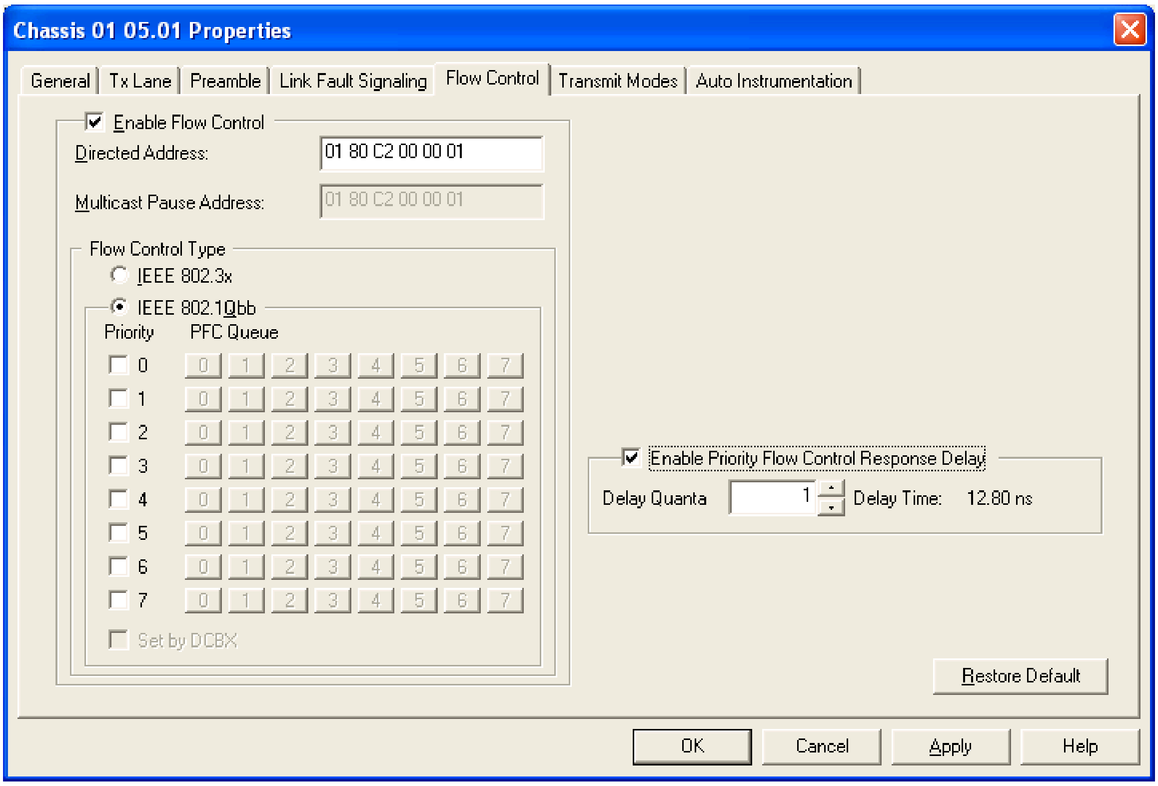


Figure:40/100 GE (in Data Center mode)Port Properties—Flow Control



The fields and controls in this tab are described in the following table:

Section	Field/Control	Description
Enable Flow Control	(check box)	Enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type	IEEE 802.3x or IEEE 802.1Qbb	Priority-based Flow Control. When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
	Priority	Priority-based Flow Control.
	PFC Queue	Priority-based Flow Control.
Enable Priority Flow Control Response Delay	(check box)	If selected, enables to increase the number of frames that is sent when a pause frame is received. Priority Flow Control (PFC) pause allows to set the delay of flow control. When a pause frame is

Section	Field/Control	Description
		received for a certain priority, a count of the number of timestamp ticks increments up to a desired offset and then releases the pause request to the TX engine. For example, if running at 100% line rate and there is no delay in the pause request, the TX pipeline transmits the specified number of frames once the pause request is received. With this feature, a delay by number of timestamp ticks is programmed.
	Delay Quanta	This field allows to set the delay quanta of flow control.
	Delay Time	The delay time, in nanoseconds, of frames.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

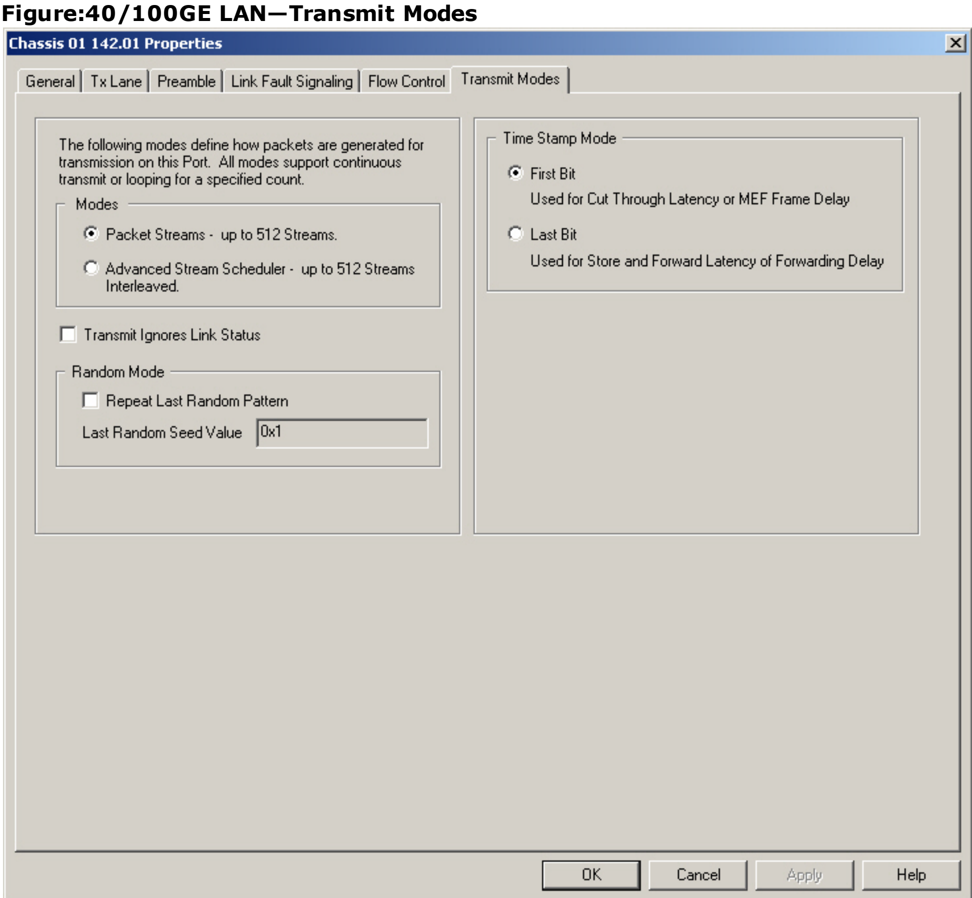
40/100GE Port Properties–Transmit Modes

NOTE For Xcellon-Multis module, *Xcellon-Multis Port Properties—Transmit Modes*.

For Novus module, see *Novus Port Properties—Transmit Modes.*

The *Transmit Modes* tab for 40/100GE LAN load modules is shown in the following figure. It is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the *Properties* menu option. Then select the *Transmit Modes* tab.

Figure:40/100GE LAN—Transmit Modes



The fields and controls for this tab are described in the following table:

Table:100GE LSM XMV LAN Configuration

Section	Field/Control	Description
Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure up to 512 streams which become active sequentially. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets the operating mode for the port to interleaved packet streams. This allows to configure up to 512 streams which are concurrently active. They will transmit packets in an interleaved fashion. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Time Stamp Mode	First Bit	(Default) When selected, used for Cut-Through Latency or MEF Frame Delay The time stamp inserted in the transmitted packet will be the time of the first bit out, for that packet.
	Last Bit	When selected, used for Store and Forward Latency of Forwarding Delay. The time stamp inserted in the transmitted packet will be the time of the last bit out, for that packet.

[This page intentionally left blank]

Chapter 22 - Port Properties–NGY Family

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the NGY LSM10GXM module family port properties.

Port Properties for NGY Modules

The *Port Properties* dialog is accessed by right-clicking a port in the Resources window, then selecting the *Properties* menu option.

The complete specification for the LSM10GXM type boards can be found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for NGY modules (LSM10GXM family):

- *NGY Port Properties—General*
- *NGY Port Properties–Operation Mode*
- *NGY Port Properties–Preamble*
- *NGY Port Properties–Link Fault Signaling*
- *NGY Port Properties–Flow Control*
- *NGY Port Properties–Transmit Modes*
- *NGY Port Properties–XFP*
- *NGY Port Properties–SFP*
- *NGY Port Properties–Auto Instrumentation*
- *NGY Port Properties–OAM*
- *NGY 10GBASE-T Port Properties–LASI*

NGY Port Properties—General

The *General* tab is accessed by right-clicking a port in the Resources pane, selecting the *Properties* menu options, then selecting the *General* tab.

The NGY Port Properties *General* tab is shown in *Figure: NGY—General tab: LAN Mode*. The 10GBASE-T version of NGY is shown in *Figure:NGY–General Tab: 10GBASE-T Version*

NOTE For the NGY LSM10GXM load modules, the General tab Clock area is disabled. Clocking is configured in the Card Properties dialog for these modules. See *NGY LSM10GXM 2, 4 and 8-port Modules*.

Figure:NGY—General tab: LAN Mode

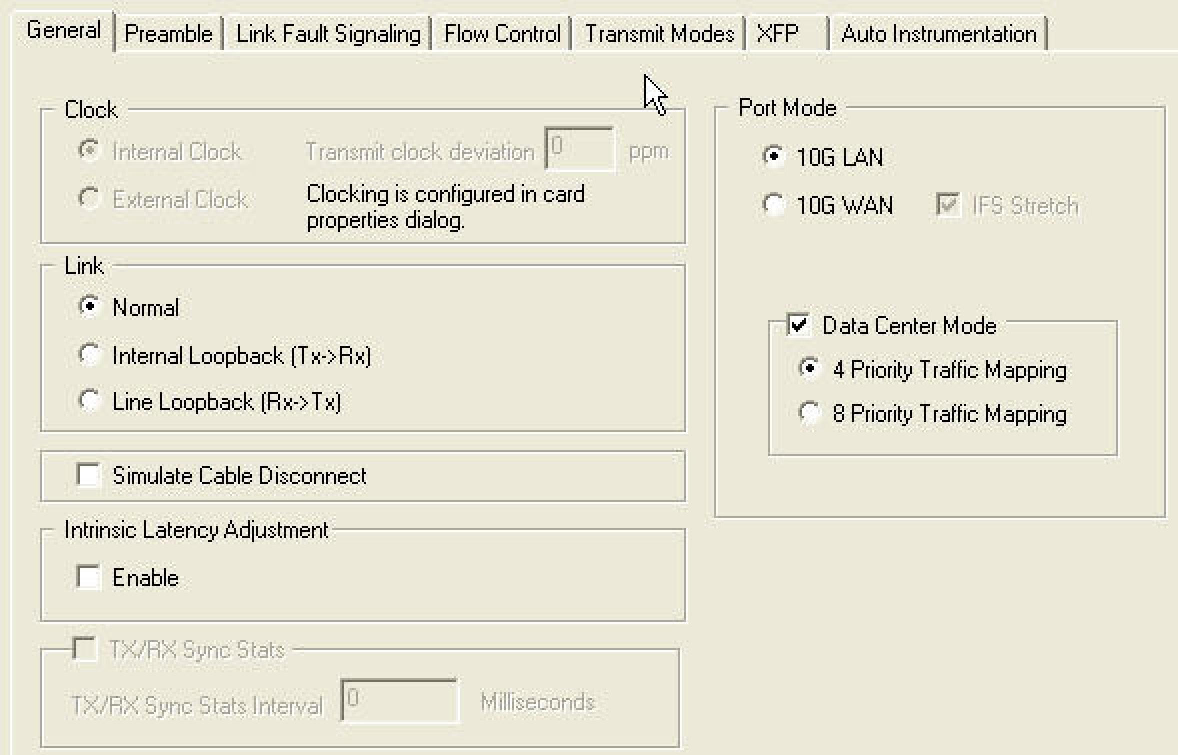


Figure:NGY–General Tab: 10GBASE-T Version

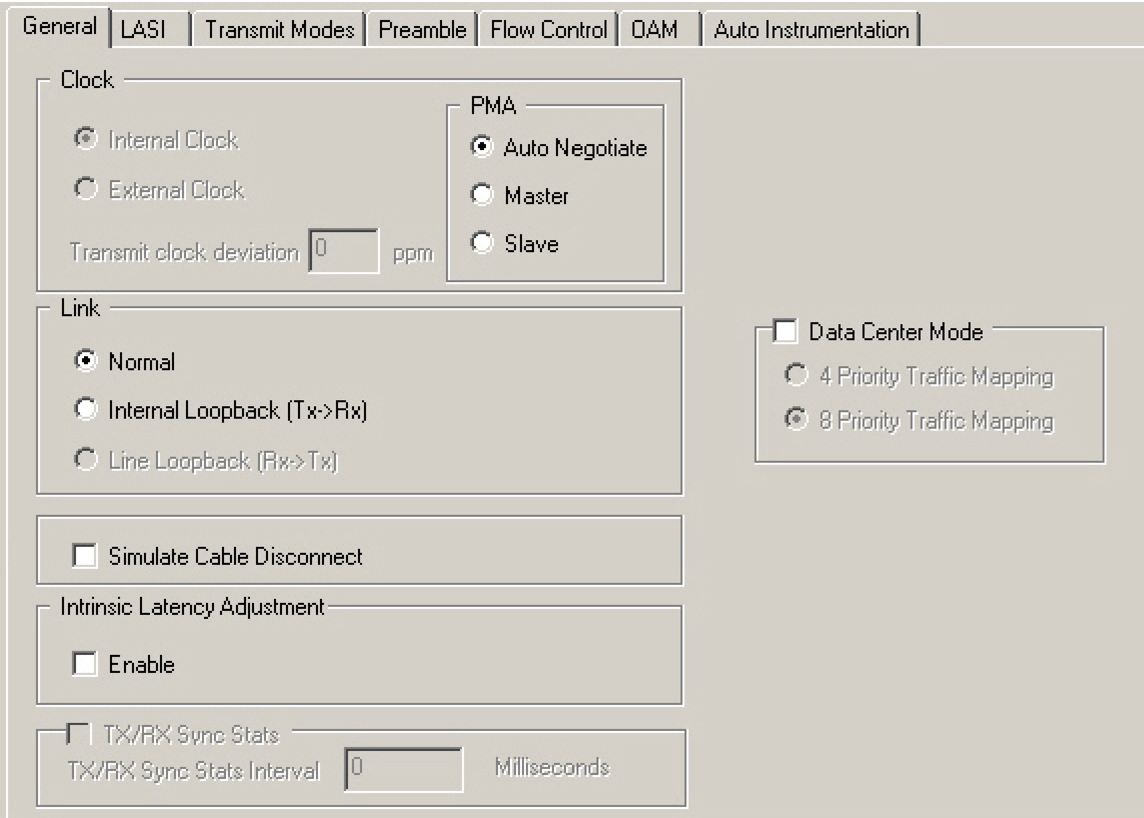
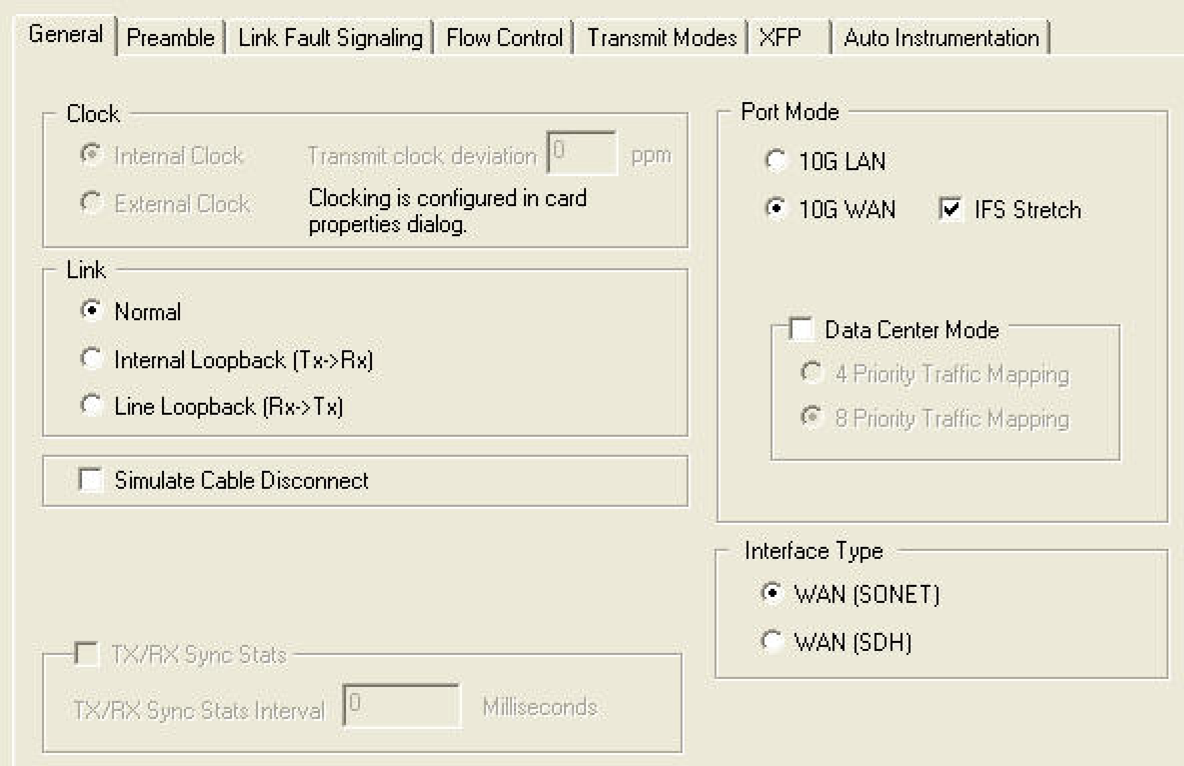


Figure:NGY–General Tab: WAN Version



The controls for the *General* tab configuration are described in *Table:NGY General Tab Configuration*.

Table:NGY General Tab Configuration

Section	Control/Field	Usage
Clock		NOTE For the NGY LSM10GXM modules, the Clock area is disabled. Clocking is configured in the Card Properties dialog for these modules. See *NGY LSM10GXM 2, 4 and 8-port Modules*.
Link	Normal	Normal operation of the card.
	Internal Loopback (Tx -> Rx)	Check this box to enable/turn on the Internal Loopback–Transmit to Receive.
	Line Loopback (Rx -> Tx)	Check this box to enable/turn on the Line Loopback–Receive to Transmit.
Port Mode	10G LAN	Sets the port to 10GE LAN mode
	10G WAN	Sets the port to 10GE WAN mode When set to WAN mode, IFS Stretch becomes selectable. NOTE the OAM tab will not be present in Port Properties when WAN mode is selected.
	IFS Stretch	(WAN mode only) check box to enable WAN

Section	Control/Field	Usage
		Interframe Spacing Stretch. Using this method, the frame rate is slightly lowered by adding additional IPG. In Packet Streams or Advanced Streams view with IFS Stretch mode enabled, the Line Rate will be 9,286 Mbps instead of 9,294 Mbps. And in Statistic View, the Line Speed will be characterized as 10GE WAN with IFSS. For details, see *IFS Stretch* in Chapter 18 of the *Ixia Hardware & Reference Manual*.
PMA	Auto Negotiate	(10GBASE-T Version only) If selected, determining which port is Master or Slave is performed **automatically**. (Checking this box will disable the manual option for selecting Master or Slave.
	Master	If selected, port will be configured as Master.
	Slave	If selected, port will be configured as Slave.
Data Center Mode		Frame Data for FCoE Support.
Interface Type	WAN (SONET)	WAN mode only. Selects the SONET interface type.
	WAN (SDH)	WAN mode only. Selects the SDH interface type.
Simulate Cable Dis-connect		If this is selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	LAN mode only. Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific trans-ceiver. It is available if a value exists (in the .xml file). For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*. NOTE NGY LSM10GXM modules do not sup-port Latency Calibration, although they do support Latency Adjustment.

NGY Port Properties–Operation Mode

For NGY-NP load modules (only), the Port Operation Mode tab allows selection of Stream/Capture/Latency mode (the default), TSO/LRO (Transmit Segmentation Off-load/Large Receive Offload) mode, or L7 Mode as shown in *Figure:Operation Mode Selec-tion in Port Properties (NGY-NP)*. The L7 Mode is reserved for use in the IxLoad application, where it is the default setting.

Figure:Operation Mode Selection in Port Properties (NGY-NP)

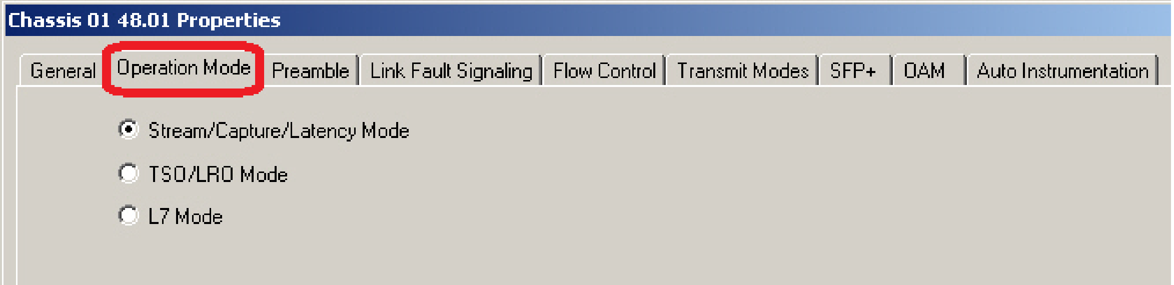
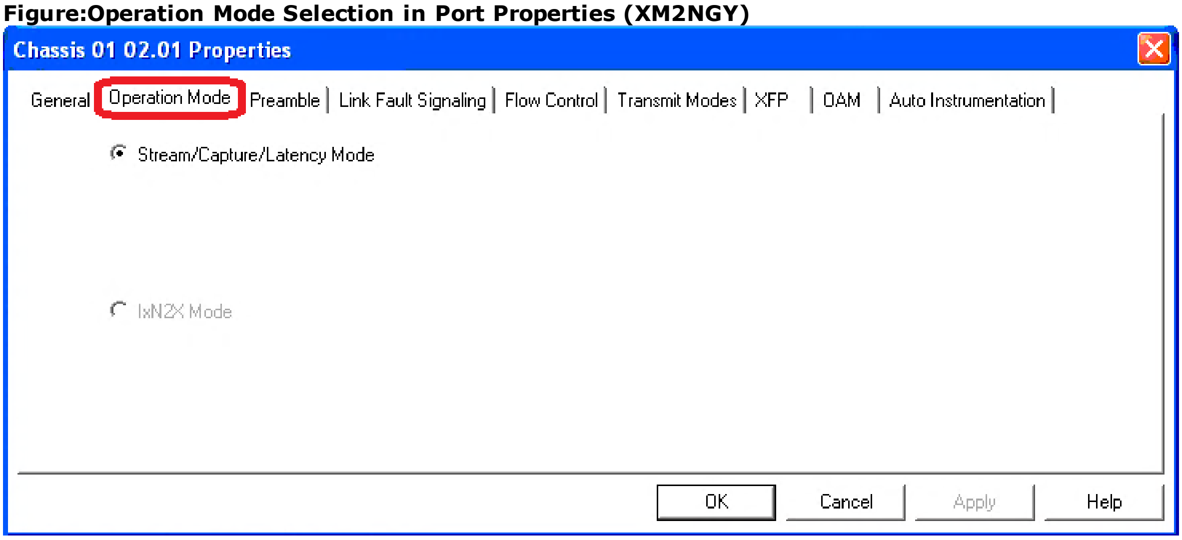


Figure:Operation Mode Selection in Port Properties (XM2NGY)



NOTE For fusion enabled NGY load modules (10GLSMXM2NG, 10GLSMXM4NG and 10GLSMXM8NG), the Port Operation Mode tab shows the selection of Stream/Capture/Latency mode (the default) or IxN2X Mode as shown in the above figure. The IxN2X Mode is reserved for use in the IxN2X application, where it is the default setting. The current operation mode is shown for reference and cannot be changed from IxExplorer.

Stream/Capture/Latency Mode

If Stream/Capture/Latency Mode (the default) is selected, then the other Port Properties tabs will appear as listed below:

- *Transmit Modes*, same as that illustrated in *NGY Port Properties–Transmit Modes*
- *Flow Control*, same as that described in *NGY Port Properties–Flow Control*.
- *General* tab, same as that illustrated in *NGY Port Properties—General*.
- *Auto Instrumentation*, same as that described in *NGY Port Properties–Auto Instrumentation*
- *OAM*, same as that illustrated in *NGY Port Properties–OAM*.

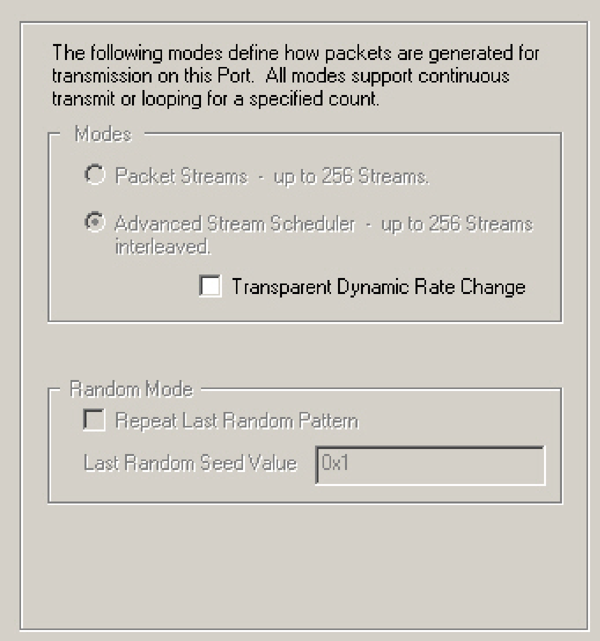
TSO/LRO Mode

When TSO/LRO Mode is selected, IxOS downloads a different FPGA and restarts the CPU. If TSO/LRO Mode is selected, then the Transmit Modes tab will change as shown below.

Transit Mode Tab in TSO/LRO Mode

The *Transmit Modes* tab for the NGY modules in TSO/LRO port operation mode is shown in *Figure:Transmit Modes tab in TSO/LRO Mode*. The only option is *Transparent Dynamic Rate Change*.

Figure:Transmit Modes tab in TSO/LRO Mode



L7 Mode

L7 Operation mode is intended for use only in the IxLoad application, where it is the default selection. When in L7 mode, the following changes occur on other tabs of Port Properties:

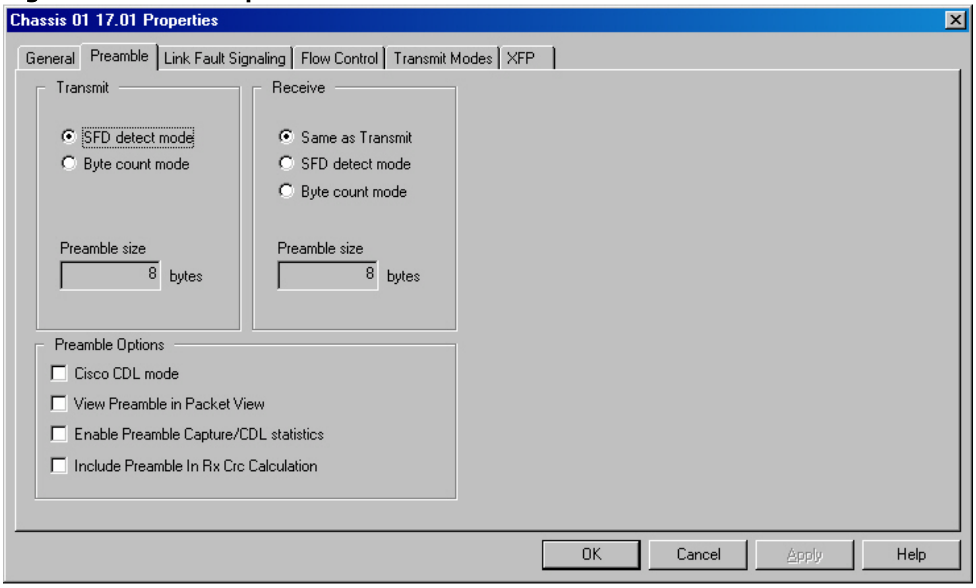
- General tab–there is no Port Mode 10G LAN or 10G WAN, and no Intrinsic Latency Adjustment.
- Preamble tab–the options Cisco CDL Mode and View Preamble in Packet View are both unavailable.
- Transmit Modes tab–only Packet Streams is available.

NGY Port Properties–Preamble

The NGY *Preamble* tab allows to select the method for detecting the start of a frame. The preamble precedes the frame, but is not part of the frame itself, so a method must be used to determine the first of the bytes making up the frame itself —SFD detect mode or Byte count mode. The Preamble page for a 10GE XAUI module is shown in *Figure:NGY Port Properties—Preamble*.

The choice in this tab for transmitted frames is reflected in the *Frame Data* tab in the *Stream Properties* dialog. The number of configurable bytes in the preamble depends on the start-of-frame mode.Preamble Size Box for additional information.

Figure:NGY Port Properties—Preamble



The fields and controls in this tab are described in *Table:NGY Port Properties—Preamble*.

Table:NGY Port Properties—Preamble

Section	Choices	Description
Transmit	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case), and considers the next byte (9th) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the *Frame Data* tab in the *Stream Properties* dialog. This value is currently fixed at 8 bytes (the default).
Receive	Same as Transmit	The Receive side will accept the same choices/entries that were made for the Transmit side.
	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case) and considers the next byte (9th byte) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the

Section	Choices	Description
		Frame Data tab in the *Stream Properties* dialog. This value is currently fixed at 8 bytes (the default).
Preamble Options	Cisco CDL Mode	Enables the use of Cisco's Converged Data Link (CDL) packets, which substitutes the six preamble bytes and the SFD byte with a specific seven byte CDL header (does not apply to UNIPHY modules in 10GE LAN Mode). Selecting this disables the Transmit SFD detect mode.
	Preamble View Mode	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side) (does not apply to UNIPHY modules in 10GE LAN Mode).
	Enable Preamble Capture/CDL Stats	When this check box is selected, the preamble is included for all packets captured through capture engine and will enable passing preamble data through Rx engine in order for CDL statistics to function.
	Include Preamble In Rx CRC Calculation	When this check box is selected, the CRC calculation takes into account the preamble length.

NGY Port Properties–Link Fault Signaling

Link Fault Signaling is a simple method to indicate certain types of faults between Ethernet stations. The Reconciliation Sublayer (RS) controls whether the MAC is allowed to transmit. In the typical scenario, the RS that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

In the NGY configuration, you can select the option to have the transmitting RS ignore link faults from the receiving RS.

NOTE In general, if a NGY port appears to be transmitting according to the Frames Sent statistic, be aware that Link Fault State may override this. For details, see *NGY Fault Handling*.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab. The 100GE *Link Fault Signaling* tab is shown in *Figure:NGY Link Fault Signaling*.

Figure:NGY Link Fault Signaling

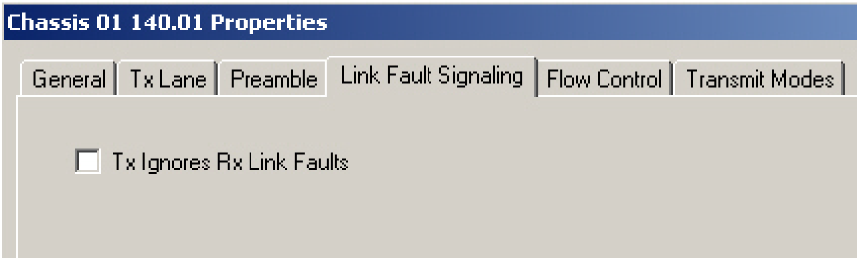


Table:NGY Link Fault Signaling tab describes the fields in NGY Link Fault Signaling tab.

Table:NGY Link Fault Signaling tab

Field/Control	Description
Tx Ignores Rx Link Faults	If selected, ongoing transmission continues even if Link Fault messages are received by the sending RS.

NGY Port Properties–Flow Control

When a port is receiving data at a faster rate than it can handle from another, directly connected port, the receiving port can send a MAC control PAUSE frame to the sending port to temporarily halt transmission of frames. The PAUSE function is defined in IEEE 802.3 and IEEE 802.1Qbb. Priority-based Flow Control for details.

The *Flow Control* tabis accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Flow Control* tab. The *Flow Control* tab for NGY **not** in Data Center mode is shown in *Figure:NGY (non Data Center mode) Port Properties—Flow Control*.

Figure:NGY (non Data Center mode) Port Properties—Flow Control

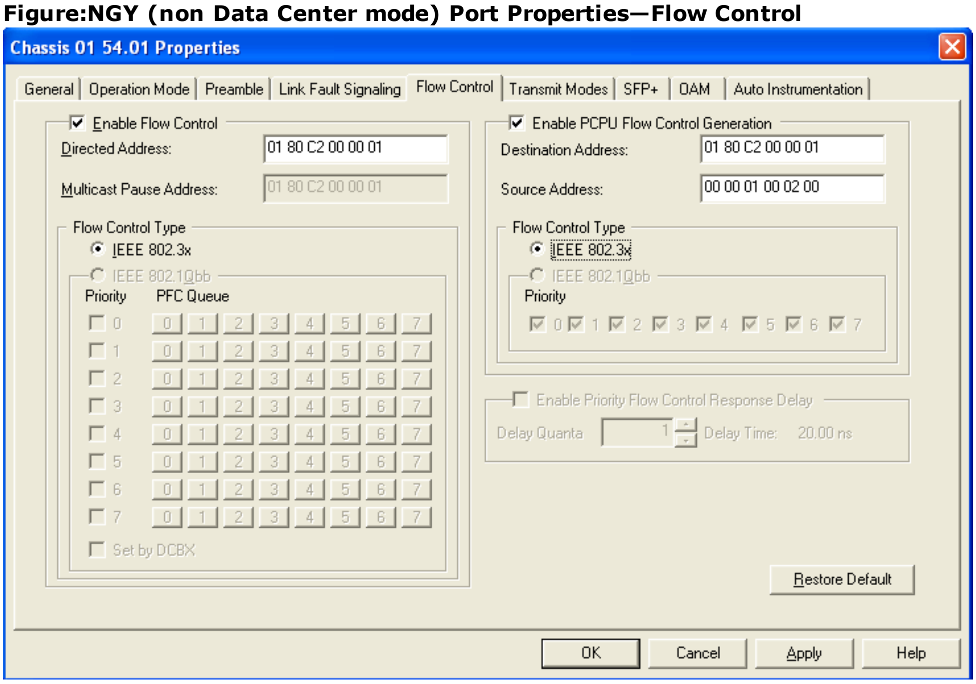
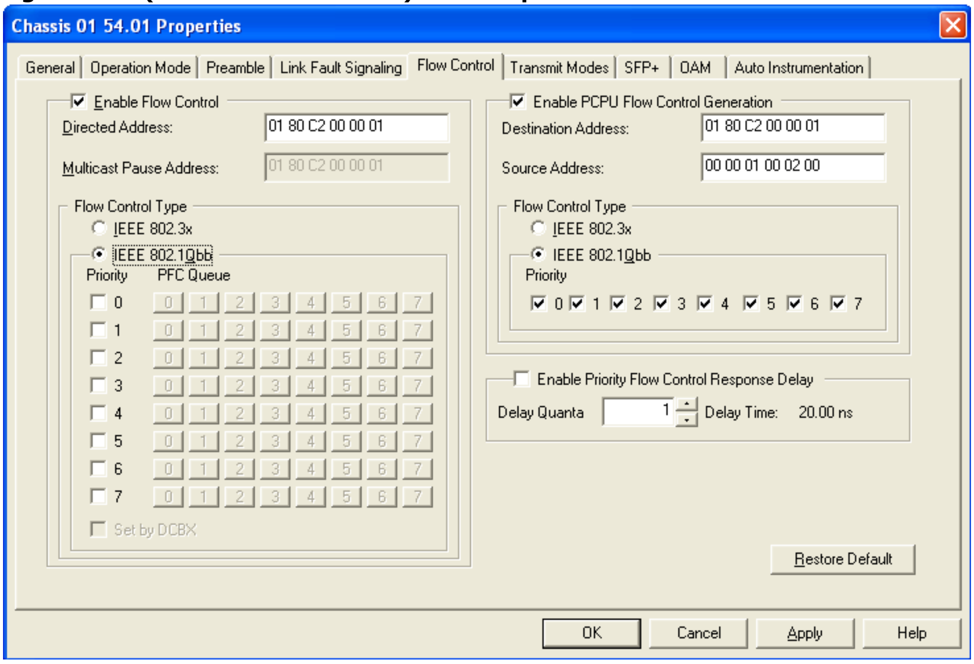


Figure:NGY (in Data Center mode) Port Properties—Flow Control



The fields and controls in this tab are described in *Table:NGY–Flow Control tab*.

Table:NGY–Flow Control tab

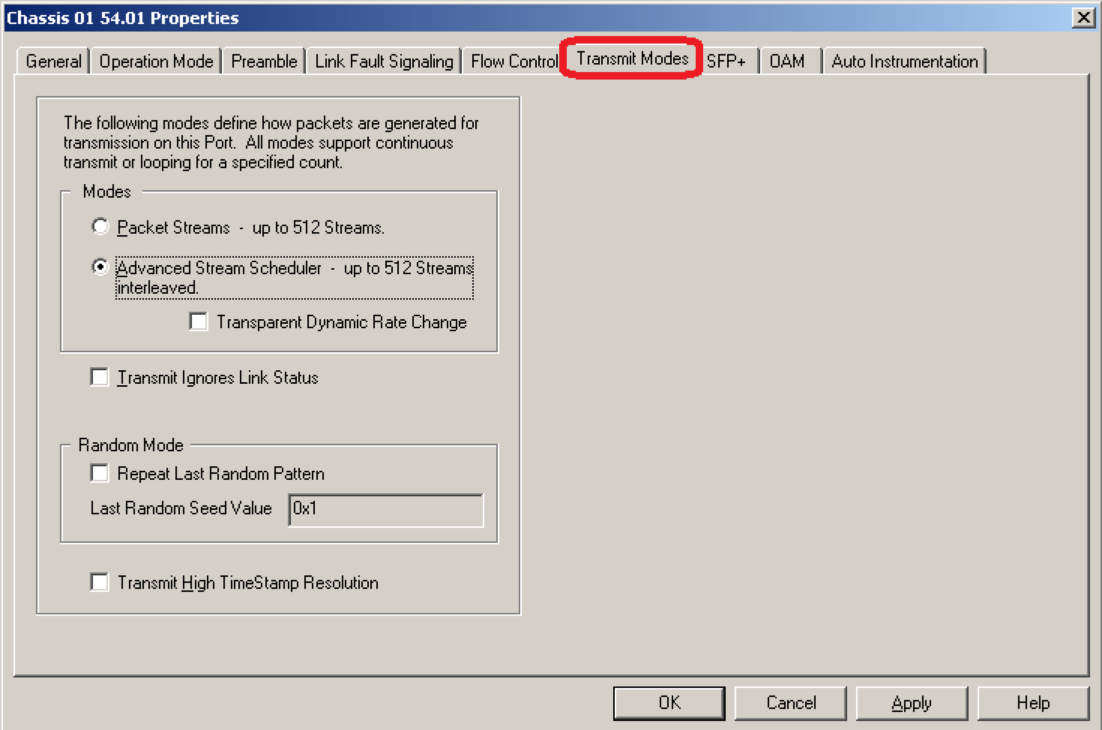
Section	Field/Control	Description
Enable Flow Control	(check box)	Enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type	IEEE 802.3x or IEEE 802.1Qbb	Priority-based Flow Control. When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
	Priority	Priority-based Flow Control
	PFC Queue	Priority-based Flow Control
Enable PCPU Flow Control Generation	(check box)	Enables port CPU flow control generation. When the rate of incoming packets is more than the port CPU can keep up with, a pause packet will be sent to the DUT, causing it to pause transmitting for a fixed interval.
	Destination Address	The DA and SA, taken together, identify the pause packet (to the DUT).

Section	Field/Control	Description
	Source Address	See Destination Address, above.
	Flow Control Type	See Flow Control Type, above.
	Priority	In Data Center mode, when flow control type IEEE 802.1Qbb is selected, these are the channels of data that can be paused. Click to select one or more channels.
Enable Priority Flow Control Response Delay	(check box)	If selected, enables to increase the number of frames that is sent when a pause frame is received. Priority Flow Control (PFC) pause allows to set the delay of flow control. When a pause frame is received for a certain priority, a count of the number of timestamp ticks increments up to a desired offset and then releases the pause request to the TX engine. For example, if running at 100% line rate and there is no delay in the pause request, the TX pipeline transmits the specified number of frames once the pause request is received. With this feature, a delay by number of timestamp ticks is programmed.
	Delay Quanta	This field allows to set the delay quanta of flow control.
	Delay Time	The delay time, in nanoseconds, of frames.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

NGY Port Properties–Transmit Modes

The *Transmit Modes* tab for NGY modules is accessed by double-clicking a port in Resources pane, or by right-clicking a port and selecting the *Properties* menu option. Then select the *Transmit Modes* tab. *Figure:NGY—Transmit Modes* shows the *Transmit Modes* tab for the NGY load module in normal LAN mode (not Data Center mode).

Figure:NGY—Transmit Modes



The fields and controls for the Transmit Modes tab are described in *Table:NGY Transmit Modes Configuration*.

Table:NGY Transmit Modes Configuration

Section	Field/Control	Description
Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 256 streams. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets. NGY LSM10GXM 4 and 8-port modules can generate up to 512 streams.
	Advanced Stream Scheduler	Sets up the transmission of up to 256 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams. NGY LSM10GXM 4 and 8-port modules can transmit up to 512 streams (up to 256 streams in Data Center mode).
	Transparent Dynamic Rate Change	If selected, the dynamic rate control will allow rate change across counters, for this port.
	Transmit Ignores Link Status	If selected, will allow transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including

Section	Field/Control	Description
		payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Transmit High TimeStamp Resolution		If selected, NGY load module will support 10ns Resolution Timestamp on selected modes.

NGY Port Properties–XFP

NGY load modules can support XFP interfaces. The XFP is a hot pluggable small footprint serial-to-serial data-agnostic multi-rate optical transceiver, intended to support Telecom (SONET OC-192 and G.709 'OTU-2') and Datacom applications (10 Gb/s Ethernet and 10 Gb/s Fibre Channel).

This tab also allows to set the carrier and laser power settings. The *XFP* tab is shown in *Figure:NGY—XFP tab*.

Figure:NGY—XFP tab

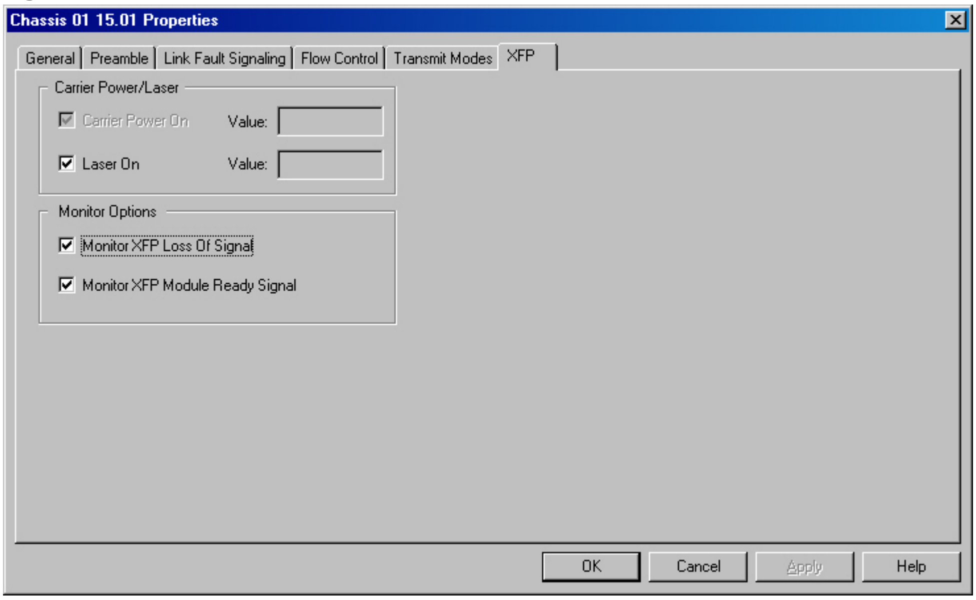


Table:NGY XFP tab Page Usage explains the configuration options of the *XFP* tab.

Table:NGY XFP tab Page Usage

Heading	Field	Usage
Carrier Power/Laser	Carrier Power On	Select this check box to enable the carrier power. Note that the actual reading will be displayed in the *Value* field.
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the *Value* field.
Monitor Options	Monitor XFP Loss of Signal	When selected, indicates the interface will conform to XFP specifications and require the absence of a Loss of Signal for transmitting and receiving.
	Monitor XFP Module Ready Signal	When selected, indicates the interface will conform to XFP specifications and require the detection of a Module Ready signal for transmitting and receiving.

NGY Port Properties–SFP

The following NGY load modules can support SFP+ interfaces.

- LSM10GXM(R)8S-01, LSM10GXM(R)4S-01, and LSM10GXM(R)2S-01–NGY full and reduced feature versions

This tab allows to set the carrier and laser power settings, the transceiver type, and the monitor options. The *SFP* tab is shown in *Figure:NGY—SFP tab*.

Figure:NGY—SFP tab

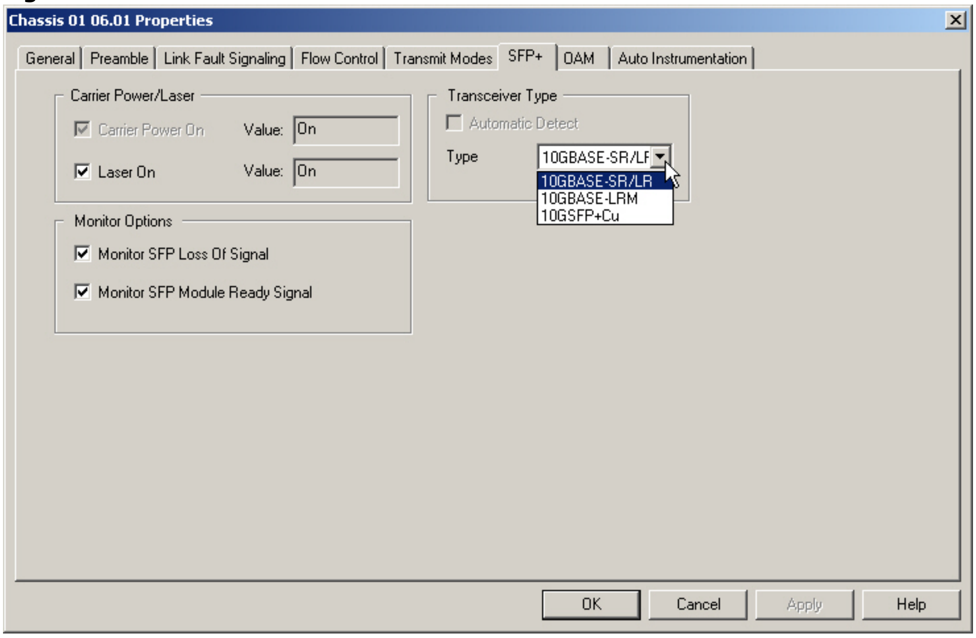


Table:SFP tab Page Usage explains the configuration options of the *SFP* tab.

Table:SFP tab Page Usage

Heading	Field	Usage
Carrier Power/Laser	Carrier Power On	If selected, enables the carrier power. The actual reading is displayed in the *Value* field.
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the *Value* field.
Monitor Options	Monitor SFP Loss of Signal	When selected, indicates the interface will conform to SFP specifications and require the absence of a Loss of Signal for transmitting and receiving.
	Monitor SFP Module Ready Signal	When selected, indicates the interface will conform to SFP specifications and require the detection of a Module Ready signal for transmitting and receiving.

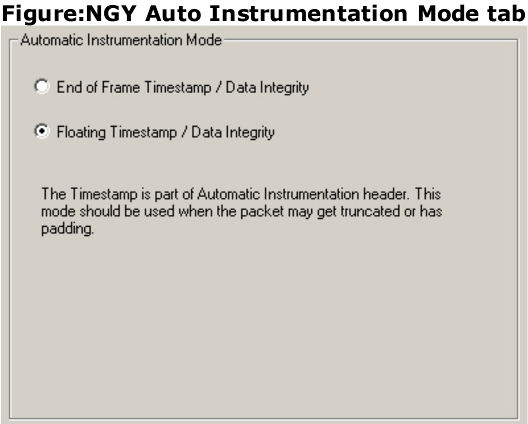
NGY Port Properties–Auto Instrumentation

For specified load modules, the timestamp can be inserted into the Auto Instrumentation header instead of the usual locations such as before CRC or at user-specified offset. This is called *Floating Timestamp/Data Integrity*. Timestamp and Data Integrity generation will be stream-based (while the Rx analysis is port-based) if Auto Instrumentation is enabled. The Port Properties Auto Instrumentation tab is shown in *Figure:NGY Auto Instrumentation Mode tab*.

The Auto Instrumentation tab is present in the following NGY load modules:

- LSM10GXM2/4/8R and 2/4/8XP reduced and extra performance NGY

Figure:NGY Auto Instrumentation Mode tab



Options on this tab are described in *Table:NGY Auto Instrumentation Configuration*.

Table:NGY Auto Instrumentation Configuration

Field/Control	Description
End of Frame Timestamp / Data Integrity	Inserts the Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	The timestamp is part of Automatic Instrumentation header. This mode should be used when the packet may get truncated or has padding.

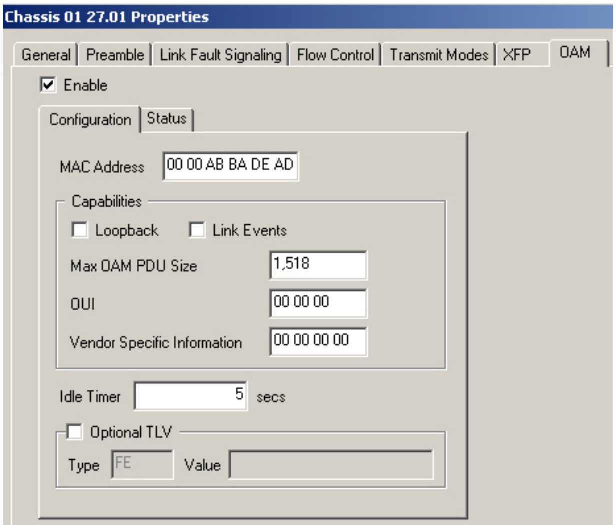
NGY Port Properties–OAM

The *OAM* tab is not present when port mode is 10G WAN.

The *OAM* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *OAM* tab. The *OAM* tab for NGY load modules allows to configure local stateful OAM Data Terminating Entities (DTE) and view the status of both local and remote OAM PDUs.

The OAM Configuration tab is shown in .

Figure:OAM tab for NGY, Configuration



The Operations, Administration, and Maintenance (OAM) sublayer provides mechanisms useful for monitoring link operation such as remote fault indication and remote loopback control. In general, OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAM PDUs). OAM PDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links.

The fields and controls in this tab are in *Table:OAM Configuration tab for NGY*.

After making configuration changes, click **Apply** to send the changes to the chassis without leaving the tab. Click **OK** to send changes and close the Properties window.

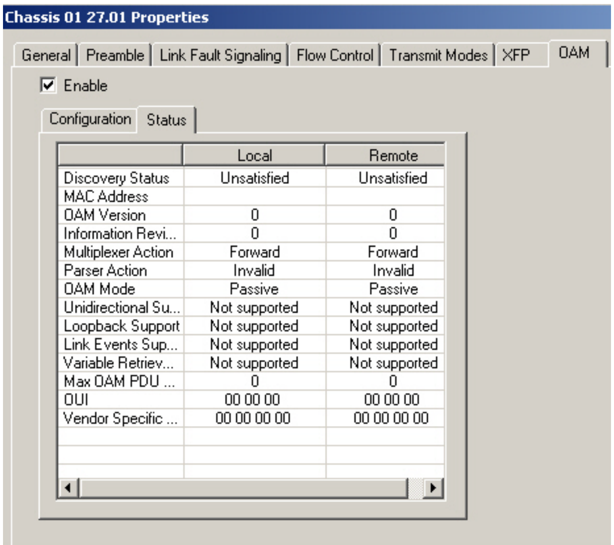
Table:OAM Configuration tab for NGY

Section	Field/Control	Description
	Enable	Enables and starts OAM state machine configuration
MAC Address		The individual source MAC address of the Ixia port acting as DTE (through which the OAM PDU is transmitted)
Capabilities	Loopback	Advertises OAM remote loopback capability
	Link Events	Advertises link event capability
	Max OAM PDU Size	11-bit field which represents the largest OAM

Section	Field/Control	Description
		PDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.
	OUI	24-bit 3-octet field, Organizationally Unique Identifier. Example: 00 00 00
	Vendor Specific Information	4-octet field, 32-bit identifier that may be used to differentiate a vendor's product models/versions.
Idle Timer		local_lost_link_timer Timer used to reset the Discovery state. Duration: 5 sec ± 10%.
Optional TLV	Type	This is any Information TLV that you want to send. This one-octet field indicates the nature of the data carried in this TLV-tuple. • 0x00 End of TLV marker • 0x01 Local Information • 0x02 Remote Information • 0x03-0xFD Reserved - shall not be transmitted, should be ignored on reception by OAM client • 0xFE Organization Specific Information • 0xFF Reserved - shall not be transmitted, should be ignored on reception by OAM client
	Value	This field indicates the value of the Information TLV. This field's length and contents are unspecified.

The OAM Status tab is shown in *Figure:OAM tab for NGY, Status*.

Figure:OAM tab for NGY, Status



The fields and controls in the Status tab are described in *Table:OAM Status tab*. for each category, there is both a Local and a Remote status indicator.

Table:OAM Status tab

Field/Control	Description
Discovery Status	Detects the presence of an OAM sublayer at the remote DTE
MAC Address	Defined in *Table:OAM Configuration tab for NGY*
OAM Version	This one-octet field indicates the version supported by the DTE. This field always contains the value 0x01.
Information Revision	This two-octet field indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes.
Multiplexer Action	Forward (0) = Device is forwarding non-OAMPDUs to the lower sublayer (local_mux_action = FWD). Discard (1) = Device is discarding non-OAMPDUs (local_mux_action = DISCARD).
Parser Action	00 = Device is forwarding non-OAMPDUs to higher sublayer (local_par_action = FWD). 01 = Device is looping back non-OAMPDUs to the lower sublayer (local_par_action = LB). 10 = Device is discarding non-OAMPDUs (local_par_action = DISCARD). 11 = Reserved. In Local Information TLVs, this value shall not be sent. If the value 11 is received, it should be ignored and not change the last received value.
OAM Mode	1 = DTE configured in Active mode. 0 = DTE configured in Passive mode.
Unidirectional Support	1 = DTE is capable of sending OAMPDUs when the receive path is non-operational. 0 = DTE is not capable of sending OAMPDUs when the receive path is non-operational.
Loopback Support	Defined in *Table:OAM Configuration tab for NGY*
Link Events Support	Defined in *Table:OAM Configuration tab for NGY*
Variable Retrieval Support	1 = DTE supports sending Variable Response OAMPDUs. 0 = DTE does not support sending Variable Response OAMPDUs.
Max OAM PDU Size	Defined in *Table:OAM Configuration tab for NGY*
OUI	Defined in *Table:OAM Configuration tab for NGY*
Vendor Specific Information	Defined in *Table:OAM Configuration tab for NGY*

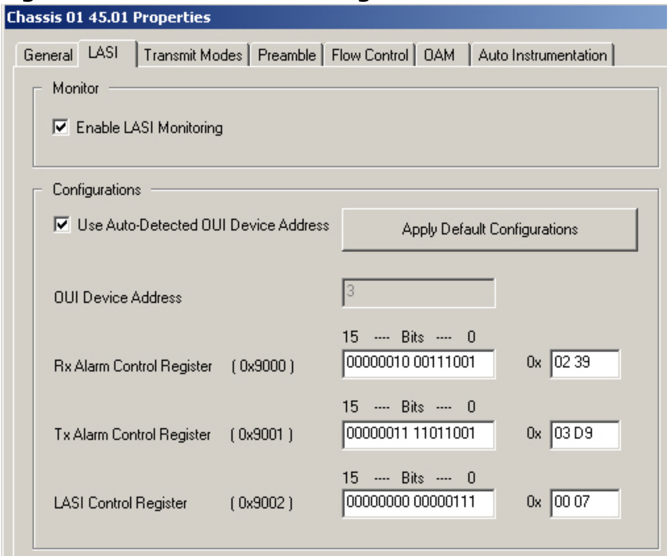
NGY 10GBASE-T Port Properties–LASI

The Link Alarm Status Interrupt (LASI) is an active-low output from the 10GBASE-T adapter that indicates a link fault condition has been asserted or has been cleared. Control registers are provided so that LASI may be programmed to assert only for specific fault conditions.

For more detailed information on LASI, see the Link Alarm Status Interrupt (LASI) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The *LASI* tab page is shown in *Figure:10GBASE-T LASI Configuration*.

Figure:10GBASE-T LASI Configuration



The controls for LASI configuration are described in *Table:LASI Configuration*.

Table:LASI Configuration

Section	Control/Field	Usage
Monitor		Activates the LASI monitoring feature.
	Enable LASI Monitoring	Selecting this check box enables LASI monitoring.
Configurations		Controls LASI configuration.
	Use Auto-Detected OUI Device Address	Selecting this check box sets the OUI address to the detected address. If this is selected, then the OUI *Device Address* field is disabled.
	Apply Default Configuration	Selecting this button resets the LASI values to their default settings.
	OUI Device Address	The Organizationally Unique Identifier (OUI) device address, which signifies the device where the LASI control/status registers are located.
	Rx Alarm Control Register	Controls the register written at offset 0x9000, and indicates what type of receive path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.

Section	Control/Field	Usage
	Tx Alarm Control Register	Controls the register written at offset 0x9001, and indicates what type of transmit path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	LASI Control Register	Controls the register written at offset 0x9002, and indicates what type of alarms are enabled. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.

NGY Port Properties–SFP

The following NGY load modules can support SFP+ interfaces.

- LSM10GXM(R)8S-01, LSM10GXM(R)4S-01, and LSM10GXM(R)2S-01–NGY full and reduced feature versions

This tab allows to set the carrier and laser power settings, the transceiver type, and the monitor options. The *SFP* tab is shown in *Figure:NGY—SFP tab*.

Figure:NGY—SFP tab

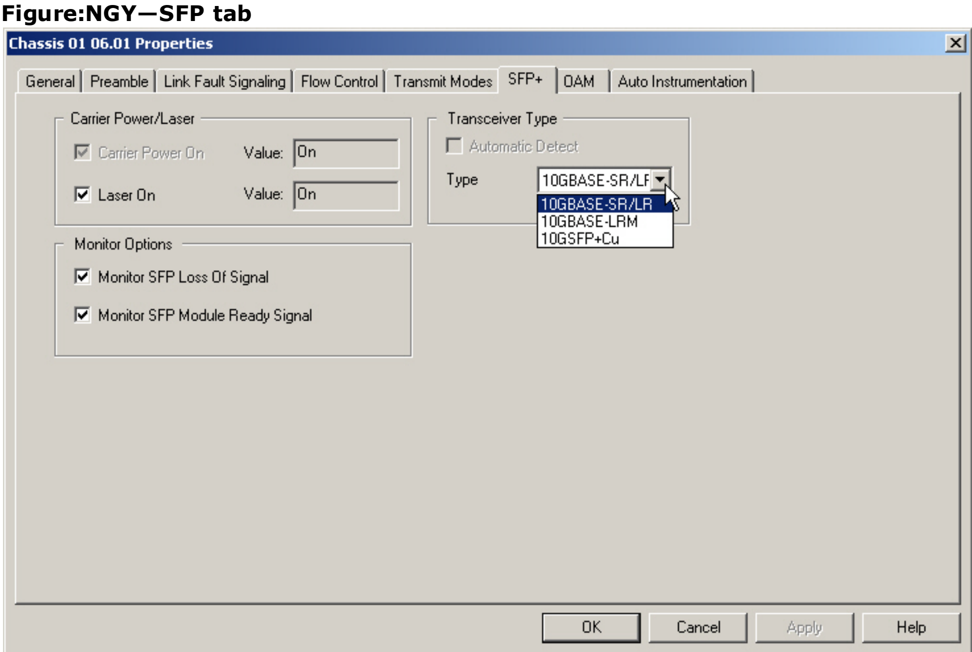


Table:SFP tab Page Usage explains the configuration options of the *SFP* tab.

Table:SFP tab Page Usage

Heading	Field	Usage
Carrier Power/Laser	Carrier Power On	If selected, enables the carrier power. The actual reading is displayed in the *Value* field.
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the *Value* field.
Monitor Options	Monitor SFP Loss of Signal	When selected, indicates the interface will conform to SFP specifications and require the absence of a Loss of Signal for transmitting and receiving.
	Monitor SFP Module Ready Signal	When selected, indicates the interface will conform to SFP specifications and require the detection of a Module Ready signal for transmitting and receiving.

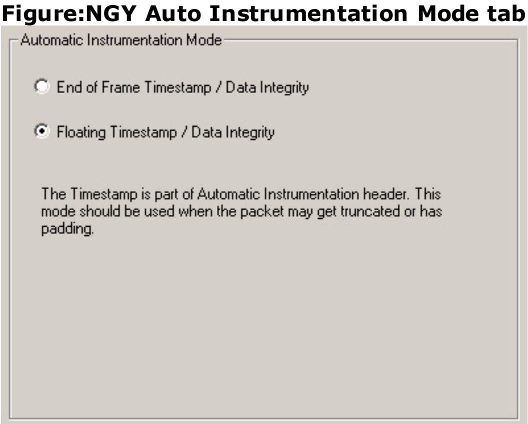
NGY Port Properties–Auto Instrumentation

For specified load modules, the timestamp can be inserted into the Auto Instrumentation header instead of the usual locations such as before CRC or at user-specified offset. This is called *Floating Timestamp/Data Integrity*. Timestamp and Data Integrity generation will be stream-based (while the Rx analysis is port-based) if Auto Instrumentation is enabled. The Port Properties Auto Instrumentation tab is shown in *Figure:NGY Auto Instrumentation Mode tab*.

The Auto Instrumentation tab is present in the following NGY load modules:

- LSM10GXM2/4/8R and 2/4/8XP reduced and extra performance NGY

Figure:NGY Auto Instrumentation Mode tab



Options on this tab are described in *Table:NGY Auto Instrumentation Configuration*.

Table:NGY Auto Instrumentation Configuration

Field/Control	Description
End of Frame Timestamp / Data Integrity	Inserts the Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	The timestamp is part of Automatic Instrumentation header. This mode should be used when the packet may get truncated or has padding.

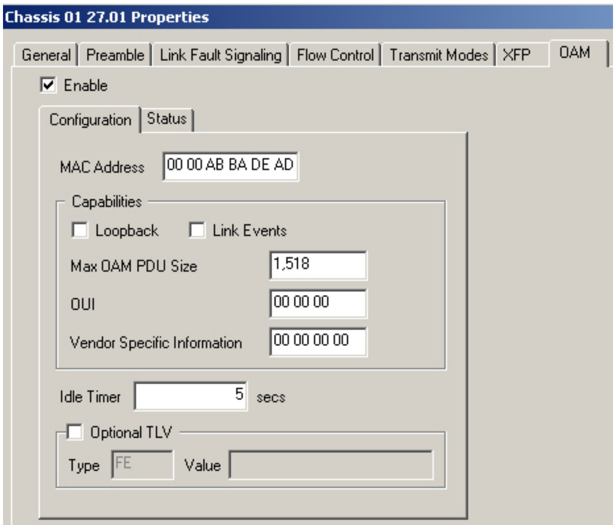
NGY Port Properties–OAM

The *OAM* tab is not present when port mode is 10G WAN.

The *OAM* tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *OAM* tab. The *OAM* tab for NGY load modules allows to configure local stateful OAM Data Terminating Entities (DTE) and view the status of both local and remote OAM PDUs.

The OAM Configuration tab is shown in .

Figure:OAM tab for NGY, Configuration



The Operations, Administration, and Maintenance (OAM) sublayer provides mechanisms useful for monitoring link operation such as remote fault indication and remote loopback control. In general, OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAM PDUs). OAM PDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links.

The fields and controls in this tab are in *Table:OAM Configuration tab for NGY*.

After making configuration changes, click **Apply** to send the changes to the chassis without leaving the tab. Click **OK** to send changes and close the Properties window.

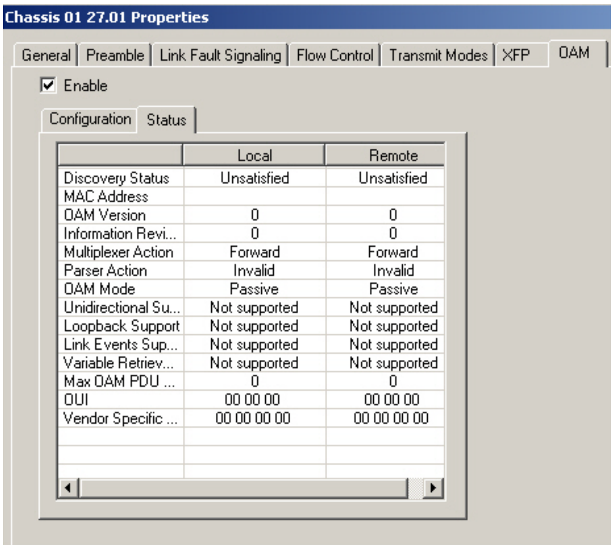
Table:OAM Configuration tab for NGY

Section	Field/Control	Description
	Enable	Enables and starts OAM state machine configuration
MAC Address		The individual source MAC address of the Ixia port acting as DTE (through which the OAM PDU is transmitted)
Capabilities	Loopback	Advertises OAM remote loopback capability
	Link Events	Advertises link event capability
	Max OAM PDU Size	11-bit field which represents the largest OAM

Section	Field/Control	Description
		PDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.
	OUI	24-bit 3-octet field, Organizationally Unique Identifier. Example: 00 00 00
	Vendor Specific Information	4-octet field, 32-bit identifier that may be used to differentiate a vendor's product models/versions.
Idle Timer		local_lost_link_timer Timer used to reset the Discovery state. Duration: 5 sec ± 10%.
Optional TLV	Type	This is any Information TLV that you want to send. This one-octet field indicates the nature of the data carried in this TLV-tuple. • 0x00 End of TLV marker • 0x01 Local Information • 0x02 Remote Information • 0x03-0xFD Reserved - shall not be transmitted, should be ignored on reception by OAM client • 0xFE Organization Specific Information • 0xFF Reserved - shall not be transmitted, should be ignored on reception by OAM client
	Value	This field indicates the value of the Information TLV. This field's length and contents are unspecified.

The OAM Status tab is shown in *Figure:OAM tab for NGY, Status*.

Figure:OAM tab for NGY, Status



The fields and controls in the Status tab are described in *Table:OAM Status tab*. for each category, there is both a Local and a Remote status indicator.

Table:OAM Status tab

Field/Control	Description
Discovery Status	Detects the presence of an OAM sublayer at the remote DTE
MAC Address	Defined in *Table:OAM Configuration tab for NGY*
OAM Version	This one-octet field indicates the version supported by the DTE. This field always contains the value 0x01.
Information Revision	This two-octet field indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes.
Multiplexer Action	Forward (0) = Device is forwarding non-OAMPDUs to the lower sublayer (local_mux_action = FWD). Discard (1) = Device is discarding non-OAMPDUs (local_mux_action = DISCARD).
Parser Action	00 = Device is forwarding non-OAMPDUs to higher sublayer (local_par_action = FWD). 01 = Device is looping back non-OAMPDUs to the lower sublayer (local_par_action = LB). 10 = Device is discarding non-OAMPDUs (local_par_action = DISCARD). 11 = Reserved. In Local Information TLVs, this value shall not be sent. If the value 11 is received, it should be ignored and not change the last received value.
OAM Mode	1 = DTE configured in Active mode. 0 = DTE configured in Passive mode.
Unidirectional Support	1 = DTE is capable of sending OAMPDUs when the receive path is non-operational. 0 = DTE is not capable of sending OAMPDUs when the receive path is non-operational.
Loopback Support	Defined in *Table:OAM Configuration tab for NGY*
Link Events Support	Defined in *Table:OAM Configuration tab for NGY*
Variable Retrieval Support	1 = DTE supports sending Variable Response OAMPDUs. 0 = DTE does not support sending Variable Response OAMPDUs.
Max OAM PDU Size	Defined in *Table:OAM Configuration tab for NGY*
OUI	Defined in *Table:OAM Configuration tab for NGY*
Vendor Specific Information	Defined in *Table:OAM Configuration tab for NGY*

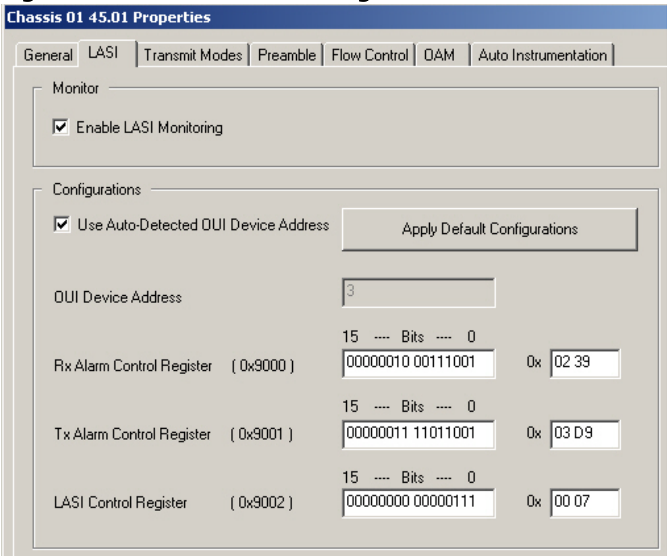
NGY 10GBASE-T Port Properties–LASI

The Link Alarm Status Interrupt (LASI) is an active-low output from the 10GBASE-T adapter that indicates a link fault condition has been asserted or has been cleared. Control registers are provided so that LASI may be programmed to assert only for specific fault conditions.

For more detailed information on LASI, see the Link Alarm Status Interrupt (LASI) section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.

The *LASI* tab page is shown in *Figure:10GBASE-T LASI Configuration*.

Figure:10GBASE-T LASI Configuration



The controls for LASI configuration are described in *Table:LASI Configuration*.

Table:LASI Configuration

Section	Control/Field	Usage
Monitor		Activates the LASI monitoring feature.
	Enable LASI Monitoring	Selecting this check box enables LASI monitoring.
Configurations		Controls LASI configuration.
	Use Auto-Detected OUI Device Address	Selecting this check box sets the OUI address to the detected address. If this is selected, then the OUI *Device Address* field is disabled.
	Apply Default Configuration	Selecting this button resets the LASI values to their default settings.
	OUI Device Address	The Organizationally Unique Identifier (OUI) device address, which signifies the device where the LASI control/status registers are located.
	Rx Alarm Control Register	Controls the register written at offset 0x9000, and indicates what type of receive path fault generates an alarm. The register can be modified using the bit field

Section	Control/Field	Usage
		or hex field. Modifying one automatically updates the other.
	Tx Alarm Control Register	Controls the register written at offset 0x9001, and indicates what type of transmit path fault generates an alarm. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.
	LASI Control Register	Controls the register written at offset 0x9002, and indicates what type of alarms are enabled. The register can be modified using the bit field or hex field. Modifying one automatically updates the other.

Chapter 23 - Port Properties–FCM Family

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the Fibre Channel Module (FCM) family port properties.

Port Properties for FCM Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the GXM8 and GXM4 type boards is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for FCM modules (GXM family):

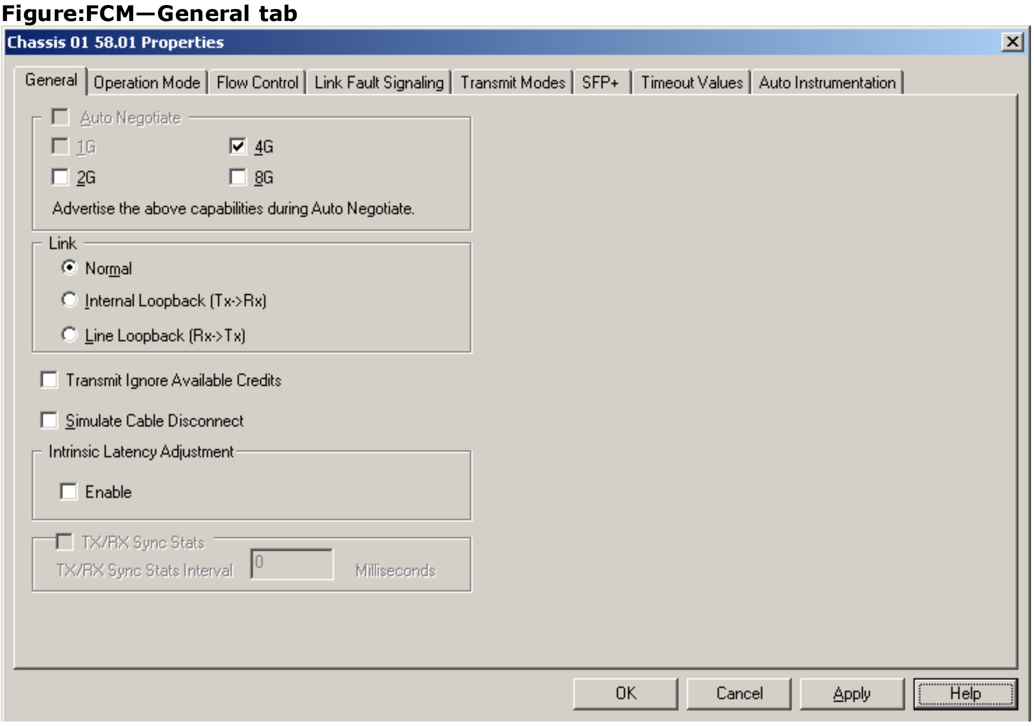
- *FCM Port Properties—General*
- *FCM Port Properties—Operation Mode*
- *FCM Port Properties—Flow Control*
- *FCM Port Properties—Link Fault Signaling*
- *FCM Port Properties—Transmit Modes*
- *FCM Port Properties—SFP+*
- *FCM Port Properties—Timeout Values*
- *FCM Port Properties—Auto Instrumentation*

FCM Port Properties—General

The FCM **General** tab is accessed by right-clicking an FCM port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **General** tab.

The FCM Port Properties **General** tab is shown in *Figure:FCM—General tab*.

Figure:FCM—General tab



The controls for FCM **General** tab configuration are described in *Table:General Configuration*.

Table:General Configuration

Section	Control/Field	Usage
Auto Negotiate		This field is disabled for use in Fibre Channel load module (FCM).
	1G	This field is disabled for use in Fibre Channel load module (FCM).
	2G	If selected, sets the speed of the Fibre Channel card at 2G.
	4G	If selected, sets the speed of the Fibre Channel card at 4G.
	8G	If selected, sets the speed of the Fibre Channel card at 8G.
Link	Normal	Normal operation of the card.
	Internal Loopback (Tx->Rx)	If selected, enables the Internal Loopback-Transmit to Receive.
	Line Loopback (Rx->Tx)	If selected, enables the Line Loopback-Receive to Transmit. In Line Loopback state, the port that is in loopback mode cannot transmit packets on its own. It transmits only those packets that it receives. For example, if Port A transmits 100 packets to Port B which is in loopback mode, Port B will transmit the same 100 packets to Port A that it receives from Port A.

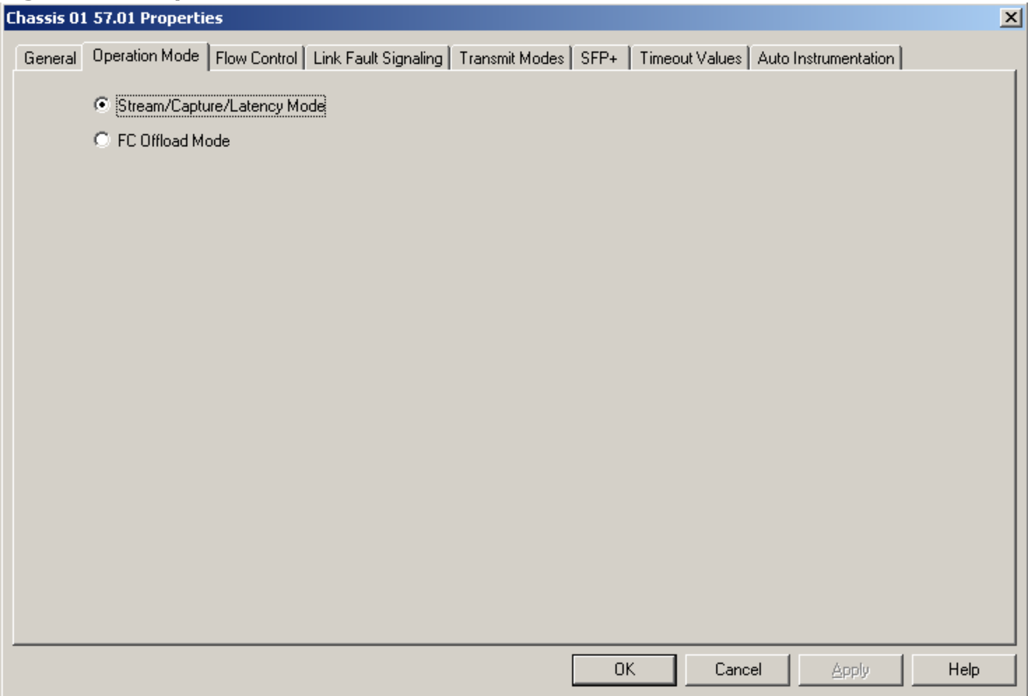
Section	Control/Field	Usage
Transmit Ignore Available Credits		If selected, the transmitting port does not listen to flow control. It keeps transmitting packets irrespective of available credits. For example, connect two Fibre Channel ports back-to-back. Enable 'Transmit ignore available credits' option on the transmitting port and 'Don't send R_RDY' option on the receiving port. Once transmit starts, the port transmits at full rate even though it does not have credits. The transmitting port ignores available credit and keeps transmitting.
Simulate Cable Dis-connect		If selected, the port responds as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	If selected, enables the intrinsic latency adjust-ment. The **Enable** check box is disabled when no value exists in the system for the specific trans-ceiver. It is available if a value exists (in the xml file).
TX/RX Sync Stats	TX/RX Sync Stats Interval	This field is disabled for Fibre Channel load mod-ule.

FCM Port Properties—Operation Mode

The FCM **Operation Mode** tab is accessed by right-clicking an FCM port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Operation Mode** tab.

The FCM Port Properties **Operation Mode** tab is shown in *Figure:FCM—Operation Mode tab*.

Figure:FCM—Operation Mode tab



The controls for FCM **Operation Mode** tab configuration are described in *Table:Operation Mode Configuration*.

Table:Operation Mode Configuration

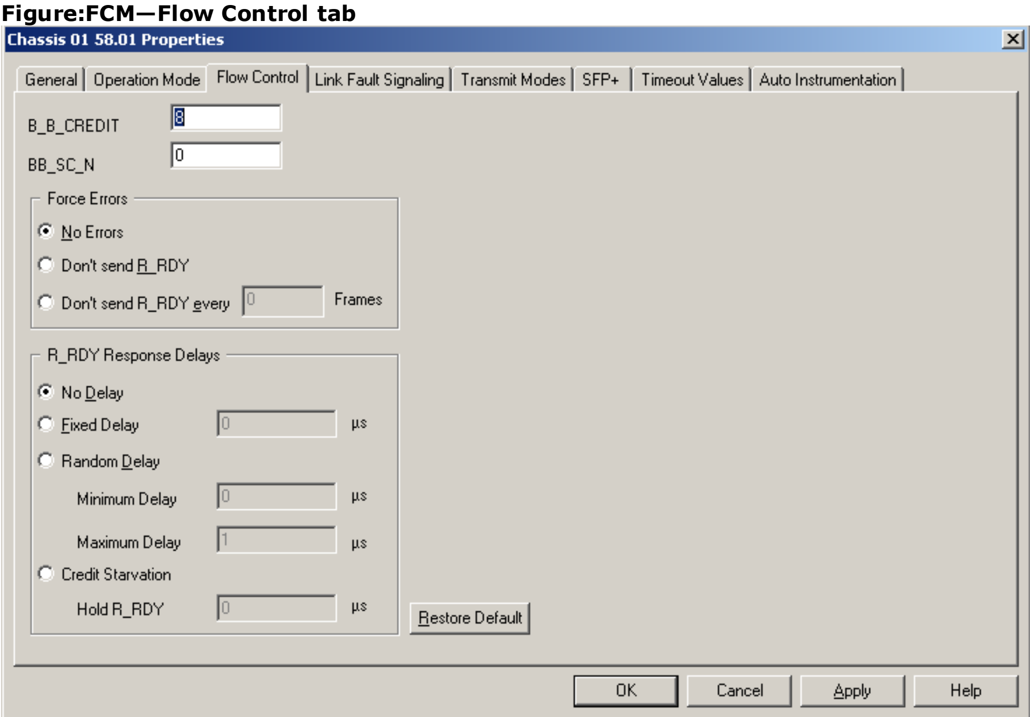
Section	Control/Field	Usage
Operation Mode	Stream/Capture/Latency Mode	If selected, allows to configure packet stream and enables capture and latency mode. When this option is not selected, the Packet Streams option does not appear under the FC port node.
	FC Offload Mode	If selected, enables the hardware assisted acceleration for sending data over FC port. You may enable this option for maximum performance or disable if IXIA Streams traffic is also running on this port.

FCM Port Properties—Flow Control

The FCM **Flow Control** tab is accessed by right-clicking an FCM port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

The FCM Port Properties **Flow Control** tab is shown in *Figure:FCM—Flow Control tab*.

Figure:FCM—Flow Control tab



The controls for FCM **Flow Control** tab configuration are described in *Table:Flow Control Configuration*.

Table:Flow Control Configuration

Section	Control/Field	Usage
B_B_CREDIT		Buffer-to-buffer Credit is the number of received buffers supported by an FC Port for receiving Class 1 and 6/SOFc1, Class 2, or Class 3 frames. BB_Credit values of the attached FC Ports are mutually conveyed to each other during the Fabric Login through the Buffer-to-buffer Credit field of the FLOGI Common Service Parameters. The minimum or default value of BB_Credit is one. BB_Credit is used as the controlling parameter in buffer-to-buffer flow control.
BB_SC_N		The buffer-to-buffer State Change Number. It is the log2 of BB_Credit Recovery modulus. The default value is 0.
Force Errors		Allows to set error messages for frames of data.
	No Errors	If selected, does not send error messages.
	Don't send R_RDY	If selected, does not send Receiver_Ready (R_RDY) Primitive error signal.
	Don't send R_RDY_ every_ frames	If selected, does not send Receiver_Ready (R_RDY) Primitive error signal for every specified number of data frames.
R_RDY Response		Allows to set response delays for R_RDY. The

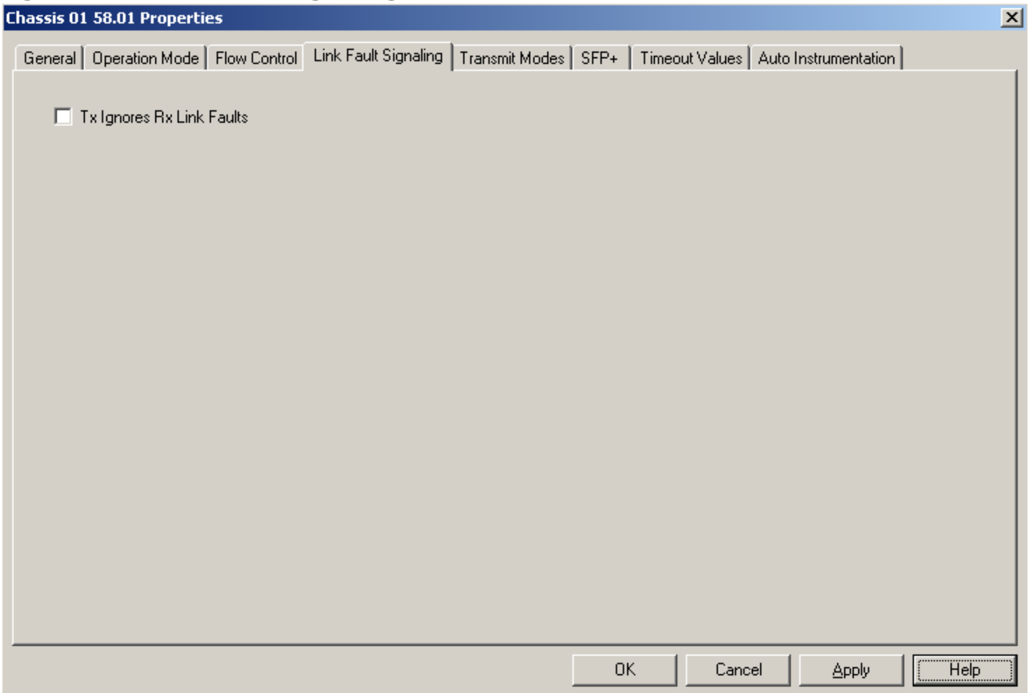
Section	Control/Field	Usage
Delays		Receiver_Ready (R_RDY) Primitive Signal is used in the buffer-to-buffer Credit management mechanisms Validity of the frame is not implied by R_RDY.
	No Delay	If selected, does not set any delay period for R_RDY response. The responses come without any delay in time.
	Fixed Delay	If selected, sets fixed delays in milliseconds for R_RDY response.
	Random Delay	If selected, you can control the delay in time at which R_RDY response is received from the port. The options are as follows: • Minimum Delay: Sets the minimum delay in milliseconds. • Maximum delay: Sets the maximum delay in milliseconds. When the minimum and maximum delays are set, the port internally selects a random value between the minimum and maximum values and starts sending the R_RDY response at the random value delay.
	Credit Starvation	If selected, user-specified timer is activated and the port schedules the first R_RDY transmission.
Restore Default		If clicked, restores the default setting.

FCM Port Properties—Link Fault Signaling

The FCM *Link Fault Signaling* tab is accessed by right-clicking an FCM port in the *Explore Network Resources* pane, selecting the *Port Properties* menu options, then selecting the *Link Fault Signaling* tab.

The FCM Port Properties *Link Fault Signaling* tab is shown in *Figure:FCM—Link Fault Signaling tab*.

Figure:FCM—Link Fault Signaling tab



The controls for FCM *Link Fault Signaling* tab configuration are described in *Table:Link Fault Signaling tab*.

Table:Link Fault Signaling tab

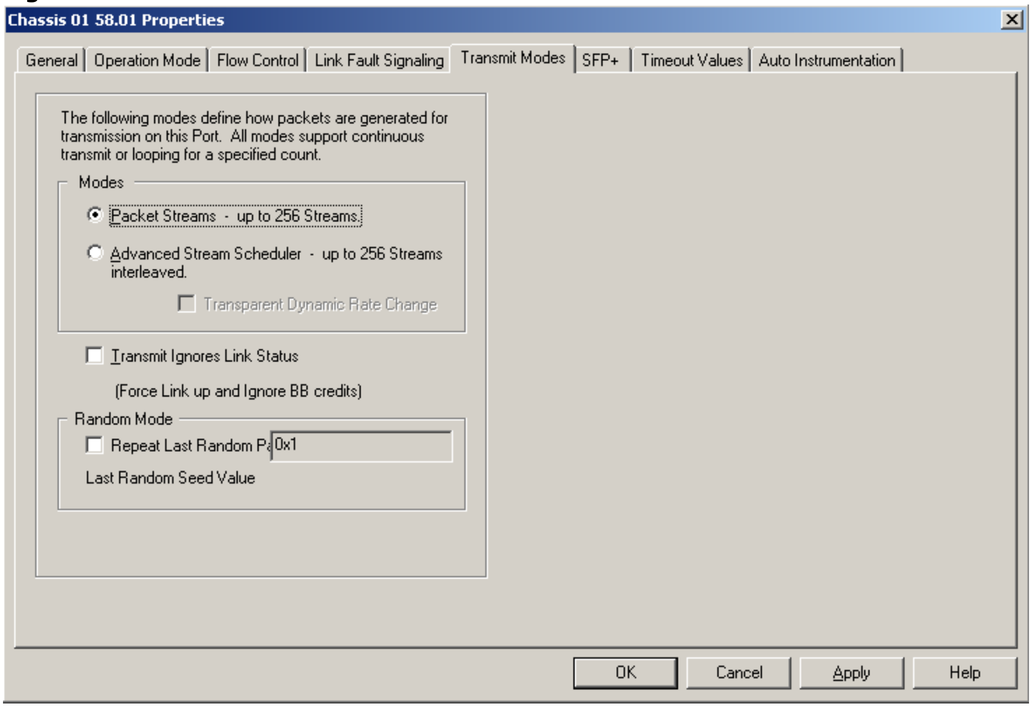
Field/Control	Description
Tx Ignores Rx Link Faults	If selected, ongoing transmission continues even if Link Fault messages are received by the sending RS.

FCM Port Properties—Transmit Modes

The FCM *Transmit Modes* tab is accessed by right-clicking an FCM port in the *Explore Network Resources* pane, selecting the *Port Properties* menu options, then selecting the *Transmit Modes* tab.

The FCM Port Properties *Transmit Modes* tab is shown in *Figure:FCM—Transmit Modes tab*.

Figure:FCM—Transmit Modes tab



The controls for FCM *Transmit Modes* tab configuration are described in *Table:Transmit Modes Configuration*.

Table:Transmit Modes Configuration

Section	Control/Field	Usage
Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. This allows to configure up to 256 streams. A stream is programmed for continuous packet generation for generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets up the transmission of up to 256 interleaved packet streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Transparent Dynamic Rate Change	If selected, the dynamic rate control allows rate change across counters, for this port.
	Transmit Ignores Link Status	If selected, allows transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	If selected, causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This is used before transmission (in which case the seed from the first packet stream is used), or immediately after a stream is sent (in which case the last stream's random seed is used).

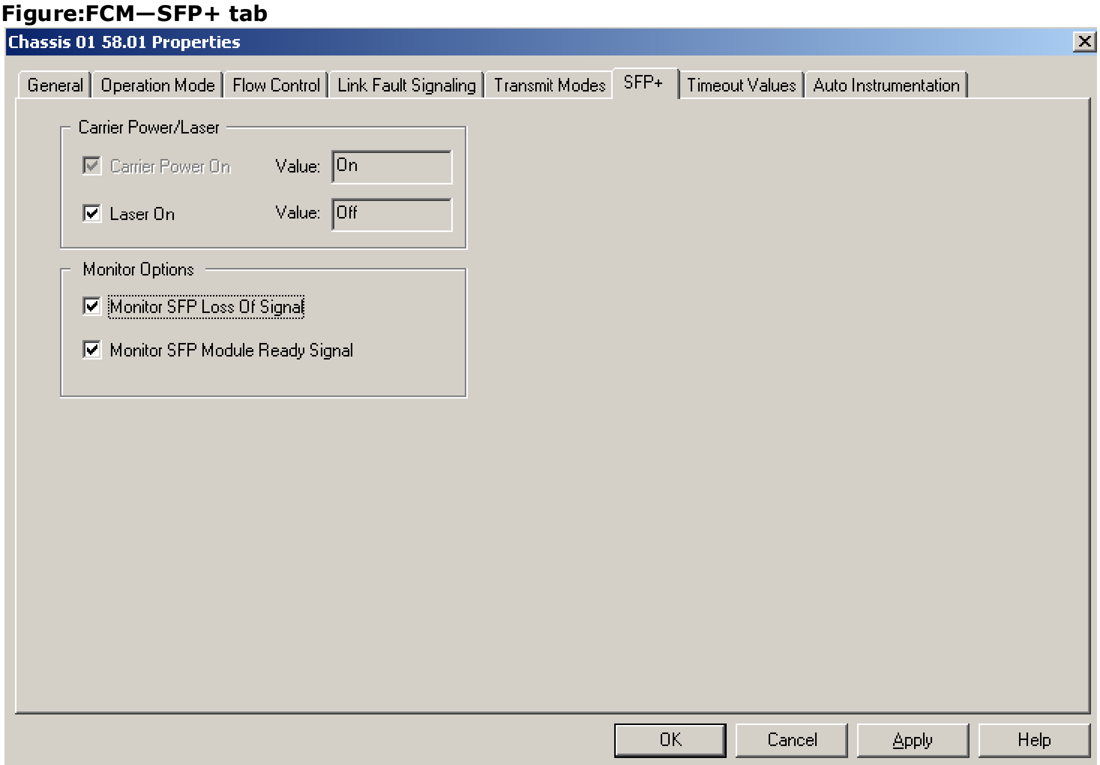
Section	Control/Field	Usage
		For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware uses to seed its random number generators. NOTE It is not a one-to-one mapping.

FCM Port Properties—SFP+

The FCM *SFP+* tab is accessed by right-clicking an FCM port in the *Explore Network Resources* pane, selecting the *Port Properties* menu options, then selecting the *SFP+* tab.

The FCM Port Properties *SFP+* tab is shown in *Figure:FCM—SFP+ tab*.

Figure:FCM—SFP+ tab



The controls for FCM *SFP+* tab configuration are described in *Table:SFP Configuration*.

Table:SFP Configuration

Section	Control/Field	Usage
Carrier Power/Laser	Carrier Power On	If selected, enables the carrier power. The actual reading is displayed in the *Value* field.
	Laser On	If selected, enables the laser power. The actual reading is displayed in the *Value* field.
Monitor Options	Monitor SFP Loss of Signal	If selected, indicates that the interface conforms to SFP specifications and requires the absence of a Loss of Signal for transmitting and

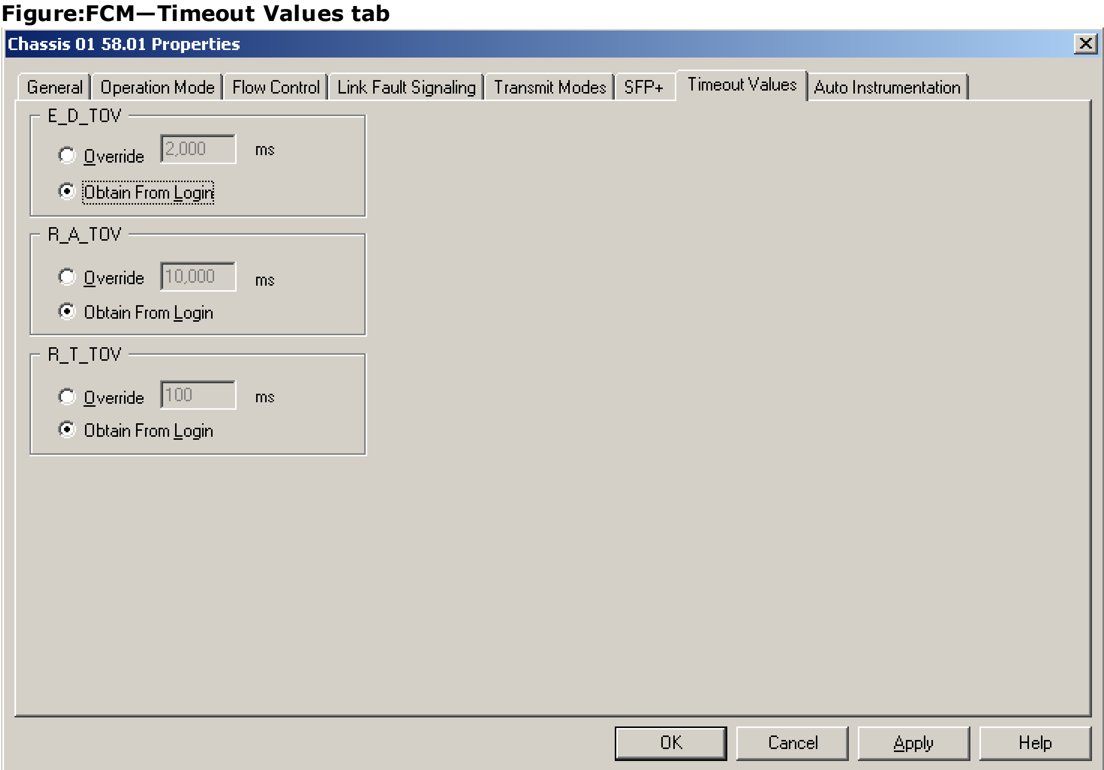
Section	Control/Field	Usage
		receiving.
	Monitor SFP Module Ready Signal	If selected, indicates that the interface conforms to SFP specifications and requires the detection of a Module Ready signal for transmitting and receiving.

FCM Port Properties—Timeout Values

The FCM *Timeout Values* tab is accessed by right-clicking an FCM port in the *Explore Network Resources* pane, selecting the *Port Properties* menu options, then selecting the *Timeout Values* tab.

The FCM Port Properties *Timeout Values* tab is shown in *Figure:FCM—Timeout Values tab*.

Figure:FCM—Timeout Values tab



The controls for FCM *Timeout Values* tab configuration are described in *Table:Timeout Values Configuration*.

Table:Timeout Values Configuration

Section	Control/Field	Usage
E_D_TOV	Error_Detect_Timeout Value (E_D_TOV) is a short timeout value. The E_D_TOV is used as the timeout value for detecting an error condition. The value of E_D_TOV represents a timeout value for detection of a response to a timed event. For example, during Data frame transmission it represents a timeout value for a Data frame to be delivered, the destination Nx_Port to transmit a Link_Response, and the Link_Response to be delivered to the Sequence Initiator.	

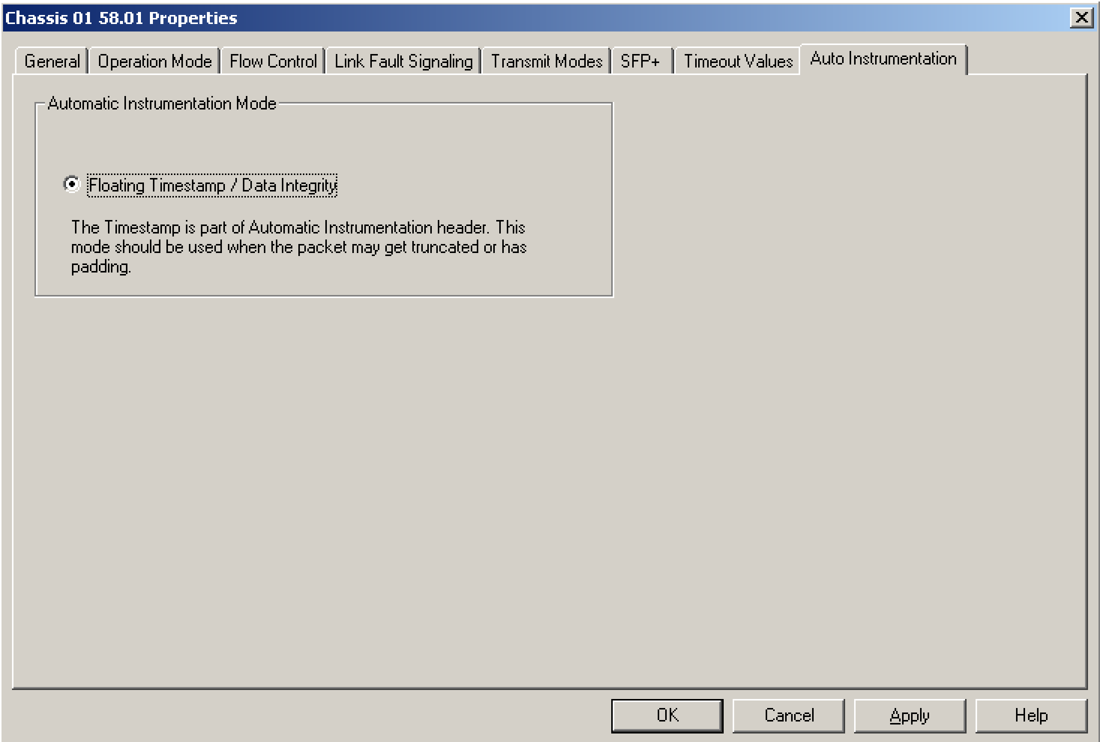
Section	Control/Field	Usage
	Override	If selected, error detection overrides 10,000 milliseconds.
	Obtain From Login	If selected, obtains response from login ID.
R_A_TOV	Resource_Allocation_Timeout Value (R_A_TOV) is a long timeout value. The R_A_TOV is used as the timeout value for determining when to Reinstate a Recovery_Qualifier. The value of R_A_TOV represents E_D_TOV and twice the maximum time that a frame may be delayed within a Fabric and still be delivered. The default value of R_A_TOV is 10 seconds or 10,000 milliseconds.	
	Override	If selected, error detection overrides 10,000 milliseconds.
	Obtain From Login	If selected, obtains response from login ID.
R_T_TOV		The Receiver_Transmitter timeout value (R_T_TOV) is used by the receiver logic to detect Loss-of-Synchronization. The default value for R_T_TOV is 100 milliseconds. A shorter value of 100 microseconds is also allowed. FC Ports that use the shorter value indicate this by setting the R_T_TOV bit in the Common Service Parameters during Login. An FC Port may determine another FC Port's R_T_TOV value using the Read Timeout Value (RTV) ELS.
	Override	If selected, error detection overrides 10,000 milliseconds.
	Obtain From Login	If selected, obtains response from login ID.

FCM Port Properties—Auto Instrumentation

The FCM *Auto Instrumentation* tab is accessed by right-clicking an FCM port in the *Explore Network Resources* pane, selecting the *Port Properties* menu options, then selecting the *General* tab.

The FCM Port Properties *Auto Instrumentation* tab is shown in *Figure:FCM—Auto Instrumentation tab*.

Figure:FCM—Auto Instrumentation tab



The controls for FCM *Auto Instrumentation* tab configuration are described in *Table:Auto Instrumentation Configuration*.

Table:Auto Instrumentation Configuration

Section	Control/Field
End of Frame Timestamp / Data Integrity	This field is disabled for Fibre Channel load module.
Floating Timestamp / Data Integrity	The timestamp is part of Automatic Instrumentation header. This mode should be used when the packet may get truncated or has padding.

Chapter 24 - Port Properties–Xcellon-Flex Family

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the port properties of the Xcellon-Flex card family. The cards belonging to this family are FlexAP10G16S and FlexFE10G16S. FlexAP10G16S is a 10 Gigabit Ethernet L2–L7 Accelerated Performance Load Module. It has a 16-port LAN, SFP+ interface. FlexFE10G16S is a 10 Gigabit Ethernet L2–L3 Full Emulation Load Module. It has a 16-port LAN, SFP+ interface.

Port Properties for Flex Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the FlexAP10G16S and FlexFE10G16S type boards is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for Flex modules (Xcellon-Flex family):

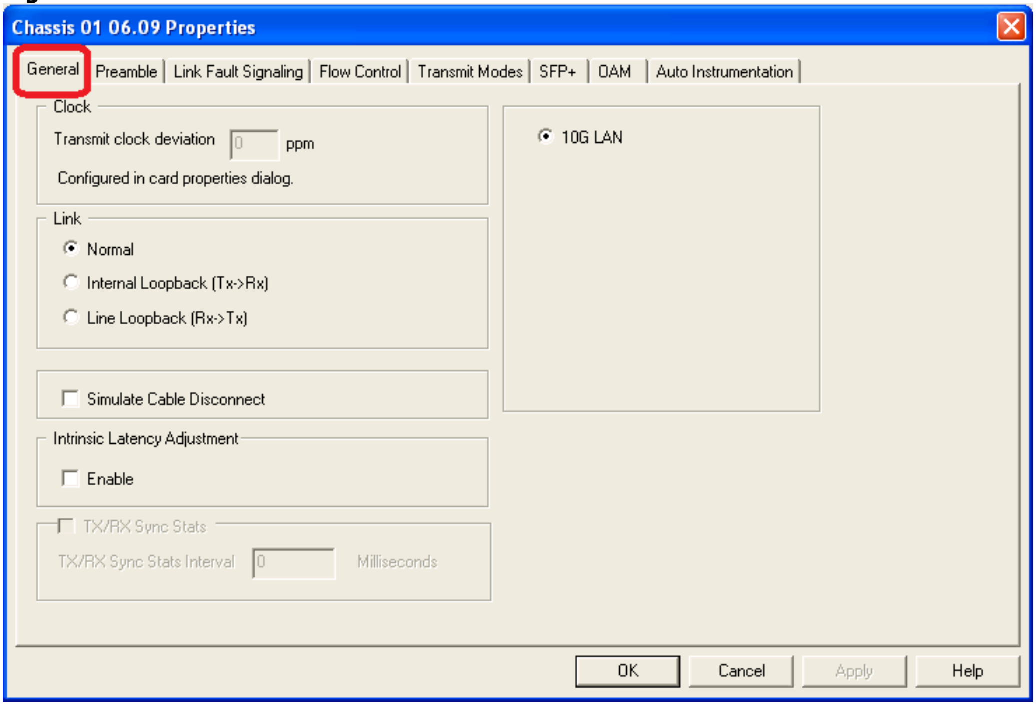
- *Flex Port Properties—General*
- *Flex Port Properties—Preamble*
- *Flex Port Properties—Link Fault Signaling*
- *Flex Port Properties—Flow Control*
- *Flex Port Properties—Transmit Modes*
- *Flex Port Properties—SFP+*
- *Flex Port Properties—OAM*
- *Flex Port Properties—Auto Instrumentation*
- *Flex Port Properties—QSFP*

Flex Port Properties—General

The Flex **General** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, and then selecting the **General** tab.

The Flex Port Properties **General** tab is shown in the following figure:

Figure:Flex—General tab



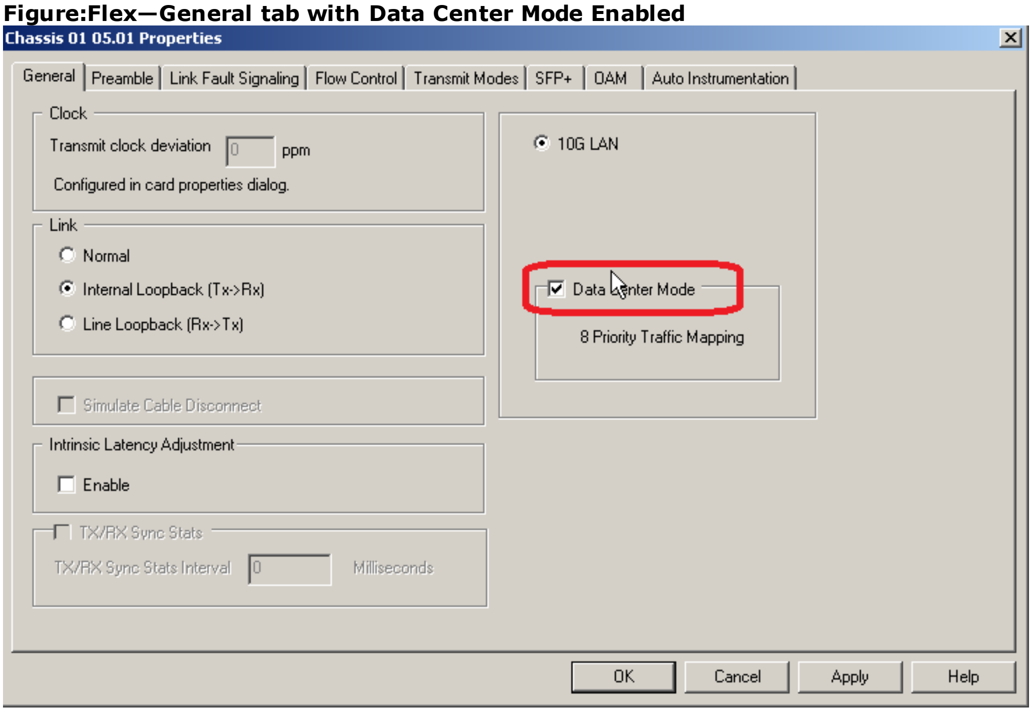
The controls for Flex **General** tab configuration are described in the following table:.

Table:General Configuration

Section	Control/Field	Usage
Clock	Transmit clock deviation	Shows the status of the transmit clock.
Link	Normal	Normal operation of the port.
	Internal Loopback (Tx->Rx)	If selected, enables the Internal Loopback-Transmit to Receive.
	Line Loopback (Rx->Tx)	If selected, enables the Line Loopback-Receive to Transmit.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	If selected, enables the intrinsic latency adjustment. The **Enable** check box is disabled when no value exists in the system for the specific transceiver. It is available if a value exists (in the xml file).
TX/RX Sync Stats	TX/RX Sync Stats Interval	This field is disabled for Flex load module.

The General tab for Flex card with Data Center Mode enabled is shown in the following figure:

Figure:Flex—General tab with Data Center Mode Enabled



Flex Port Properties—Preamble

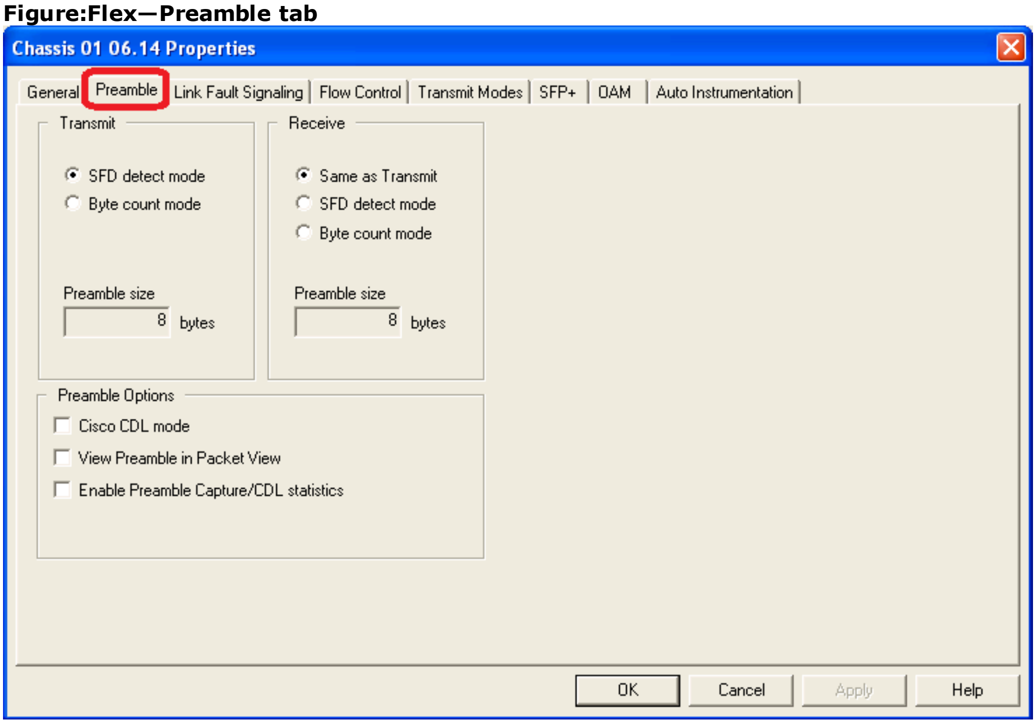
The Flex **Preamble** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Preamble** tab.

The Flex Preamble tab allows to select the method for detecting the start of a frame. The preamble precedes the frame, but is not part of the frame itself, so a method must be used to determine the first of the bytes making up the frame itself -SFD detect mode or Byte count mode.

The choice in this tab for transmitted frames is reflected in the **Frame Data** tab in the **Stream Properties** dialog. The number of configurable bytes in the preamble depends on the start-of-frame mode. Ethernet Frames for additional information.

The Flex Port Properties **Preamble** tab is shown in the following figure:

Figure:Flex—Preamble tab



The controls for Flex **Preamble** tab configuration are described in the following table:.

Table:Preamble Configuration

Section	Control/Field	Usage
Transmit	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case), and considers the next byte (9th) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the **Frame Data** tab in the **Stream Properties** dialog. This value is currently fixed at 8 bytes (the default).
Receive	Same as Transmit	The Receive side accepts the same choices/entries that were made for the Trans-mit side.
	SFD detect mode	The Start of Frame Descriptor (SFD) is the last byte in the preamble (the 8th byte, in this case). This mode checks for the first occurrence of the SFD byte. The next byte is considered the start of the frame.
	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case) and considers the next byte (9th byte) the first byte of the frame.

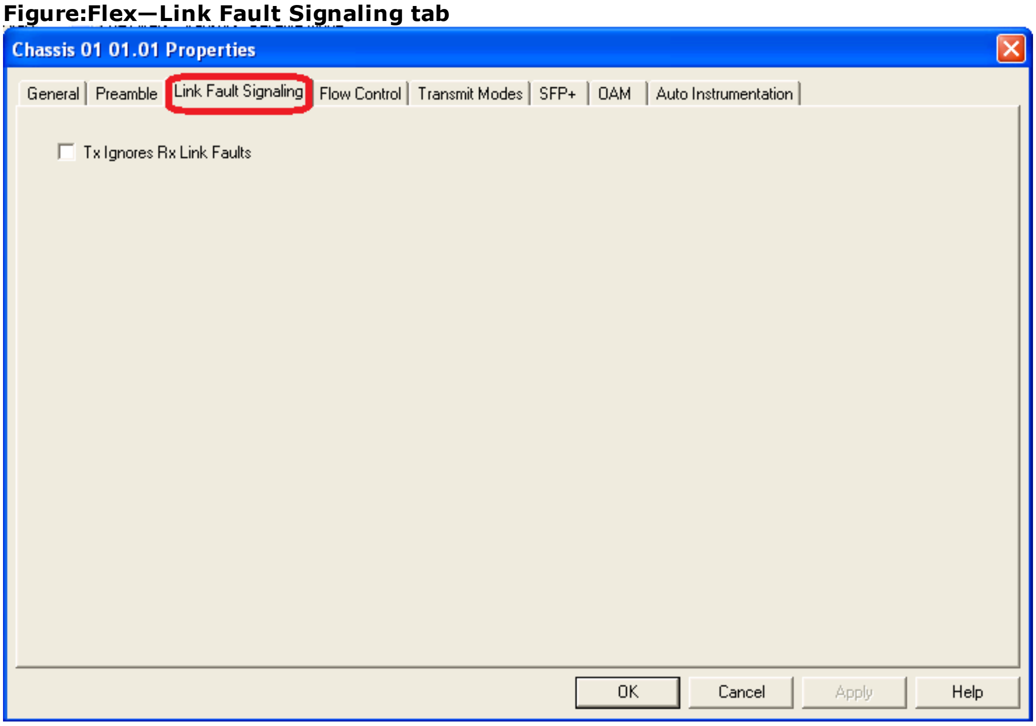
Section	Control/Field	Usage
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the **Frame Data** tab in the **Stream Properties** dialog. This value is currently fixed at 8 bytes (the default).
Preamble Options	Cisco CDL Mode	Enables the use of Cisco's Converged Data Link (CDL) packets, which substitutes the six preamble bytes and the SFD byte with a specific seven byte CDL header. Selecting this option disables the Transmit SFD detect mode.
	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side).
	Enable Preamble Capture/CDL statistics	When this check box is selected, the preamble is included for all packets captured through capture engine and will enable passing preamble data through Rx engine in order for CDL statistics to function.

Flex Port Properties—Link Fault Signaling

The Flex **Link Fault Signaling** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Link Fault Signaling** tab.

The Flex Port Properties **Link Fault Signaling** tab for Xcellon-Flex cards other than Xcellon FlexAP10/4016SQ is shown in the following figure:

Figure:Flex—Link Fault Signaling tab



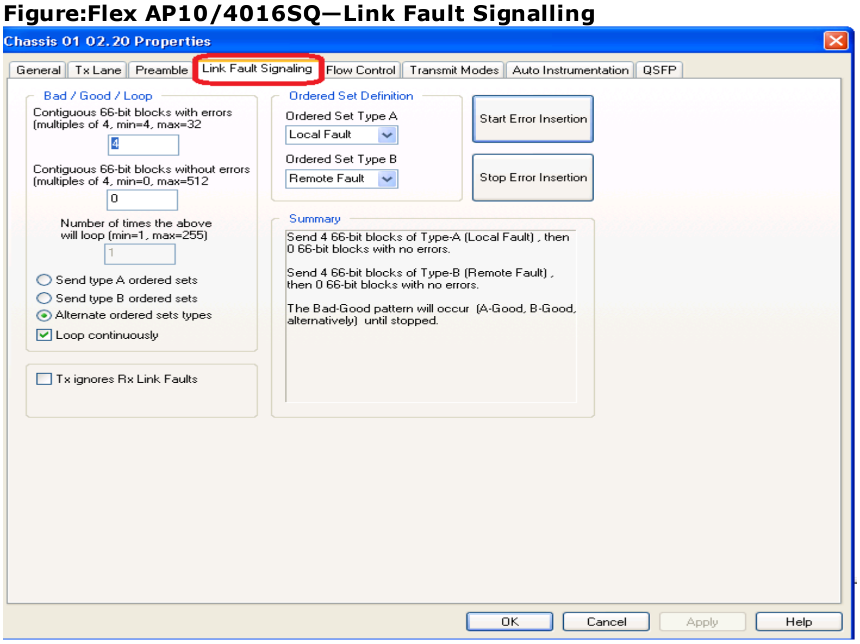
The controls for Flex **Link Fault Signaling** tab configuration are described in the following table:.

Table:Link Fault Signaling Configuration

Section	Field/Control	Description
Link Fault Signaling	Tx Ignores Rx Link Faults	If selected, ongoing transmission continues even if Link Fault messages are received by the sending RS.

The Flex Port Properties **Link Fault Signaling** tab for Xcellon FlexAP10/4016SQ is shown in the following figure:

Figure:Flex AP10/4016SQ—Link Fault Signalling



The controls for Flex **Link Fault Signaling** tab configuration are described in the following table:

Figure:Link Fault Signaling Configuration

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 0, max = 512)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive regular data sequences allowed are minimum 0 sequences

Section	Field/Control	Description
		and maximum 512 sequences.
	Number of times the above will loop (min = 1, max = 255)	Specifies the number of loops for the user defined sequence. There are two modes: • Discrete iterations: i) Minimum of 1 iteration ii) Maximum of 255 iterations • Continuous loop i) User cannot specify number of iterations
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets—A and B—are defined in the *Ordered Set Definition* box in this tab.) This pattern will be combined with the Good block-s/Bad blocks pattern for transmission. • Only Type A fault sequence and regular good data sequences • Only Type B fault sequence and regular good data sequences • Alternate Type A, regular good data sequences and Type B fault sequence, reg-ular good data sequences
	Loop continuously	If selected, the loop defined by the combination of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the *Stop Error Insertion* button is clicked. NOTE If fixed loop count is selected, and Send type A or Send type B is selec-ted, one loop iteration will consist of Error-Good pattern; if the Alternate ordered set types option is selected, one loop iteration will consist of Error-Good-Error-Good pattern.
Ordered Set Defin-ition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault
Tx ignores Rx Link Faults		If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.
Summary (Win-dow)		(Read-only) Displays descriptions of the patterns that will be transmitted.
Start Error Inser-		Press this button to start the transmission of the

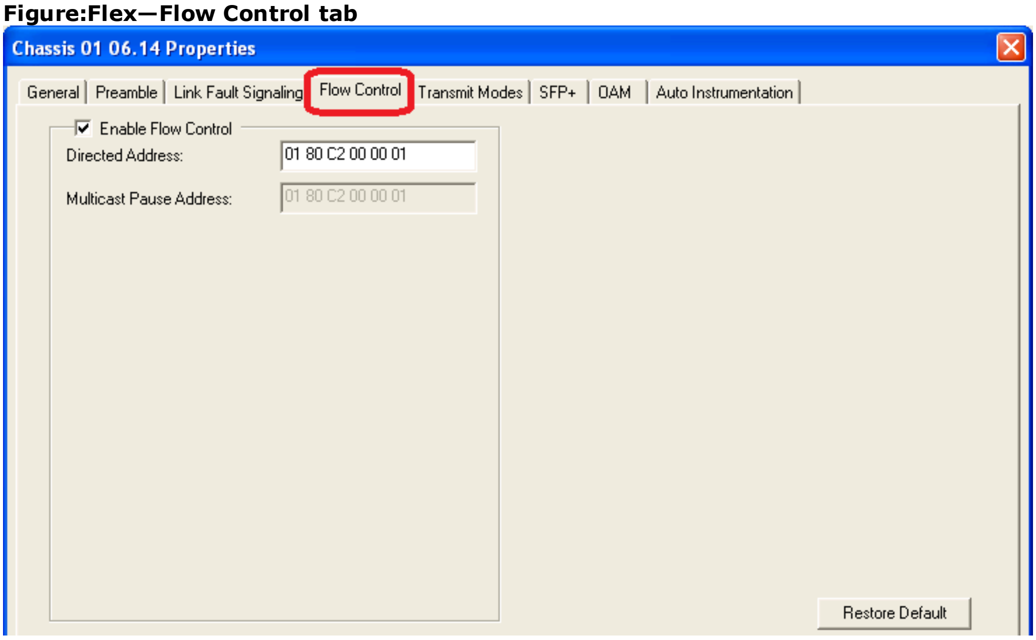
Section	Field/Control	Description
tion		configured error patterns.
Stop Error Insertion		(Available only for use with the *Loop continuously* option.) Press this button to stop the transmission of the configured error patterns.

Flex Port Properties—Flow Control

The Flex **Flow Control** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

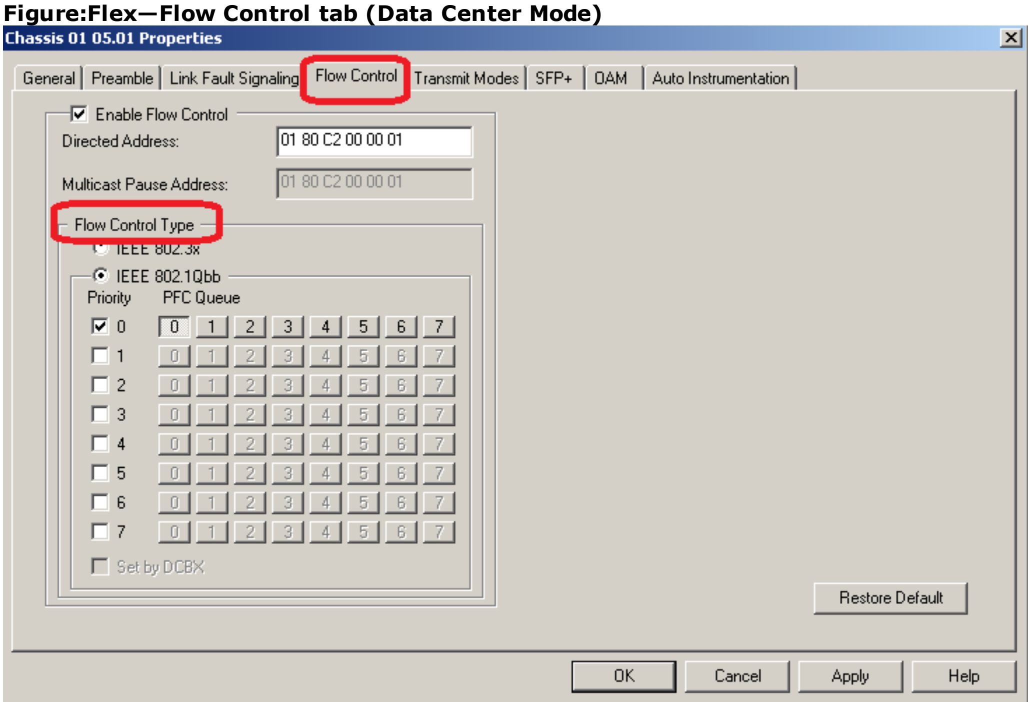
The Flex Port Properties **Flow Control** tab (non-Data Center Mode) is shown in the following figure:

Figure:Flex—Flow Control tab



The Flex Port Properties **Flow Control** tab (in Data Center Mode) is shown in the following figure:

Figure:Flex—Flow Control tab (Data Center Mode)



The controls for Flex **Flow Control** tab configuration are described in the following table:

Table:Flow Control Configuration

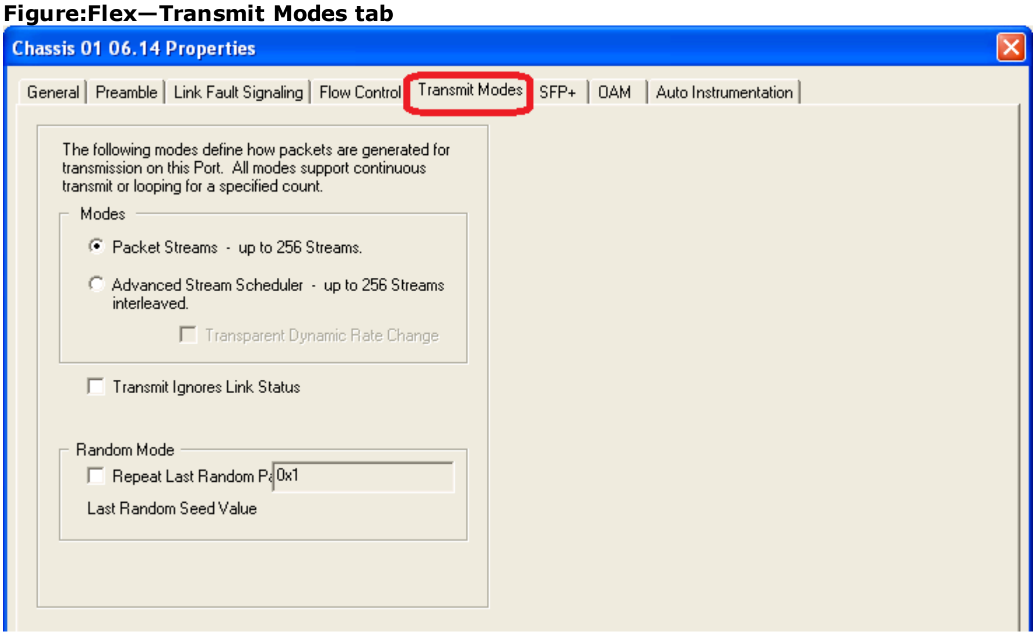
Section	Field/Control	Description
Enable Flow Control	(check box)	If selected, enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port listens on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port listens on for a multicast pause message.
Flow Control Type	IEEE 802 3x IEEE 802.1Qbb	When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
Priority		When flow control type IEEE 802.1Qbb is selected in Data Center mode, priority options are the channels of data that can be paused. Click to select one or more channels.
PFC Queue		The PFC Queue can be mapped to the priority field in the frame.

Flex Port Properties—Transmit Modes

The Flex **Transmit Modes** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Transmit Modes** tab.

The Flex Port Properties **Transmit Modes** tab is shown in the following figure:

Figure:Flex—Transmit Modes tab



The controls for Flex **Transmit Modes** tab configuration are described in the following table:.

Table:Transmit Modes Configuration

Section	Control/Field	Usage
Modes	Packet Streams	Sets the basic operating mode for the port to sequential packet streams. A stream is programmed for continuous packet generation for generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets up the transmission of interleaved packet streams. FlexAP10G16S card supports up to 512 streams and FlexFE10G16S card supports up to 256 streams. In Data Center Mode it supports up to 256 streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
	Transparent Dynamic Rate Change	If selected, the dynamic rate control allows rate change across counters, for this port.
	Transmit Ignores Link Status	If selected, allows transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	If selected, causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This is used before transmission (in which case the seed from the first packet stream is used),

Section	Control/Field	Usage
		or immediately after a stream is sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware uses to seed its random number generators. NOTE It is not a one-to-one mapping

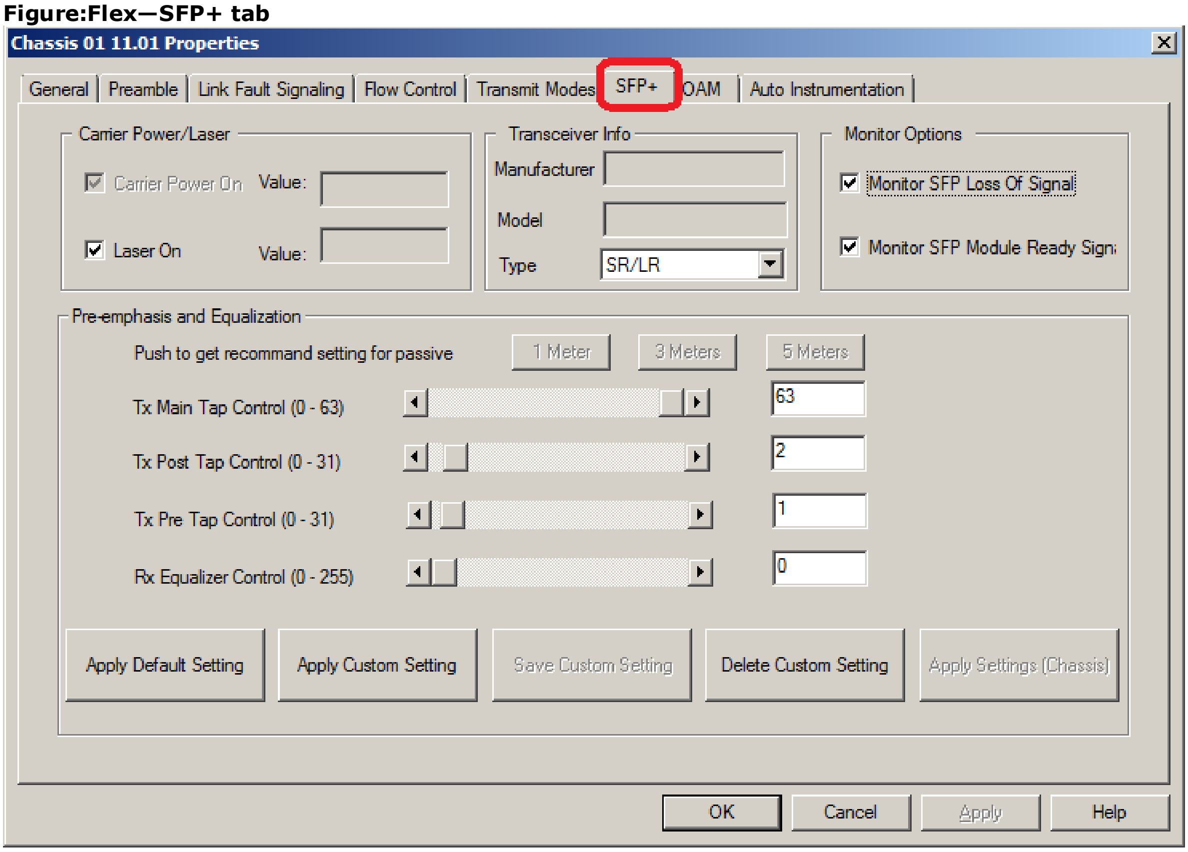
Flex Port Properties—SFP+

The Flex **SFP+** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **SFP+** tab.

SFP+ interfaces allow to set the carrier and laser power settings, the transceiver type, and the monitor options.

The Flex Port Properties **SFP+** tab is shown in the following figure:.

Figure:Flex—SFP+ tab



The controls for Flex **SFP+** tab configuration are described in the following table:

Table:SFP+ Configuration

Section	Control/Field	Usage
Carrier Power/Laser	Carrier Power On	If selected, enables the carrier power. The actual reading is displayed in the Value field.
	Laser On	If selected, enables the laser power. Note that the actual reading is displayed in the Value field.
Transceiver info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
	Type	Automatically detect which kind of cable is connected or plugged in. Also it can be set manually.
Monitor Options	Monitor SFP Loss of Signal	If selected, indicates the interface to conform to SFP specifications. It requires the absence of a Loss of Signal for transmitting and receiving.
	Monitor SFP Module Ready Signal	If selected, indicates the interface to conform to SFP specifications. It requires the detection of a Module Ready signal for transmitting and receiving.
Tranceiver Type	Automatic Detect	Automatically detect Manufacturer name and Model.
	Type	Automatically detect. Also can be set manually.
Pre-emphasis and Equalisation	Push to get recommended setting for passive	This will be disabled on Flex.
	Tx Main Tap Control (0-63)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-31)	This helps to control the Post Tap value for Tx.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Rx Eqalizer Control (0-255)	This helps to control the Equalizer value for Rx..
	Apply Default Settings	If clicked, a default setting will be applied to the current user setting for the current adapter-/xcvr type and to the actual hardware.
	Apply Custom Settings	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the

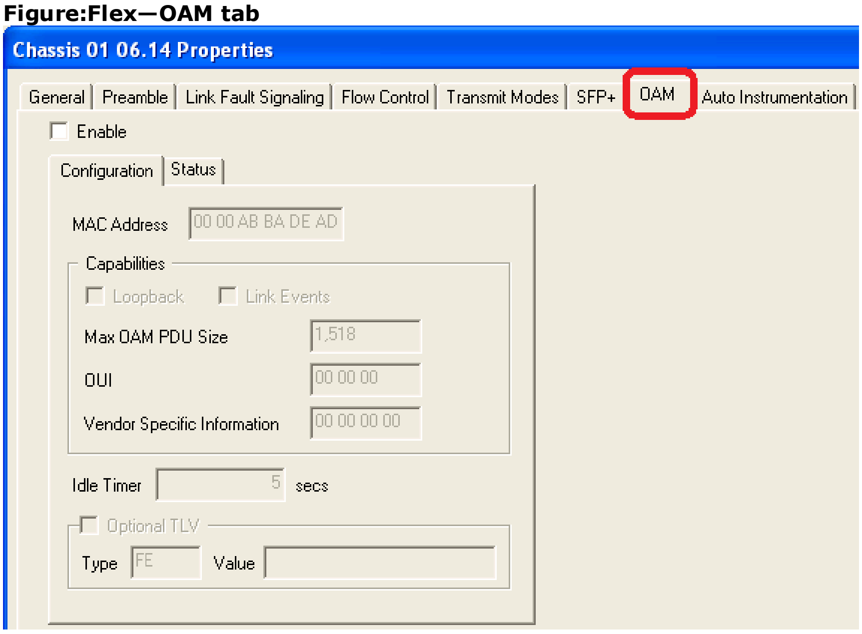
Section	Control/Field	Usage
		xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Flex Port Properties—OAM

The Flex **OAM** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **OAM** tab.

The Flex Port Properties **OAM** tab is shown in the following figure:

Figure:Flex—OAM tab



The Operations, Administration, and Maintenance (OAM) sublayer provides mechanisms useful for monitoring link operation such as remote fault indication and remote loopback control. In general, OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAM PDUs). OAM PDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links.

The controls for Flex **OAM** tab configuration are described in the following table:

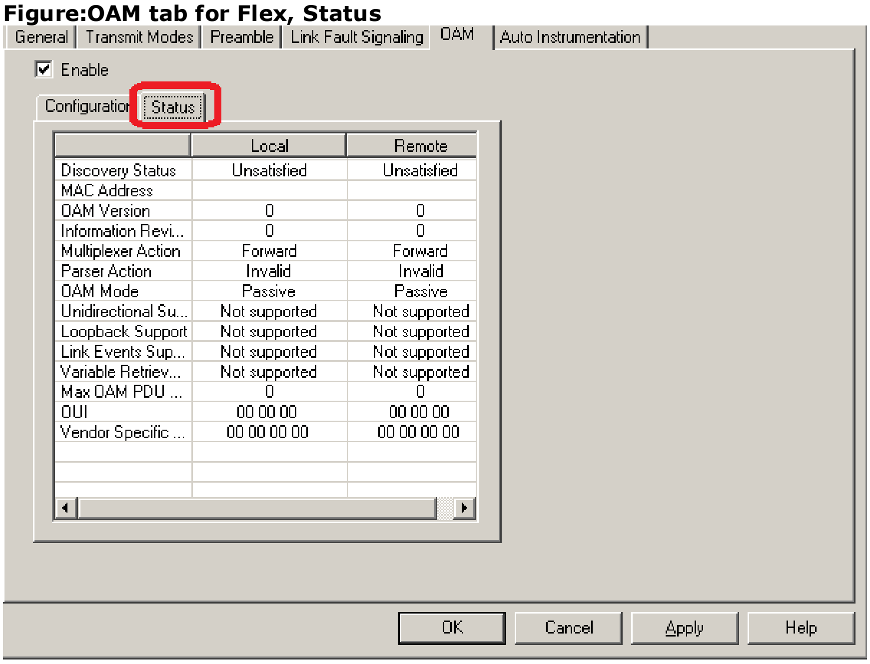
After making configuration changes, click **Apply** to send the changes to the chassis without leaving the tab. Click **OK** to send changes and close the Properties window.

Table:OAM Configuration

Section	Field/Control	Description
	Enable	Enables and starts OAM state machine configuration.
MAC Address		The individual source MAC address of the Ixia port acting as DTE (through which the OAM PDU is transmitted).
Capabilities	Loopback	Advertises OAM remote loopback capability.
	Link Events	Advertises link event capability.
	Max OAM PDU Size	11-bit field which represents the largest OAM PDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.
	OUI	24-bit 3-octet field, Organizationally Unique Identifier. Example: 00 00 00.
	Vendor Specific Information	4-octet field, 32-bit identifier that may be used to differentiate a vendor's product models/versions.
Idle Timer		local_lost_link_timer Timer used to reset the Discovery state. Duration: 5 sec ± 10%.
Optional TLV	Type	This is any Information TLV that you want to send. This one-octet field indicates the nature of the data carried in this TLV-tuple. • 0x00 End of TLV marker • 0x01 Local Information • 0x02 Remote Information • 0x03-0xFD Reserved - shall not be transmitted, should be ignored on reception by OAM client • 0xFE Organization Specific Information • 0xFF Reserved - shall not be transmitted, should be ignored on reception by OAM client
	Value	This field indicates the value of the Information TLV. This field's length and contents are unspecified.

The OAM Status tab is shown in the following figure:

Figure:OAM tab for Flex, Status



The fields and controls in the **Status** tab are described in the following table. For each category, there is both a Local and a Remote status indicator.

Table:OAM Status tab

Field/Control	Description
Discovery Status	Detects the presence of an OAM sublayer at the remote DTE.
MAC Address	Defined in *Table:OAM Configuration*.
OAM Version	This one-octet field indicates the version supported by the DTE. This field always contains the value 0x01.
Information Revision	This two-octet field indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes.
Multiplexer Action	Forward (0) = Device is forwarding non-OAMPDUs to the lower sublayer (= FWD). Discard (1) = Device is discarding non-OAMPDUs (local_mux_action = DISCARD).
Parser Action	00 = Device is forwarding non-OAMPDUs to higher sublayer (local_par_action = FWD). 01 = Device is looping back non-OAMPDUs to the lower sublayer (local_par_action = LB). 10 = Device is discarding non-OAMPDUs (local_par_action = DISCARD). 11 = Reserved. In Local Information TLVs, this value shall not be sent.

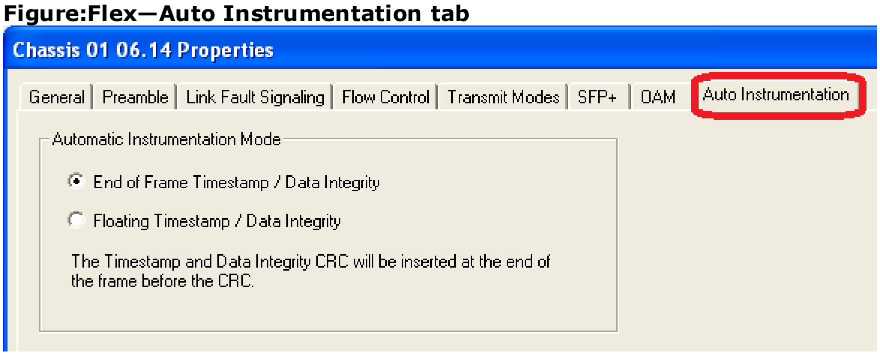
Field/Control	Description
	If the value 11 is received, it should be ignored and not change the last received value.
OAM Mode	1 = DTE configured in Active mode. 0 = DTE configured in Passive mode.
Unidirectional Support	1 = DTE is capable of sending OAMPDUs when the receive path is non-operational. 0 = DTE is not capable of sending OAMPDUs when the receive path is non-operational.
Loopback Support	Defined in *Table:OAM Configuration*.
Link Events Support	Defined in *Table:OAM Configuration*.
Variable Retrieval Support	1 = DTE supports sending Variable Response OAMPDUs. 0 = DTE does not support sending Variable Response OAMPDUs.
Max OAM PDU Size	Defined in *Table:OAM Configuration*.
OUI	Defined in *Table:OAM Configuration*.
Vendor Specific Information	Defined in *Table:OAM Configuration*.

Flex Port Properties—Auto Instrumentation

The Flex **Auto Instrumentation** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The Flex Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure:Flex—Auto Instrumentation tab



The options and controls in this tab are described in the following table.

Table:Auto Instrumentation Configuration

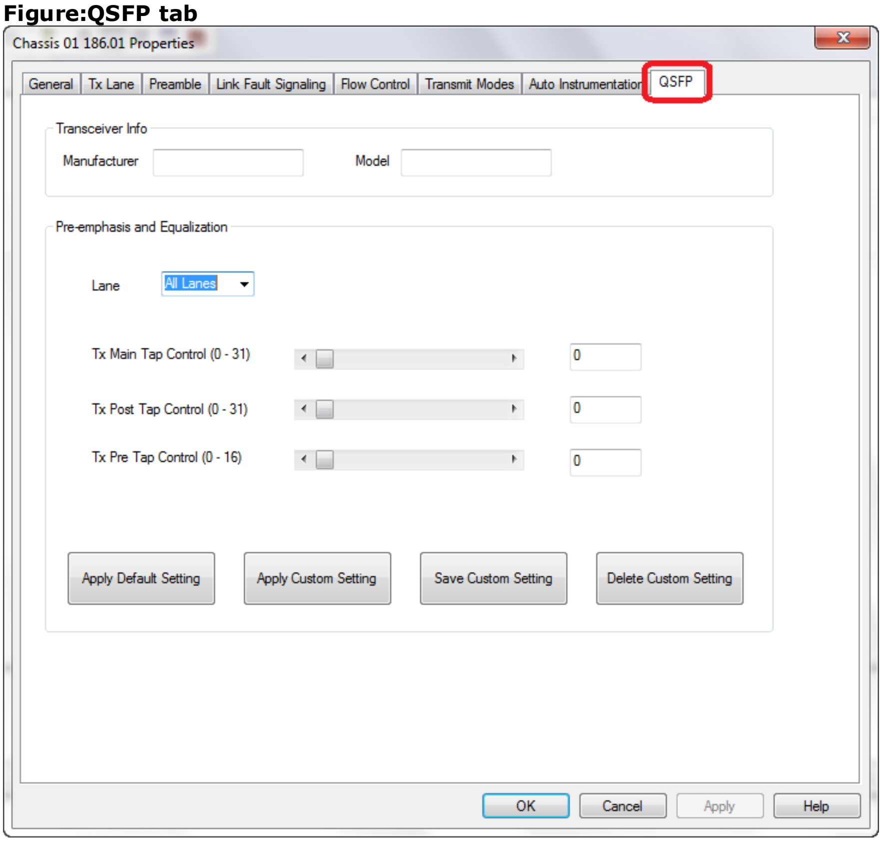
Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Flex Port Properties—QSFP

The Flex **QSFP** tab is accessed by right-clicking a Flex port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **QSFP** tab.

The Flex Port Properties **QSFP** tab is shown in the following figure:

Figure:QSFP tab



The options and controls in this tab are described in the following table.

Table:QSFP Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
Pre-emphasis and Equalization		
	Lane	Specifies in which lane (from 0-3) the current settings are.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-31)	This helps to control the Post Tap value for Tx.

Section	Field/Control	Description
	Tx Pre Tap Control (0-16)	This helps to control the Pre Tap value for Tx.
	Apply Default Setting	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hardware.
	Apply Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

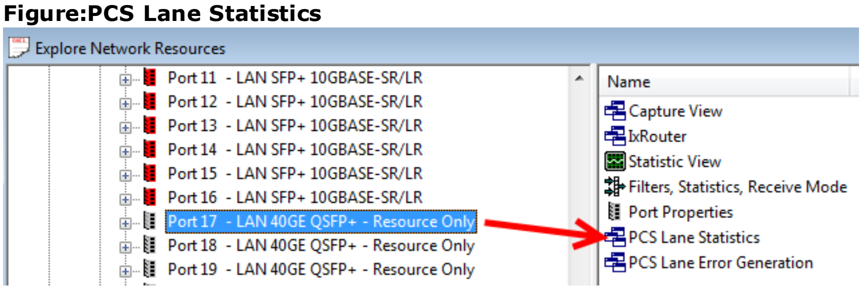
PCS Lane Statistics for Flex modules

The PCS Lane Statistics are available for FlexAP1040SQ 4GE QSFP load modules. The PCS Labe Statistics table allows you to view the statistics for the configured PCS lanes. It is part of the Port Properties for the module.

To open the PCS Lane Statistics table:

1. Select the FlexAP1040SQ Load module in the left pane of the IxExplorer window.
2. Expand the node, and select the Port object. In the right window pane, double-click the PCS Lane Statistics object as shown in the following figure:

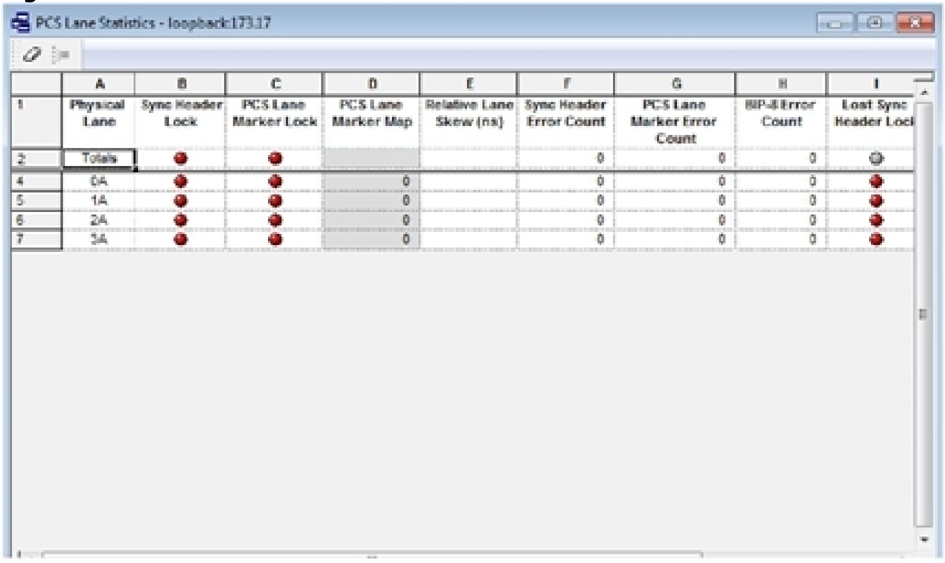
Figure:PCS Lane Statistics



The PCS Lane Statistics table opens. Use this table to view the PCS lane statistics for each lane. The statistics are for the **receive** side.

The PCS Lane Statistics table is shown in the following figure:

Figure:PCS Lane Statistics table



The following table explains the entries in the PCS Lane Statistics table:

Table:PCS Lane Statistics Data

Field/Control	Description
Physical Lane	The identifier for the Receive physical lane. This is a tag /fixed label to ID each lane.
Sync Header Lock	Indicates if the received PCS lane achieved sync-bit lock. Green indicates success, red indicates failure.
PCS Lane Marker Lock	Indicates if the received PCS lane has achieved alignment marker lock. Green indicates success, red indicates failure.
PCS Lane Marker Map	The VL number identified by the alignment marker. This is only valid when VL Lock is green.
Relative Lane Skew (ns)	Shows the actual skew in nanoseconds. Skew measurements are valid only when all lanes are locked with 20 unique lane markers. The first VL markers to arrive have skew of 0. All other lane skews are relative to them.
Sync Header Error Count	The number of synchronization bit errors received.
PCS Lane Marker Error Count	The number of incorrect PCS lane markers received while in PCS lane lock state.
BIP-8 Error Count	The number of BIP-8 errors for a PCS lane. BIP-8 = Bit-Interleaved Parity with eight bit errors (BIP-8). Each bit in the BIP field is an even parity calculation over all previous selected bits of a PCS lane.

Field/Control	Description
Lost Sync Header Lock	When lit, indicates the loss of sync header lock since the last statistic was read. If colored gray, there is no error. If colored red, an error has occurred.
Lost PCS Lane Marker Lock	When lit, indicates the loss of PCS lane marker lock since the last statistic was read. If colored gray, there is no error. If colored red, an error has occurred.

Chapter 25 - Port Properties–XDM10G32S Load Module

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the port properties of the XDM10G32S load module.

Port Properties for XDM10G32S Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the XDM10G32S is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for XDM10G32S modules:

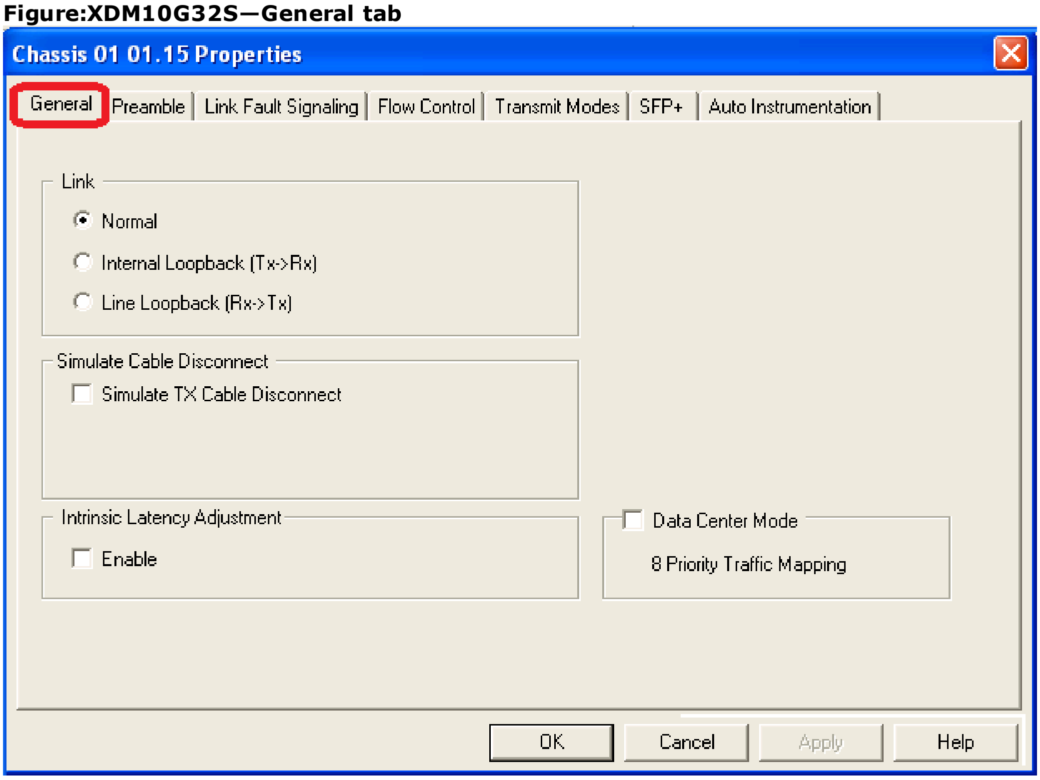
- *XDM10G32S Port Properties—General*
- *XDM10G32S Port Properties—Preamble*
- *XDM10G32S Port Properties—Link Fault Signaling*
- *XDM10G32S Port Properties—Flow Control*
- *XDM10G32S Port Properties—Transmit Modes*
- *XDM10G32S Port Properties—SFP+*

XDM10G32S Port Properties—General

The XDM10G32S **General** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, and then selecting the **General** tab.

The Port Properties **General** tab is shown in the following figure:

Figure:XDM10G32S—General tab



The controls for **General** tab configuration are described in the following table:

Table:General Configuration

Section	Control/Field	Usage
Link	Normal	Normal operation of the port.
	Internal Loopback (Tx->Rx)	If selected, enables the Internal Loopback-Transmit to Receive.
	Line Loopback (Rx->Tx)	If selected, enables the Line Loopback-Receive to Transmit.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	If selected, enables the intrinsic latency adjustment. The **Enable** check box is disabled when no value exists in the system for the specific transceiver. It is available if a value exists (in the xml file).
Data Center Mode		If selected, enables the Data Center Mode option. When Data Center Mode option is selected, the following changes take place: • The selected port is automatically placed into Advanced Stream mode. In this case, Packet Stream mode is not supported. • Only Auto Intrumentation mode (Floating

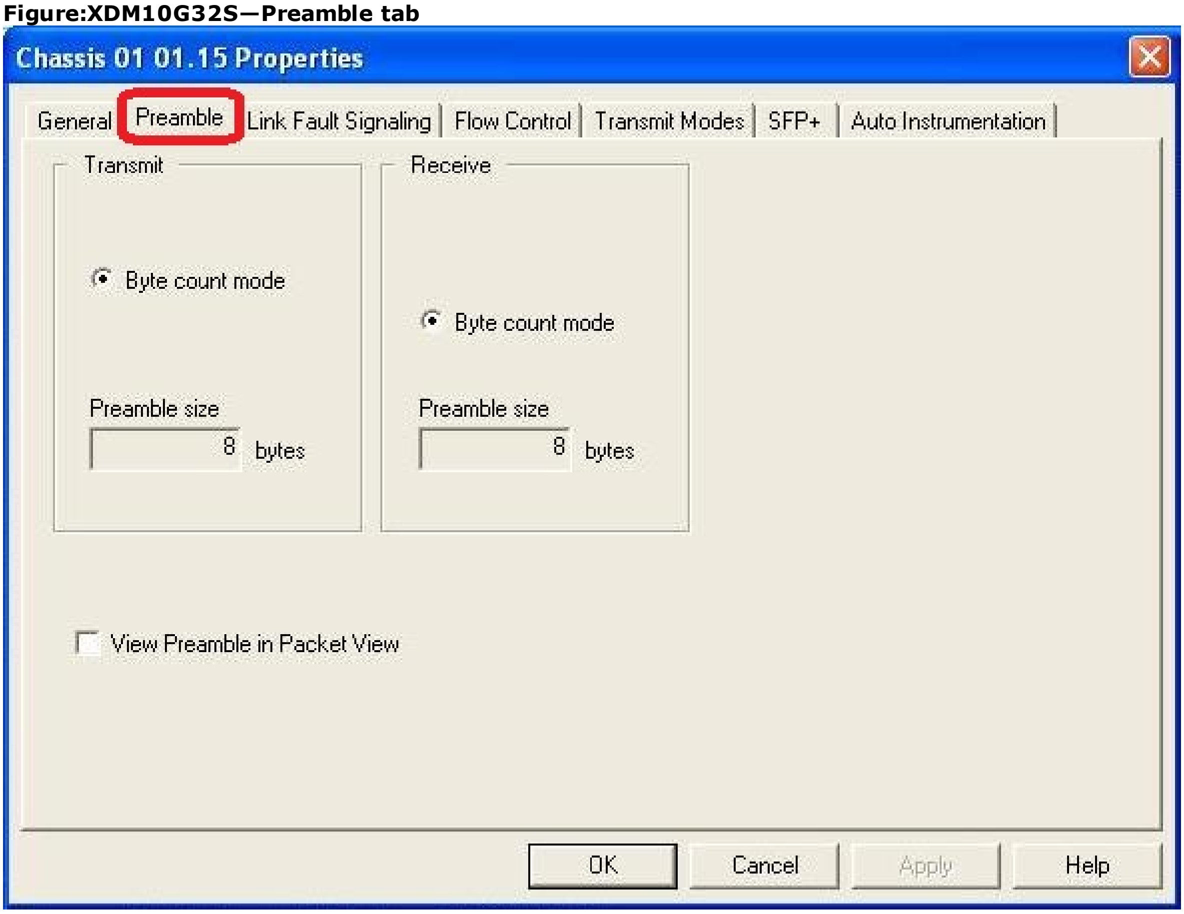
Section	Control/Field	Usage
		Timestamp/Data Integrity) is supported, both for transmit and receive. • 8-Priority Traffic Mapping is enabled. It supports various frame size for each PFC control (0-8). • FCoE protocol can be edited for Ethernet II and Ethernet Snap in Frame Data tab. NOTE XDM10G32S supports Advanced Stream Mode and Auto Instrumentation Mode even in non-Data Center Mode.

XDM10G32S Port Properties—Preamble

The XDM10G32S Preamble tab allows to select the method for detecting the start of a frame. The preamble precedes the frame, but is not part of the frame itself. In case of XDM10G32S load module, the frame is made up by Byte count mode. The **Preamble** dialog box of XDM10G32S module is shown in the following figure:

The XDM10G32S Port Properties **Preamble** tab is shown in the following figure:

Figure:XDM10G32S—Preamble tab



The controls for **Preamble** tab configuration are described in the following table:

Table:Preamble Configuration

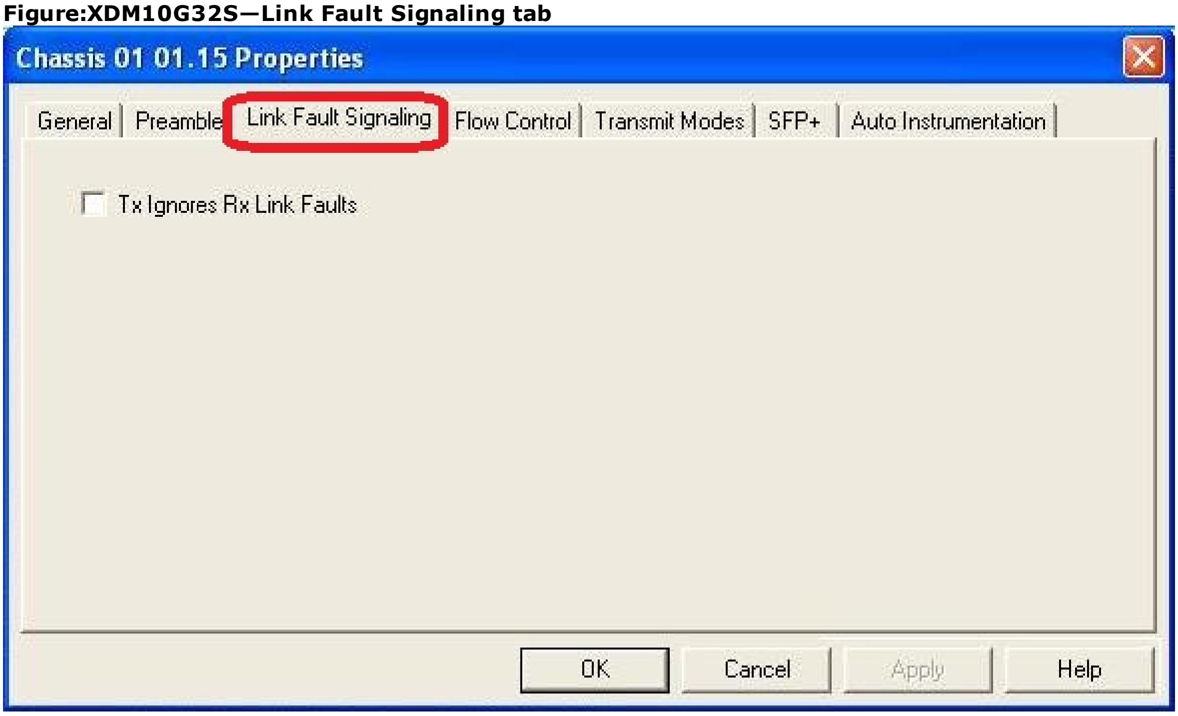
Section	Control/Field	Usage
Transmit	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case), and considers the next byte (9th) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the **Frame Data** tab in the **Stream Properties** dialog. This value is currently fixed at 8 bytes (the default).
Receive	Byte count mode	This mode counts the bytes of the preamble (8 bytes in this case) and considers the next byte (9th byte) the first byte of the frame.
	Preamble size (in bytes)	(Read-only) The length of the preamble, in bytes. This field shows the value set in the **Frame Data** tab in the **Stream Properties** dialog. This value is currently fixed at 8 bytes (the default).
Preamble Options	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side).

XDM10G32S Port Properties—Link Fault Signaling

The XDM10G32S **Link Fault Signaling** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Link Fault Signaling** tab.

The XDM10G32S Port Properties **Link Fault Signaling** tab is shown in the following figure:

Figure:XDM10G32S—Link Fault Signaling tab



The controls for **Link Fault Signaling** tab configuration are described in the following table:

Table:Link Fault Signaling Configuration

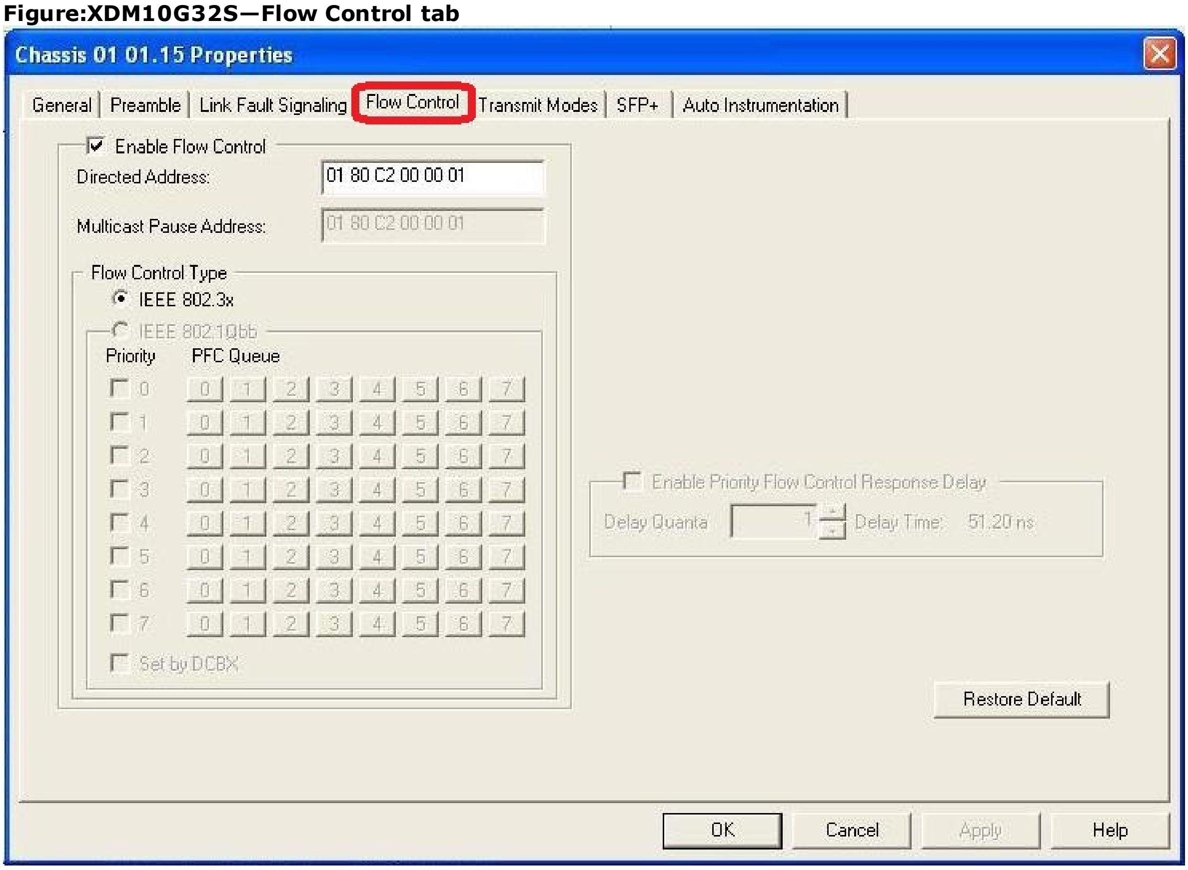
Section	Field/Control	Description
Link Fault Signaling	Tx Ignores Rx Link Faults	If selected, ongoing transmission continues even if Link Fault messages are received by the sending RS.

XDM10G32S Port Properties—Flow Control

The XDM10G32S **Flow Control** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

The Port Properties **Flow Control** tab is shown in the following figure:

Figure:XDM10G32S—Flow Control tab



The controls for **Flow Control** tab configuration are described in the following table:

Table:Flow Control Configuration

Section	Field/Control	Description
Enable Flow Control	(check box)	If selected, enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port listens on for a directed pause message.
	Multicast Pause	(Read-only) This is the MAC address that the port

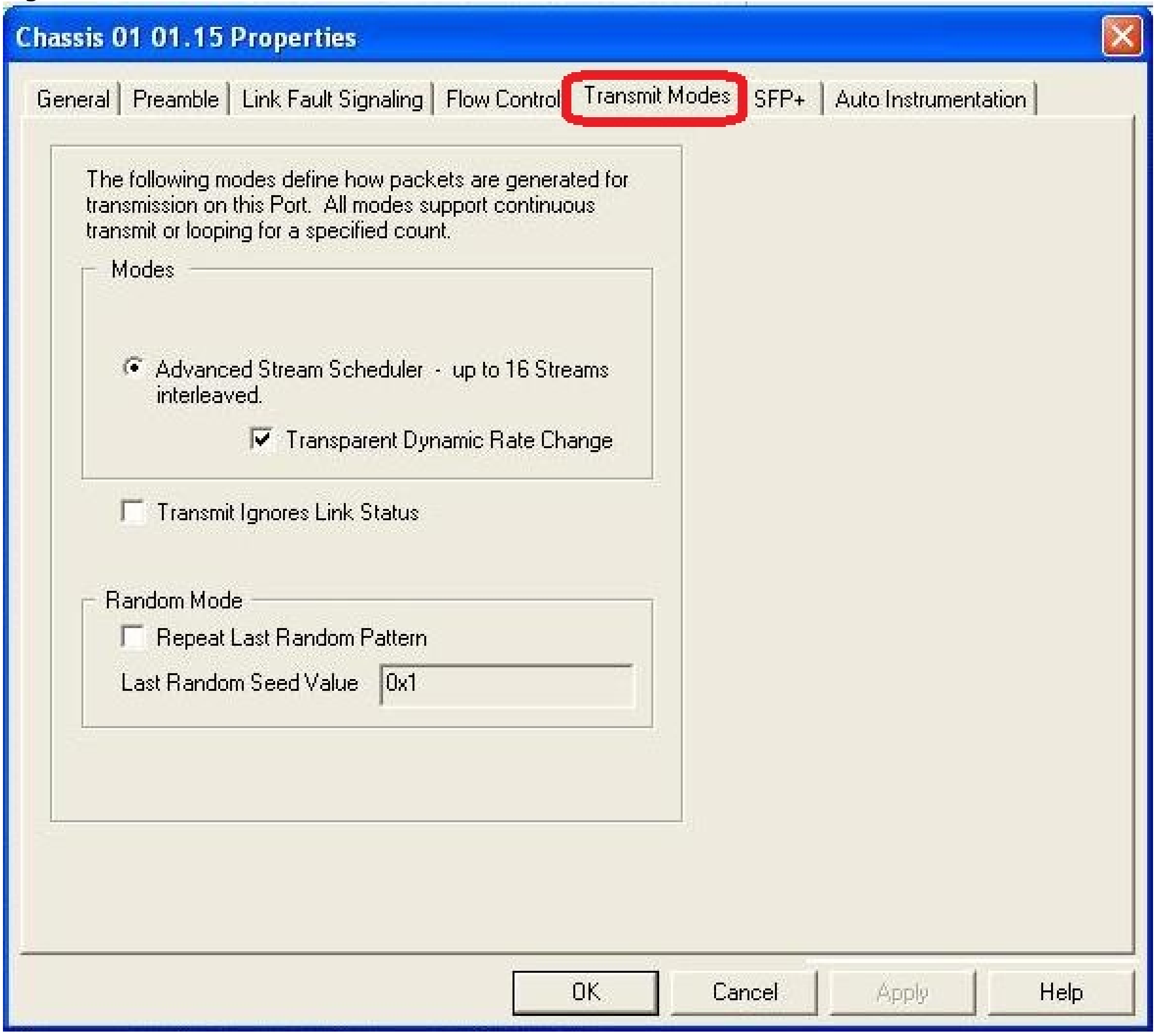
Section	Field/Control	Description
	Address	listens on for a multicast pause message.

XDM10G32S Port Properties—Transmit Modes

The XDM10G32S **Transmit Modes** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Transmit Modes** tab.

The Port Properties **Transmit Modes** tab is shown in the following figure:

Figure:XDM10G32S—Transmit Modes tab



The controls for **Transmit Modes** tab configuration are described in the following table:

Table:Transmit Modes Configuration

Section	Control/Field	Usage
Modes	Advanced Stream Scheduler	Sets up the transmission of interleaved packet streams up to 16 streams. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.

Section	Control/Field	Usage
	Transparent Dynamic Rate Change	If selected, the dynamic rate control allows rate change across counters, for this port.
	Transmit Ignores Link Status	If selected, allows transmission of packets even if the link is down.
Random Mode	Repeat Last Random Pattern	If selected, causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This is used before transmission (in which case the seed from the first packet stream is used), or immediately after a stream is sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware uses to seed its random number generators.

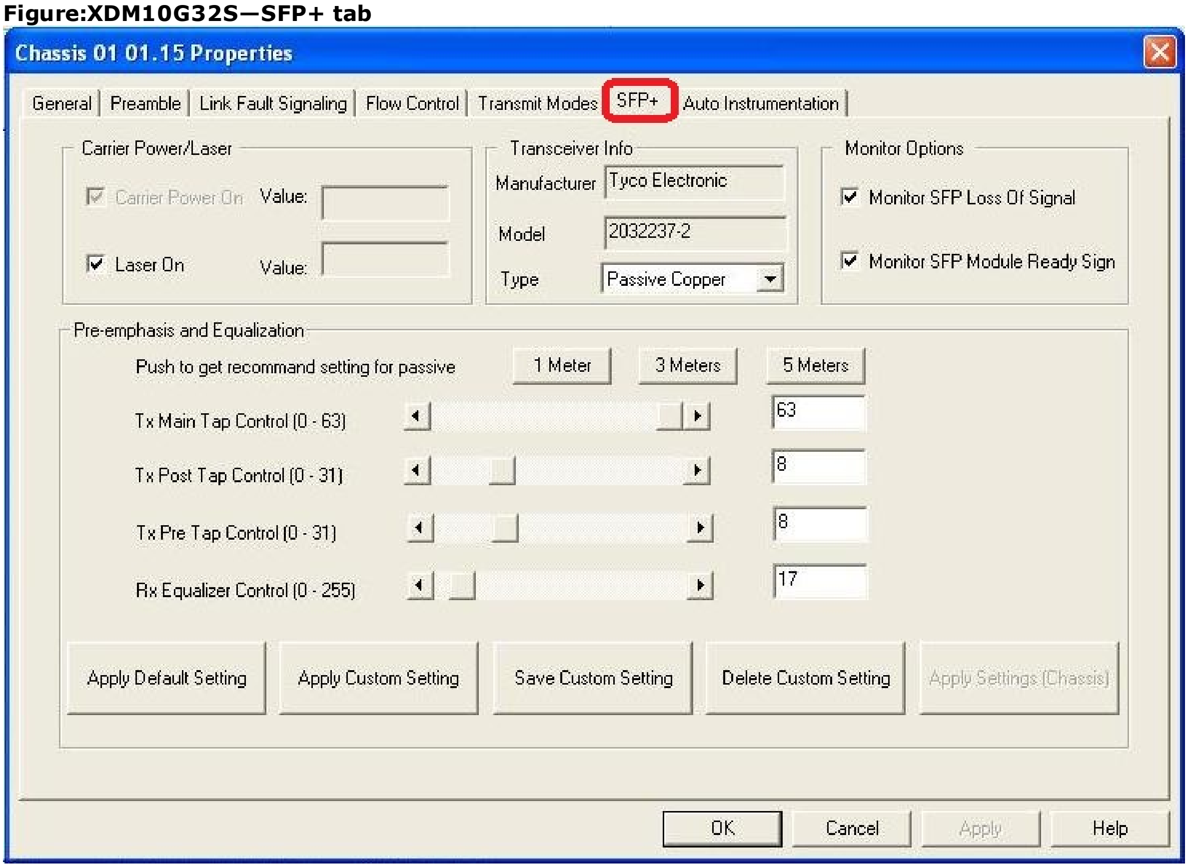
XDM10G32S Port Properties—SFP+

The XDM10G32S **SFP+** tab is accessed by right-clicking a X-density port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **SFP+** tab.

SFP+ interfaces allow to set the carrier and laser power settings, the transceiver type, and the monitor options.

The XDM10G32S Port Properties **SFP+** tab is shown in the following figure:

Figure:XDM10G32S—SFP+ tab



The controls for XDM10G32S **SFP+** tab configuration are described in the following table:

Table:SFP+ Configuration

Section	Control/Field	Usage
Carrier Power/Laser	Carrier Power On	If selected, enables the carrier power. The actual reading is displayed in the Value field.
	Laser On	If selected, enables the laser power. Note that the actual reading is displayed in the Value field.
Transceiver info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
	Type	Automatically detect which kind of cable is connected or plugged in. Also it can be set manually.
Monitor Options	Monitor SFP Loss of Signal	If selected, indicates the interface to conform to SFP specifications. It requires the absence of a Loss of Signal for transmitting and receiving.
	Monitor SFP Module Ready Signal	If selected, indicates the interface to conform to SFP specifications. It requires the detection of a Module Ready signal for transmitting and receiving.
Tranceiver Type	Automatic Detect	Automatically detect Manufacturer name and

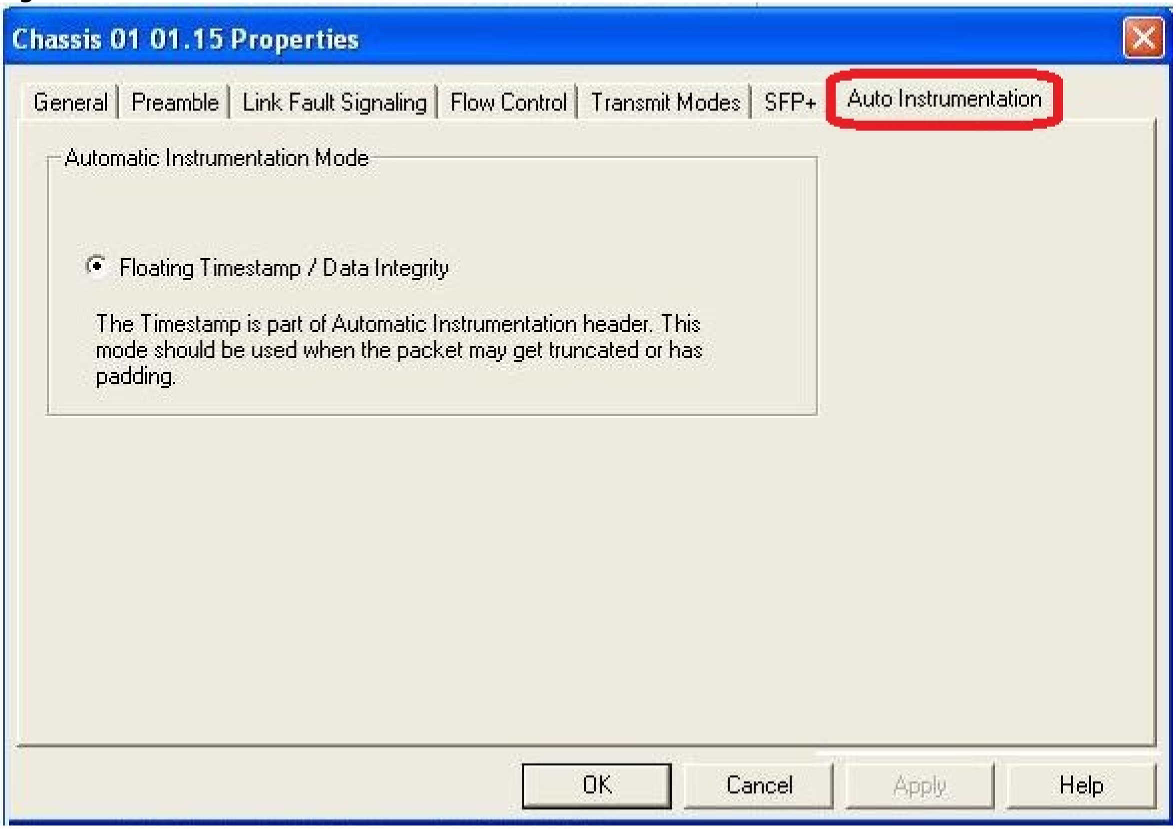
Section	Control/Field	Usage
		Model.
	Type	Automatically detect. Also can be set manually.
Pre-emphasis and Equalisation	Push to get recommended setting for passive	If selectd, default setting for 1/3/5 Meter will be applied to the current user setting for the current adapter/xcvr type and to the actual hardware.
	Tx Main Tap Control (0-63)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-31)	This helps to control the Post Tap value for Tx.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Rx Eqalizer Control (0-255)	This helps to control the Equalizer value for Rx.
	Apply Default Settings	If clicked, a default setting will be applied to the current user setting for the current adapter-/xcvr type and to the actual hardware.
	Apply Custom Settings	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The “TapConfigurations.xml” file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

XDM10G32S Port Properties—Auto Instrumentation

The XDM10G32S **Auto Instrumentation** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The XDM10G32S Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure:XDM10G32S—Auto Instrumentation tab



The options and controls in this tab are described in the following table:

Table:Auto Instrumentation Configuration

Field/Control	Description
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Chapter 26 - Port Properties–Xcellon-Lava Load Module

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the port properties of the Lava load module.

Port Properties for Lava Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the Lava is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for Lava modules:

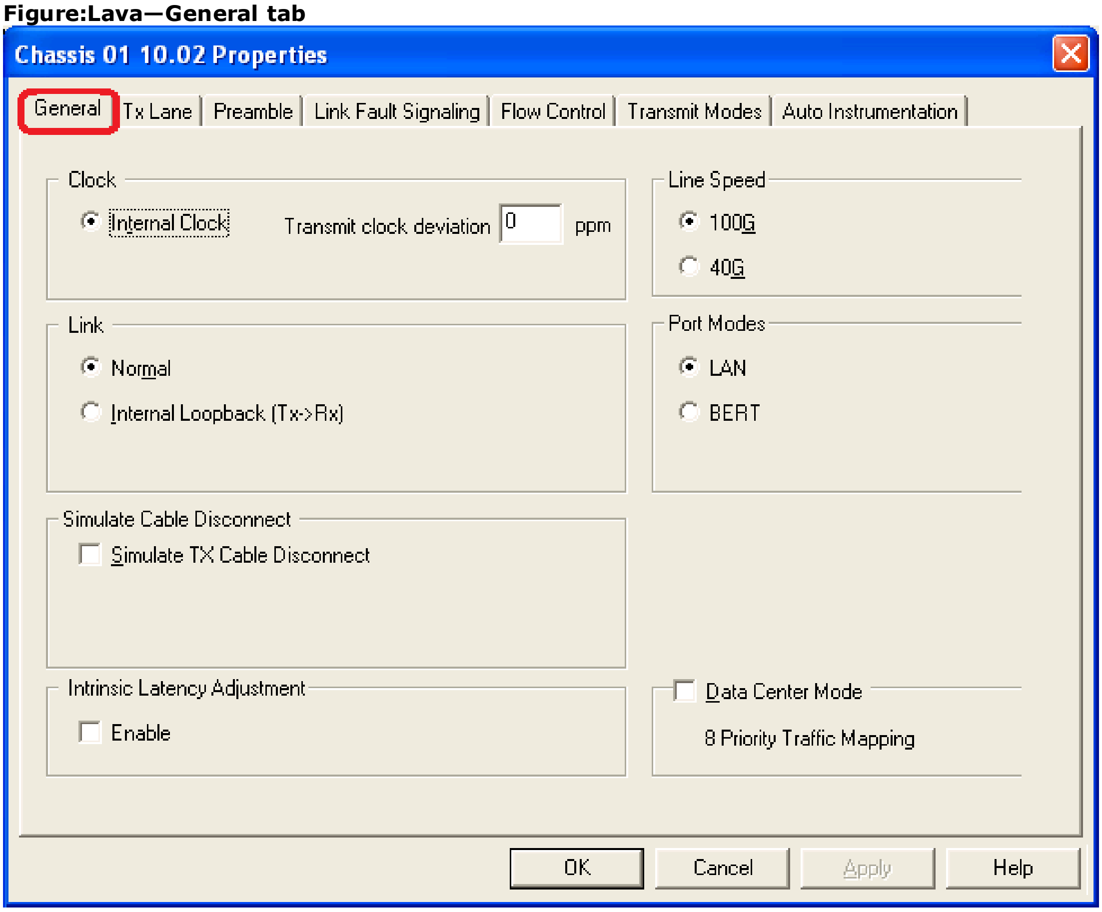
- *Lava Port Properties—General*
- *Lava Port Properties—TX-Lane*
- *Lava Port Properties—Preamble*
- *Lava Port Properties—Link Fault Signaling*
- *Lava Port Properties—Flow Control*
- *Lava Port Properties—Transmit Modes*
- *Lava Port Properties—Auto Instrumentation*
- *Lava Port Properties—CFPtoQSFP*
- *Lava Port Properties—CFPtoCXP*

Lava Port Properties—General

The Lava **General** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, and then selecting the **General** tab.

The Port Properties **General** tab is shown in the following figure:

Figure:Lava—General tab



The controls for **General** tab configuration are described in the following table:

Table:General Configuration

Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	Transmit Clock Deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port. 40/100 GE LSM cards can be adjusted from -100 to +100 ppm from the initial rate.
Link	Normal	Normal operation
	Internal Loopback (Tx -> Rx)	Internal Loopback—Transmit to Receive.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	Click to enable the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific transceiver. It is available if a value exists (in the .xml file).

Section	Control/Field	Usage
		For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
Line Speed		Select 100G or 40G
Port Modes		Select LAN or BERT. If BERT is selected, all the Port Properties tabs except *General* will disappear. *BERT Mode*.
Data Center Mode		Frame Data for FCoE Support.

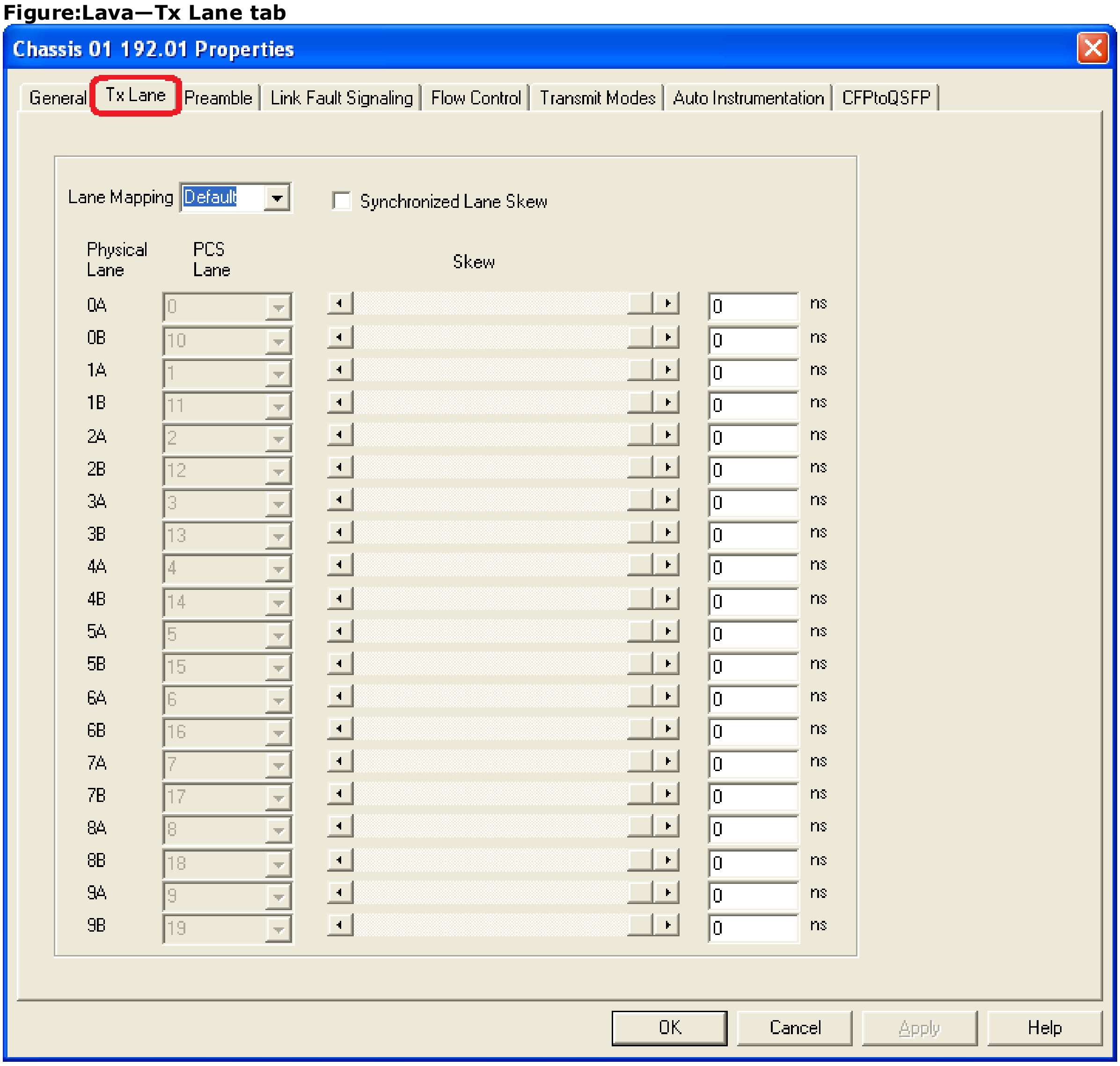
Lava Port Properties—TX-Lane

The *Tx Lane* tab allows to control the PCS lane order and skew rate for each lane.

For more information on Lane Skewing, see the Lane Skew topic in the ‘Multilane Distribution Configuration’ chapter of the *Ixia Platform Reference Manual*. The Lane Skew topic is located under ‘Types of Ports’ / ‘100GE’.

The Lava Port Properties *Tx Lane* tab is shown in the following figure:

Figure:Lava—Tx Lane tab



The controls for the *Tx Lane* tab configuration are described in the following table:

Table:Tx Lane Tab Configuration

Field	Description
Lane Mapping	Allows you to select a PCS lane ordering method. There are five options: • Default–the default ordering method. The default order is each physical port corresponds to 2 PCS lanes that are n and n+10, where n = physical lane number. • Increment–orders the lanes from 0 to 19, straight down the list. • Decrement–orders the lanes from 19 to 0, straight down the list. • Custom–allows to put the lanes in any order by manually entering the numbers in the fields. The starting order is the last selected mapping.

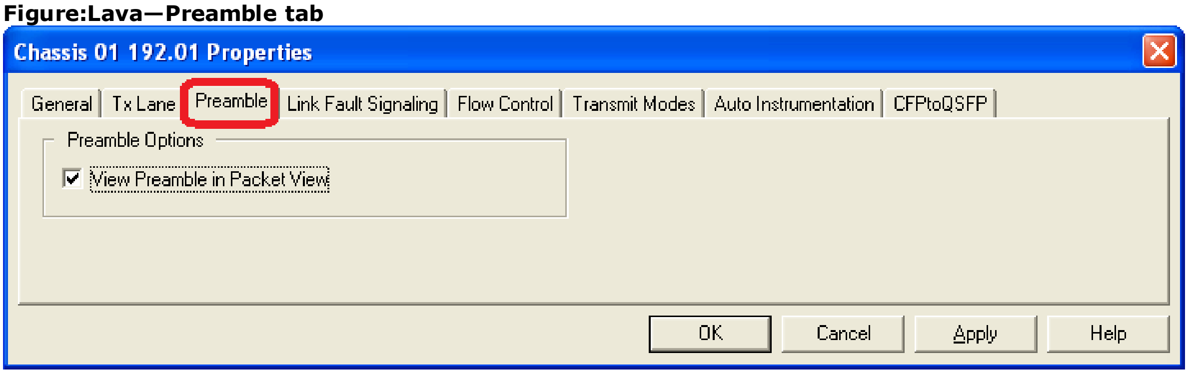
Field	Description
	• Random - Allows to put the lanes in any random order, values will be any value from 0 to 19.
Synchronized Lane Skew	All lanes are skewed by the same amount of skew.
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
PCS Lane	A number identifier for the PCS lane. The PCS lane is paired with a corresponding physical lane.
Skew	The skew slider is used to set a skew value for the PCS lane, in nanoseconds, on the transmit side. Lane Skew is the ability to independently delay one or more of the 20 PCS lanes. When the slider is moved, the nanoseconds field is correspondingly adjusted. You can also enter a nano second value directly into this field. When the slider is fully pushed to the right, the skew injected into the transmit stream is 0 (minimum). When the slider is pushed all the way to the left. the skew injected into the transmit stream is 3 uS (maximum).

Lava Port Properties—Preamble

The preamble precedes the frame, but is not part of the frame itself.

The Lava Port Properties **Preamble** tab is shown in the following figure:

Figure:Lava—Preamble tab



The fields and controls in this tab are described in the following table:

Table:Preamble Configuration

Section	Choices	Description
Preamble Options	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side).

Lava Port Properties—Link Fault Signaling

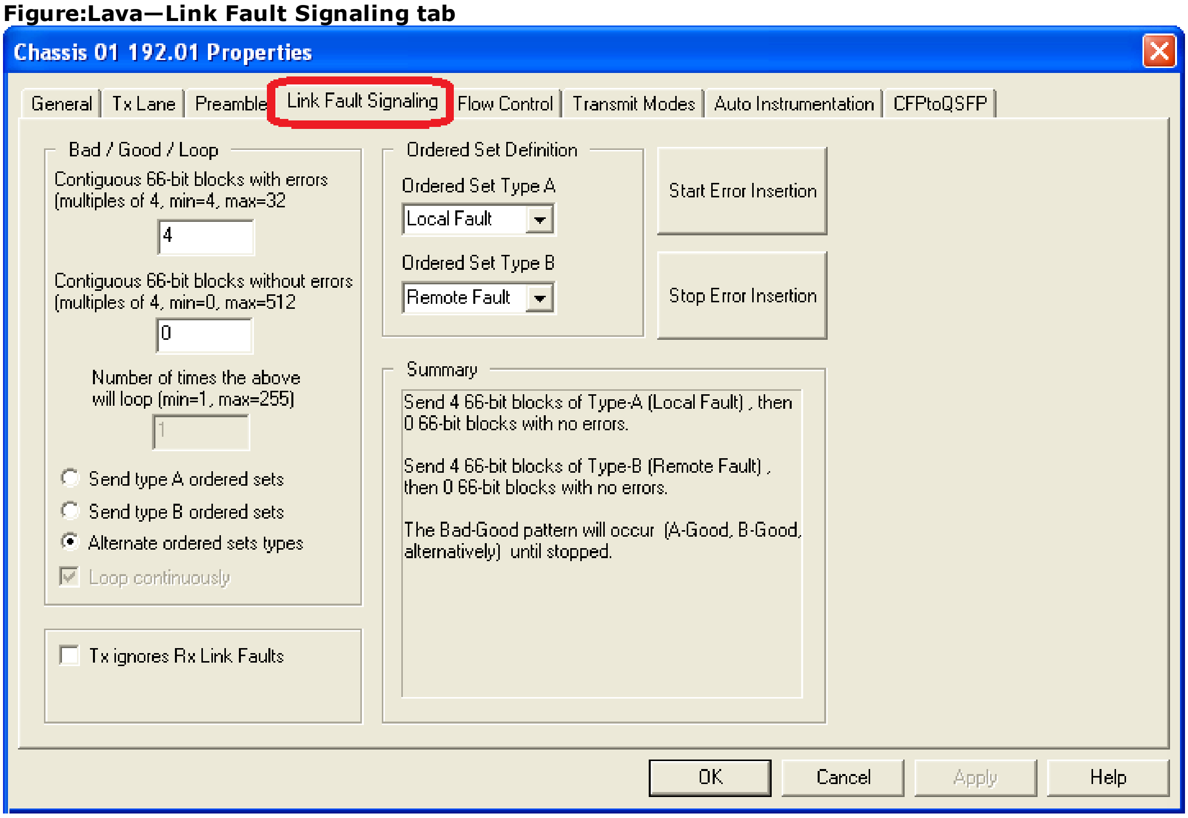
Link Fault Signaling is defined in Section 81.3.3.3 of the IEEE 802.3ba specification for 40 Gb/s and 100 Gb/s Ethernet. Link Fault Signaling is defined in Section 46 of the IEEE 802.3ae specification for 10 Gigabit Ethernet. When the feature is enabled, four statistics will be added to the list in Statistic View for the port. One is for monitoring the Link Fault State. Two provide a count of the Local Faults and Remote Faults. The last one is for indicating the state of error insertion, whether or not it is ongoing.

Link Fault Signaling for Lava originates with the PHY sending an indication of a local fault condition in the link being used as a path for MAC data. In the typical scenario, the Reconciliation Sublayer (RS) that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab.

The *Link Fault Signaling* tab for Lava load module is shown in the following figure:

Figure:Lava—Link Fault Signaling tab



The controls for **Link Fault Signaling** tab configuration are described in the following table:

Table:Link Fault Signaling Configuration

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (multiples of	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern.

Section	Field/Control	Description
	4; min = 4, max = 32)	This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	Number of times the above will loop (min = 1, max = 255)	This field is available only when the *Loop continuously* check box is **NOT** selected. It is the number of times that the combination of Bad/Good and Type patterns will be repeated. After all of the 66-bit blocks have been sent, the transmission will automatically stop.
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets—A and B—are defined in the *Ordered Set Definition* box in this tab.) This pattern will be combined with the Good blocks/Bad blocks pattern for transmission. • Type A only • Type B only • Alternate Type A and Type B.
	Loop continuously	If selected, the loop defined by the combination of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the *Stop Error Insertion* button is clicked. NOTE If fixed loop count is selected, and Send type A or Sed type B is selected, one loop iteration will consist of Error-Good pattern; if the Alternate ordered set types option is selected, one loop iteration will consist of Error-Good-Error-Good pattern.
Ordered Set Definition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault
Tx Ignores Rx Link Faults		If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.
Summary (Win-		(Read-only) Displays descriptions of the patterns

Section	Field/Control	Description
dow)		that will be transmitted.
Start Error Insertion		Press this button to start the transmission of the configured error patterns.
Stop Error Insertion		(Available only for use with the *Loop continuously* option.) Press this button to stop the transmission of the configured error patterns.

Lava Port Properties—Flow Control

The Lava **Flow Control** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

The Port Properties **Flow Control** tab is shown in the following figure:

Figure:Lava (non Data Center mode) Flow Control tab

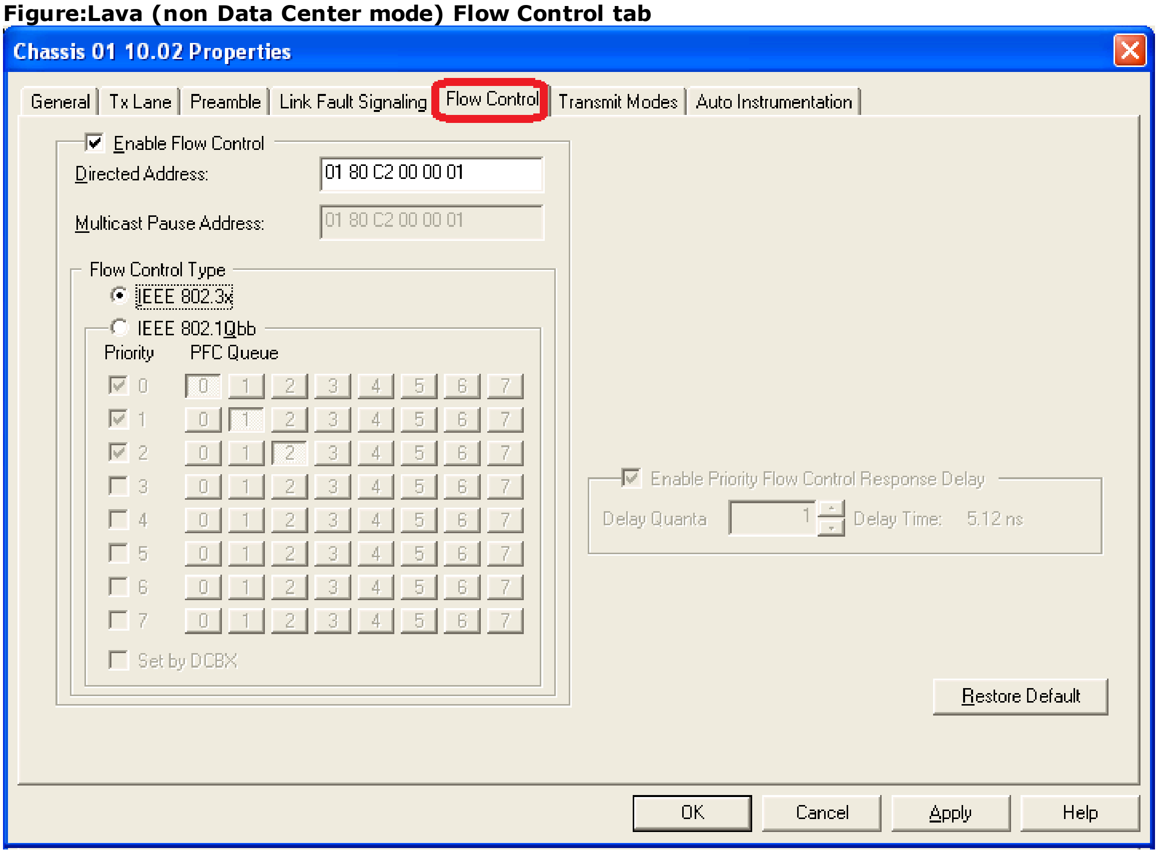
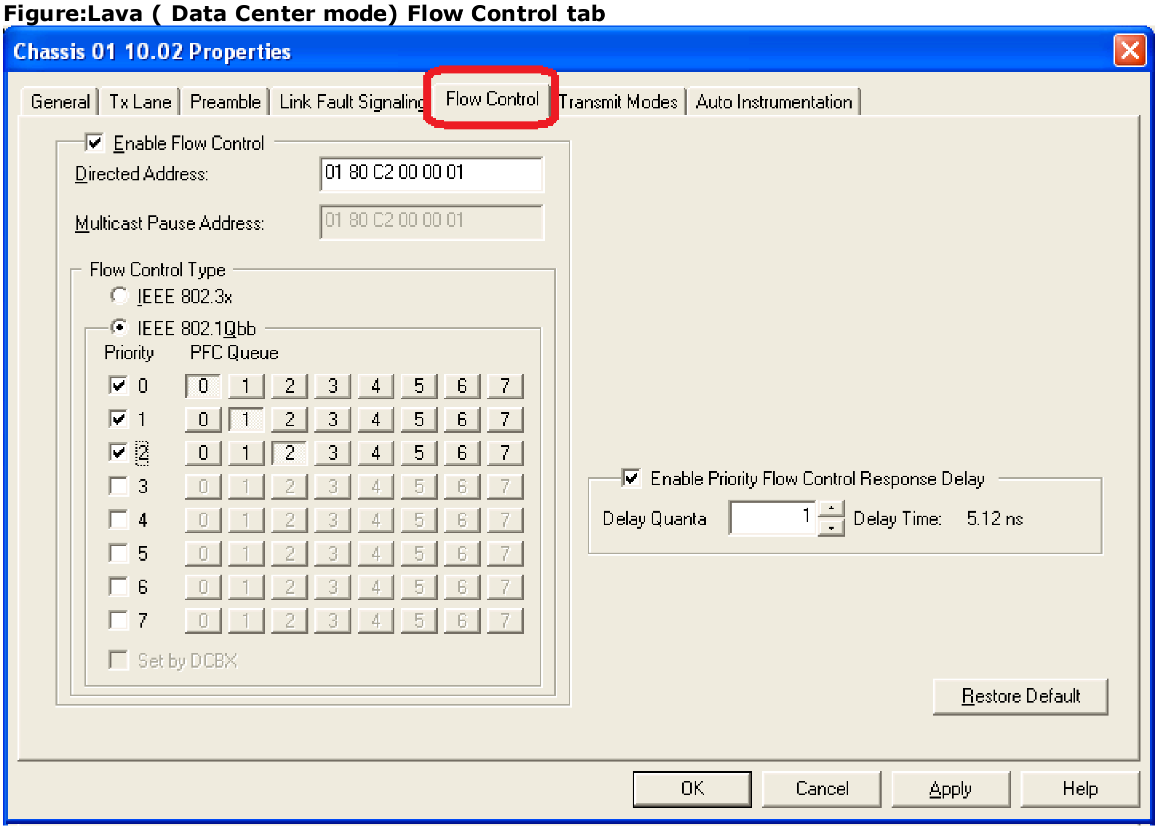


Figure:Lava (Data Center mode) Flow Control tab



The controls for **Flow Control** tab configuration are described in the following table:

Section	Field/Control	Description
Enable Flow Control	(check box)	Enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type	IEEE 802.3x or IEEE 802.1Qbb	*Priority-based Flow Control* When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
	Priority	*Priority-based Flow Control*.
	PFC Queue	*Priority-based Flow Control*
Enable Priority Flow Control Response Delay	(check box)	If selected, enables to increase the number of frames that is sent when a pause frame is received. Priority Flow Control (PFC) pause allows to set

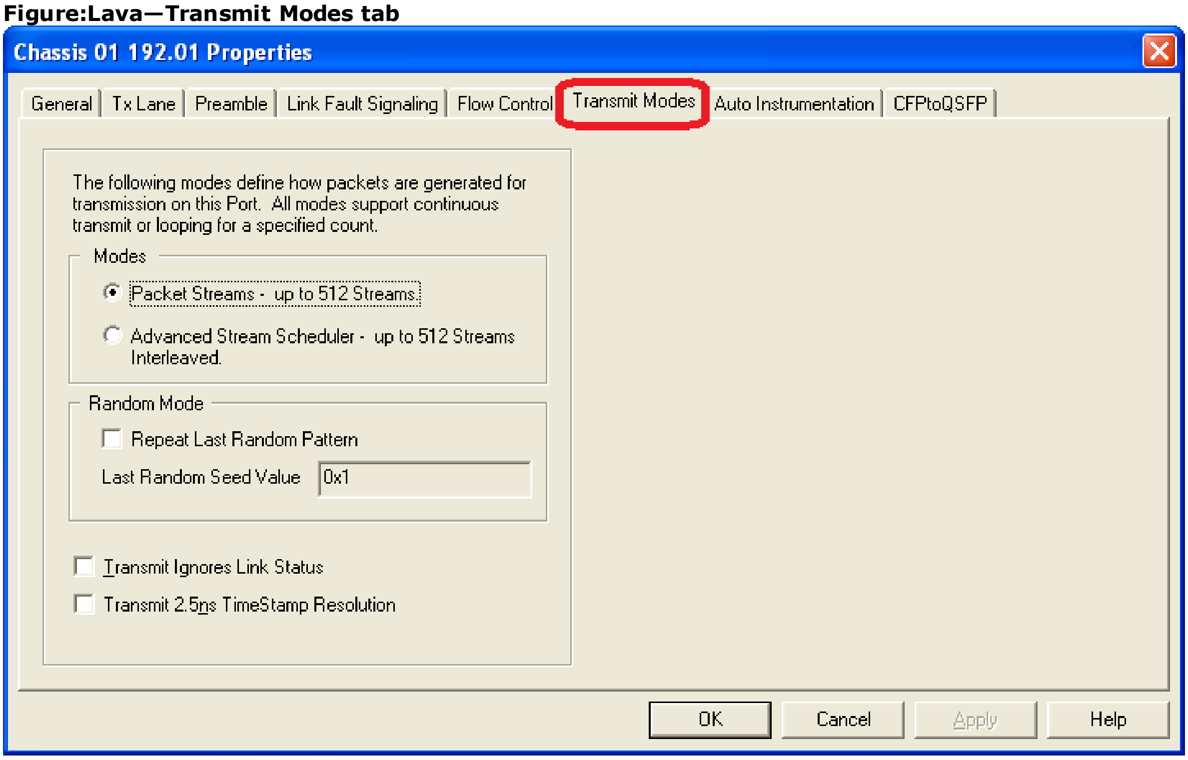
Section	Field/Control	Description
		the delay of flow control. When a pause frame is received for a certain priority, a count of the number of timestamp ticks increments up to a desired offset and then releases the pause request to the TX engine. For example, if running at 100% line rate and there is no delay in the pause request, the TX pipeline transmits the specified number of frames once the pause request is received. With this feature, a delay by number of timestamp ticks is programmed.
	Delay Quanta	This field allows to set the delay quanta of flow control.
	Delay Time	The delay time, in nanoseconds, of frames.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

Lava Port Properties—Transmit Modes

The **Transmit Modes** tab for Lava load modules is shown in the following figure. It is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the **Properties** menu option. Then select the **Transmit Modes** tab.

The Port Properties **Transmit Modes** tab is shown in the following figure:

Figure:Lava—Transmit Modes tab



The controls for **Transmit Modes** tab configuration are described in the following table:

Table:Transmit Modes Configuration

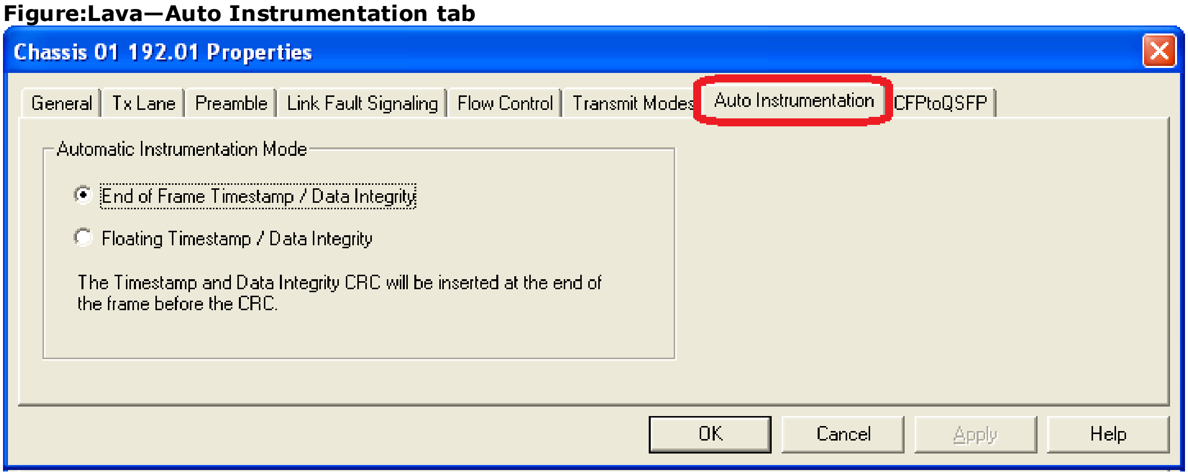
Section	Field/Control	Description
Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure up to 512 streams which become active sequentially. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets the operating mode for the port to interleaved packet streams. This allows to configure up to 512 streams which are concurrently active. They will transmit packets in an interleaved fashion. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream, including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Transmit Ignores Link Status		If selected, will allow transmission of packets even if the link is down.
Transmit 2.5ns Time stamp Resolution		If selected, it will check for the high resolution time stamp.

Lava Port Properties—Auto Instrumentation

The Lava **Auto Instrumentation** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The Lava Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure:Lava—Auto Instrumentation tab



The options and controls in this tab are described in the following table:

Table:Auto Instrumentation Configuration

Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Lava Port Properties—CFPtoQSFP

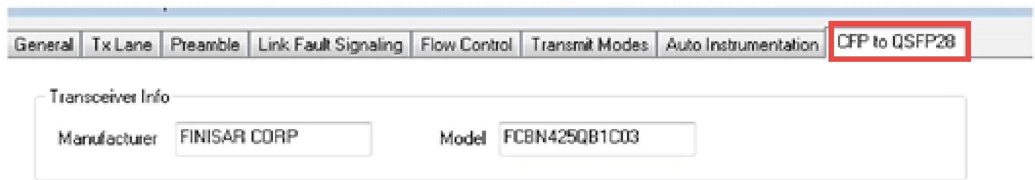
.The Lava **CFPtoQSFP** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **CFPtoQSFP** tab. CFPtoQSFP tab only exists if a CFPtoQSFP adapter is plugged in, otherwise it is not visible.

For more information on the adapters, see the *Ixia Platform Reference Guide*.

NOTE If the QSFP28 adapter is plugged in, the CFP to QSFP28 tab is shown. The Port Properties are similar to the ones for the CFPtoQSFP tab.

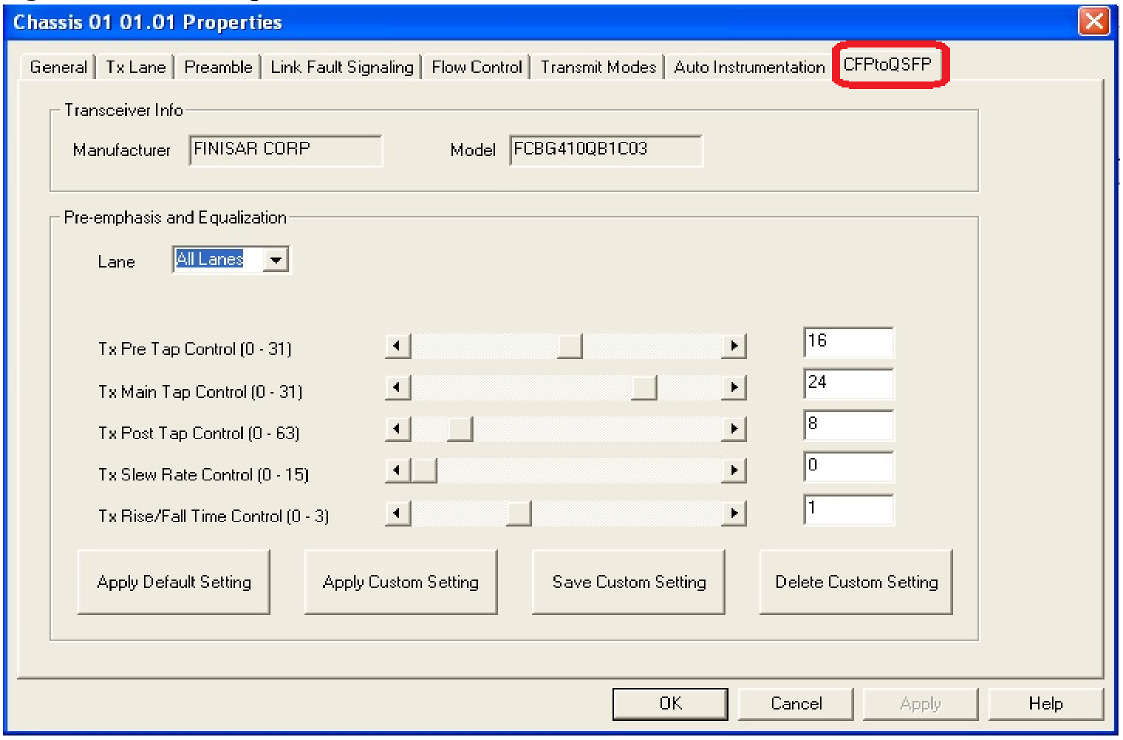
The Lava Port Properties **CFP to QSFP28** tab is shown in the following figure:

Figure:Lava—CFP to QSFP28 tab



The Lava Port Properties **CFPtoQSFP** tab is shown in the following figure:

Figure:Lava—CFPtoQSFP tab



The options and controls in this tab are described in the following table:

Table:CFPtoQSFP Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
Pre-emphasis and Eqalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Tx Slew Rate Control (0-15)	This helps to control the slewrate value for Tx.
	Tx Rise/Fall Time Control (0-3)	This helps to control the Post Tap value for Tx.
	Apply Default Set-tings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hard-ware.
	Apply Custom Set-	If clicked, if there exists a custom setting in

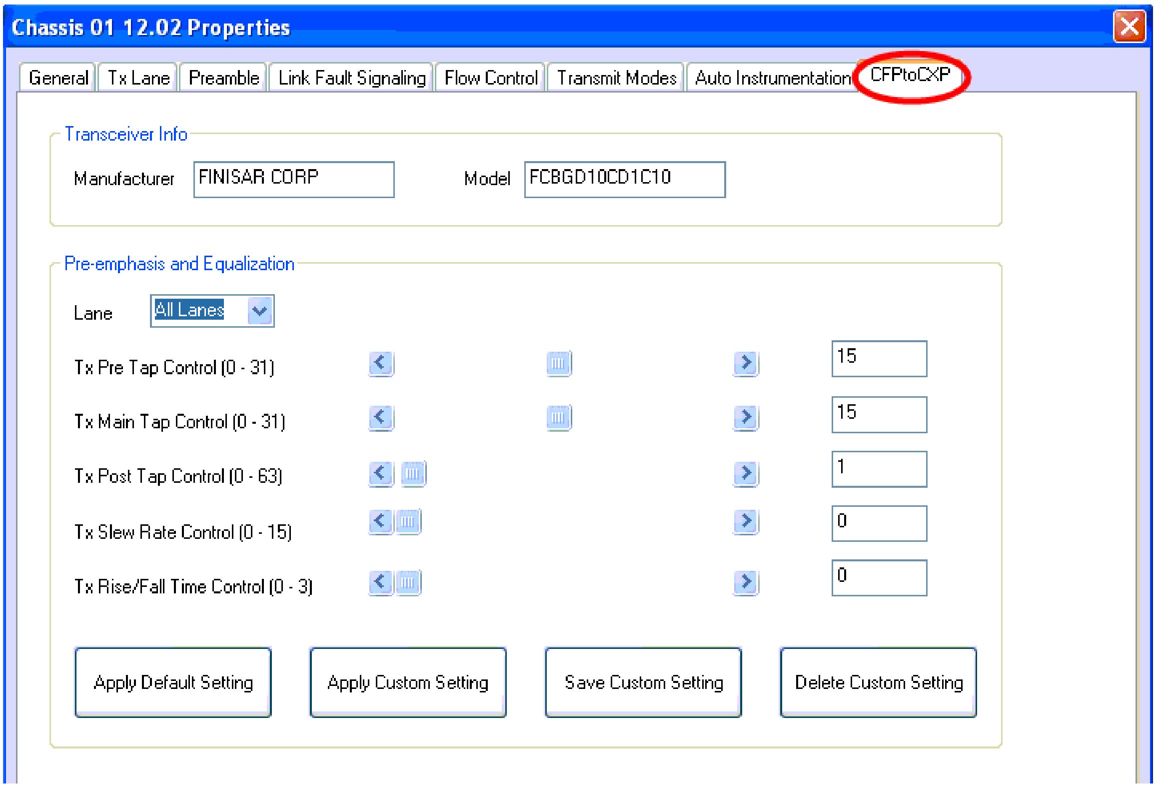
Section	Field/Control	Description
	tings	the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Lava Port Properties—CFPtoCXP

The Lava **CFPtoCXP** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **CFPtoCXP** tab. CFPtoCXP tab only exists if a CFPtoCXP adapter is plugged in, otherwise it is not visible.

The Lava Port Properties **CFPtoCXP** tab is shown in the following figure:

Figure:Lava—CFPtoCXP tab



The options and controls in this tab are described in the following table:

Table:CFPtoCXP Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
Pre-emphasis and Eqalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Tx Slew Rate Control (0-15)	This helps to control the slewrate value for Tx.
	Tx Rise/Fall Time Control (0-3)	This helps to control the Post Tap value for Tx.
	Apply Default Set- tings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hard- ware.
	Apply Custom Set-	If clicked, if there exists a custom setting in

Section	Field/Control	Description
	tings	the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Chapter 27 - Port Properties–Xcellon-Multis Load Module

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the port properties of the Xcellon-Multis load module.

Port Properties for Xcellon-Multis Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the Xcellon-Multis is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for Xcellon-Multis modules:

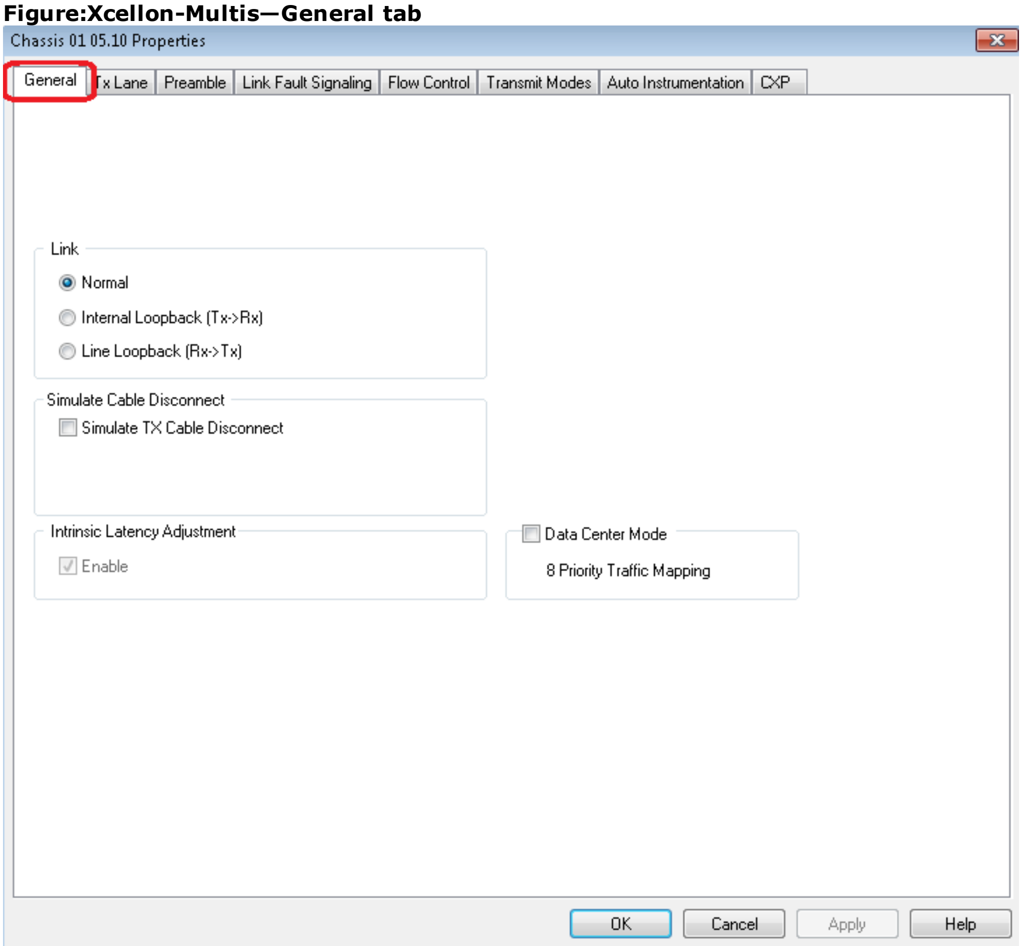
- Xcellon-Multis Port Properties—General
- Xcellon-Multis Port Properties—TX-Lane
- Xcellon-Multis Port Properties—Preamble
- Xcellon-Multis Port Properties—Link Fault Signaling
- Xcellon-Multis Port Properties—Flow Control
- Xcellon-Multis Port Properties—Transmit Modes
- Xcellon-Multis Port Properties—Auto Instrumentation
- Xcellon-Multis Port Properties—CXP
- Xcellon-Multis Port Properties—QSFP
- Xcellon-Multis Port Properties—QSFP28
- Xcellon-Multis Port Properties—CFP4
- Xcellon-Multis CXP Port Properties—Auto Negotiation
- Xcellon-Multis QSFP Port Properties—Auto Negotiation
- Xcellon-Multis CFP4 Port Properties—Auto Negotiation
- Xcellon-Multis QSFP28 Port Properties—Auto Negotiation

Xcellon-Multis Port Properties—General

The Xcellon-Multis **General** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, and then selecting the **General** tab.

The Port Properties **General** tab is shown in the following figure:

Figure:Xcellon-Multis—General tab



The controls for **General** tab configuration are described in the following table:

Table:General Configuration

Section	Control/Field	Usage
Link	Normal	Normal operation
	Internal Loopback (Tx -> Rx)	Internal Loopback—Transmit to Receive.
	Line Loopback (Rx -> Tx)	Enable/disable the Line Loopback—Receive to Transmit. NOTE The **Line Loopback** option is not available for Multis QSFP28 load modules.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	The Enable check box is selected by default. This enables the intrinsic latency adjustment. The *Enable* check box is grayed out when no value exists in the system for the specific transceiver. It is available if a value exists (in the .xml file).

Section	Control/Field	Usage
		For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
Data Center Mode		See Frame Data for FCoE Support.

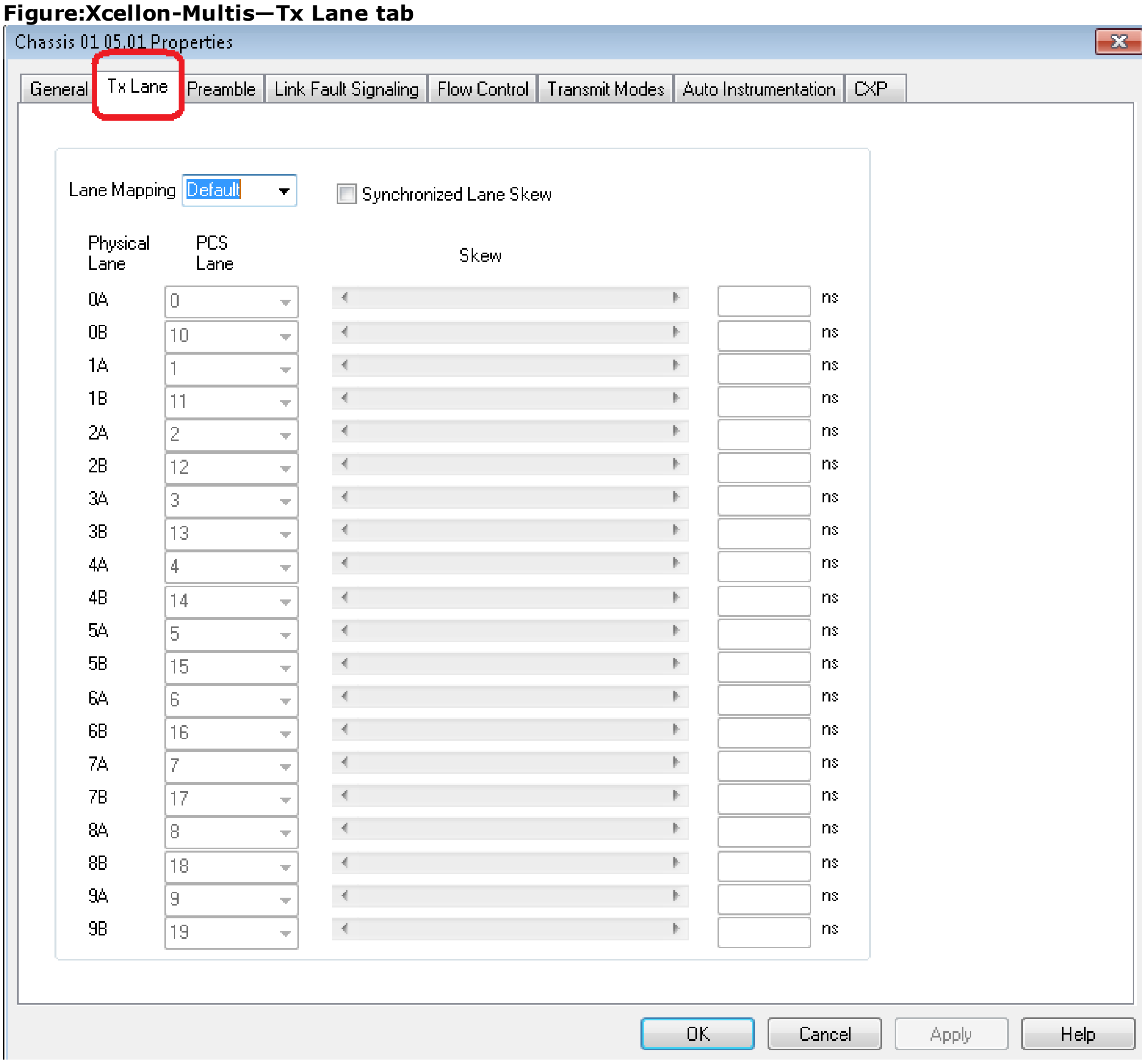
Xcellon-Multis Port Properties—TX-Lane

The *Tx Lane* tab allows to control the PCS lane order and skew rate for each lane.

For more information on Lane Skewing, see the Lane Skew topic in the 'Multilane Distribution Configuration' chapter of the *Ixia Platform Reference Manual*. The Lane Skew topic is located under 'Types of Ports' / '100GE'.

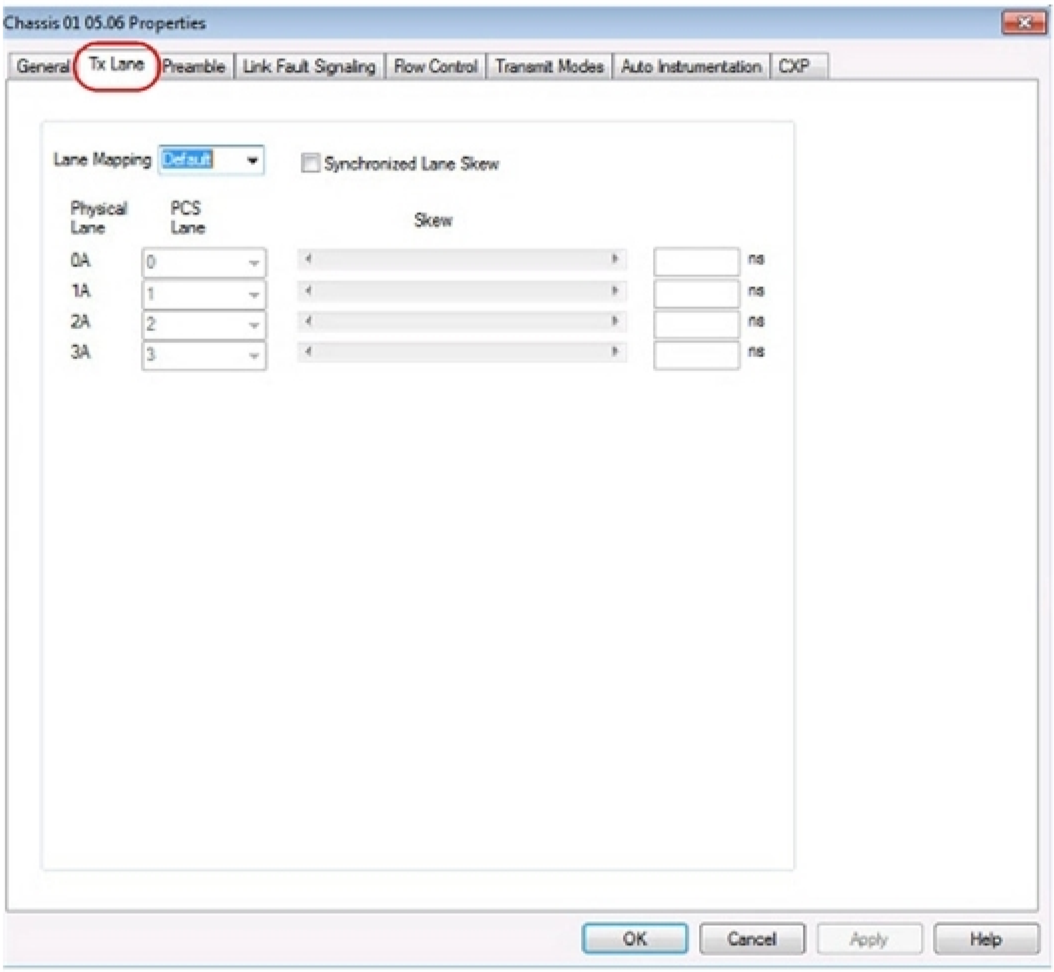
The Xcellon-Multis Port Properties *Tx Lane* tab for the 100GE mode is shown in the following figure:

Figure:Xcellon-Multis—Tx Lane tab



The Xcellon-Multis Port Properties *Tx Lane* tab for the 40GE mode is shown in the following figure:

Figure:Xcellon-Multis—Tx Lane tab



The controls for the *Tx Lane* tab configuration are described in the following table:

Table:Tx Lane Tab Configuration

Field	Description
Lane Mapping	Allows you to select a PCS lane ordering method. There are five options: • Default–the default ordering method. The default order is each physical port corresponds to 2 PCS lanes that are n and n+10, where n = physical lane number. • Increment–orders the lanes from 0 to 19, straight down the list. • Decrement–orders the lanes from 19 to 0, straight down the list. • Custom–allows to put the lanes in any order by manually entering the numbers in the fields. The starting order is the last selected mapping. • Random - Allows to put the lanes in any random order, values will be any value from 0 to 19.
Synchronized Lane Skew	All lanes are skewed by the same amount of skew.

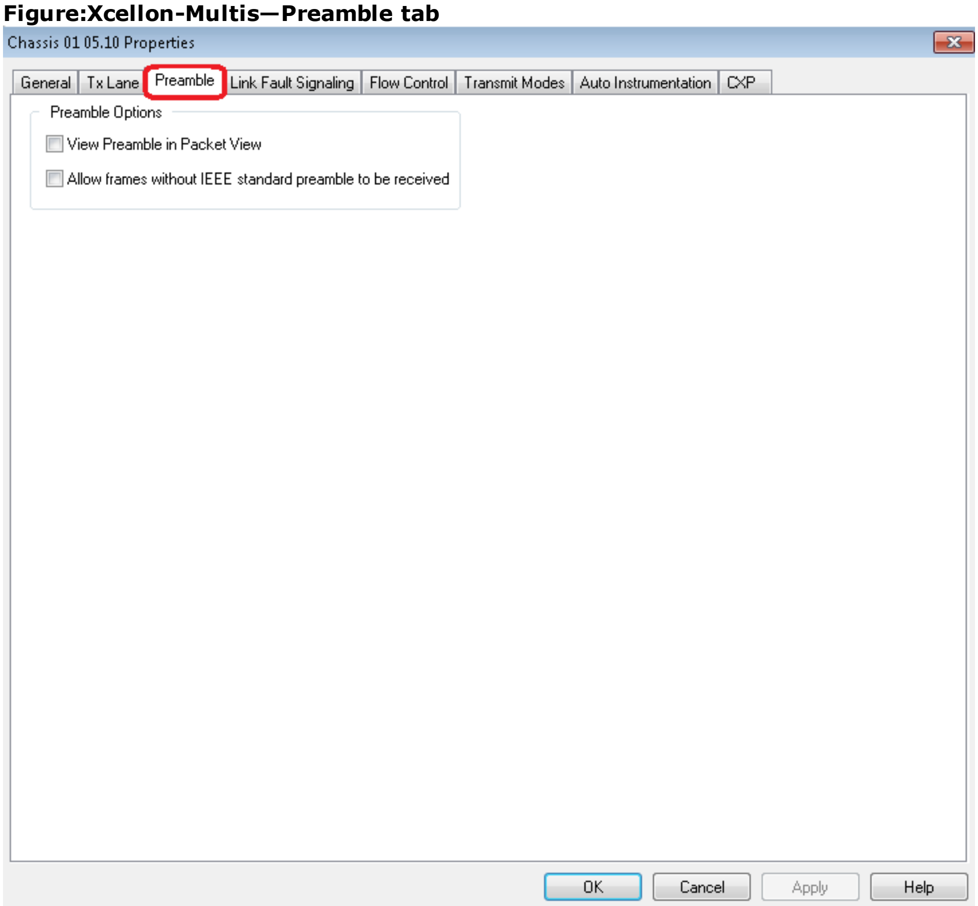
Field	Description
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
PCS Lane	A number identifier for the PCS lane. The PCS lane is paired with a corresponding physical lane.
Skew	The skew slider is used to set a skew value for the PCS lane, in nanoseconds, on the transmit side. Lane Skew is the ability to independently delay one or more of the 20 PCS lanes. When the slider is moved, the nanoseconds field is correspondingly adjusted. You can also enter a nano second value directly into this field. When the slider is fully pushed to the right, the skew injected into the transmit stream is 0 (minimum). When the slider is pushed all the way to the left. the skew injected into the transmit stream is 3 uS (maximum).

Xcellon-Multis Port Properties—Preamble

the preamble precedes the frame, but is not part of the frame itself.

The Xcellon-Multis Port Properties **Preamble** tab is shown in the following figure:

Figure:Xcellon-Multis—Preamble tab



The fields and controls in this tab are described in the following table:

Table:Preamble Configuration

Section	Choices	Description
Preamble Options	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side).
	Allow frames without IEE standard preamble to be received	When this check box is selected, it allows frames without IEEE standard preamble to be received.

Xcellon-Multis Port Properties—Link Fault Signaling

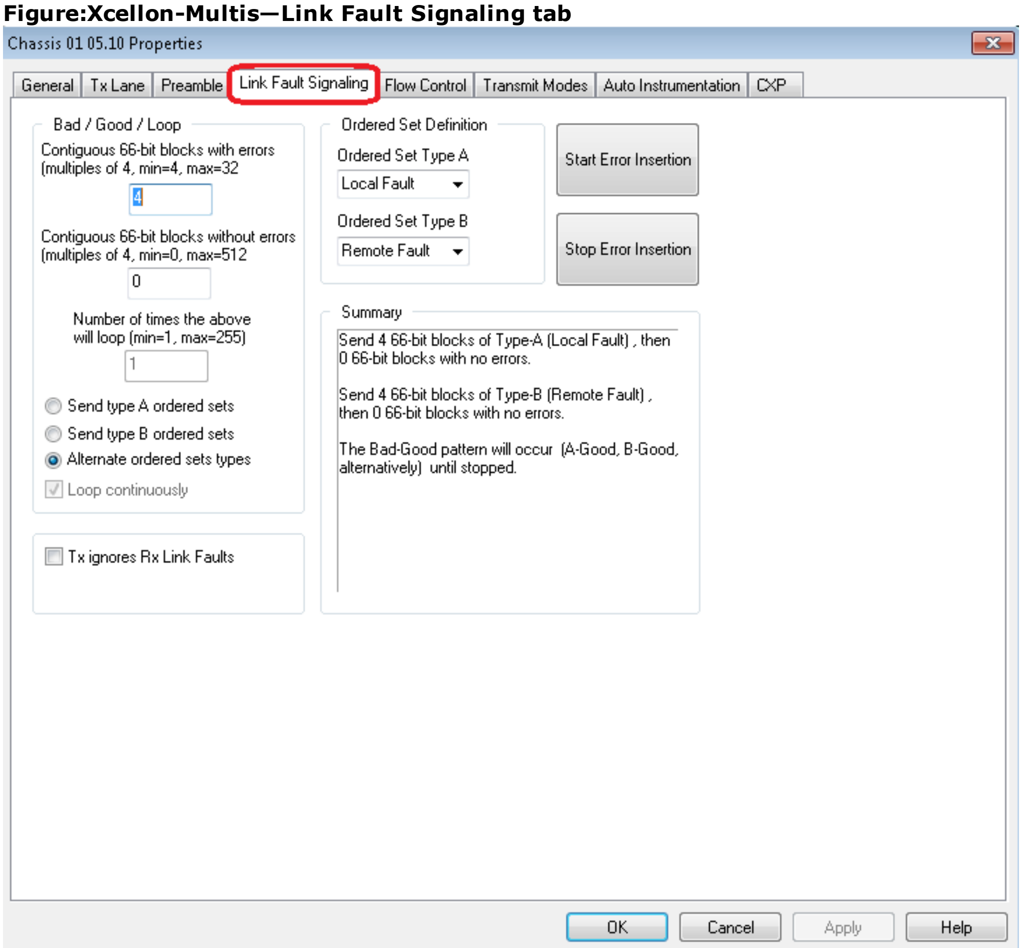
Link Fault Signaling is defined in Section 81.3.3.3 of the IEEE 802.3ba specification for 40 Gb/s and 100 Gb/s Ethernet. Link Fault Signaling is defined in Section 46 of the IEEE 802.3ae specification for 10 Gigabit Ethernet. When the feature is enabled, four statistics will be added to the list in Statistic View for the port. One is for monitoring the Link Fault State. Two provide a count of the Local Faults and Remote Faults. The last one is for indicating the state of error insertion, whether or not it is ongoing.

The 3x10GE and 8x10GE CXP and QSFP Multis ports support Link Fault Signaling. Link Fault Signaling for Xcellon-Multis originates with the PHY sending an indication of a local fault condition in the link being used as a path for MAC data. In the typical scenario, the Reconciliation Sublayer (RS) that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab.

The *Link Fault Signaling* tab for Xcellon-Multis load module is shown in the following figure:

Figure:Xcellon-Multis—Link Fault Signaling tab



The controls for **Link Fault Signaling** tab configuration are described in the following table:

Table:Link Fault Signaling Configuration

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 0, max = 512)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive regular data sequences allowed are minimum 0 sequences and maximum 512 sequences.
	Number of times the above will loop (min = 1, max =	Specifies the number of loops for the user defined sequence. There are two modes:

Section	Field/Control	Description
	255)	• Discrete iterations: i) Minimum of 1 iteration ii) Maximum of 255 iterations • Continuous loop i) User cannot specify number of iterations
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets—A and B—are defined in the *Ordered Set Definition* box in this tab.) This pattern will be combined with the Good block-s/Bad blocks pattern for transmission. • Only Type A fault sequence and regular good data sequences • Only Type B fault sequence and regular good data sequences • Alternate Type A, regular good data sequences and Type B fault sequence, regular good data sequences NOTE If this field is available, and the Alternate ordered set types option is selected, the minimum value for this field should be '2,' to allow the entire pattern to be sent once. If left at the minimum value of '1'— only two groups of blocks (one of good blocks and one of bad blocks) will be sent, which means that only the first ordered set will be sent. A minimum of eight blocks is required for one complete pattern including Types A and B.
	Loop continuously	If selected, the loop defined by the combination of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the *Stop Error Insertion* button is clicked.
Ordered Set Definition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault
Tx ignores Rx Link Faults		If selected, ongoing transmission will continue even if Link Fault messages are received by the sending RS.
Summary (Win-		(Read-only) Displays descriptions of the patterns

Section	Field/Control	Description
dow)		that will be transmitted.
Start Error Insertion		Press this button to start the transmission of the configured error patterns.
Stop Error Insertion		(Available only for use with the *Loop continuously* option.) Press this button to stop the transmission of the configured error patterns.

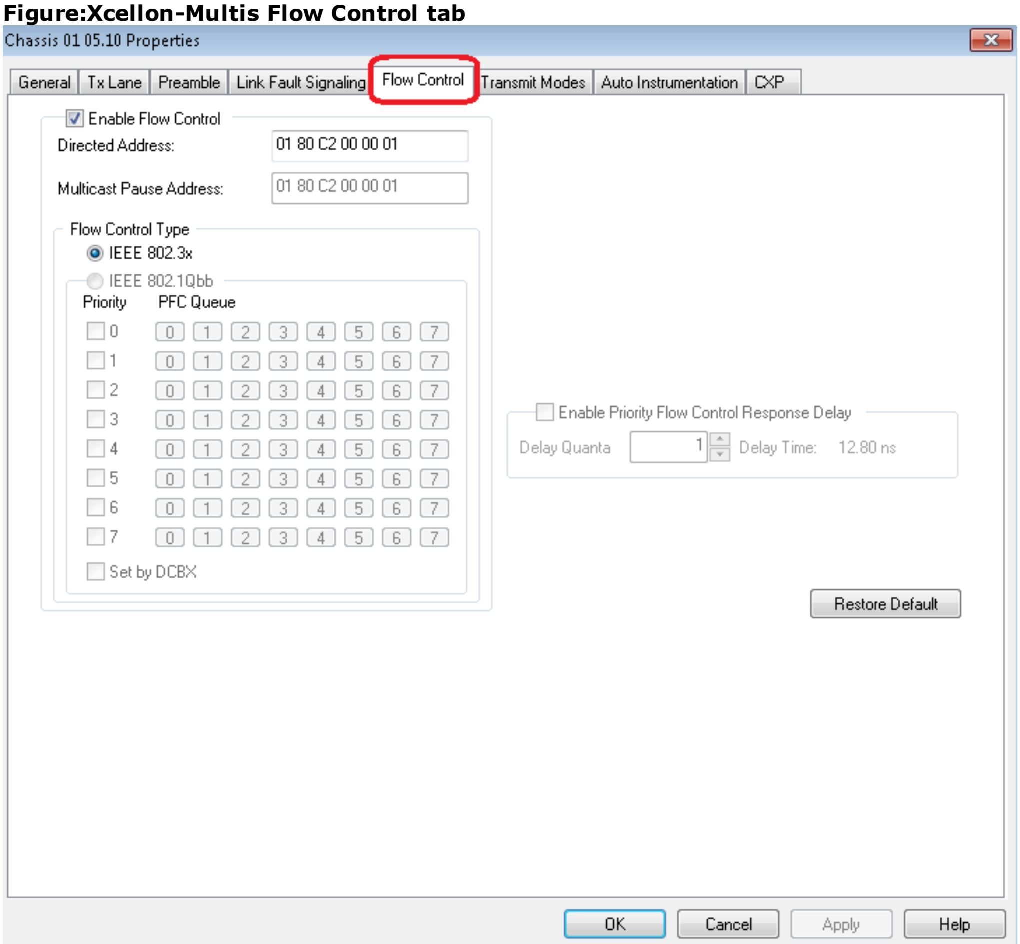
Xcellon-Multis Port Properties—Flow Control

The Xcellon-Multis **Flow Control** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

NOTE You can view this help page for the Port Properties - Flow Control tab by clicking the Help button and not F1.

The Port Properties **Flow Control** tab is shown in the following figure:

Figure:Xcellon-Multis Flow Control tab



The controls for **Flow Control** tab configuration are described in the following table:

Section	Field/Control	Description
Enable Flow Con-	(check box)	Enables the port's MAC Flow control mechanisms

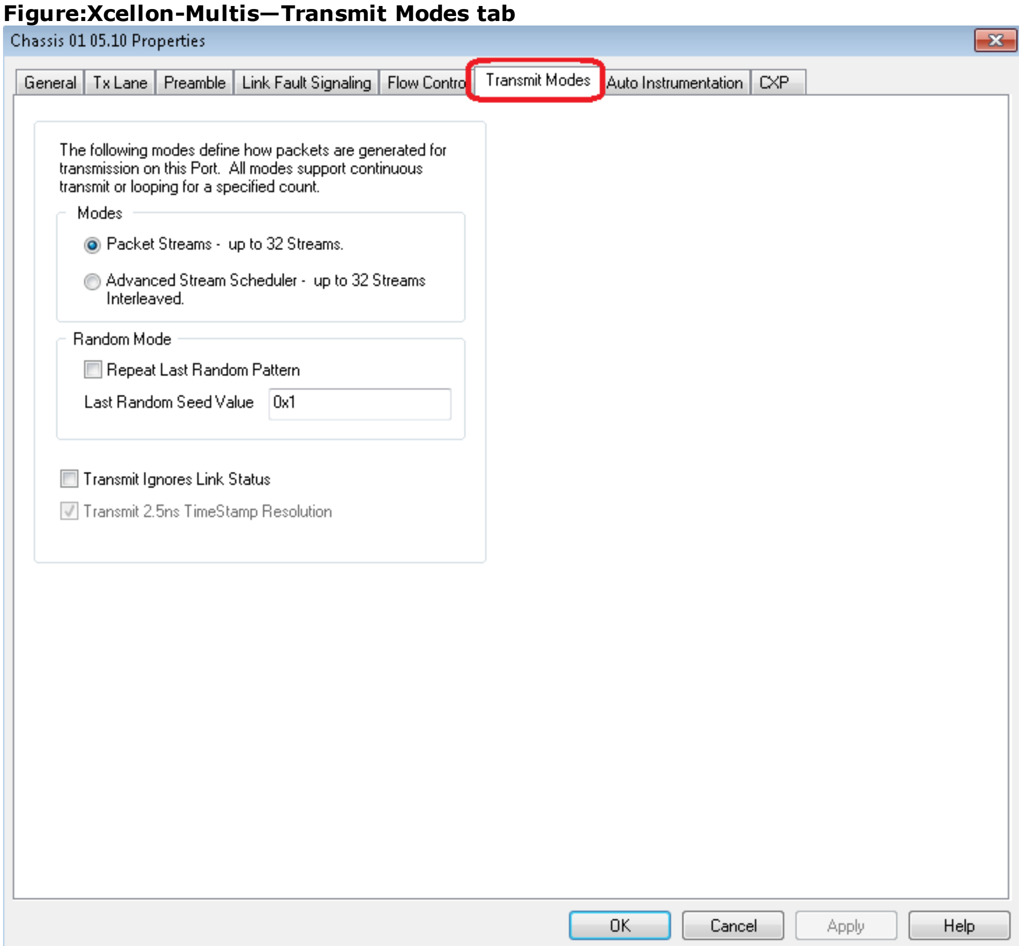
Section	Field/Control	Description
trol		to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type	IEEE 802.3x or IEEE 802.1Qbb	Priority-based Flow Control. When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
	Priority	Priority-based Flow Control.
	PFC Queue	Priority-based Flow Control
Enable Priority Flow Control Response Delay	(check box)	If selected, enables to increase the number of frames that is sent when a pause frame is received. Priority Flow Control (PFC) pause allows to set the delay of flow control. When a pause frame is received for a certain priority, a count of the number of timestamp ticks increments up to a desired offset and then releases the pause request to the TX engine. For example, if running at 100% line rate and there is no delay in the pause request, the TX pipeline transmits the specified number of frames once the pause request is received. With this feature, a delay by number of timestamp ticks is programmed.
	Delay Quanta	This field allows to set the delay quanta of flow control.
	Delay Time	The delay time, in nanoseconds, of frames.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

Xcellon-Multis Port Properties—Transmit Modes

The **Transmit Modes** tab for Xcellon-Multis load modules is shown in the following figure. It is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the **Properties** menu option. Then select the **Transmit Modes** tab.

The Port Properties **Transmit Modes** tab is shown in the following figure:

Figure:Xcellon-Multis—Transmit Modes tab



The controls for **Transmit Modes** tab configuration are described in the following table:

Table:Transmit Modes Configuration

Section	Field/Control	Description
Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure up to 128 streams in 100G and 32 streams in both 40G and 10G modes. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets the operating mode for the port to interleaved packet streams. This allows to configure up to 128 streams in 100G and 32 streams in both 40G and 10G modes. They will transmit packets in an interleaved fashion. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream,

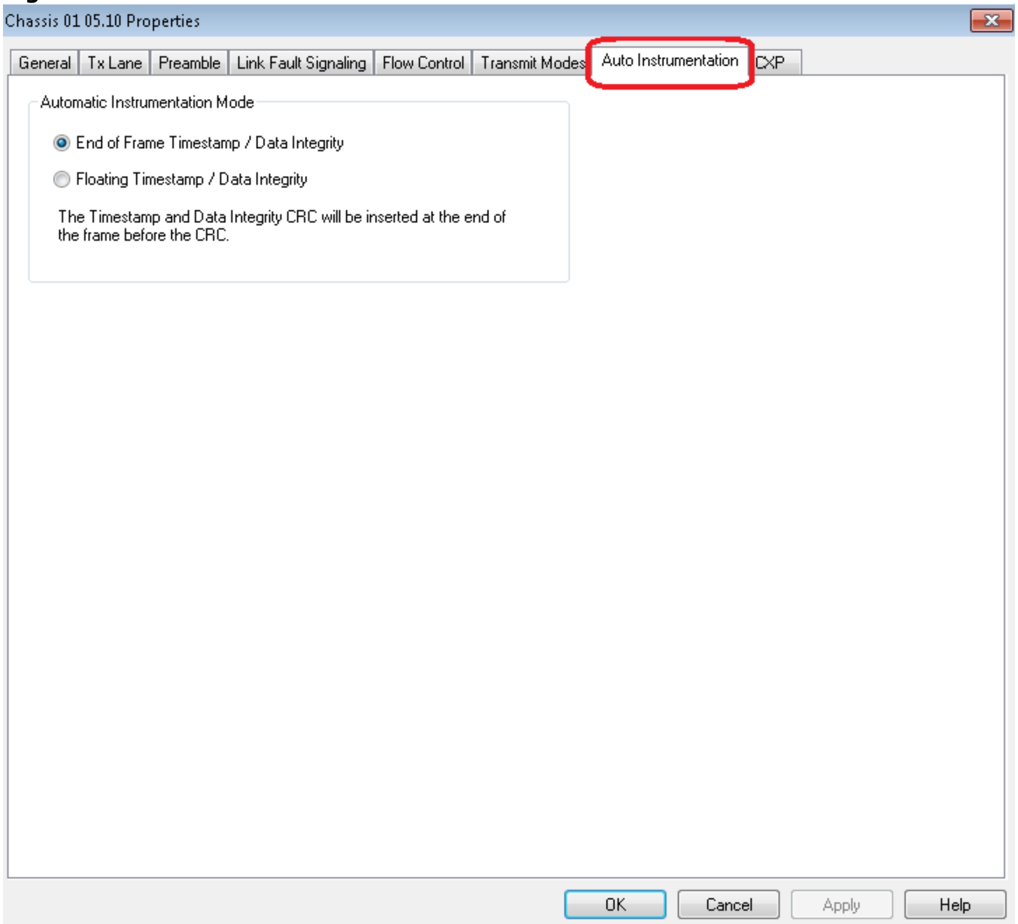
Section	Field/Control	Description
		including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Transmit Ignores Link Status		If selected, will allow transmission of packets even if the link is down.
Transmit 2.5ns Time stamp Resolution		If selected, it will check for the high resolution time stamp. The check box is selected by default.

Xcellon-Multis Port Properties—Auto Instrumentation

The Xcellon-Multis **Auto Instrumentation** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The Xcellon-Multis Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure:Xcellon-Multis—Auto Instrumentation tab



The options and controls in this tab are described in the following table:

Table:Auto Instrumentation Configuration

Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

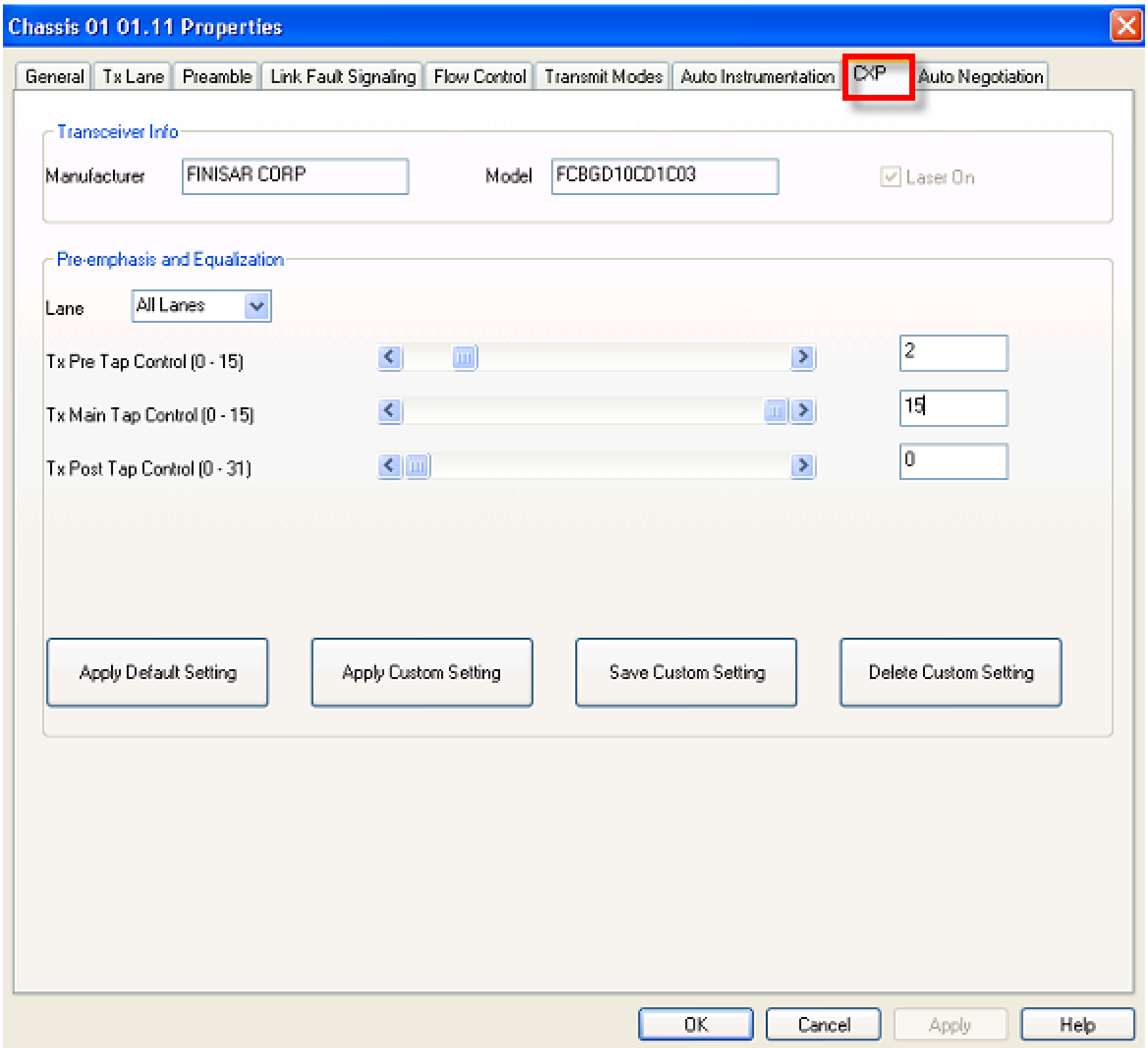
Xcellon-Multis Port Properties—CXP

The Xcellon-Multis **CXP** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **CXP** tab. CXP tab only exists if a CXP adapter is plugged in, otherwise it is not visible.

NOTE The QSFP tab for Xcellon-Multis provides the QSFP Port properties of the Multis modules—see *Xcellon-Multis Port Properties—QSFP*

The Xcellon-Multis Port Properties **CXP** tab is shown in the following figure:

Figure:Xcellon-Multis—CXP tab



The options and controls in this tab are described in the following table:

Table:CXP Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
	Laser On	Select this check box to enable the laser power. The laser is the actual data emitting device within the transceiver. The Laser On is available only for connectors that permit cutting the laser off. These connectors are not supported on Active Optical Cable Assembly (AOCs).
Pre-emphasis and Eqalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control	This helps to control the Pre Tap value for Tx.

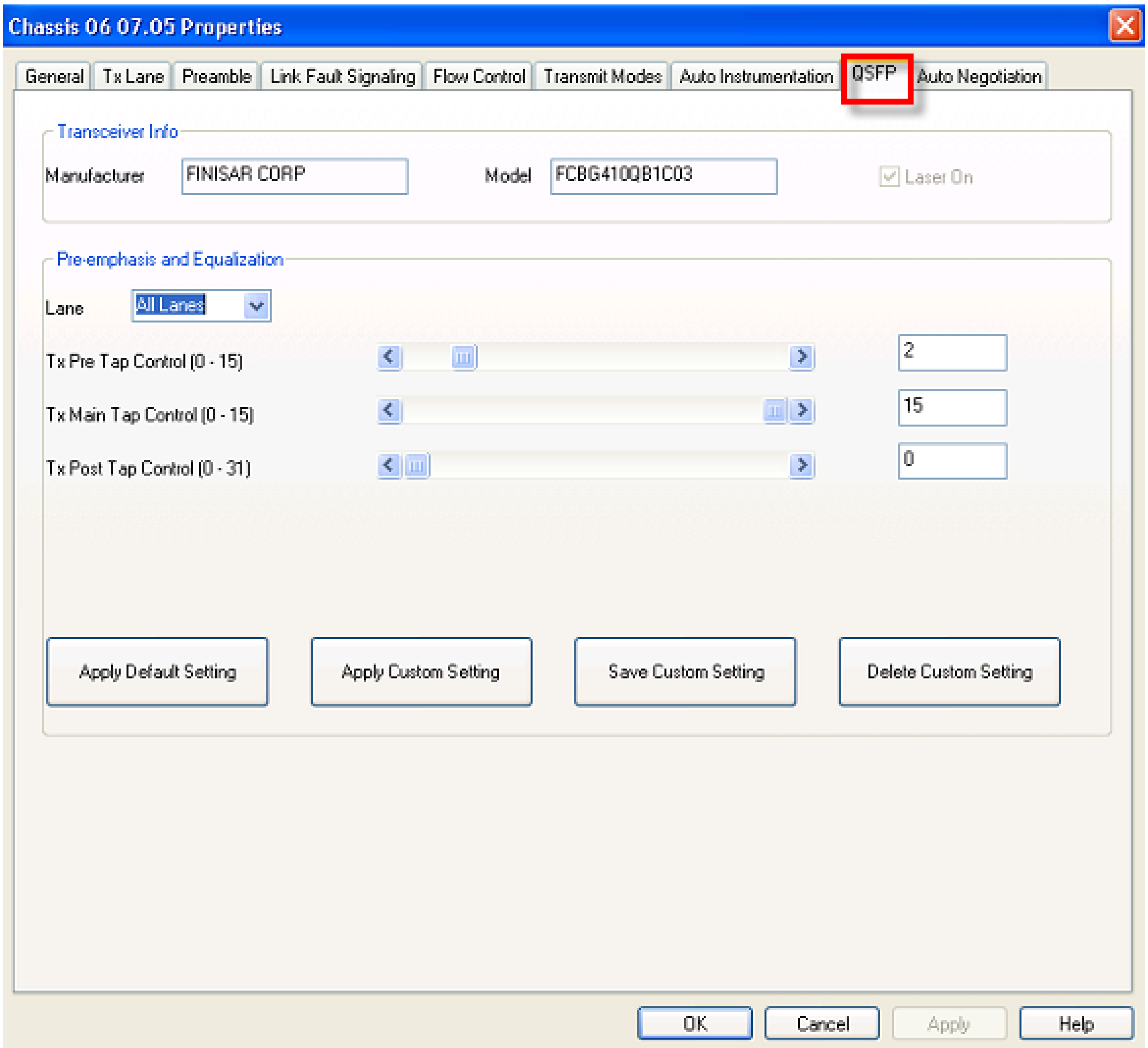
Section	Field/Control	Description
	(0-31)	
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Apply Default Settings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hardware.
	Apply Custom Settings	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Xcellon-Multis Port Properties—QSFP

The Xcellon-Multis **QSFP** tab is accessed by right-clicking a Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **QSFP** tab.

The Xcellon-Multis Port Properties **QSFP** tab is shown in the following figure:

Figure: QSFP tab



The options and controls in this tab are described in the following table.

Table:QSFP Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
	Laser On	Select this check box to enable the laser power. The laser is the actual data emitting device within the transceiver. The Laser On is available only for connectors that permit cutting the laser off. These connectors are not supported on Active Optical Cable Assembly (AOCs).
Pre-emphasis and Equalization		
	Lane	Specifies in which lane (from 0-3) the current

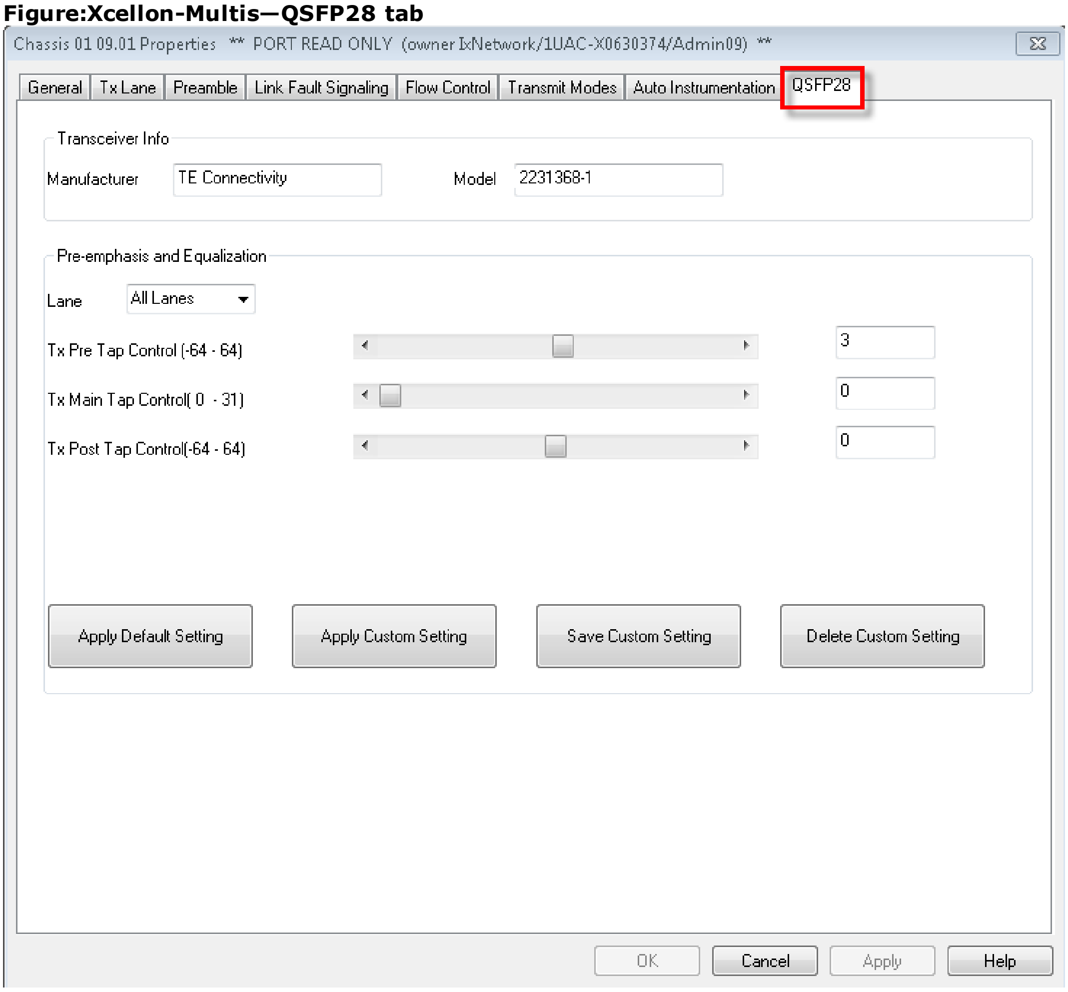
Section	Field/Control	Description
		settings are.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-31)	This helps to control the Post Tap value for Tx.
	Tx Pre Tap Control (0-16)	This helps to control the Pre Tap value for Tx.
	Apply Default Setting	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hardware.
	Apply Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Xcellon-Multis Port Properties—QSFP28

The Xcellon-Multis **QSFP28**tab is accessed by right-clicking an Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **QSFP28** tab.

The Xcellon-Multis Port Properties **QSFP28** tab is shown in the following figure:

Figure:Xcellon-Multis—QSFP28 tab



The options and controls in this tab are described in the following table:

Table:QSFP28 Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
Pre-emphasis and Eqalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Apply Default Set-tings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hard-ware.
	Apply Custom Set-	If clicked, if there exists a custom setting in

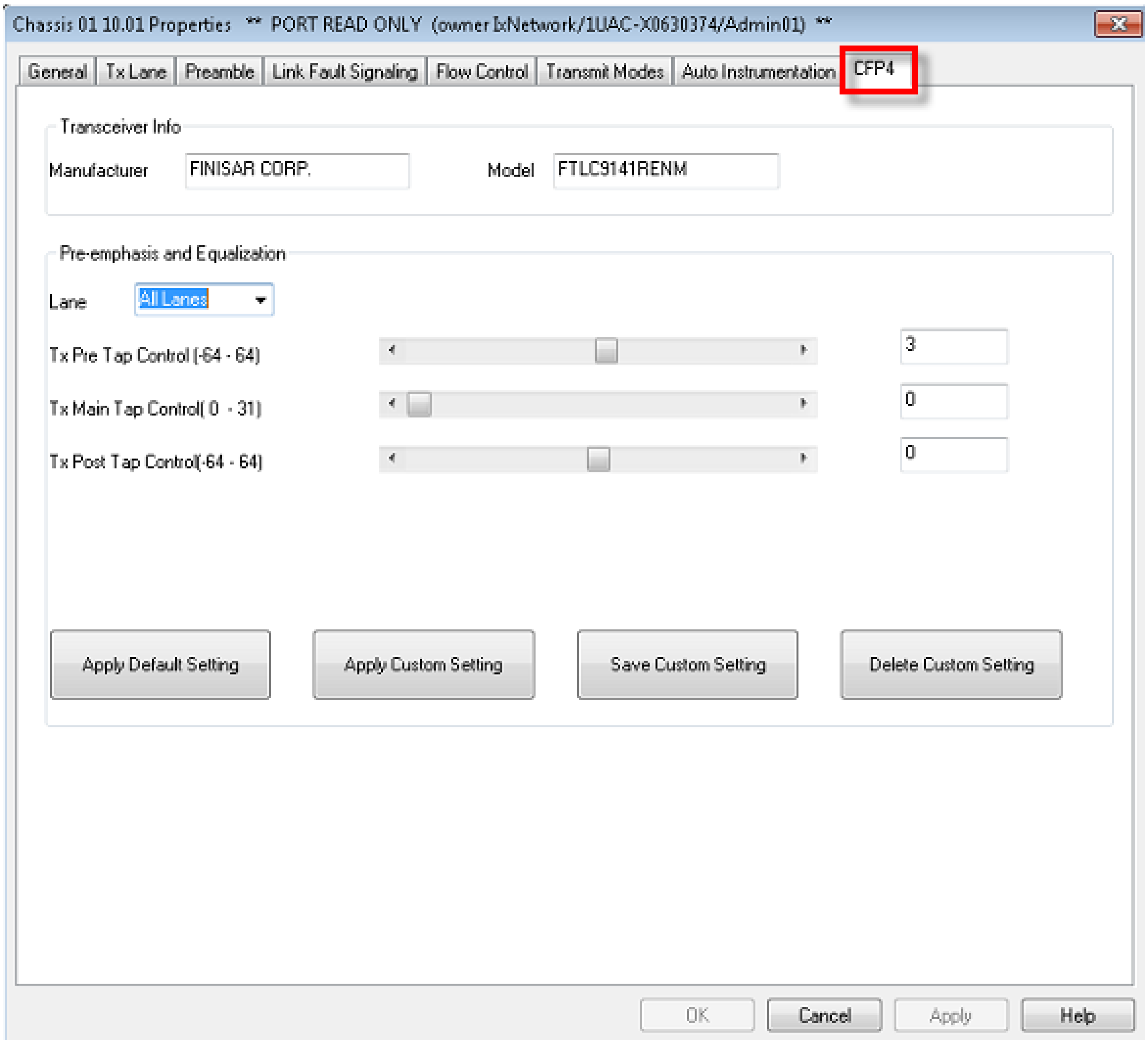
Section	Field/Control	Description
	tings	the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Xcellon-Multis Port Properties—CFP4

The Xcellon-Multis **CFP4**tab is accessed by right-clicking an Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **CFP4** tab.

The Xcellon-Multis Port Properties **CFP4** tab is shown in the following figure:

Figure: Xcellon-Multis—CFP4 tab



The options and controls in this tab are described in the following table:

Table:CFP4 Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.
Pre-emphasis and Equalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Apply Default Set-tings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hard-

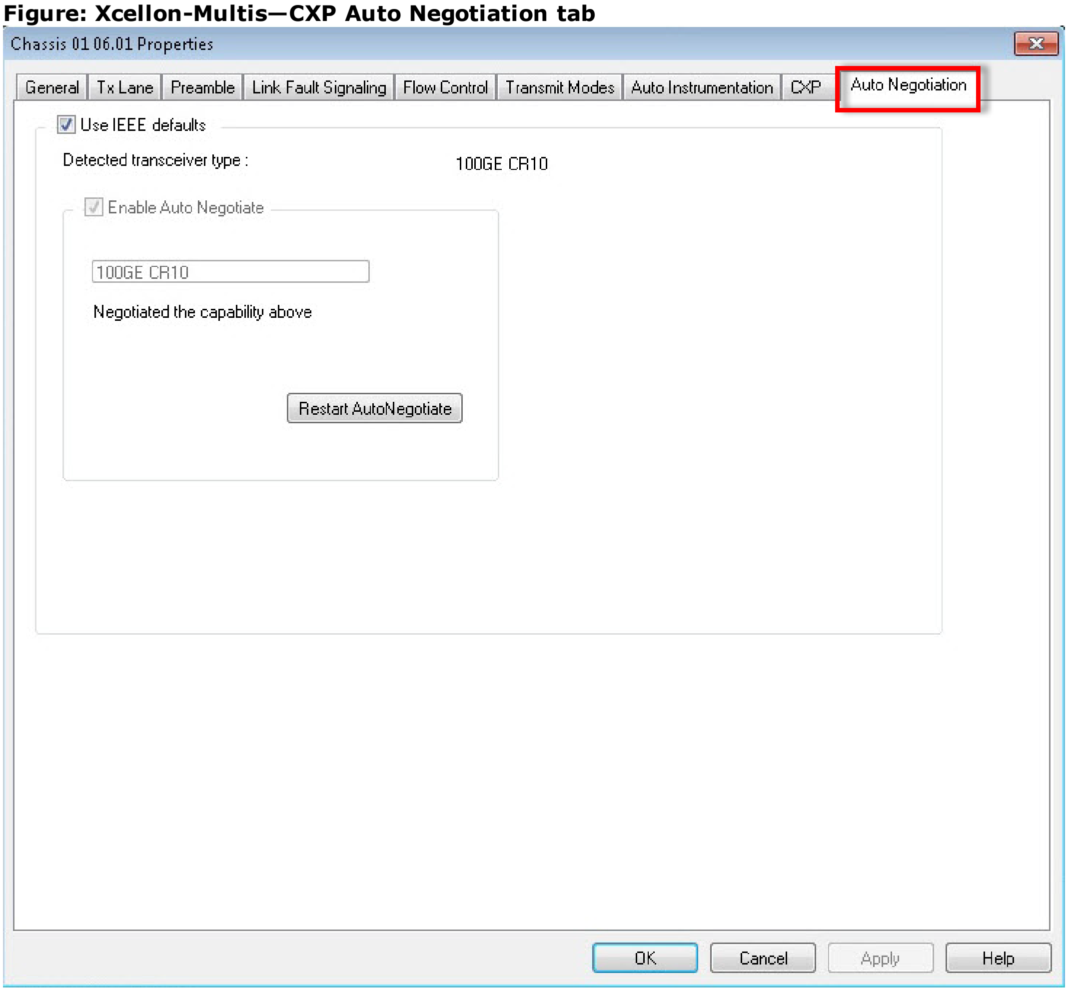
Section	Field/Control	Description
		ware.
	Apply Custom Settings	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Xcellon-Multis CXP Port Properties—Auto Negotiation

The Xcellon-Multis **Auto Negotiation** tab is accessed by right-clicking a Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Negotiation** tab.

The Port Properties **Auto Negotiation** tab for Xcellon-Multis CXP is shown in the following figure:

Figure: Xcellon-Multis—CXP Auto Negotiation tab



The fields and controls in this tab are described in the following table:

Table: Xcellon-Multis CXP Auto Negotiation tab

Field/Control	Description
Use IEEE defaults	When you select the Use IEEE Defaults check box, the L1 parameters like Autonegotiation, Link Training, and FEC, are enabled or disabled per IEEE requirements, and you will not be able to enable or disable these manually. If the check box is cleared, you will be able to manually enable or disable L1 features – even if it violates IEEE specifications. By default the check box is selected.
Detected transceiver type	When a transceiver is inserted into the load module, the software reads IEEE registers to determine the transceiver capabilities and media type. If the transceiver contains this information, it is shown in this read-only field. If the transceiver is capable of multiple speeds, the highest supported speed is shown. **Note**: The speed at which the Resource Group is currently operating, does not affect this. For example, if the Resource

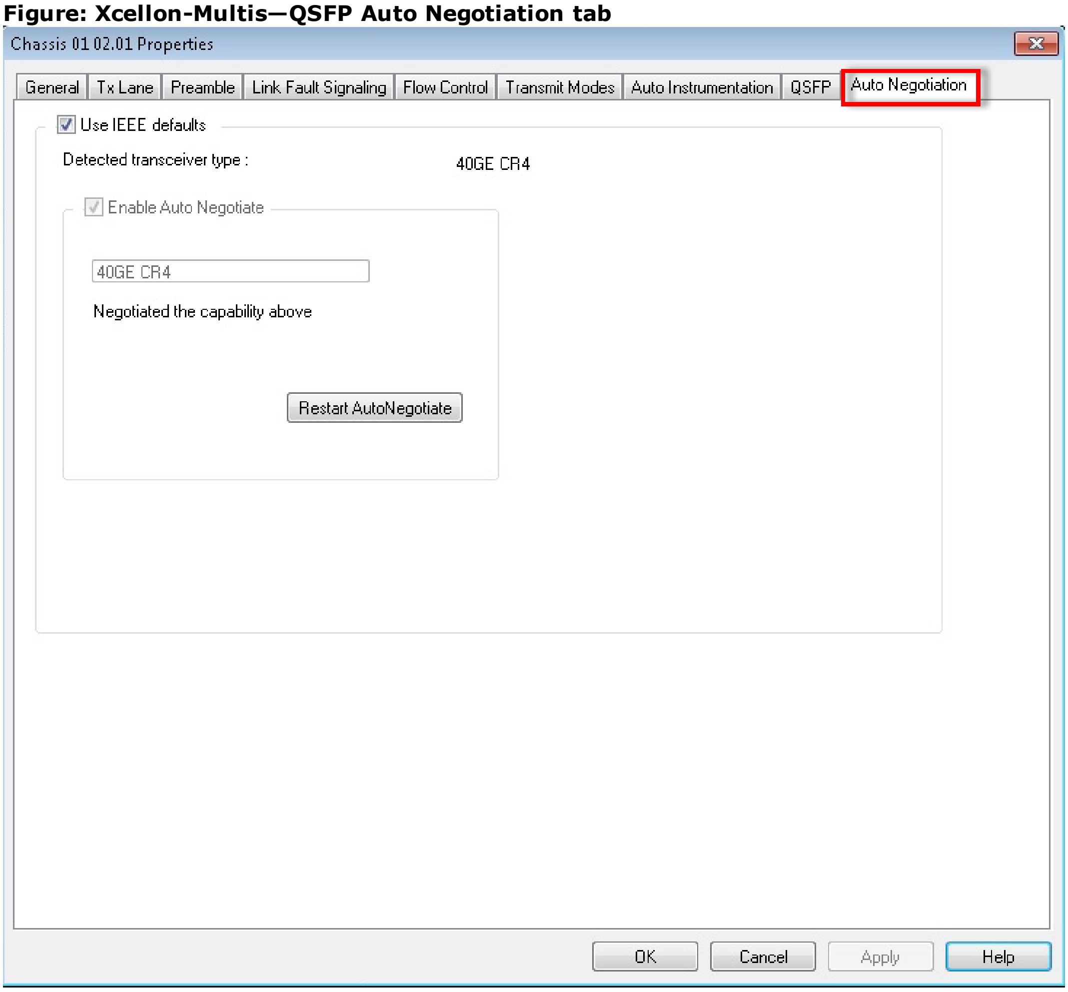
Field/Control	Description
	Group is configured to operate in 40GE mode, but the transceiver is capable of 100G and 40G, then the Detected transceiver type still indicates 100GBASE.
Enable Auto Negotiate	Auto negotiation controls how a port communicates with other ports. If you select the check box, it allows auto-negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during auto-negotiation. Auto-Negotiation starts when: • Link is attempting to be established • Link has dropped and is re-establishing • **Restart Auto-Negotiate** button is clicked (this does a forced restart) For Xcellon-Multis QSFP 40GE load modules, autonegotiate will advertise 40 Gbps full duplex operation. **Note**: The **Enable Auto Negotiate** check box is available for selection only if the **Use IEEE Defaults** check box is cleared. Auto Negotiation is supported on 40GE and 100GE.
Negotiated the capability above	The text box indicates the speed that was negotiated due to Auto-Negotiation. **Note**: This speed may be different than the speed indicated for the transceiver detected. For example: If you insert a 100GBASE-CR10 CXP cable that fans out to three 40G QSFP cables, the transceiver detected is indicated as 100GBASE-CR10. If you configure the Resource Group for 3x40G mode, Ixia advertises 40G speed during Auto-Negotiation. The negotiated capability will be 40GBASE-CR4.
Restart AutoNegotiate	Restarts the Auto Negotiate sequence.

Xcellon-Multis QSFP Port Properties—Auto Negotiation

The Xcellon-Multis **Auto Negotiation**tab is accessed by right-clicking an Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Negotiation** tab.

The Port Properties **Auto Negotiation** tab for Xcellon-Multis QSFP is shown in the following figure:

Figure: Xcellon-Multis—QSFP Auto Negotiation tab



The fields and controls in this tab are described in the following table:

Table: Xcellon-Multis QSFP Auto Negotiation tab

Field/Control	Description
Use IEEE defaults	When you select the Use IEEE Defaults check box, the L1 parameters like Autonegotiation, Link Training, and FEC, are enabled or disabled per IEEE requirements, and you will not be able to enable or disable these manually. If the check box is cleared, you will be able to manually enable or disable L1 features – even if it violates IEEE specifications. By default the check box is selected.
Detected transceiver type	When a transceiver is inserted into the load module, the software reads IEEE registers to determine the transceiver capabilities and media type. If the transceiver contains this information, it is shown in this read-only field. If the transceiver is capable of multiple speeds, the highest supported speed is shown. **Note**: The speed at which the Resource Group is currently operating, does not affect this. For example, if the Resource

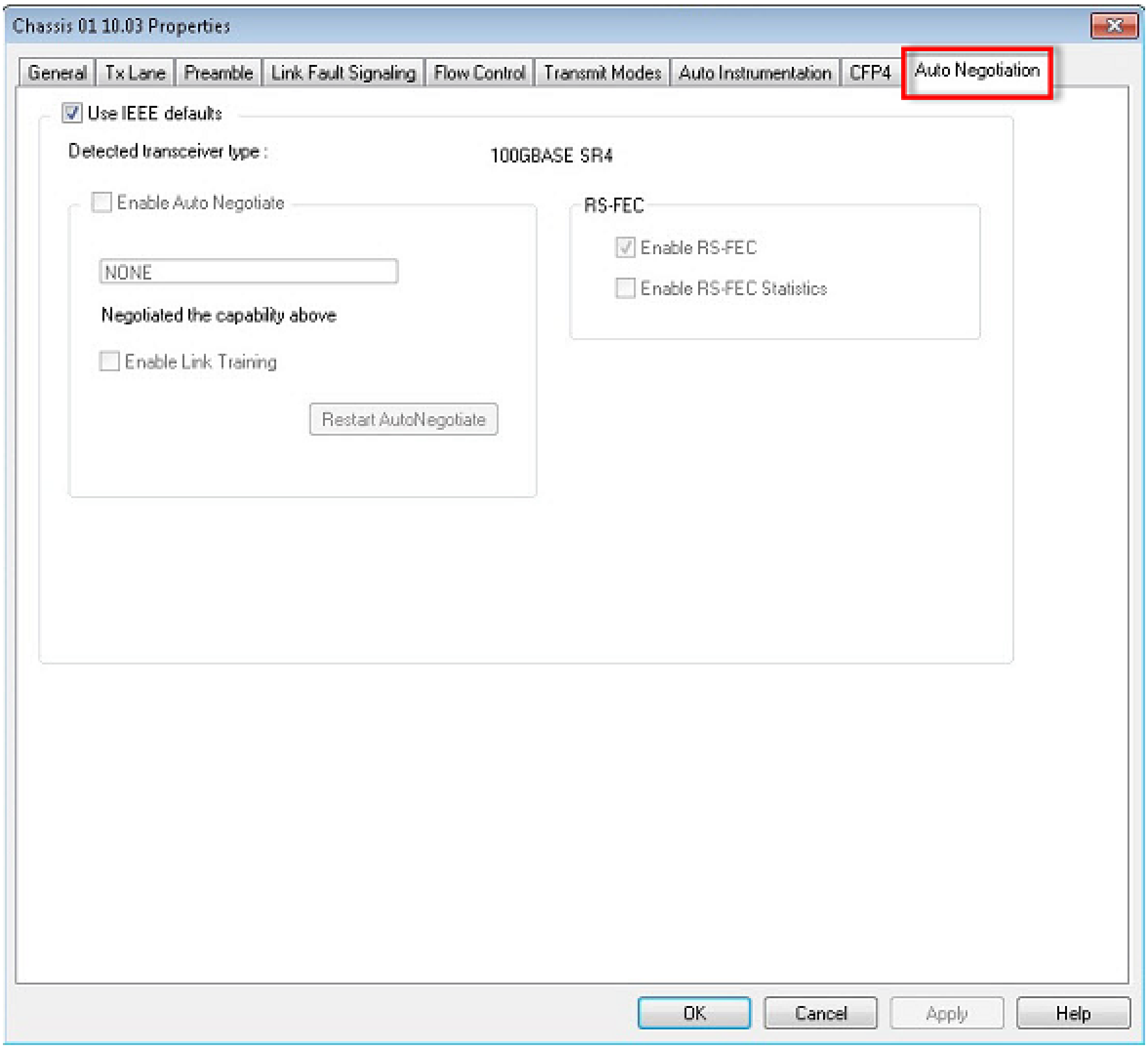
Field/Control	Description
	Group is configured to operate in 40GE mode, but the transceiver is capable of 100G and 40G, then the Detected transceiver type still indicates 100GBASE.
Enable Auto Negotiate	Auto negotiation controls how a port communicates with other ports. If you select the check box, it allows auto-negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during auto-negotiation. Auto-Negotiation starts when: • Link is attempting to be established • Link has dropped and is re-establishing • **Restart Auto-Negotiate** button is clicked (this does a forced restart) For Xcellon-Multis QSFP 40GE load modules, autonegotiate will advertise 40 Gbps full duplex operation. **Note**: The **Enable Auto Negotiate** check box is available for selection only if the **Use IEEE Defaults** check box is cleared. Auto Negotiation is supported on 40GE and 100GE.
Negotiated the capability above	The text box indicates the speed that was negotiated due to Auto-Negotiation. **Note**: This speed may be different than the speed indicated for the transceiver detected. For example: If you insert a 100GBASE-CR10 CXP cable that fans out to three 40G QSFP cables, the transceiver detected is indicated as 100GBASE-CR10. If you configure the Resource Group for 3x40G mode, Ixia advertises 40G speed during Auto-Negotiation. The negotiated capability will be 40GBASE-CR4.
Restart AutoNegotiate	Restarts the Auto Negotiate sequence.

Xcellon-Multis CFP4 Port Properties—Auto Negotiation

The Xcellon-Multis **CFP4**tab is accessed by right-clicking an Xcellon-Multis port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **CFP4** tab.

The Xcellon-Multis Port Properties **CFP4** tab is shown in the following figure:

Figure: Xcellon-Multis—CFP4 Auto Negotiation tab



The fields and controls in this tab are described in the following table:

Table: Xcellon-Multis CFP4 Auto Negotiation Tab

Field/Control	Description
Use IEEE defaults	When you select the Use IEEE Defaults check box, the L1 parameters like Autonegotiation, Link Training, and FEC, are enabled or disabled per IEEE requirements, and you will not be able to enable or disable these manually. If the check box is cleared, you will be able to manually enable or disable L1 features – even if it violates IEEE specifications. By default the check box is selected.
Detected transceiver type	When a transceiver is inserted into the load module, the software reads IEEE registers to determine the transceiver capabilities and media type. If the transceiver contains this information, it is shown in this read-only field. If the transceiver is capable of multiple speeds, the highest supported speed is shown.

Field/Control	Description
	Note: The speed at which the Resource Group is currently operating, does not affect this. For example, if the Resource Group is configured to operate in 40GE mode, but the transceiver is capable of 100G and 40G, then the Detected transceiver type still indicates 100GBASE.
Enable Auto Negotiate	Auto negotiation controls how a port communicates with other ports. If you select the check box, it allows auto-negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during auto-negotiation. Auto-Negotiation starts when: • Link is attempting to be established • Link has dropped and is re-establishing • **Restart Auto-Negotiate** button is clicked (this does a forced restart) For Xcellon-Multis QSFP 40GE load modules, autonegotiate will advertise 40 Gbps full duplex operation. **Note**: The **Enable Auto Negotiate** check box is available for selection only if the **Use IEEE Defaults** check box is cleared. Auto Negotiation is supported on 40GE and 100GE.
Negotiated the capability above	The text box indicates the speed that was negotiated due to Auto-Negotiation. **Note**: This speed may be different than the speed indicated for the transceiver detected. For example: If you insert a 100GBASE-CR10 CXP cable that fans out to three 40G QSFP cables, the transceiver detected is indicated as 100GBASE-CR10. If you configure the Resource Group for 3x40G mode, Ixia advertises 40G speed during Auto-Negotiation. The negotiated capability will be 40GBASE-CR4.
Enable Link Training	Select the check box to allow longer length copper cables to be used. This means that during the next Auto-Negotiation, KR training will be used. **Note**: This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. KR Training is not available on Multis QSFP+ and CXP load modules.
Restart AutoNegotiate	Restarts the Auto Negotiate sequence.
Enable RS-FEC	FEC or Forward Error Correction is available for XM100GE4CFP4+ENH load module. If you select this check box, RS-FEC is used. FEC encrypts data sent on the line using some overhead for error correction code. This allows bit errors in flight to be corrected on the receiving side. The benefit of FEC is that it

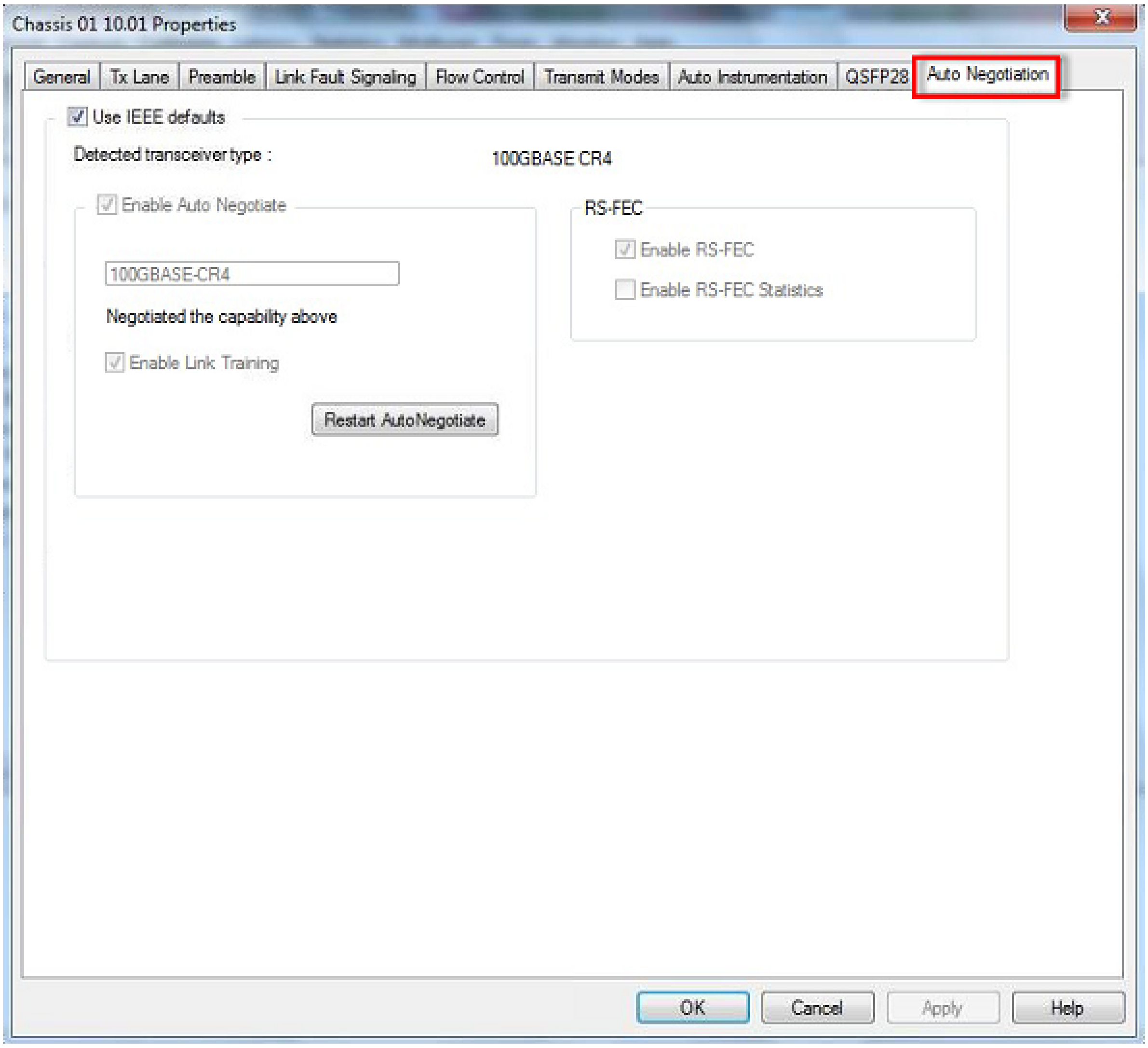
Field/Control	Description
	allows very long copper cables to be used and allows cheaper parts to be used in optical transceivers as errors will be corrected. RS-FEC is compatible with Auto-Negotiation and KR Training. **Note**: • This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. • FEC should be enabled on both back-to-back ports for the link to be up. • CXP and QSFP+ load modules do not support FEC.
Enable RS-FEC Statistics	If you select this check box, RS-FEC Statistics is available. An RS-FEC codeword is a block of contiguous packets on the line. All RS-FEC codewords are of the same size. Thus, a block can represent many packets, few packets, portions of packets, or no packets at all. The two RS-FEC statistics are: • RS-FEC Corrected Codeword Count - Indicates that at least one error was encountered in a block that was able to be corrected. • RS-FEC Uncorrected Codeword Count - Indicates that too many errors existed within a block to be corrected. These statistics can increment when a link pair is idle. Any uncorrected FEC block can indicate any of the following problems: • Ixia is unable to insert RS-FEC errors. • Ixia is unable to drill-down into any FEC block to show what it represented. **Note**: By default, the check box is not available for selection. It is available only if the **Use IEEE Defaults** check box is cleared.

Xcellon-Multis QSFP28 Port Properties—Auto Negotiation

This tab is available for XM100GE4QSFP28+ENH load module. The Xcellon-Multis Auto Negotiation tab is accessed by right-clicking a Xcellon-Multis port in the Explore Network Resources pane, selecting the Port Properties menu option, then selecting the Auto Negotiation tab.

The Port Properties **Auto Negotiation** tab for Xcellon-Multis QSFP28 is shown in the following figure:

Figure: Xcellon-Multis—QSFP28 Auto Negotiation tab



The fields and controls in this tab are described in the following table:

Table: Xcellon-Multis QSFP28 Auto Negotiation Tab

Field/Control	Description
Use IEEE defaults	When you select the Use IEEE Defaults check box, the L1 parameters like Autonegotiation, Link Training, and FEC, are enabled or disabled per IEEE requirements, and you will not be able to enable or disable these manually. If the check box is cleared, you will be able to manually enable or disable L1 features – even if it violates IEEE specifications. By default the check box is selected.
Detected transceiver type	When a transceiver is inserted into the load module, the software reads IEEE registers to determine the transceiver capabilities and media type. If the transceiver contains this information, it is shown in this read-only field. If the transceiver is capable of multiple speeds, the highest supported speed is shown.

Field/Control	Description
	Note: The speed at which the Resource Group is currently operating, does not affect this. For example, if the Resource Group is configured to operate in 40GE mode, but the transceiver is capable of 100G and 40G, then the Detected transceiver type still indicates 100GBASE.
Enable Auto Negotiate	Auto negotiation controls how a port communicates with other ports. If you select the check box, it allows auto-negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during auto-negotiation. Auto-Negotiation starts when: • Link is attempting to be established • Link has dropped and is re-establishing • **Restart Auto-Negotiate** button is clicked (this does a forced restart) For Xcellon-Multis QSFP 40GE load modules, autonegotiate will advertise 40 Gbps full duplex operation. **Note**: The **Enable Auto Negotiate** check box is available for selection only if the **Use IEEE Defaults** check box is cleared. Auto Negotiation is supported on 40GE and 100GE.
Negotiated the capability above	The text box indicates the speed that was negotiated due to Auto-Negotiation. **Note**: This speed may be different than the speed indicated for the transceiver detected. For example: If you insert a 100GBASE-CR10 CXP cable that fans out to three 40G QSFP cables, the transceiver detected is indicated as 100GBASE-CR10. If you configure the Resource Group for 3x40G mode, Ixia advertises 40G speed during Auto-Negotiation. The negotiated capability will be 40GBASE-CR4.
Enable Link Training	Select the check box to allow longer length copper cables to be used. This means that during the next Auto-Negotiation, KR training will be used. **Note**: This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. KR Training is not available on Multis QSFP+ and CXP load modules.
Restart AutoNegotiate	Restarts the Auto Negotiate sequence.
Enable RS-FEC	FEC or Forward Error Correction is available for XM100GE4QSFP28+ENH load module. If you select this check box, RS-FEC is used. FEC encrypts data sent on the line using some overhead for error correction code. This allows bit errors in flight to be corrected on the receiving side. The benefit of FEC is that it

Field/Control	Description
	allows very long copper cables to be used and allows cheaper parts to be used in optical transceivers as errors will be corrected. RS-FEC is compatible with Auto-Negotiation and KR Training. **Note**: • This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. • FEC should be enabled on both back-to-back ports for the link to be up. • CXP and QSFP+ load modules do not support FEC.
Enable RS-FEC Statistics	If you select this check box, RS-FEC Statistics is available. An RS-FEC codeword is a block of contiguous packets on the line. All RS-FEC codewords are of the same size. Thus, a block can represent many packets, few packets, portions of packets, or no packets at all. The two RS-FEC statistics are: • RS-FEC Corrected Codeword Count - Indicates that at least one error was encountered in a block that was able to be corrected. • RS-FEC Uncorrected Codeword Count - Indicates that too many errors existed within a block to be corrected. These statistics can increment when a link pair is idle. Any uncorrected FEC block can indicate any of the following problems: • Ixia is unable to insert RS-FEC errors. • Ixia is unable to drill-down into any FEC block to show what it represented. **Note**: By default, the check box is not available for selection. It is available only if the **Use IEEE Defaults** check box is cleared.

PCS Lane Statistics for Xcellon-Multis modules

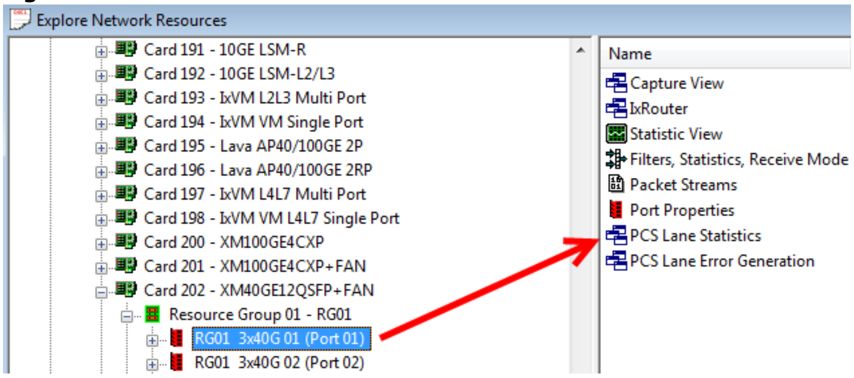
The PCS Lane Statistics table allows you to view the statistics for the configured PCS lanes. It is part of the Port Properties for the module.

NOTE PCS Lane Statistics is not available for the 3x10GE and 8x10GE CXP and QSFP Multis modes.

To open the PCS Lane Statistics table:

1. Select the Xcellon-Multis module in the left pane of the IxExplorer window
2. Expand the node, and select the Port object. In the right window pane, double-click the PCS Lane Statistics object as shown in the following figure:

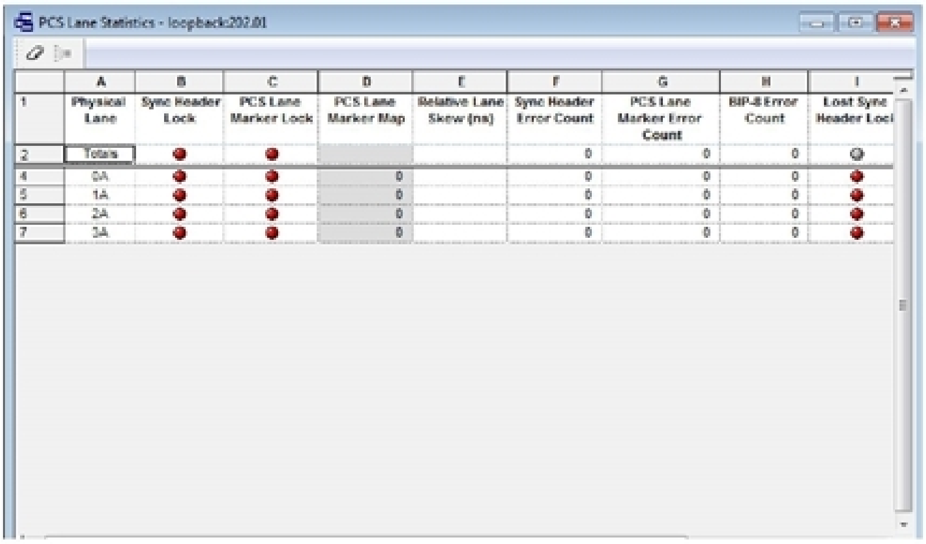
Figure:PCS Lane Statistics



The PCS Lane Statistics table opens. Use this table to view the PCS lane statistics for each lane. The statistics are for the **receive** side.

The PCS Lane Statistics table is shown in the following figure:

Figure:PCS Lane Statistics table for Multis



The following table explains the entries in the PCS Lane Statistics table:

Table:PCS Lane Statistics Data

Field/Control	Description
Physical Lane	The identifier for the Receive physical lane. This is a tag /fixed label to ID each lane.
Sync Header Lock	Indicates if the received PCS lane achieved sync-bit lock. Green indicates success, red indicates failure.
PCS Lane Marker Lock	Indicates if the received PCS lane has achieved alignment marker lock. Green indicates success, red indicates failure.
PCS Lane Marker Map	The VL number identified by the alignment marker. This is only valid when VL Lock is green.
Relative Lane Skew (ns)	Shows the actual skew in nanoseconds. Skew measurements are valid only when all lanes are

Field/Control	Description
	locked with 20 unique lane markers. The first VL markers to arrive have skew of 0. All other lane skews are relative to them.
Sync Header Error Count	The number of synchronization bit errors received.
PCS Lane Marker Error Count	The number of incorrect PCS lane markers received while in PCS lane lock state.
BIP-8 Error Count	The number of BIP-8 errors for a PCS lane. BIP-8 = Bit-Interleaved Parity with eight bit errors (BIP-8). Each bit in the BIP field is an even parity calculation over all previous selected bits of a PCS lane.
Lost Sync Header Lock	When lit, indicates the loss of sync header lock since the last statistic was read. If colored gray, there is no error. If colored red, an error has occurred.
Lost PCS Lane Marker Lock	When lit, indicates the loss of PCS lane marker lock since the last statistic was read. If colored gray, there is no error. If colored red, an error has occurred.

[This page intentionally left blank]

Chapter 28 - Port Properties–Novus and Novus-R QSFP28 Load Modules

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog varies according to the module type. The following sections describe the functions and configuration of the port properties of the Novus and Novus-R QSFP28 load modules.

NOTE The GUI for both Novus and Novus-R QSFP28 load modules are the same. In this chapter, the port properties are explained as per the Novus load module, but the documentation is also applicable for the Novus-R load module.

Port Properties for Novus Load Modules

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the Novus is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for Novus modules:

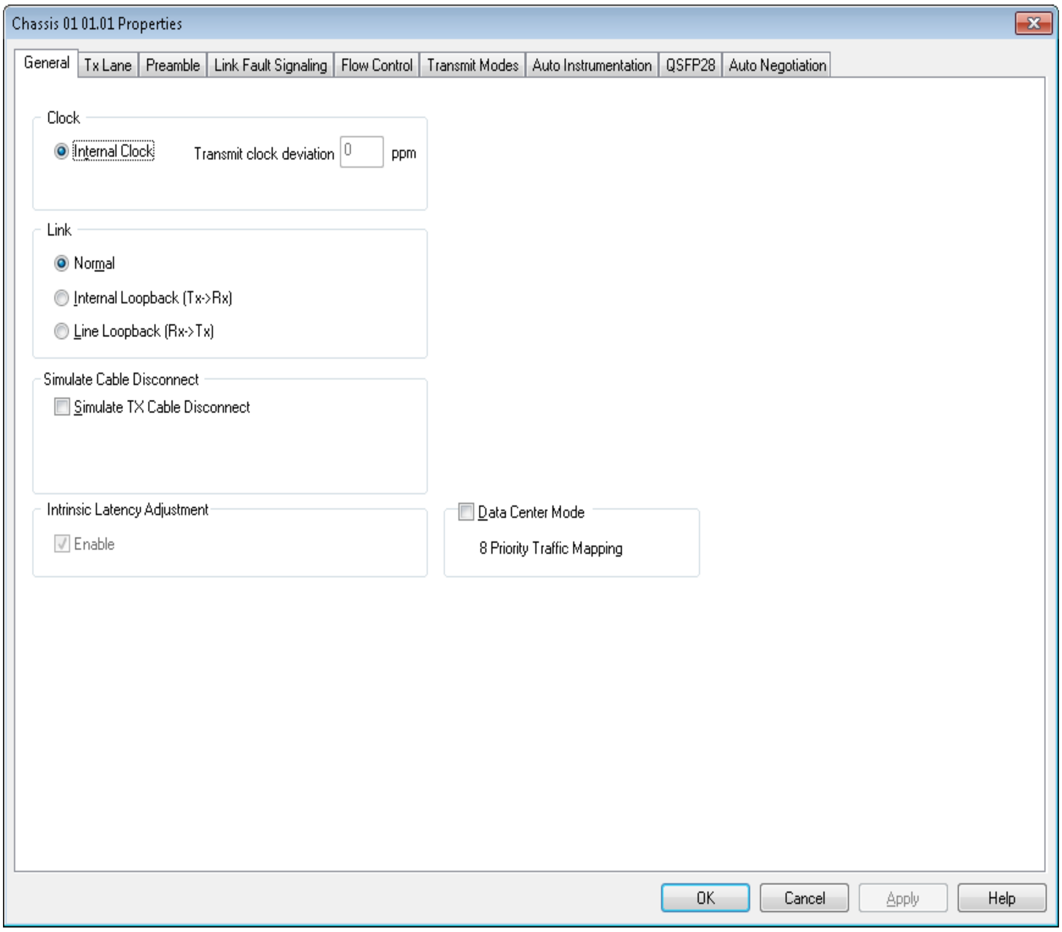
- Novus Port Properties—General
- Novus Port Properties—TX-Lane
- Novus Port Properties—Preamble
- Novus Port Properties—Link Fault Signaling
- Novus Port Properties—Flow Control
- Novus Port Properties—Transmit Modes
- Novus Port Properties—Auto Instrumentation
- Novus Port Properties—QSFP28
- Novus Port Properties—Auto Negotiation

Novus Port Properties—General

The Novus **General** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, and then selecting the **General** tab.

The Port Properties **General** tab is shown in the following figure:

Figure: Novus—General tab



The controls for **General** tab configuration are described in the following table:

Table:General Configuration

Section	Control/Field	Usage
Clock	Internal Clock	If selected, the timing for the SerDes reference clock comes from an internal oscillator.
	Transmit clock deviation	Allows to adjust the line transmit frequency for the port. The initial rate is controlled by the chassis chain reference clock. Then you can adjust the line transmit frequency for the port.
Link	Normal	Normal operation
	Internal Loopback (Tx -> Rx)	Internal Loopback—Transmit to Receive.
	Line Loopback (Rx -> Tx)	Enable/disable the Line Loopback—Receive to Transmit. NOTE The **Line Loopback** option is not available for Multis QSFP28 load modules.
Simulate Cable Disconnect		If selected, the port acts as if the cable has been disconnected.
Intrinsic Latency Adjustment	Enable	The Enable check box is selected by default. This enables the intrinsic latency adjustment.

Section	Control/Field	Usage
		The *Enable* check box is grayed out when no value exists in the system for the specific transceiver. It is available if a value exists (in the .xml file). For details, see *Intrinsic Latency Adjustment* in Chapter 16 of the *Ixia Platform Reference Manual*.
Data Center Mode		See Frame Data for FCoE Support.

Novus Port Properties—TX-Lane

The *Tx Lane* tab allows to control the PCS lane order and skew rate for each lane.

For more information on Lane Skewing, see the Lane Skew topic in the 'Multilane Distribution Configuration' chapter of the *Ixia Platform Reference Manual*. The Lane Skew topic is located under 'Types of Ports' / '100GE'.

The Novus Port Properties *Tx Lane* tab for the 100GE mode is shown in the following figure:

Figure: Novus—Tx Lane tab

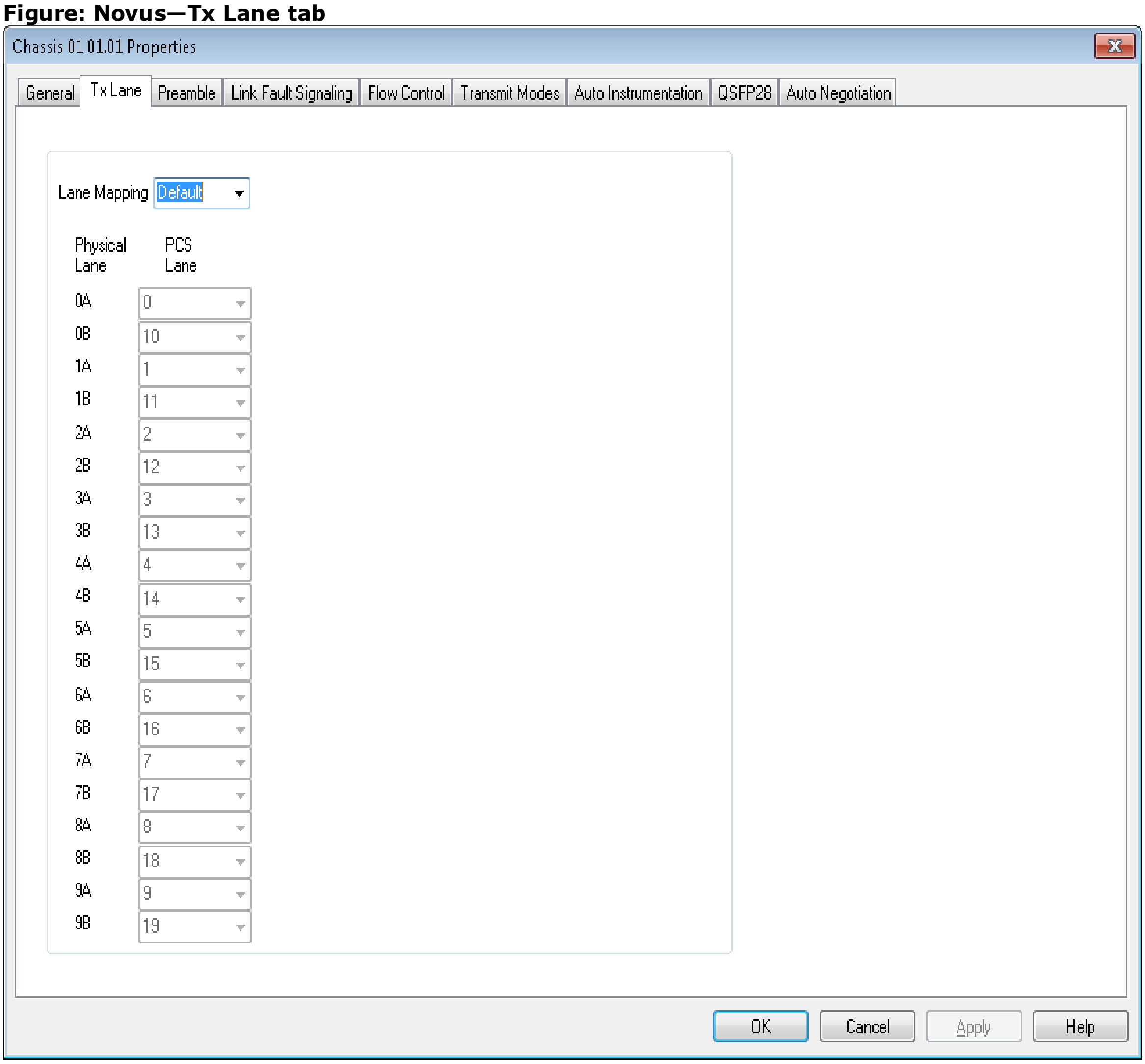


Table:Tx Lane Tab Configuration

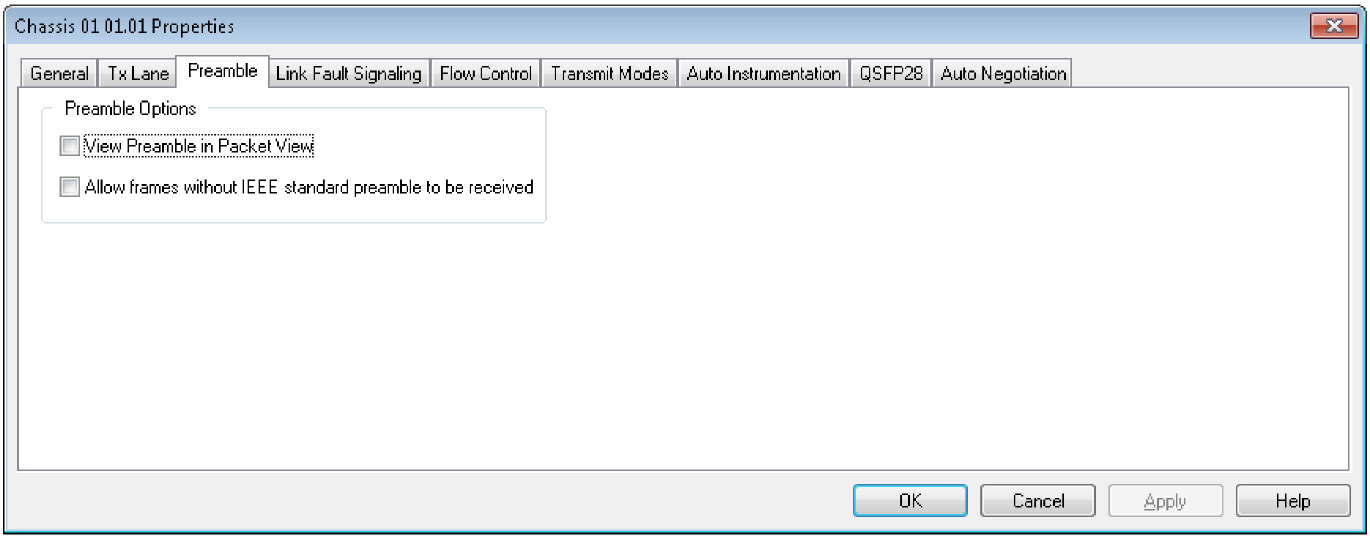
Field	Description
Lane Mapping	Allows you to select a PCS lane ordering method. There are five options: • Default–the default ordering method. The default order is each physical port corresponds to 2 PCS lanes that are n and n+10, where n = physical lane number. • Increment–orders the lanes from 0 to 19, straight down the list. • Decrement–orders the lanes from 19 to 0, straight down the list. • Custom–allows to put the lanes in any order by manually entering the numbers in the fields. The starting order is the last selected mapping. • Random - Allows to put the lanes in any random order, values will be any value from 0 to 19.
Physical Lane	The physical lane identifier. The physical lane is paired with a corresponding PCS lane.
PCS Lane	A number identifier for the PCS lane. The PCS lane is paired with a corresponding physical lane.

Novus Port Properties—Preamble

The preamble precedes the frame, but is not part of the frame itself.

The Novus Port Properties **Preamble** tab is shown in the following figure:

Figure: Novus —Preamble tab



The fields and controls in this tab are described in the following table:

Table:Preamble Configuration

Section	Choices	Description
Preamble Options	View Preamble in Packet View	When this check box is selected, the preamble data will be visible in the Packet View (transmit side) and the Capture View (receive side).
	Allow frames without IEE standard preamble to be received	When this check box is selected, it allows frames without IEEE standard preamble to be received.

Novus Port Properties—Link Fault Signaling

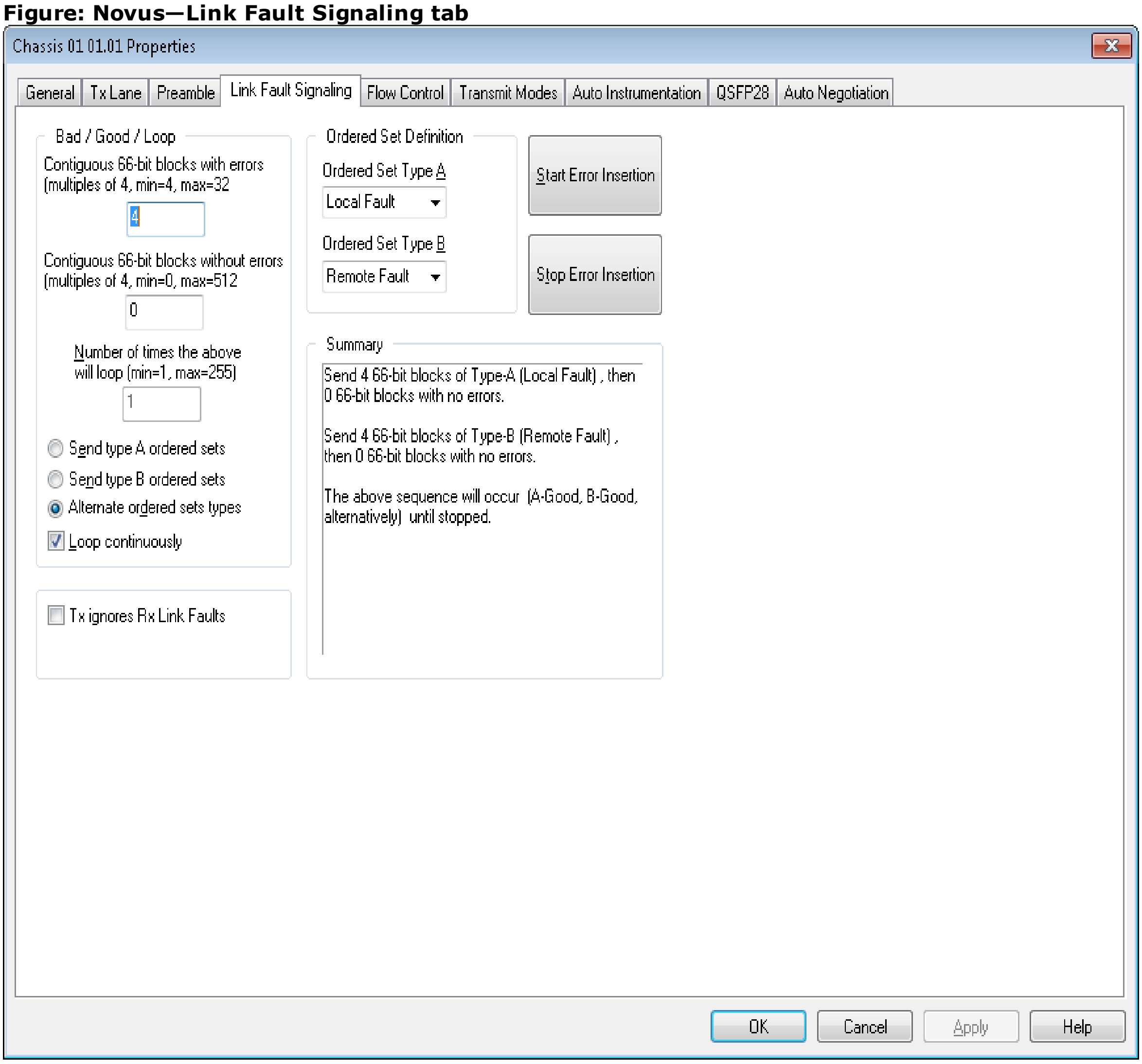
Link Fault Signaling is defined in Section 81.3.3.3 of the IEEE 802.3ba specification for 40 Gb/s and 100 Gb/s Ethernet. Link Fault Signaling is defined in Section 46 of the IEEE 802.3ae specification for 10 Gigabit Ethernet. When the feature is enabled, four statistics will be added to the list in Statistic View for the port. One is for monitoring the Link Fault State. Two provide a count of the Local Faults and Remote Faults. The last one is for indicating the state of error insertion, whether or not it is ongoing.

The 1x100GE Novus ports support Link Fault Signaling. Link Fault Signaling for Novus originates with the PHY sending an indication of a local fault condition in the link being used as a path for MAC data. In the typical scenario, the Reconciliation Sublayer (RS) that had been receiving the data will receive this Local Fault status, and then send a Remote Fault status to the RS that was sending the data. Upon receipt of this Remote Fault status message, the sending RS will terminate transmission of MAC Data, sending only 'Idle' control characters until the link fault is resolved.

The Link Fault Signaling tab is accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Link Fault Signaling* tab.

The *Link Fault Signaling* tab for Novus load module is shown in the following figure:

Figure: Novus—Link Fault Signaling tab



The controls for **Link Fault Signaling** tab configuration are described in the following table:

Table:Link Fault Signaling Configuration

Section	Field/Control	Description
Bad/Good/Loop	(Bad) Contiguous 66-bit blocks with errors (multiples of 4; min = 4, max = 32)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks with errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive fault sequences allowed are minimum 4 sequences and maximum 32 sequences.
	(Good) Contiguous 66-bit blocks without errors (multiples of 4; min = 0, max = 512)	Part of the Bad block/Good block alternating pattern. Enter the number of 66-bit blocks without errors that should be included in the pattern. This value must be a multiple of 4. The number of consecutive regular data sequences allowed are minimum 0 sequences

Section	Field/Control	Description
		and maximum 512 sequences.
	Number of times the above will loop (min = 1, max = 255)	Specifies the number of loops for the user defined sequence. There are two modes: • Discrete iterations: i) Minimum of 1 iteration ii) Maximum of 255 iterations • Continuous loop i) User cannot specify number of iterations
	Choose one of: • Send type A ordered sets • Send type B ordered sets • Alternate ordered set types	Defines the ordered set pattern that will be sent. (The two Ordered Sets—A and B—are defined in the *Ordered Set Definition* box in this tab.) This pattern will be combined with the Good block-s/Bad blocks pattern for transmission. • Only Type A fault sequence and regular good data sequences • Only Type B fault sequence and regular good data sequences • Alternate Type A, regular good data sequences and Type B fault sequence, regular good data sequences NOTE If this field is available, and the Alternate ordered set types option is selected, the minimum value for this field should be '2,' to allow the entire pattern to be sent once. If left at the minimum value of '1'— only two groups of blocks (one of good blocks and one of bad blocks) will be sent, which means that only the first ordered set will be sent. A minimum of eight blocks is required for one complete pattern including Types A and B.
	Loop continuously	If selected, the loop defined by the combination of the Bad and Good blocks plus the pattern of ordered sets, will be transmitted continuously until the *Stop Error Insertion* button is clicked.
Ordered Set Definition	Ordered Set Type A	Choose one of: • Local Fault • Remote Fault
	Ordered Set Type B	Choose one of: • Local Fault • Remote Fault
Tx ignores Rx Link		If selected, ongoing transmission will continue

Section	Field/Control	Description
Faults		even if Link Fault messages are received by the sending RS.
Summary (Win-dow)		(Read-only) Displays descriptions of the patterns that will be transmitted.
Start Error Inser-tion		Press this button to start the transmission of the configured error patterns.
Stop Error Inser-tion		(Available only for use with the *Loop con-tinuously* option.) Press this button to stop the transmission of the configured error patterns.

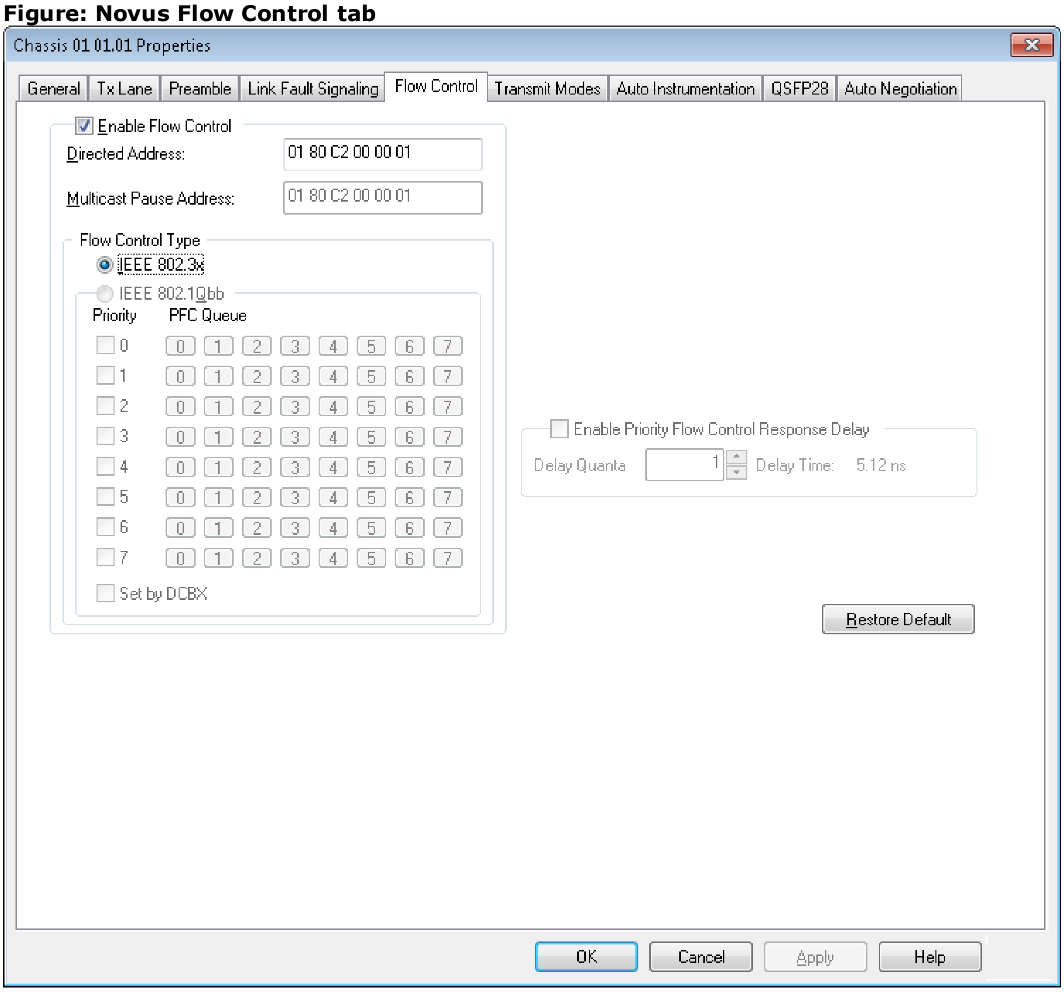
Novus Port Properties—Flow Control

The Novus **Flow Control** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Flow Control** tab.

NOTE You can view this help page for the Port Properties - Flow Control tab by clicking the Help button and not F1.

The Port Properties **Flow Control** tab is shown in the following figure:

Figure: Novus Flow Control tab



The controls for **Flow Control** tab configuration are described in the following table:

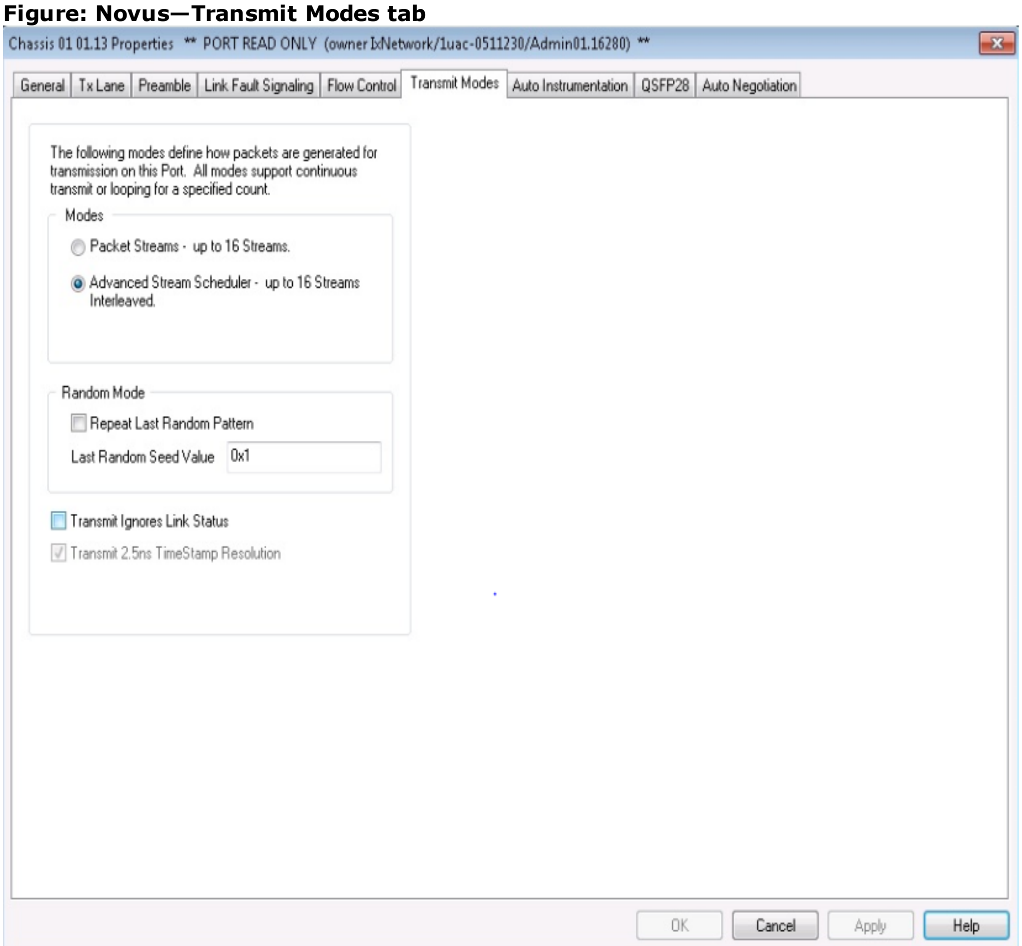
Section	Field/Control	Description
Enable Flow Control	(check box)	Enables the port's MAC Flow control mechanisms to listen for a directed address pause message.
	Directed Address	This is the MAC address that the port will listen on for a directed pause message.
	Multicast Pause Address	(Read-only) This is the MAC address that the port will listen on for a multicast pause message.
Flow Control Type	IEEE 802.3x or IEEE 802.1Qbb	Priority-based Flow Control. When in Data Center mode, the port responds to either IEEE 802.3x pause frame or to IEEE 802.1Qbb Priority-based Flow Control (PFC) frame. When not in Data Center mode, only IEEE 802.3x is available.
	Priority	Priority-based Flow Control.
	PFC Queue	Priority-based Flow Control
Enable Priority Flow Control Response Delay	(check box)	If selected, enables to increase the number of frames that is sent when a pause frame is received. Priority Flow Control (PFC) pause allows to set the delay of flow control. When a pause frame is received for a certain priority, a count of the number of timestamp ticks increments up to a desired offset and then releases the pause request to the TX engine. For example, if running at 100% line rate and there is no delay in the pause request, the TX pipeline transmits the specified number of frames once the pause request is received. With this feature, a delay by number of timestamp ticks is programmed.
	Delay Quanta	This field allows to set the delay quanta of flow control.
	Delay Time	The delay time, in nanoseconds, of frames.
Restore Default		Resets the Directed Address back to the default value of *01 80 C2 00 00 01.*

Novus Port Properties—Transmit Modes

The **Transmit Modes** tab for Novus load modules is shown in the following figure. It is accessed by double-clicking a port in Resources window, or by right-clicking a port and selecting the **Properties** menu option. Then select the **Transmit Modes** tab.

The Port Properties **Transmit Modes** tab is shown in the following figure:

Figure: Novus—Transmit Modes tab



The controls for **Transmit Modes** tab configuration are described in the following table:

Table:Transmit Modes Configuration

Section	Field/Control	Description
Modes	Packet Streams	Sets the operating mode for the port to sequential packet streams. This allows to configure 32 streams in 100G mode and 16 streams in 25G mode. A stream may be programmed for continuous packet generation—generating a continuous, infinite number of packets.
	Advanced Stream Scheduler	Sets the operating mode for the port to interleaved packet streams. This allows to configure 32 streams in 100G mode and 16 streams in 25G mode. They will transmit packets in an interleaved fashion. Refer to *Stream Control for Advanced Streams* for additional information on Advanced Streams.
Random Mode	Repeat Last Random Pattern	Selecting this check box causes the port to retransmit the last random pattern of data sent. This affects any random data in the stream,

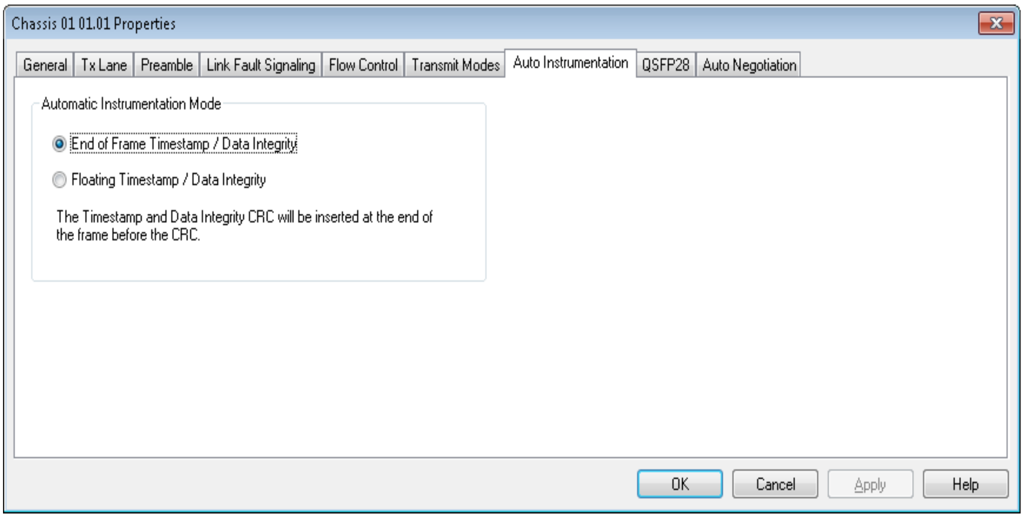
Section	Field/Control	Description
		including payload, frame size, UDFs, and so forth. This can be used before transmission (in which case the seed from the first packet stream will be used), or immediately after a stream has been sent (in which case the last stream's random seed is used). For more information, see the Repeat Last Random Pattern section in the 'Theory of Operation: General' chapter of the *Ixia Platform Reference Manual*.
	Last Random Seed Value	This read only field represents the initial value that hardware will use to seed its random number generators. Note that it is not a one-to-one mapping.
Transmit Ignores Link Status		If selected, will allow transmission of packets even if the link is down.
Transmit 2.5ns Time stamp Resolution		If selected, it will check for the high resolution time stamp. The check box is selected by default.

Novus Port Properties—Auto Instrumentation

The Novus **Auto Instrumentation** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The Novus Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure: Novus—Auto Instrumentation tab



The options and controls in this tab are described in the following table:

Table:Auto Instrumentation Configuration

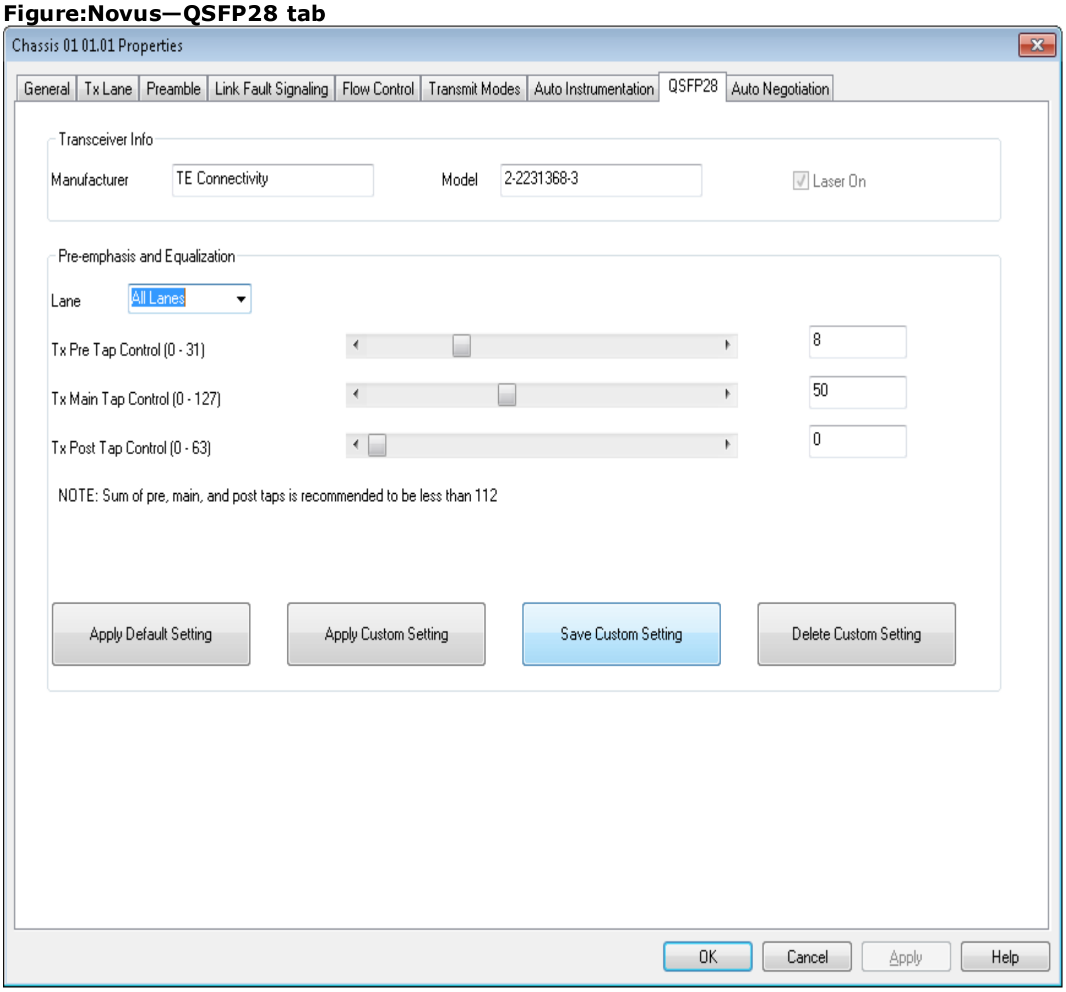
Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Novus Port Properties—QSFP28

The Novus **QSFP28**tab is accessed by right-clicking an Novus port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **QSFP28** tab.

The Novus Port Properties **QSFP28** tab is shown in the following figure:

Figure:Novus—QSFP28 tab



The options and controls in this tab are described in the following table:

Table:QSFP28 Configuration

Section	Field/Control	Description
Transceiver Info	Manufacturer	This is the Vendor Name field read from the actual transceiver currently being plugged in.
	Model	This is the Part Number field read from the actual transceiver currently being plugged in.

Section	Field/Control	Description
	Laser On	Select this check box to enable the laser power. Note that the actual reading will be displayed in the Value field.
Pre-emphasis and Eqalization	Lane	Specifies in which lane (from 0-3) the current settings on.
	Tx Pre Tap Control (0-31)	This helps to control the Pre Tap value for Tx.
	Tx Main Tap Control (0-31)	This helps to control the Main Tap Control for Tx.
	Tx Post Tap Control (0-63)	This helps to control the Post Tap value for Tx.
	Apply Default Settings	If clicked, a default setting will be applied to the current user setting for the current adapter/xcvr type and to the actual hardware.
	Apply Custom Settings	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, this custom setting will be applied to the current user setting and to the actual hardware.
	Save Custom Setting	If clicked, if there exists a custom setting in the xml file for the same adapter/xcvr type, users will be prompted to choose to cancel or overwrite the record from that xml file. If no custom setting exists, the setting will be saved to the xml file. The "TapConfigurations.xml" file will be created at the Ixia\IxOS folder once users click the Save Custom Setting. All the custom settings (if any) are stored in this folder.
	Delete Custom Setting	If clicked, if there exists a custom setting in the xm file for the same adapter/xcvr type, users will be prompted to confirm that they are about to delete it and they will have to choose to ok or cancel with that. If no custom setting exists, users will be prompted that nothing will be deleted.

Novus Port Properties—Auto Negotiation

This tab is available for Novus load module. The Novus Auto Negotiation tab is accessed by right-clicking a Novus port in the Explore Network Resources pane, selecting the Port Properties menu option, then selecting the Auto Negotiation tab.

The Port Properties **Auto Negotiation** tabs for Novus are shown in the following figures:

Figure: Novus 100GE—Auto Negotiation tab

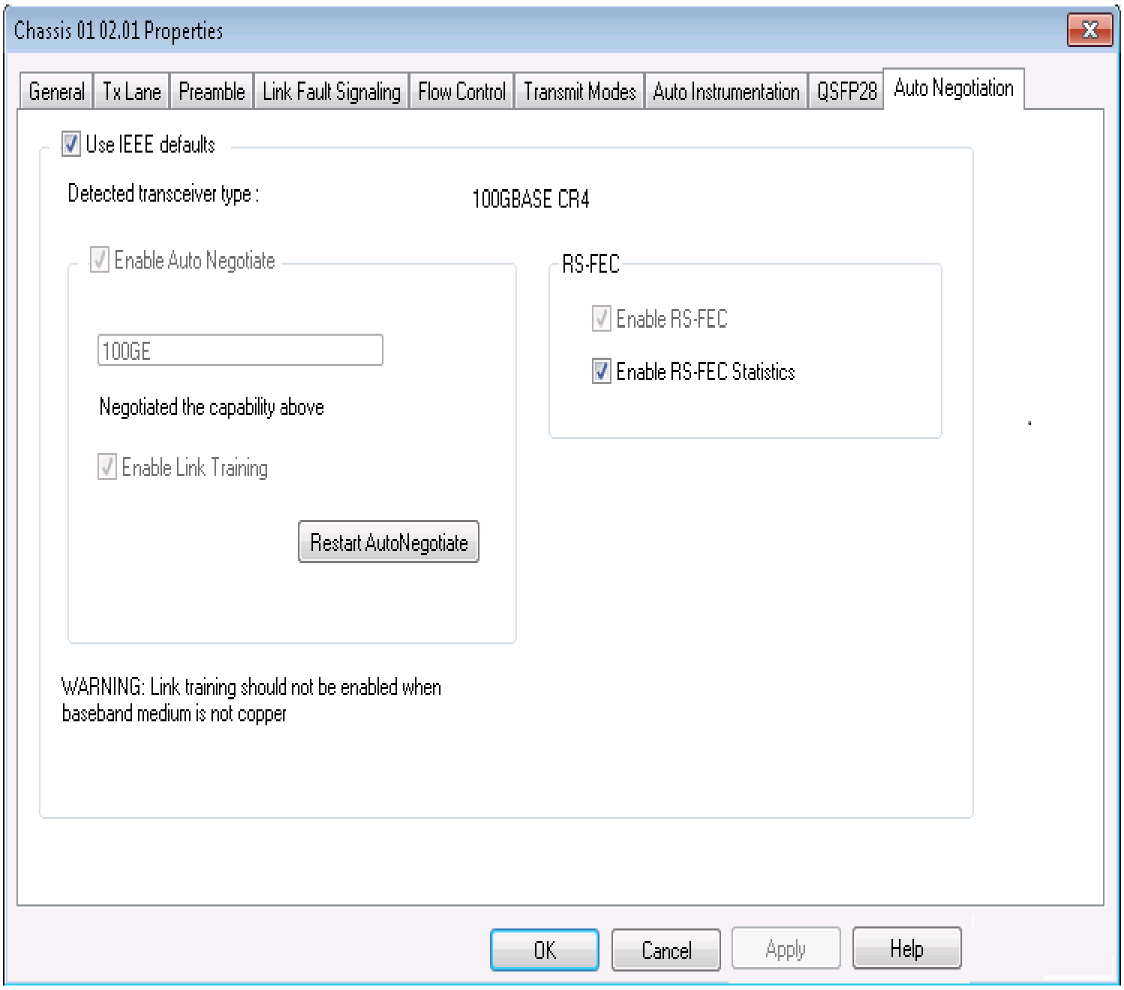
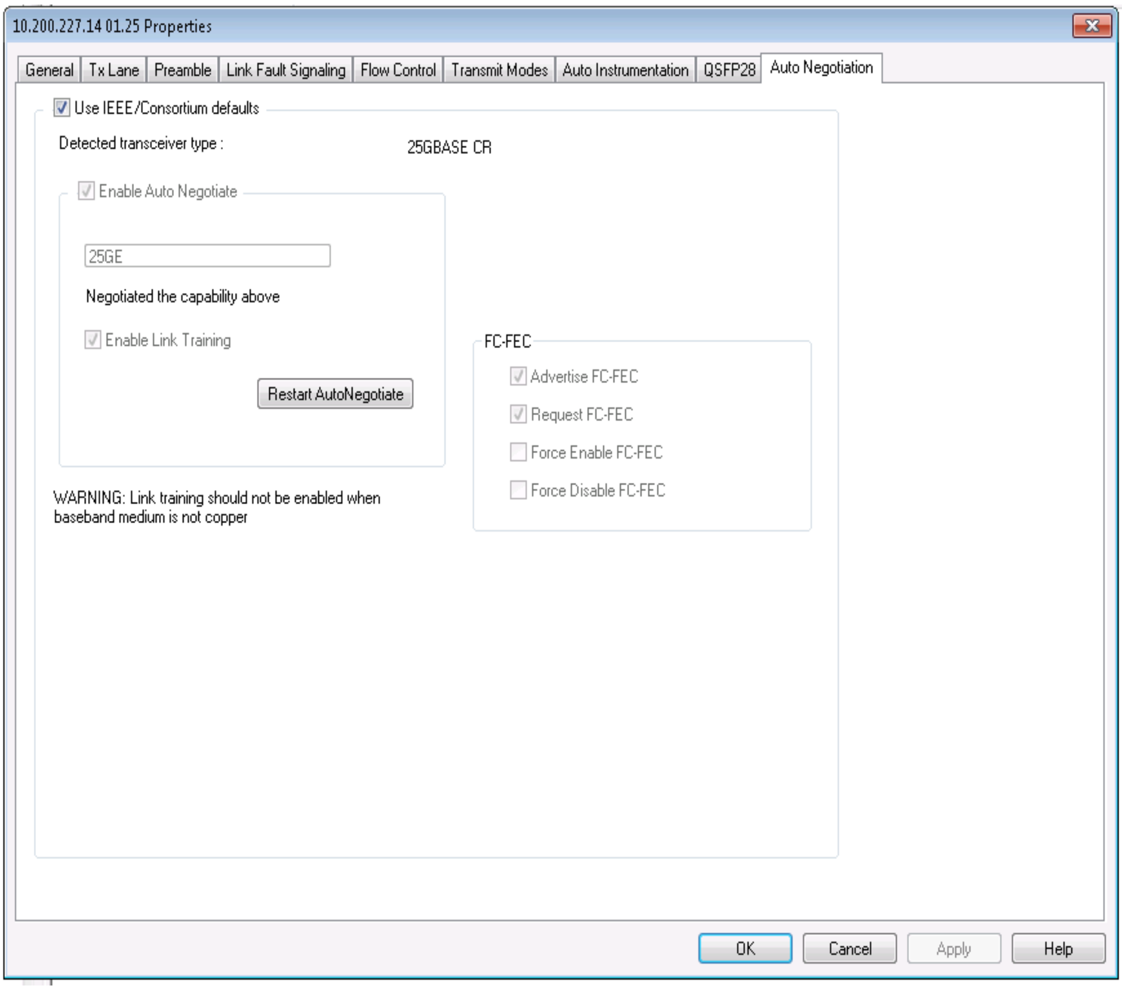


Figure: Novus 25GE—Auto Negotiation tab



The fields and controls in these tabs are described in the following table:

Table: Novus Auto Negotiation Tab

Field/Control	Description
Use IEEE defaults	When you select the Use IEEE Defaults check box, the L1 parameters like Autonegotiation, Link Training, and FEC, are enabled or disabled per IEEE requirements, and you will not be able to enable or disable these manually. If the check box is cleared, you will be able to manually enable or disable L1 features – even if it violates IEEE specifications. By default the check box is selected.
Detected transceiver type	When a transceiver is inserted into the load module, the software reads IEEE registers to determine the transceiver capabilities and media type. If the transceiver contains this information, it is shown in this read-only field. If the transceiver is capable of multiple speeds, the supported speed is shown. NOTE The speed at which the Resource Group is currently operating, does not affect this. For example, if the Resource Group is configured

Field/Control	Description
	NOTE to operate in 100GE mode, then the Detected transceiver type still indicates 100GE. If the Resource Group is configured to operate in 25GE mode, then the Detected transceiver type indicates 25GE.
Enable Auto Negotiate	Auto negotiation controls how a port communicates with other ports. If you select the check box, it allows auto-negotiation of speed and duplex operation based on the various choices. The capabilities that are selected are advertised during auto-negotiation. Auto-Negotiation starts when: • Link is attempting to be established • Link has dropped and is re-establishing • **Restart Auto-Negotiate** button is clicked (this does a forced restart) NOTE The **Enable Auto Negotiate** check box is available for selection only if the **Use IEEE Defaults** check box is cleared.
Negotiated the capability above	The text box indicates the speed that was negotiated due to Auto-Negotiation. NOTE This speed may be different than the speed indicated for the transceiver detected. For example: If the detected transceiver type is 100GBASE CR4, the negotiated speed is 100GE.
Enable Link Training	Select the check box to allow longer length copper cables to be used. This means that during the next Auto-Negotiation, KR training will be used. Link Training is enabled by default when Auto-Negotiation is enabled. NOTE This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. KR Training is not available on Multis QSFP+ and CXP load modules.
Restart AutoNegotiate	Restarts the Auto Negotiate sequence.
Enable RS-FEC	FEC or Forward Error Correction is available for NOVUS100GE8Q28+FAN load module. If you select this check box, RS-FEC is used. FEC encrypts data sent on the line using some overhead for error correction code. This allows bit errors in flight to be corrected on the receiving side. The benefit of FEC is that it allows very long copper cables to be used and allows cheaper parts to be used in optical transceivers as errors

Field/Control	Description
	will be corrected. RS-FEC is compatible with Auto-Negotiation and KR Training. NOTE • This check box is available for selection only if the **Use IEEE Defaults** check box is cleared • FEC should be enabled on both back-to-back ports for the link to be up • CXP and QSFP+ load modules do not support FEC
Enable RS-FEC Statistics	If you select this check box, RS-FEC Statistics is available. An RS-FEC codeword is a block of contiguous packets on the line. All RS-FEC codewords are of the same size. Thus, a block can represent many packets, few packets, portions of packets, or no packets at all. The two RS-FEC statistics are: • RS-FEC Corrected Codeword Count - Indicates that at least one error was encountered in a block that was able to be corrected. • RS-FEC Uncorrected Codeword Count - Indicates that too many errors existed within a block to be corrected. These statistics can increment when a link pair is idle. Any uncorrected FEC block can indicate any of the following problems: • Ixia is unable to insert RS-FEC errors. • Ixia is unable to drill-down into any FEC block to show what it represented. NOTE This check box is enable by default.
• Advertise FC-FEC • Request FC-FEC • Force Enable FC-FEC • Force Disable FC-FEC	FC-FEC or Fire Code-Forward Error Correction is available for NOVUS100GE8Q28+FAN+25G load module for 25G mode. RS-FEC is available for NOVUS100GE8Q28+FAN+25G load module for 100G mode. When a port participates in 25G Auto-negotiation, it tells the link partner if it supports FC-FEC and if it wants the link partner to turn FC-FEC on. The four available FC-FEC statistics are: • Advertise FC-FEC: If enabled, the port tells a link partner to support FC-FEC the next time it participates in Auto-negotiation • Request FC-FEC: If enabled, the port tells a link partner to turn on FC-FEC the next time it participates in Auto-negotiation • Force Enable FC-FEC: Turns FEC on by bypassing Auto-

Field/Control	Description
	negotiation • Force Disable FC-FEC: Turns FEC off by bypassing Auto-negotiation NOTE • This check box is available for selection only if the **Use IEEE Defaults** check box is cleared. • FEC should be enabled on both back-to-back ports for the link to be up.
FC-FEC Statistics	The three FC-FEC statistics are: • FC-FEC Corrected Block Count - Indicates that at least one error was encountered in a block that was able to be corrected. • FC-FEC Uncorrected Block Count - Indicates that too many errors existed within a block to be corrected. • FS-FEC Corrected Error Bits - Indicates that at least one error was encountered in the data (in bits) that was able to be corrected. • Fire code FEC Sync - Indicates whether the FEC engine has locked onto a FEC pattern. **Sync** indicates that FEC is up. **No Sync** indicates that FEC is not locked onto a pattern. NOTE **No Sync** is displayed even if FEC is not actively used.

[This page intentionally left blank]

Chapter 29 - Port Properties–VM

The *Port Properties* dialog controls a number of properties related to the port's operation. The *Port Properties* dialog is a display that corresponds to the module type. The following sections describe the functions and configuration of the VM family of module port properties.

Port Properties for VM Ports

The **Port Properties** dialog is accessed by right-clicking a port in the **Resources** window, then selecting the **Properties** menu option.

The complete specification for the VM is found in the *Ixia Platform Reference Manual*.

The following port property tabs are available for the various VM ports:

- *VM Port Properties—Status*
- *VM Port Properties—Transmit Modes*
- *VM Port Properties—VM Port Info*
- *VM Port Properties—Auto Instrumentation*

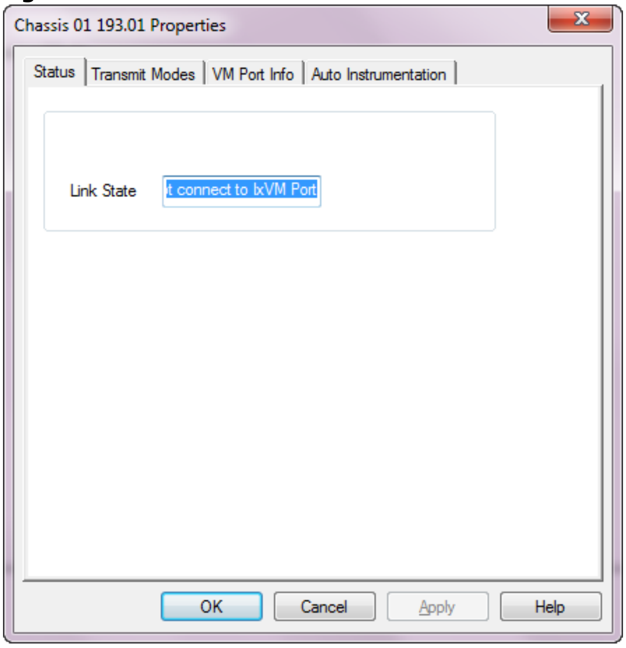
VM Port Properties—Status

The *Status* tab displays the link state and allows the port to be disabled manually. This feature also automatically disables a port which has a hardware fault—at power up or at run time. It allows the chassis to restart without taking the time to check the status of this port. The port can also be disabled if a hardware fault occurred, or for some other purpose. The *Enable Port* check box is enabled by default.

The *Status* tabis accessed by right-clicking a port in Resources pane and selecting the *Properties* menu option, or by double-clicking a port in the Detail pane. Then select the *Status* tab.

The *Status* tab is shown in the following figure.

Figure:VM Status tab



The display of the status of the link is also shown in the Statistic View for this port. The possible states are:

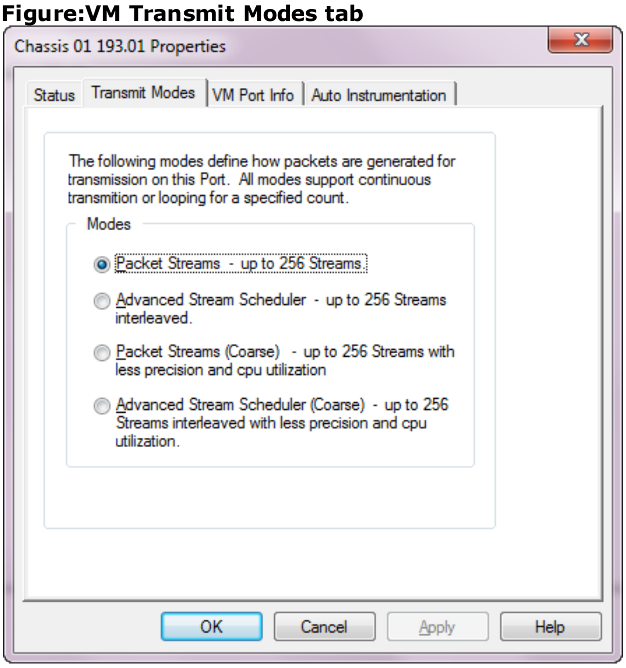
- Hardware Fault
- Disabled, Busy
- Link Up
- Link Down
- Loopback
- WriteMII
- Demo Mode
- empty (no status displayed if the chassis is disabled)

VM Port Properties—Transmit Modes

The **Transmit Modes** tab is shown in the following figure. It is accessed by right-clicking a port in Resources window and selecting the **Properties** menu option, or by double-clicking a port in the Detail pane.. Then select the **Transmit Modes** tab.

The VM Port Properties **Transmit Modes** tab is shown in the following figure:

Figure:VM Transmit Modes tab



The controls for **Transmit Modes** tab configuration are described in the following table:

Table:Transmit Modes Configuration

Field/Control	Description
Packet Streams	Sets the basic operating mode for the port to packet streams. This allows to configure up to 256 streams. A stream may be programmed for continuous burst or packet generation-generating a continuous, infinite number of packets.
Advanced Stream Scheduler	Up to 256 streams can be interleaved at the same time for IxVM. Each stream is assigned a percentage of the maximum rate. The streams are mixed in a pseudo-random manner so that each stream's long-term percentage of the total transmitted data is as assigned.
Packet Streams (Coarse)	Sets the basic operating mode for the port to packet streams with less precision and cpu utilization. This allows to configure up to 256 streams. A stream may be programmed for continuous burst or packet generation-generating a continuous, infinite number of packets.
Advanced Stream Scheduler (Coarse)	Up to 256 streams can be interleaved at the same time for IxVM with less precision and cpu utilization. Each stream is assigned a percentage of the maximum rate. The streams are mixed in a pseudo-random manner so that each stream's long-term percentage of the total transmitted data is as assigned.

NOTE

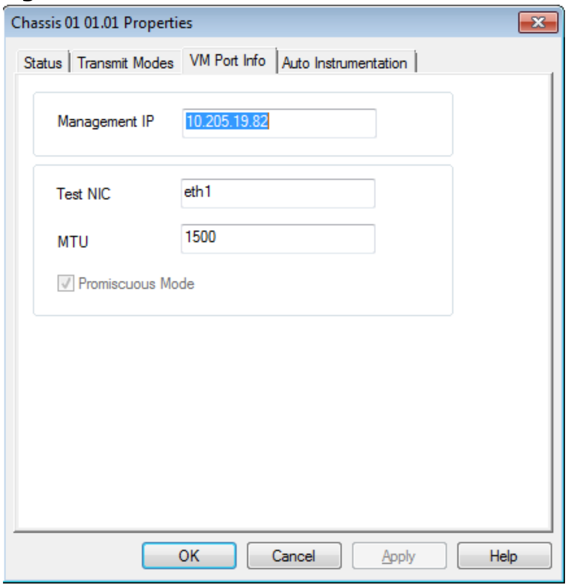
Coarse mode is used mostly on large scale setups to reduce cpu power used by ports, this comes with a precision loss because of this use it only if normal mode can’t be used.

VM Port Properties—VM Port Info

The **VM Port Info** tab is accessed by right-clicking a port in Resources pane and selecting the **Properties** menu option, or by double-clicking a port in the **Detail** pane. Then select the **VM Port Info** tab. This tab provides basic port configurations. All this options are read only and are inherited from VM Card, to change some of the options please go to Card proprieties.

The VM Port Properties **VM Port Info** tab is shown in the following figure:

Figure:VM Port Info tab



The controls for **VM Port Info** tab configuration are described in the following table:

Table:TVM Port Info Configuration

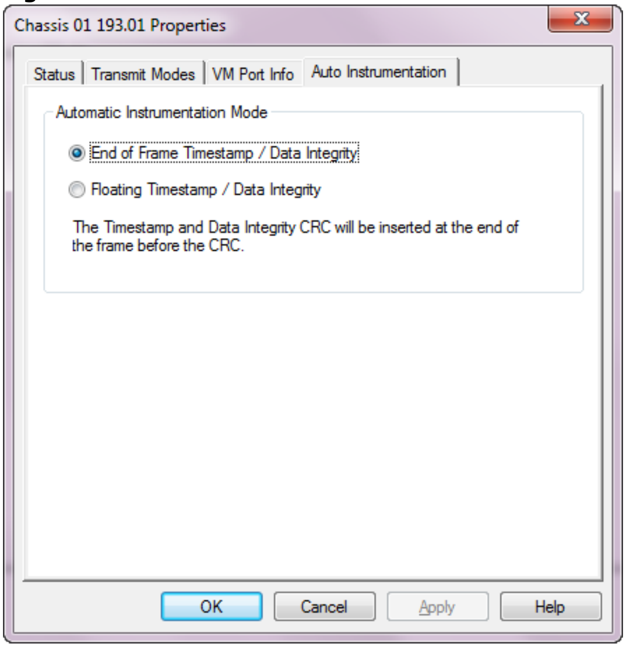
Field/Control	Description
Management IP	Management IP address of the Linux machine with the IxVM software agent installed.
Test NIC	Name of the virtual interface that will be used as a traffic generator. Virtual interface must be created before adding the port.
MTU	MTU value of test interface from a virtual machine. The minimum value is 1500 and the maximum value is 9000 and should be changed mainly when there are control plane frames bigger than 1500.
Promiscuous mode	Denote the promiscuous or non-promiscuous mode in which a virtual port is added to a virtual card.

VM Port Properties—Auto Instrumentation

The VM **Auto Instrumentation** tab is accessed by right-clicking a port in the **Explore Network Resources** pane, selecting the **Port Properties** menu option, then selecting the **Auto Instrumentation** tab.

The VM Port Properties **Auto Instrumentation** tab is shown in the following figure:

Figure:VM Auto Instrumentation tab



The options and controls in this tab are described in the following table:

Table:Auto Instrumentation Configuration

Field/Control	Description
End of Frame Timestamp / Data Integrity	Enables inserting Timestamp and Data Integrity CRC at the end of the frame before the CRC.
Floating Timestamp / Data Integrity	Enables adding timestamp as part of floating instrumentation header, and addresses similar issue in Data Integrity checking.

Chapter 30 - MII Registers

MII Register Files

Media-Independent Interface (MII) files store the settings of the PHY registers for Ethernet load modules. The MII files used on a particular chassis are located in the *MII Templates* directory in the IxExplorer Resources tree.

MII information can be displayed in IxExplorer for two modes:

- *Internal MIIs*—This MII contains the PHY register information for the internal PHY (physical layer device) for the local load module/port.
- *External MIIs*—These MIIs are only available for 10GE XAUI and 10GE XENPAK load modules/ports.

Internal MIIs

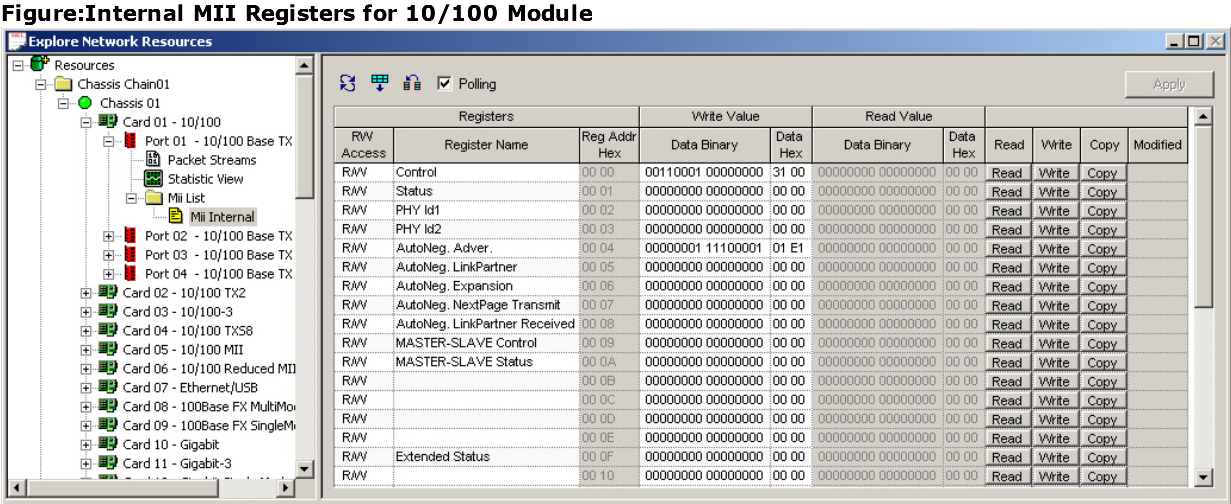
Default internal MII template files exist for each of the Ethernet-type load modules. These files can be accessed in several ways:

- *MII Lists—Internal MII Registers*
- *Auto Negotiation Tab*
- *Advanced MII Tab*

MII Lists—Internal MII Registers

These files are listed in the IxExplorer Resources Tree for each Ethernet-type port in a sub-directory named *MII List*. The contents of the MII List for a 10/100 load module consist of one file (Internal MII), as shown in *Figure:Internal MII Registers for 10/100 Module*.

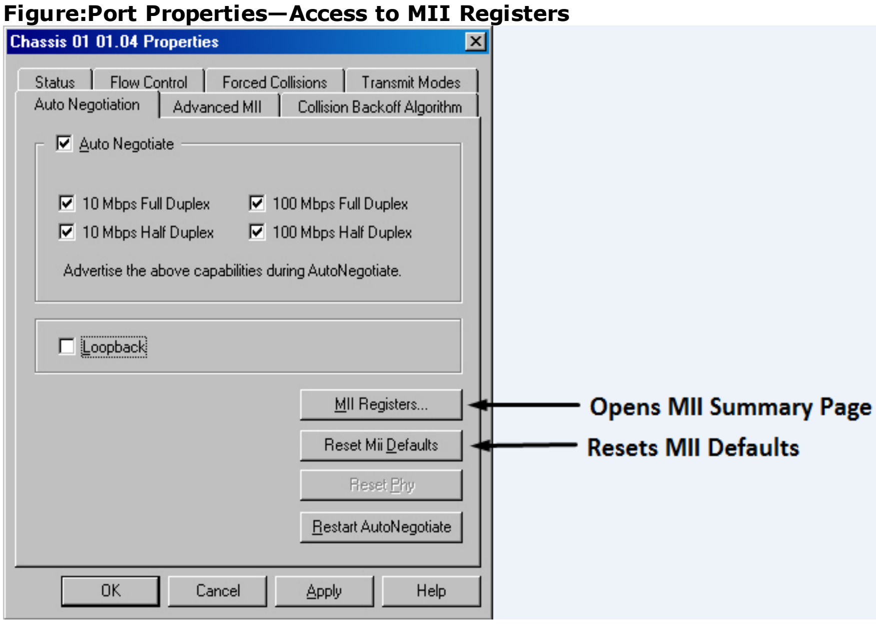
Figure:Internal MII Registers for 10/100 Module



Auto Negotiation Tab

The Internal MII register information is also available through the Port Properties *Auto Negotiation* tab for the load module, as shown in *Figure:Port Properties—Access to MII Registers*.

Figure:Port Properties—Access to MII Registers



The controls in this tab related to MII Registers are described in *Table:Access to MII Registers by Port Properties*.

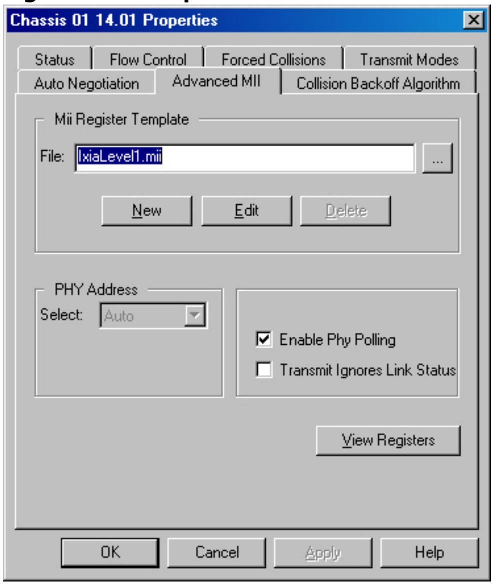
Table:Access to MII Registers by Port Properties

Control	Usage
MII Registers...	Opens a dialog with a set of tabs for the MII Registers associated with the port. These tabs allow the current MII register values to be read, written, and saved to a file.*MII Register Summary Tab*
Reset MII Defaults	Resets all of the port's PHY properties back to the default MII settings.

Advanced MII Tab

The *Advanced MII* tab in the *Port Properties* dialog allows for the proper association of MII registers to the port. The *Advanced MII* tab for a 10/100 port is shown in *Figure:Port Properties—Advanced MII Tab*.

Figure:Port Properties—Advanced MII Tab



The upper section, labeled *MII Register Template*, is used to control the selection and editing of a register template file. MII Register Template files hold the register definitions. It is initially set to use the appropriate default template that corresponds to one of the PHYs in use on that Ixia module card. Additions or corrections can be made, and even saved under a different template name. Once the proper associations are made, the current MII register values are easily read and modified using the*MII Register Summary Tab. The fields and controls in this tab are described in Table:Advanced MII Tab*

Table:Advanced MII Tab

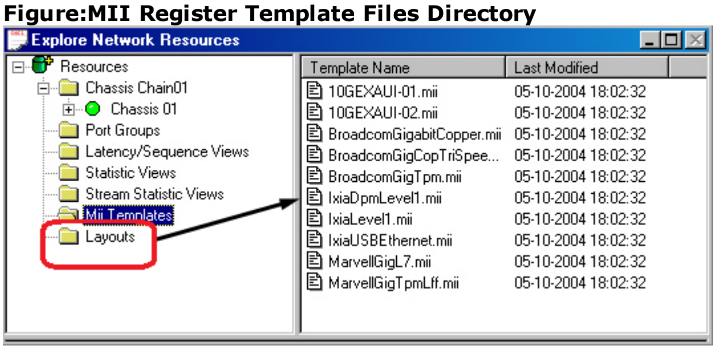
Section	Field/Control	Usage
MII Register Template	File	The name of the MII register file.
	Browse	Opens up a standard Windows file browsing window in the directory `C:\Program Files\Ixia\MII`, looking for files that end in *.mii*.
	New	Allows the creation of a new MII register Template file. *New/Edit MII Register Template Setup—Management Page for operational details.*
	Edit	Allows the editing of the indicated file. *New/Edit MII Register Template Setup—Management Page for operational details.*
	Delete	Deletes the current file after a confirmation dialog.
PHY Address	Select	Allows the address of the PHY to be set to Auto, or a constant from 0 to 31. (For other than 10/100 modules, it is configured for Auto and manual configuration is disabled.)
	Enable Phy Polling	If selected, then the PHY is continuously polled during MII setup operation.

Section	Field/Control	Usage
	Transmit Ignores Link Status	If selected, allows transmission of packets with the link down.

MII Register Template Files

The MII Register Templates are located in `C:\Program Files\Ixia\MII Templates`. A list of MII template files available in the Demo Mode is shown in *Figure:MII Register Template Files Directory*.

Figure:MII Register Template Files Directory

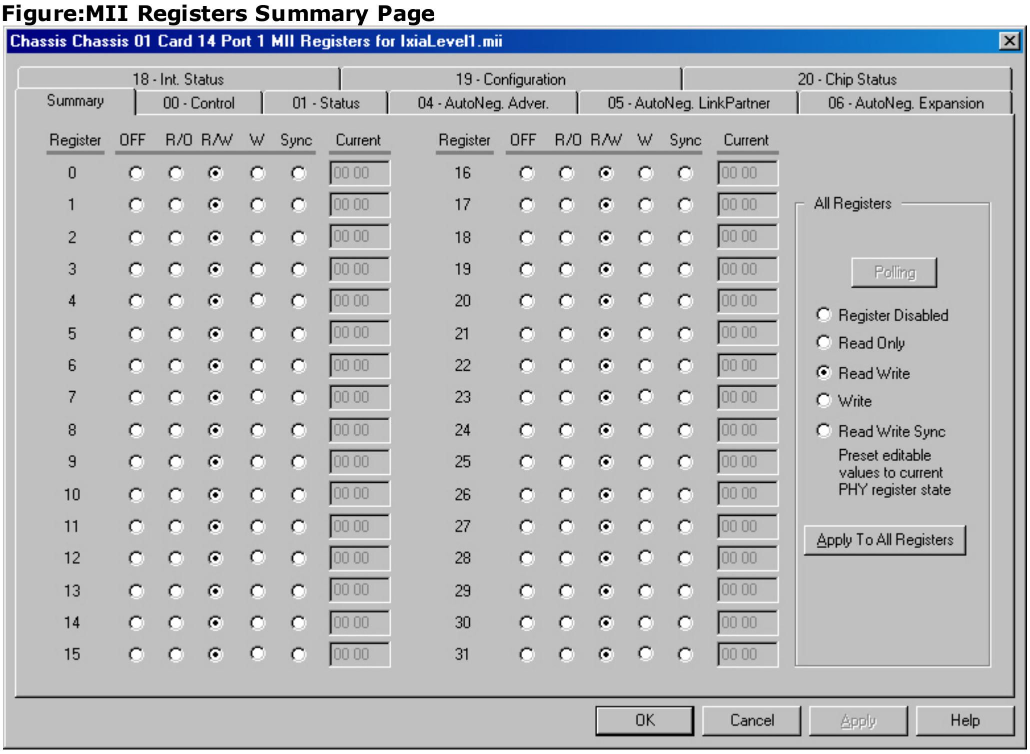


Clicking one of the file names opens a set of register dialogs for that file, with the Edit/Update dialog displayed. This template file may be saved under a different file name, by pressing the *Change Template Name...* button and renaming it in the *Save* dialog.

MII Register Summary Tab

MII register properties are available through the *MII Registers* dialog set of tabs, as shown for a `IxiaLevel1.mii` file for a 10/100 module in *Figure:MII Registers Summary Page*.

Figure:MII Registers Summary Page



The MII register *Summary* tab shows the status of all 32 MII registers. Each register's value, as well as the state of each register, is displayed. The default setting for the state is

Sync (*Read Write Sync*), but different states may be selected for individual registers on this page. The register states are one of:

- OFF (Register Disabled)—The register is neither read nor written during operation.
- R/O (Read Only)—The register is read-only.
- R/W (Read Write)—(default setting) The register may be read or written.
- W (Write)—The register is write-only.
- Sync (Read Write Sync)—The register is read and written during operation. In addition, the read values are placed into the editable fields at the same time.

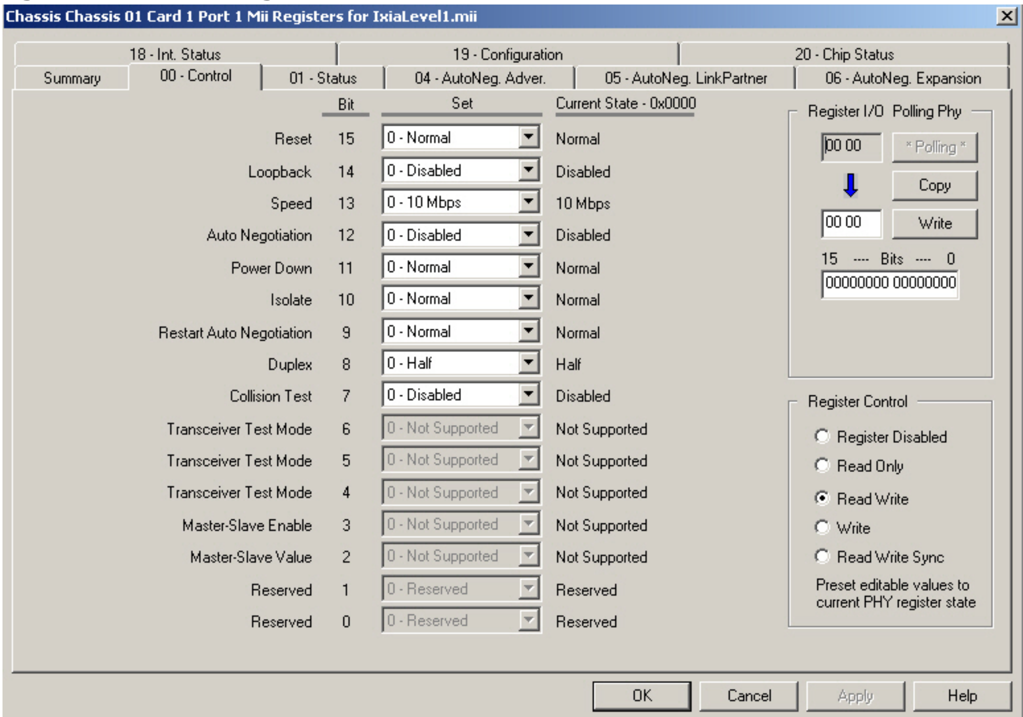
The state for all of the registers may be set at one time through the *All Registers* box. The five choices in the choice box correspond to the five states. The *Apply To All Registers* button must be clicked to apply a new choice.

The particular tabs available at the top of the dialog are dictated by the contents of the MII template in use. They correspond to the MII registers which are available for that port. The Control register is shown in *MII Control Tab.*

MII Control Tab

The MII *Control* tab for the`IxiaLevel1.mii` file is shown in *Figure:MII Control Register Tab*.

Figure:MII Control Register Tab



The 00-Control and 01-Status registers are mandatory for all PHYs, and the labels and values are usually consistent across all PHYs within each of the two groups. The properties that may be set, and the acceptable values for the required bits on the control registers, are shown in *Table:MII Control Register Properties (for IxiaLevel1.mii)*.

Table:MII Control Register Properties (for IxiaLevel1.mii)

Property	Bit	'0' Value	'1' Value
Reset	15	Normal	PHY Reset
Loopback	14	Disabled	Enabled
Speed	13	10 Mbps	100 Mbps
Auto Negotiation	12	Disabled	Enabled
Power Down	11	Normal	Power Down
Isolate	10	Normal	Isolate
Restart Auto-Negotiation	9	Normal	Restart
Duplex	8	Half	Full
Collision Test	7	Disabled	Enabled

The columns and fields in a register tab are described in *Table:MII Register Display Controls.*

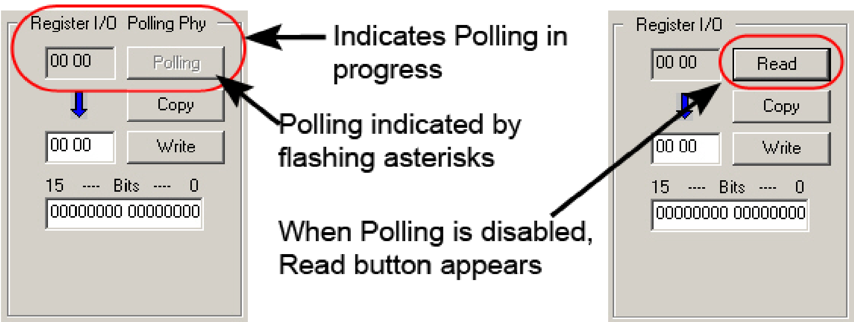
Table:MII Register Display Controls

Control	Usage
(Bit label)	The left-most column in the display is the label for the bit in the register; for example, *Reset* or *Loopback* in *Figure:MII Control Register Tab*
Bit	The position of this bit within the register. Bits are numbered from the least significant end.
Set	Reflects the value that the bit will be set to with the next use of the *Apply* button.
Current State–0x*n*	This indicates the current state of the register numbered 0x*n* (hex). This column is not shown when the Register Control is set to *Write*.
Register Control	The register may be operated in one of three states: • Register Disabled—The register is neither read nor written during operation. • Read Only—The register value is only read during operation. • Read Write—The register is read and written during operation. • Write—The register values are only written during operation. (The *Current State* column is not displayed.) • Read Write Sync—The register is read and written during operation. In addition, the read values are placed into the editable fields at the same time. (Preset editable values to current PHY register state.) The initial setting of these bits comes from the MII template in use.
Register I/O Polling Phy	The hex input field and the field labeled *15 --- Bits --- 0* allow the register values to be changed directly, instead of using the *Set* column. After any change, press the *Write* button; this will cause the Set column and other input values to reflect the new value. When the cursor is positioned within either type of numeric field, the label shown below applies to the byte or bit to the right of the

Control	Usage
	cursor. In addition, if the register is not disabled, and PHY polling is enabled in the *Advanced MII* tab in the *Port Properties* dialog), it will be continually read from the PHY. If PHY polling is not enabled, the *Read* button is visible and may be used to read current values, as shown in *Figure:Polling PHY versus Manual Read*. The current value may be copied into the hex and bit fields.
Apply	Press this button to immediately change the port's properties without leaving the dialog.
OK	Press this button to immediately change the port's properties, and exit the dialog.

The *Polling* and *Read* buttons for the Register I/O Polling Phy are shown in *Figure:Polling PHY versus Manual Read*.

Figure:Polling PHY versus Manual Read



The lower part of the tab allows the PHY address to be set. The controls available in this part of the tab are described in *Table:PHY Address Controls*.

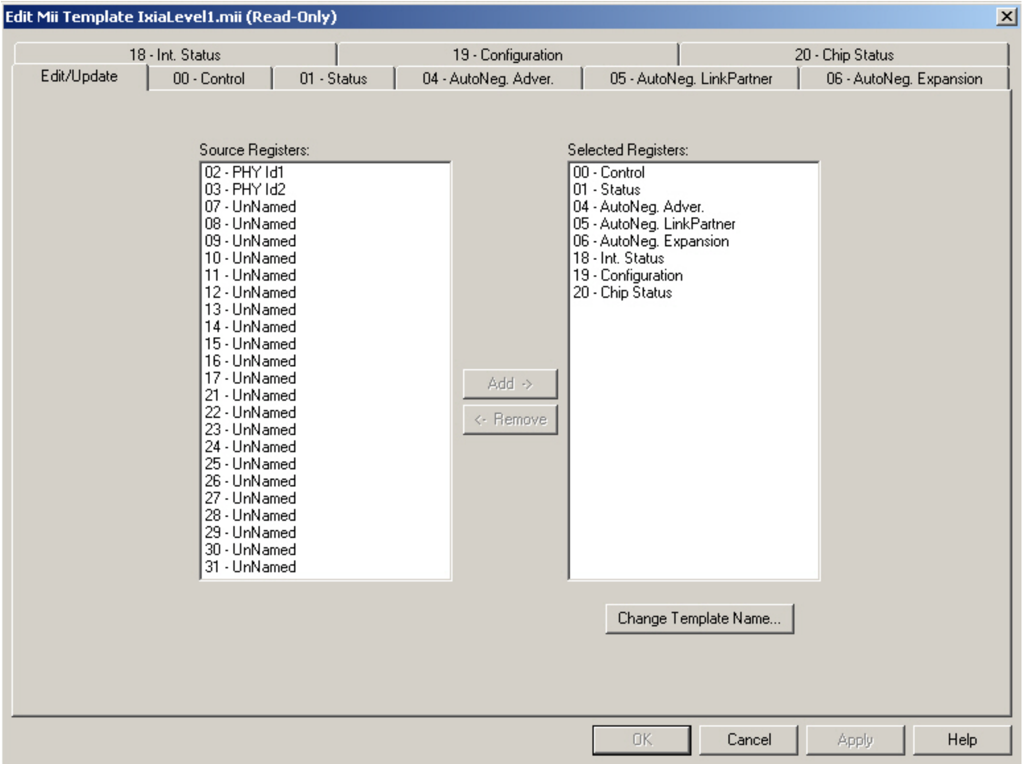
Table:PHY Address Controls

Control	Usage
PHY Address	Allows the address of the PHY to be set to Auto or a constant from 0 to 31. (For other than 10/100 modules, it is configured for Auto and manual configuration is disabled.)
Enable Phy Polling	If selected, then the PHY is continuously polled during MII setup operation.
Ignore Link	If selected, will allow transmission of packets with the link down.

New/Edit MII Register Template Setup—Management Page

Whether creating a new MII register template or editing an existing one, the operations are the same. The form of the interactive window is shown for IxiaLevel1.mii file (for a 10/100 module) in *Figure:MII Register Template Setup—Edit/Update Tab*.

Figure:MII Register Template Setup—Edit/Update Tab

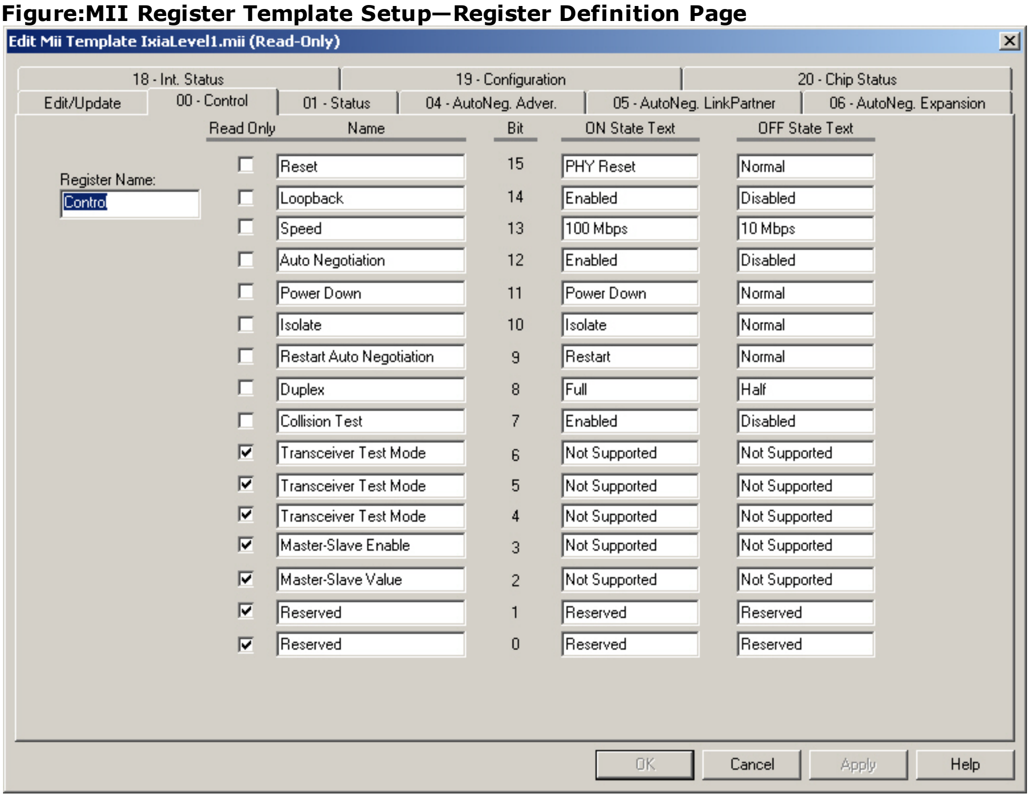


The *Edit/Update* tab controls the selection of registers that will be used from the entire 32-register set. The registers already selected are listed under *Selected Registers* at the right. In this case, the selected list begins with *00 - Control*. The unused registers are listed under *Source Registers* at the left. In this case, the unused list begins with *02 -PHY Id1.* Items are moved from the *Source Registers* to the *Selected Registers* by selecting the item (s) in the *Source Registers* and pressing the *Add ->* button. Likewise, items may be moved from the *Selected Register* list to the *Source Registers* list by selecting the item(s) in the *Selected Registers* and pressing the *<- Remove* button.

The names of the selected registers appear on the tabs at the top of the dialog set. Selecting one of the tabs displays the information about the bits in the register. An example dialog is shown in *New/Edit MII Register Template Setup—Register Page*.

New/Edit MII Register Template Setup—Register Page

Figure:MII Register Template Setup—Register Definition Page



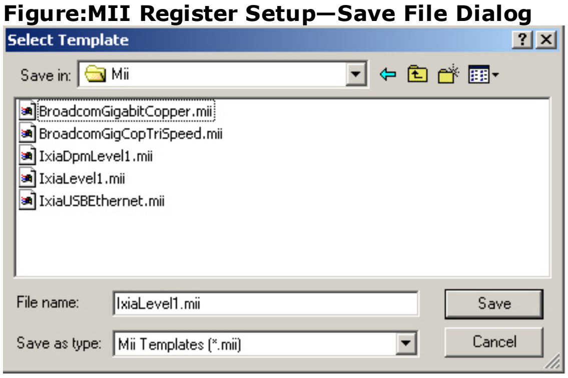
The columns on each of the register tabs are described in *Table:MII Register Setup Tab Controls*.

Table:MII Register Setup Tab Controls

Column Heading	Usage
Register Name	The name of the register, as it appears in the tab and in the Selected Register list on the main page is shown here and is editable.
Read Only	If selected, the register is read only when the MII registers are viewed.
(Name)	The text in this column holds the name of the bit in the register.
Bit	This column indicates the bit position within the register word.
ON State Text	The text in this column is shown for the ON state of the bit.
OFF State Text	The text in this column is shown for the OFF state of the bit.

The MII register template can be saved by pressing the *OK* button. If a new template is being defined when the *OK* button is clicked, or the *Change Template Name...* button was used, then a standard Windows *Save* dialog is presented to allow for saving the template as a different file on a disk. A sample dialog is shown in *Figure:MII Register Setup—Save File Dialog*. For ease of finding the file at a later time, it should be saved with an *.mii* extension.

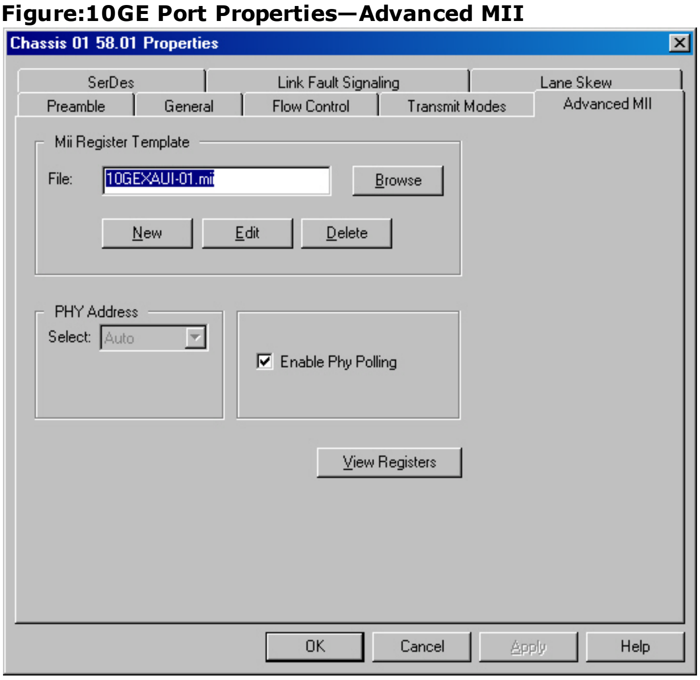
Figure:MII Register Setup—Save File Dialog



The *Apply* button can be used to immediately change the port’s properties without leaving the dialog; the *OK* button performs the same function and exits the dialog as well.

10GE Port Properties—Advanced MII

Figure:10GE Port Properties—Advanced MII



The *Advanced MII* tab for the 10GE XAUI and XENPAK modules is similar to those for the 10/100 modules. For detailed information refer to *Advanced MII Tab*.

10GE Module MII Lists

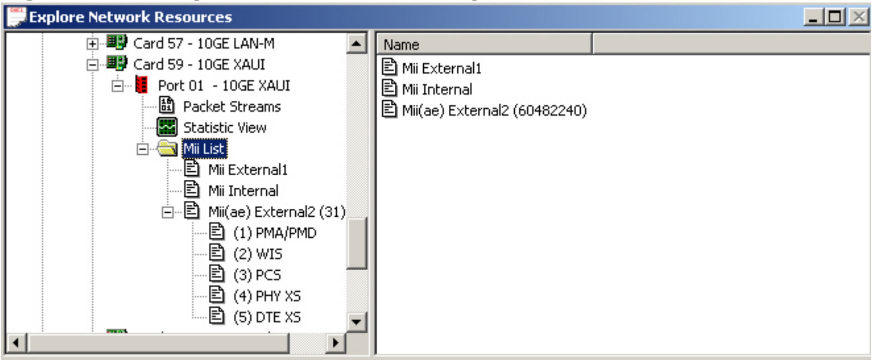
The 10GE XAUI and XENPAK modules and 10GE LSM LAN 10GBASE-T modules have an additional configuration capability for a set of unique External MII(ae) templates. In the MII List there is one default MII Internal interface for the port resident on the board. In addition, two external MII interfaces can be defined for the XAUI card, in an MII or MII(ae) format, to support two Management Data Input Output (MDIO) Devices (MMDs). The MII (ae) format also permits custom, user-defined templates. The XENPAK module and the 10GE LSM LAN 10GBASE-T module support only the MII(ae) external MII format (not the MII type). The templates are:

- *MII Internal Template*= ‘MII Internal’
- *External MIIs*

- *External MII 802.3 Clause 22*= ‘MII External’
- *External MII (ae) 802.3 Clause 45*= ‘MII(ae) External’—includes a set of default templates, and allows to define custom templates.

The MII interface templates are located in the Network Resources Tree, under the in a directory named *MII List*, as shown for a 10GE XAUI module in *Figure:MII List (shown for 10 GE XAUI)*.

Figure:MII List (shown for 10 GE XAUI)



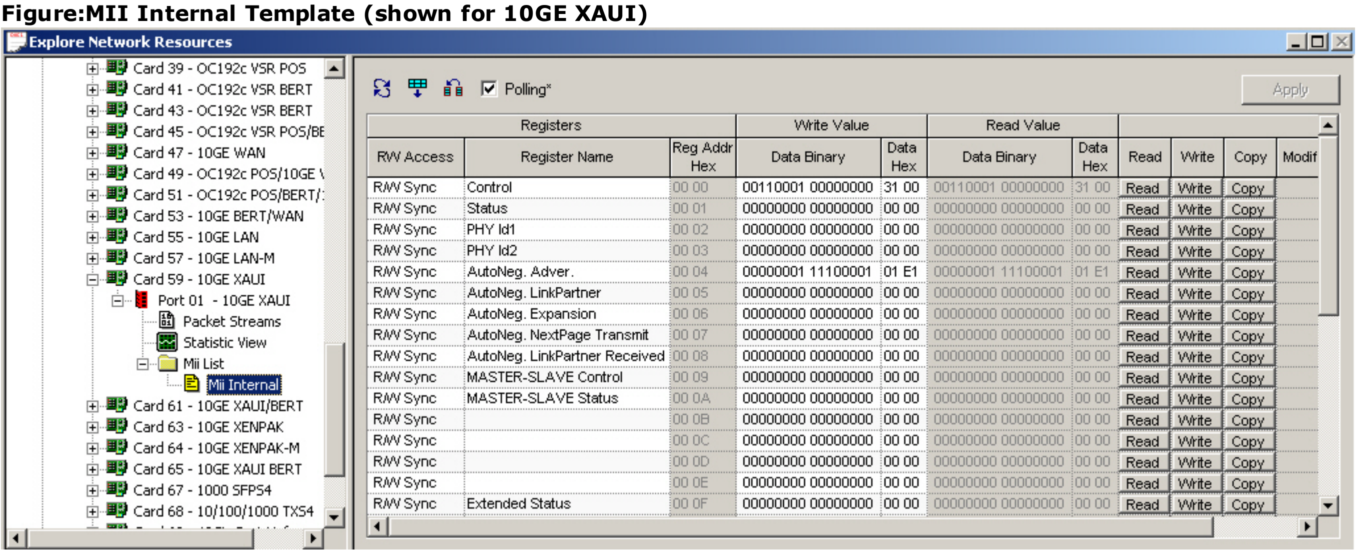
The different types of MII templates available are described in the following sections.

MII Internal Template

An example of an MII Internal template is shown in *Figure:MII Internal Template (shown for 10GE XAUI)*.

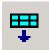
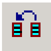
> **For MII External:**
>
> For information on the MII External template, *External MII 802.3 Clause 22*.

Figure:MII Internal Template (shown for 10GE XAUI)



The fields and controls for this window are described in *Table:Internal MII Template Window*.

Table:Internal MII Template Window

Section	Controls	Usage
Header	 Refresh (Global Read)	This icon is used to repaint the screen to update all of the values.
	 Global Write	(Applicable for registers that are set to R/W or Write Only.) When this icon is clicked, all changes made to the *Write Values* are copied to the registers and the corresponding *Read Values* columns.
	 Global Sync (Copy Read to Write)	(Applicable for registers that are set to R/W or Write Only.) When this icon is clicked, the values in the *Read Values* columns are copied to the corresponding *Write Values*.
	Polling	This check box is used to enable the polling function. The MII register values are read (polled) periodically.
	Apply	*Apply* button. This global command saves all changes.
Registers	RW Access	Choose one of: Disabled—the register is disabled. Read Only—the information in this register can only be read, not modified. Write Only—this register accepts modifications. R/W—(Read/Write) this register can accept modifications, and those modifications can be read. R/W Sync—(Read/Write Sync) this register can accept modifications.
	Register Name	The user-assigned name for this register.
	Reg Address Hex	(Read-only) The Register Address, exclicked as a hexadecimal.
Write Value	Data Binary	The binary data contained in this register.
	Data Hex	Equivalent of the binary data, exclicked in hexadecimal.
Read Value	Data Binary	The binary data contained in this register.
	Data Hex	Equivalent of the binary data, exclicked in hexadecimal.
(Controls)	Read Read	(Enabled if Read Only or R/W is selected.) If new binary data has been entered into the *Write Value* column, pressing this button causes the data to be entered into the binary field, starting with LSB and with appropriate addition of '0's. The Data Hex value is also updated to match.

Section	Controls	Usage
	 Write	(Enabled if Write Only or R/W is selected.) If new binary data has been entered into the *Write Value* column, pressing this button causes the new binary and hex data to be copied into the *Read Value* column.
	 Sync	(Enabled if Write Only or R/W is selected.) When this button is clicked, the binary and hex data in the *Read Value* columns is copied to the *Write Value* columns.
Modified		When any of the registers has been modified, an asterisk (*) is displayed in the *Modified* field of the corresponding row, to remind you that changes have been made, but not applied or copied. When the *Apply* or *Write* button is pushed, the (*) disappears.

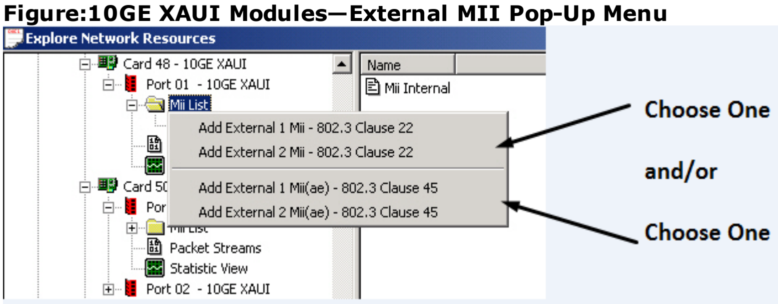
External MIIs

External MII templates may be added to the 10GE XAUI and 10GE XENPAK modules through the MII List pop-up menu selections, as shown in *Figure:10GE XAUI Modules—External MII Pop-Up Menu*:

- *External MII 802.3 Clause 22*(1 or 2)—for 10GE XAUI only
- *External MII (ae) 802.3 Clause 45*(1 or 2)—for 10GE XAUI, 10GE XENPAK and 10GE LSM LAN 10GBASE-T

For the 10GE XENPAK module, *MII(ae) External1 MII* is already listed in the MII List. To set up an External MII for the 10GE XAUI module, first right-click *MII List* under the port to display the pop-up menu. Then select an option in the menu, to add it to the MII List. A maximum of *one* External 1 MII plus *one* External 2 MII may be added for XAUI. Both MIIs may be Clause 22 or Clause 45 type MIIs, or you may select one MII of each type.

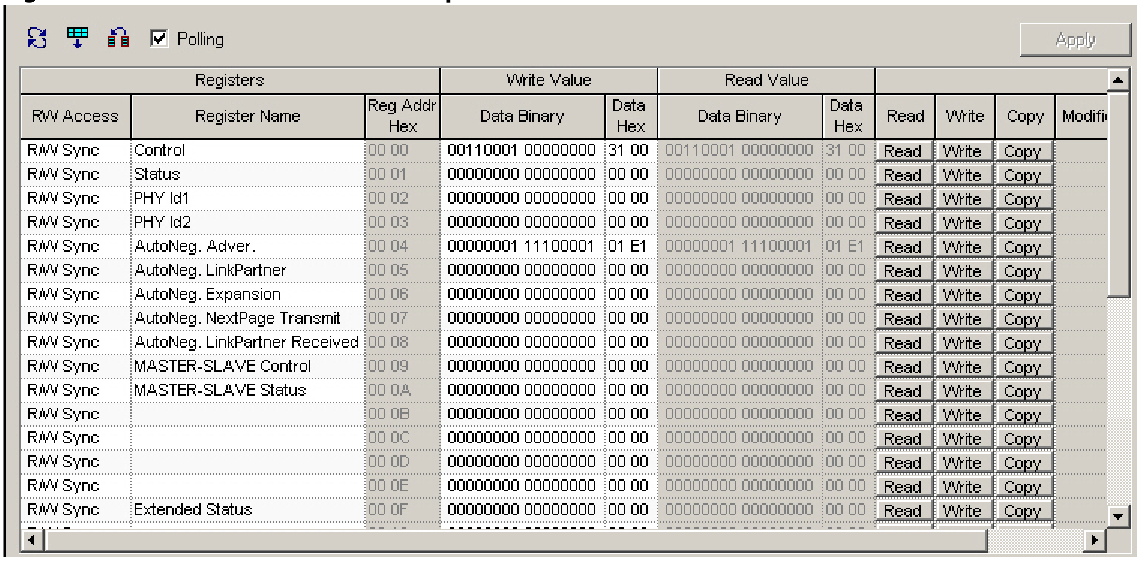
Figure:10GE XAUI Modules—External MII Pop-Up Menu



External MII 802.3 Clause 22

This External MII template is defined per Clause 22 of the IEEE 802.3 standard. An example of this template is shown in *Figure:10GE XAUI–MII External Template–802.3 Clause 22*.

Figure:10GE XAUI–MII External Template–802.3 Clause 22



Polling

Apply

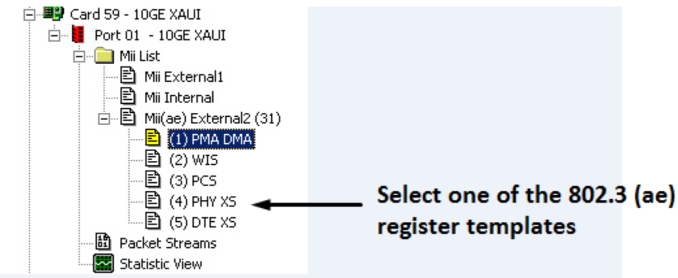
Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modifi
R/W Sync	Control	00 00	00110001 00000000	31 00	00110001 00000000	31 00	Read	Write	Copy	
R/W Sync	Status	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY Id1	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY Id2	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	AutoNeg. Adver.	00 04	00000001 11100001	01 E1	00000001 11100001	01 E1	Read	Write	Copy	
R/W Sync	AutoNeg. LinkPartner	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	AutoNeg. Expansion	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	AutoNeg. NextPage Transmit	00 07	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	AutoNeg. LinkPartner Received	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	MASTER-SLAVE Control	00 09	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	MASTER-SLAVE Status	00 0A	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync		00 0B	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync		00 0C	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync		00 0D	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync		00 0E	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Extended Status	00 0F	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

The fields and controls for this window operate in the same manner as those for the Internal MII window. Refer to *Table:Internal MII Template Window* for information about the usage.

External MII (ae) 802.3 Clause 45

When *External MII (ae) 802.3 Clause 45* is selected for a 10GE XAUI or XENPAK module or for a 10GE LSM 10GBASE-T module, a directory of templates is added to the MII list, as shown in *Figure:10GE XAUI and XENPAK—MII Register Templates for 802.3 (ae)*.

Figure:10GE XAUI and XENPAK—MII Register Templates for 802.3 (ae)



This directory includes a standard set of MII registers that are defined per Clause 45 of the IEEE specification for 802.3ae, and include an MII template for each of the following MDIO Manageable Device (MMD) addresses:

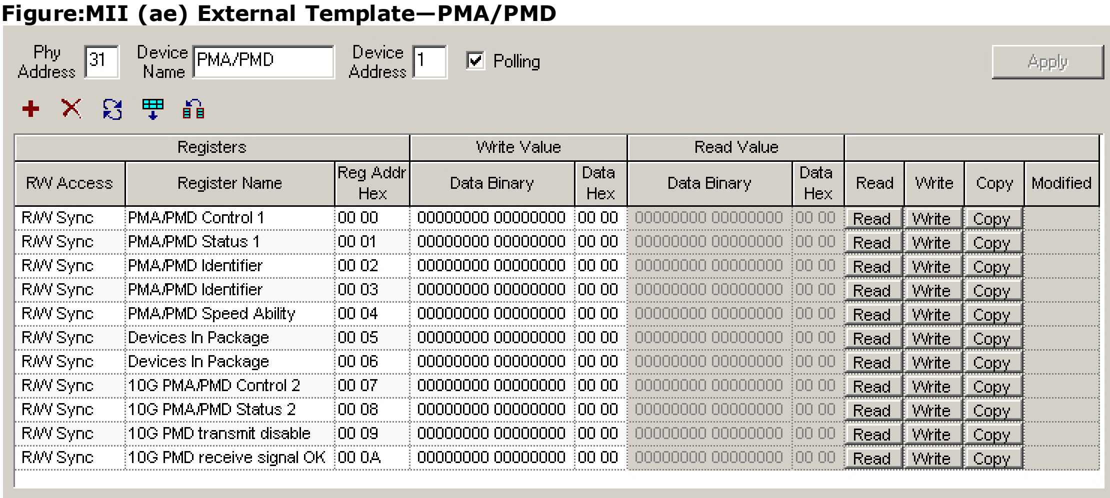
- **(1) PMA/PMD—**Physical Media Attachment Sublayer (upper)/Physical Media Dependent Sublayer (lower). These are the two lower sublayers of the PHY device. (Shown in *Figure:MII (ae) External Template—PMA/PMD.*)
- **(2) WIS—**WAN Interface Sublayer. An additional, optional PHY sublayer. For the 10GBASE-W interface, it applies a rate control mode to the MAC, resulting in a modification of the data rate to SONET STS-192c/SDH VC-4-64c levels for use with WAN applications. (Shown in *Figure:MII (ae) External Template—WIS (partial)*)
- **(3) PCS—**Physical Coding Sublayer. This is the upper sublayer of the PHY device. (Shown in *Figure:MII (ae) External Template—PCS (partial).*)

- **(4) PHY XS—**Physical Layer Device XGMII Extender Sublayer (XGXS) at the PHY End of the XAUI interface. (Shown in *Figure:MII (ae) External Template—PHY XS (partial).*) (XGMII = 10 Gigabit Media Independent Interface.)
- **(5) DTE XS—**Data Transmission Equipment XGXS at the Reconciliation Sublayer (RS) end of the XAUI interface. (Shown in *Figure:MII(ae) External Template—DTE XS*.)
- **(6) TC**—Transmission Convergence (reserved for future use)
- **(7) Auto Negotiation**—The assignment of registers in the Auto Negotiation MMD (MDIO Manageable Device). (Shown in *Figure:MII(ae) External Template—Auto Negotiation.*)

In addition, User Device MII register templates may be stored in this directory. Refer to *User Device MII(ae) Templates* for information on how to create User Device templates.

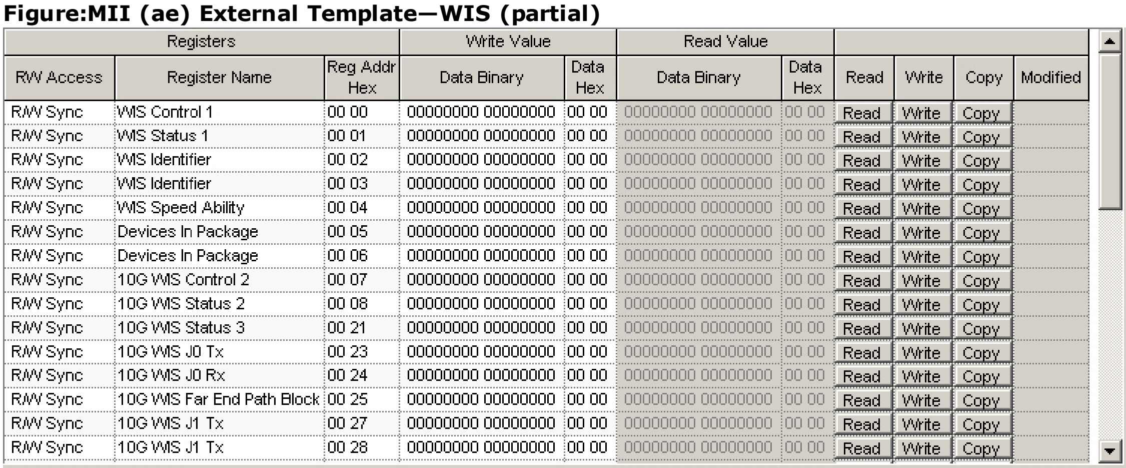
An example of a set of MII(ae) External 802.3–Clause 45 templates for a 10GE XAUI module is shown in *Figure:MII (ae) External Template—PMA/PMD* through *Figure:MII(ae) External Template—Auto Negotiation*.

Figure:MII (ae) External Template—PMA/PMD



Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W Sync	PMA/PMD Control 1	00 00	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PMA/PMD Status 1	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PMA/PMD Identifier	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PMA/PMD Identifier	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PMA/PMD Speed Ability	00 04	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PMA/PMD Control 2	00 07	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PMA/PMD Status 2	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PMD transmit disable	00 09	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PMD receive signal OK	00 0A	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Figure:MII (ae) External Template—WIS (partial)



Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W Sync	WIS Control 1	00 00	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	WIS Status 1	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	WIS Identifier	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	WIS Identifier	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	WIS Speed Ability	00 04	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS Control 2	00 07	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS Status 2	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS Status 3	00 21	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS J0 Tx	00 23	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS J0 Rx	00 24	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS Far End Path Block	00 25	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS J1 Tx	00 27	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G WIS J1 Tx	00 28	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Figure:MII (ae) External Template—PCS (partial)

Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W Sync	PCS Control 1	00 00	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PCS Status 1	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PCS Identifier	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PCS Identifier	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PCS Speed Ability	00 04	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PCS Control 2	00 07	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PCS Status 2	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-X PCS Status	00 18	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-R PCS Status 1	00 20	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-R PCS Status 2	00 21	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-R PCS Jitter Test	00 22	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-R PCS Jitter Test	00 23	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10GBASE-R PCS Jitter Test	00 24	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Figure:MII (ae) External Template—PHY XS (partial)

Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W Sync	PHY XS Control 1	00 00	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY XS Status 1	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY XS Identifier	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY XS Identifier	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY XS Speed Ability	00 04	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	PHY XS Status 2	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G PHY XGXS Lane Status	00 18	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Figure:MII(ae) External Template—DTE XS

Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W Sync	DTE XS Control 1	00 00	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	DTE XS Status 1	00 01	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	DTE XS Identifier	00 02	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	DTE XS Identifier	00 03	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	DTE XS Speed Ability	00 04	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 05	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	Devices In Package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	DTE XS Status 2	00 08	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W Sync	10G DTE XGXS Lane Status	00 18	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Figure:MII(ae) External Template—Auto Negotiation

Registers			Write Value		Read Value					
RW Access	Register Name	Reg Addr Hex	Data Binary	Data Hex	Data Binary	Data Hex	Read	Write	Copy	Modified
R/W S	AN control	00 00	00110000 00000000	30 00	00110000 00000000	30 00	Read	Write	Copy	
R/W S	AN status	00 01	00000000 10101101	00 AD	00000000 10101101	00 AD	Read	Write	Copy	
R/W S	AN device identifier	00 02	00000001 01000000	01 40	00000001 01000000	01 40	Read	Write	Copy	
R/W S	AN device identifier	00 03	01011000 01110000	58 70	01011000 01110000	58 70	Read	Write	Copy	
R/W S	AN devices in package	00 05	00000000 10011010	00 9A	00000000 10011010	00 9A	Read	Write	Copy	
R/W S	AN devices in package	00 06	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W S	AN package identifier	00 0E	00000001 01000000	01 40	00000001 01000000	01 40	Read	Write	Copy	
R/W S	AN package identifier	00 0F	01011000 01110000	58 70	01011000 01110000	58 70	Read	Write	Copy	
R/W S	AN advertisement	00 10	00010000 00000001	10 01	00010000 00000001	10 01	Read	Write	Copy	
R/W S	AN advertisement	00 11	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	
R/W S	AN advertisement	00 12	00000000 00000000	00 00	00000000 00000000	00 00	Read	Write	Copy	

Most of the column headings and controls for this window are the same as those found in the External MII and Internal MII windows. Refer to *Table:Internal MII Template Window* for information about the usage.

Additional controls which are unique to the External MII (ae) window are described in *Table:10GE XAUI and XENPAK and 10GE LSM LAN 10GBASE-T External MII (ae) Template Window*.

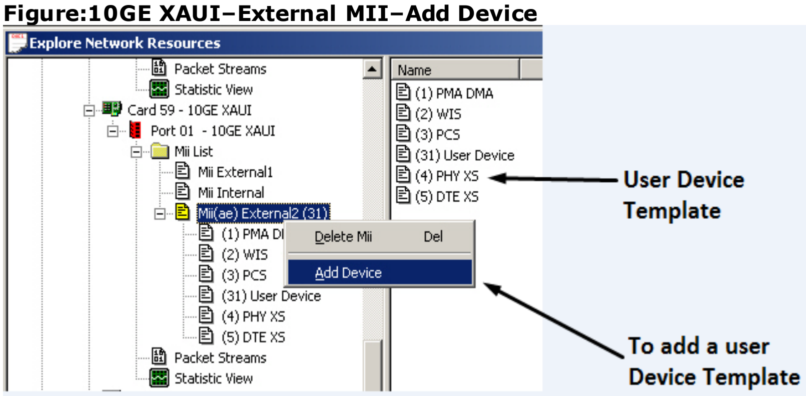
Table:10GE XAUI and XENPAK and 10GE LSM LAN 10GBASE-T External MII (ae) Template Window

Section	Controls	Usage
Header	Add Register	Adds a new register entry to the bottom of the list of registers. The new 'User Register' is set to 'Read Only' by default.
	Delete Register	Deletes selected Register(s).
	Phy Address	The numerical Phy address.
	Device Name	The name of the (MMD) device being read (for example, 'WIS').
	Device Address	The numerical address of the (MMD) device (for example, '2' for 'WIS').
	Polling	This check box enables the 'Polling' function—reading the MII registers for an MMD in a DUT. The *Apply* button must be clicked for polling to begin.
	Write Write	(Enabled if Write Only or R/W is selected.) If new binary data has been entered into the *Write Value* column, pressing this button causes the new binary and hex data to be copied into the *Read Value* column.

User Device MII(ae) Templates

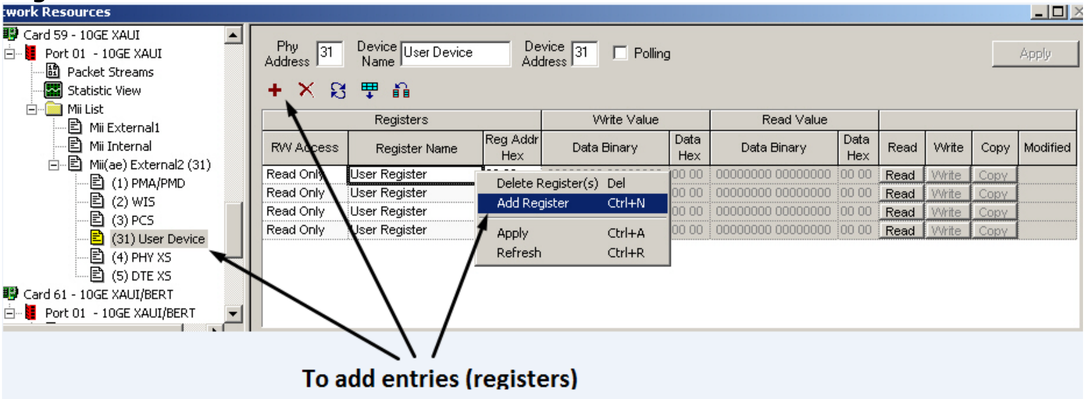
In addition to the standard MII(ae) templates, custom 'User Device' templates can be defined through the right-click menu below on MII(ae) External 1 or 2. Click *Add Device* as shown in *Figure:10GE XAUI–External MII–Add Device*, and a new, blank template form will be added to the right pane of the Resources window as shown in *Figure:10GE XAUI and XENPAK—User-Defined External MII(ae) Register with User-Defined Register Entries*.

Figure:10GE XAUI–External MII–Add Device



The new, user-defined register template that is displayed on the right side of the window will not contain any Register entries when it is first displayed. Add entries (rows) by right-clicking in the right side of the window and selecting *Add Register*, using the *Add* icon ( ), or right-clicking a Device name in the Chassis Chain Tree, as shown in *Figure:10GE XAUI and XENPAK—User-Defined External MII(ae) Register with User-Defined Register Entries*.

Figure:10GE XAUI and XENPAK—User-Defined External MII(ae) Register with User-Defined Register Entries



When the *Add Register* option is selected, the Add MII(ae) Registers dialog is displayed, as shown in *Figure:Add MII(ae) Registers Dialog*.

Figure:Add MII(ae) Registers Dialog

The configurable fields are described in *Table:Internal MII Template Window* above.

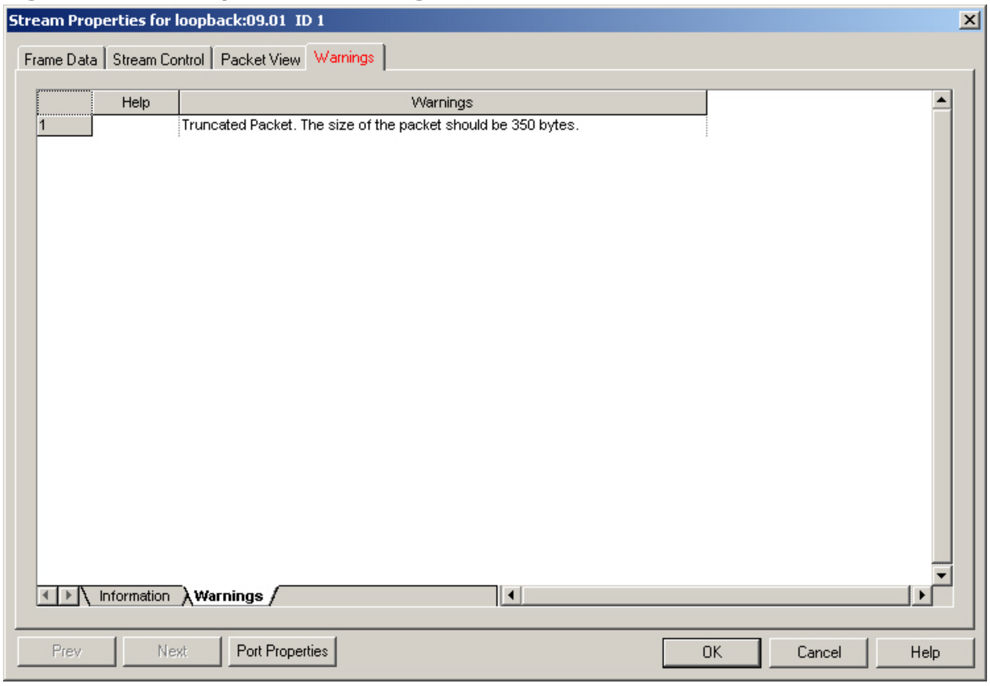
Chapter 31 - Stream Properties —Warnings/Information Messages

Various Stream Properties Warning and Information messages are provided in IxExplorer to inform you of various stream configuration conditions. These messages concern memory usage, overlapping of user-defined fields, and so forth.

Stream Properties Warnings Tab

The *Warnings* tab in the *Streams Properties* dialog is shown in *Figure:Stream Properties—Warnings Tab.*

Figure:Stream Properties—Warnings Tab



This tab consists of two sub-tab views:

- *List of Warnings*—The Warning messages specify conditions which can impact performance and traffic, including available memory
- *List of Information Messages*—The Information messages specify less serious conditions concerning memory usage, and so forth.

The *Warnings* and *Information* sub-tabs each have three columns:

- The first column assigns a number to each Warning or Information message, to indicate the order in which it was received.
- The second column is labeled *Help*, and will eventually contain links to Help information concerning the warning.
- The third column contains the Warning or Information message.

Warning and Information Message Generation

Each time an error occurs, the IxExplorer software goes through a cycle of checking the entire list of possible error messages, and redisplays the message list with the new error included. The numbering on the left-hand side of the page reflects the order of messages. The first message in the table, listed as '1,' indicates the first error that generated an error message during the checking cycle; '2' is the second error found, and so forth.

Chapter 32 - IxVM

IxVM is Ixia's virtual test port product that enables you to use Linux virtual machines (VMs) to generate test traffic.

This section describes how to use IxVM.

Discovery Server

Discovery Server is a service that finds IxVM enabled appliances that can be added as an IxVM load module to participate in a test. Discovery Server is available for download on the IxVM page of Ixia's website.

In Discovery Server, IxVM cards are called endpoints.

NOTE In order for Discovery Server to work, the Windows VM on which IxServer and Discovery Server are installed must be registered to a DNS server that can respond to queries for the VMs’ hostnames.

Discovering Endpoints

There are four types of discovery you can use to discover IxVM test ports:

- Manual Discovery allows you to discover endpoints within a specific address range.
- VMware Discovery finds all VMs running on the ESX(i) host, including those not running IxVM. Although it will discover non-IxVM VMs, it will not add them to list of available cards. VMware discovery is the slowest form of discovery. VMware Discovery is useful for conducting a server-wide search for IxVM, because VMware Discovery is not limited to a particular subnet.
- Broadcast Discovery finds endpoints by sending packets to the broadcast address of the subnets that the endpoints are on. Broadcast is the quickest way to find IxVM endpoints. Broadcast Discovery can be used when IxVM has been deployed into an ESX(i) environment where the IxVM Server and Discovery Server are on the same LAN as the IxVM test ports.
- XenKvm Discovery finds all VMs running on Xen/Kvm host, that have been deployed using the Ixia Mass Deployment Tool or manually using the Ixia .sh file. XenKvm discovery is the slowest form of discovery. XenKvm Discovery is useful for conducting a server-wide search for IxVM, because XenKvm Discovery is not limited to a particular subnet.

Discovery Server also includes an Automatic Discovery feature; this type of discovery maintains communication with endpoints that have already been discovered through Broadcast Discovery. The number of endpoints that have been discovered through Broadcast Discovery is displayed on this tab. If you need to purge the list of endpoints and re-discover them, click CLEAR DISCOVERED ENDPOINTS.

To find endpoints:

1. After you have configured Discovery Server, start the discovery process using the following command:

   Server | Discovery | Start Broadcast Discovery

   Discovery Server starts the discovery process.

2. Click the Automatic Discovery tab, and monitor the count of VMs found and the messages that display during the discovery process.

   When the discovery process has finished, the following message displays in the message area of the window:

Broadcast Discovery: Broadcast Completed

Configuring Discovery Server

Use the following procedure to configure Discovery Server.

To configure Discovery Server:

1. Start Discovery Server using the following command:

   START | ALL PROGRAMS | IXIA | IXIA DISCOVERY SERVER | IXIA DISCOVERY SERVER

   Discovery Server starts, and minimizes to the tray.
2. Double-click the DISCOVERY SERVER icon.
3. Click the BROADCAST DISCOVERY tab.

   The Broadcast Addresses list contains the list of IP addresses configured in the VM. For some installations, this may include the address of the IxVM management port (the first LAN connection), and the second LAN connection. Discovery Server displays the IP addresses for all the network adapters configured on the Windows VM so that you can select the networks that you want to search for IxVM cards.
4. Click the VMWARE DISCOVERY tab.

   Add the Hypervisor credentials for each hypervisor on which you deployed IxVM appliances You create a virtual machine on a hypervisor or on a server and then add the server IP, user name and password. Add them to the Server list. You can then discover the IxVM machines that you have created on that server.
5. Click the XENKVM DISCOVERY tab.

Add the Hypervisor credentials for the Xen or Kvm hypervisor on which you deployed IxVM appliances similarly as that for VMware.

NOTE On the Server menu, click Discovery and then click Start All plugins. This starts the Discovery and all plugins on VMware and Xen. If you have not configured the Discovery server on VMware or Xen, then it does not go through the plugin.

Adding IxVM Cards Manually

If you do not want to or cannot use Discovery Server to find IxVM cards, you can add the cards manually.

To add IxVM cards manually, perform the following steps:

1. Start the test application (IxExplorer, IxNetwork, or IxLoad) and connect to the IxVM Server IP address (LOCALHOST, if you are using IxExplorer on the Windows VM).
2. Right-click the new Chassis and select **ADD PORTS TO CHASSIS**.

You can add additional IxVM cards as you add a virtual card to a new virtual slot in a virtual chassis. There are two types of virtual cards that you can add - Single-port and Multi-NIC.

A single plus sign card icon indicates that you can add a single-port card; a multiple plus sign card icon indicates that you can add a multi-port card. You use the plus sign port icon to add additional ports to a multiple-port card. Single-port cards are identified with a checked checkbox in the Single port column.

3. In the **MANAGEMENT IP ADDRESS** field, enter the management IP address of the Linux machine with the IxVM software agent installed.
4. Select the **Pro Mode** check box to denote the promiscuous or non-promiscuous mode in which a virtual port is added to a virtual card.

   NOTE In most of the test scenarios you must select the Pro Mode check box. In this case, the virtual switch also needs to be set to accept promiscuous mode.

5. The **SOURCE MAC** field shows the MAC address of the test interface (the interface from the virtual machine). Although it can be edited, it does not modify the MAC address of the virtual machine.
6. You can use the **Link MTU** column to modify the MTU value of each test interface from a virtual machine.
   The minimum value is 1500 and the maximum value is 9000 and should be changed mainly when there are control plane frames bigger than 1500.
7. Each IxVM card has a keep-alive mechanism between the virtual chassis and the virtual card. In case either of these two components do not send or receive a keep-alive message for a certain amount of time, then the virtual card will disconnect from the virtual chassis. By default, the keep-alive timeout is 60 seconds. You can change this from the KEEP ALIVE field, when adding a virtual card.

   NOTE In case the network is not very stable, and you are doing tests with a high number of IxVM ports or cards or the hypervisor is very loaded, it is advised to change the keep-alive timeout to a bigger value (e.g. 120 seconds).

8. In the **PORT TYPE** field, select the port type. Options include the following:
   - L23: Generates layer 2-3 traffic for use with IxNetwork only.
   - L47: Generates layer 4-7 traffic for use with IxLoad only.
9. In the **TEST PORT NAME** field, enter the name of the port on the IxVM card to be used for traffic generation and measurement.
10. In the **LINE SPEED** field, select the line speed. Options include the following:
    - 100MBPS
    - 1000MBPS: 1 Gb speed
    - 10000MBPS: 10 Gb speed
11. Continue adding ports for each VM to be used as an IxVM card (use the plus and icon to add more cards or ports).

NOTE Limitations in the current open kernel of RedHat Enterprise Linux 5.x do not allow it to receive stateful traffic between ports on the same card. If you want to use stateful traffic, you must transmit from one card to another.

Virtual Load Modules

Ixia virtual load modules are of multi-port types. Multi-port load modules have multiple interfaces for generating test traffic.

All Ixia virtual load modules require one interface for management traffic, and at least one interface to generate test traffic.

Multi-port modules are virtual appliances operating in a mode that supports the management interface and one or more test traffic interfaces. On a multi-port load module, the resources are distributed across multiple test ports. On a multiport load module, eth0 interface is the card management interface, and eth1through ethN are the multiple test interfaces. With a multi-port load module, the test traffic and the emulated routing topology may traverse multiple virtual networks. One virtual chassis can control up to 32 virtual load modules.

Converting Multiport load modules

You can convert a a multi-port load module with a single test port into a multiport load module with n number of test ports. You can also add ports to an existing multi-port load module. There are three tasks required for this process:

1. For each test port that you want to add, create an additional test network.
2. Add the additional test ports to the virtual load module.
3. In the test application (IxExplorer, IxNetwork, or IxLoad), add or discover the ports added to the load module.

You can add other test port interfaces to a multi-port card with a single test port.

Create the Additional Test Networks

If you are adding ports to a multi-port card, each port should have its own network in vSphere. Use the procedure below to create an additional test network.

To create an additional test network in vSphere:

1. Login to vSphere client.
2. Select the ESX(i) host.
3. Click the CONFIGURATION tab.
4. In the Hardware area, click NETWORKING.
5. Click ADD NETWORKING (upper right).

   The Add Network Wizard displays, with the Connection Type set to Virtual Machine.
6. Click NEXT.

   The Network Access pane displays.
7. Select CREATE A VIRTUAL SWITCH, then click NEXT.
8. In the NETWORK LABEL field, enter a label for the additional test network, then click NEXT, then click FINISH.

Add Ports to the Load Module in vSphere client

To add ports to a virtual load module, use the procedure below. To add ports to a virtual load module:

1. Login to vSphere client.
2. Select the VM you want to add ports to.
3. SHUT DOWN or POWER OFF the VM.
4. Select the VM, and then click EDIT VIRTUAL MACHINE on the Getting Started tab
   The Virtual Machine Properties window appears.
5. On the Hardware tab, click ADD.
   The Add Hardware wizard displays, with the Device Type pane selected.
6. Select Ethernet Adapter, then click NEXT.
   The Network Connection pane displays.
7. In the Adapter Type field, select VMXNET3.
   In the Network Label field, select the destination test network, then click NEXT, then click FINISH
8. Repeat steps 4-8 for any additional ports you want to add.
9. Click OK to close the window.
10. Power on the VM.

IxExplorer: Adding a Multi-port Card

In IxExplorer, after adding ports to a card, you must manually add (or re-add) a card to the card list.

To manually add a multi-port card to an IxVM chassis:

1. In vSphere client, select the chassis, click CONSOLE, and login to Windows.
2. Start IxExplorer.
3. Right-click the chassis, and then select PROPERTIES.
4. Select VIRTUAL PORTS.
5. If the card you added ports to is already in the card list, select the card, and remove it.
6. Click the MULTI-ADD CARD (the +++Card) button.
   IxExplorer adds the card as a multi-port card (the SINGLE-NIC checkbox is not checked).
7. Select the card, then click ADD PORT. Repeat for each additional port you are want to add.
8. Click OK.
   In the chassis/card/port list, the card should now display multiple ports.

IxExplorer Tcl Code Example

The following code shows how to use IxVM cards and ports in Tcl.

Adding Cards

The following code fragment shows how to add an IxVM card to an IxExplorer Tcl script:

```
package req IxTclHal

ixInitialize loopback

chassis refresh loopback
```

```
chassis addVMCard loopback 10.205.15.124 2 1 60 1
```

```
card addVMPort 1 2 1 eth1 1 00:00:00:00:00:00 1500 100
```

For example, to add an L2-3 multi-port card on slot 1:

```
chassis addVMCard loopback 10.200.105.140 1 0 60 0
```

where:

10.200.105.140	card IP address
1	card number
0	multi-port card (1 selects single-port)
60	keep alive timeout
0	L2-3 card type (1 selects L4-7 card type)

Adding Ports

To add an IxVM port:

```
card addVMPort <chassis no> <card no> <port no> <test interface> <promis-
cuous mode> <MAC> <MTU> <lineSpeed>
```

For example:

```
card addVMPort 1 1 1 eth1 1
```

Removing Ports

To remove an IxVM port:

```
card removeVMPort <chassis no> <card no> <port no>
```

For example:

```
card removeVMPort 1 1 1
```

Removing Cards

To remove an IxVM card:

```
chassis removeVMCard loopback <Card no>
```

For example:

```
chassis removeVMCard loopback 1
```

Getting CardID from IP address:

```
chassis checkVMForDuplicate <chassis> <IP address>
```

For example:

```
chassis checkVMForDuplicate loopback 10.205.15.125
```

The output of the command returns the card ID, if a card with the specified IP address exists on the chassis, or 0 (zero) if no card ID was found with the specified IP address.

Appendix A: Using ScriptGen

This appendix describes the functionality details of the ScriptGen.

ScriptGen

ScriptGen is a tool that may be used to generate a Tcl script that reflects the current configuration of Ixia ports. It is intended to be used after ports have been successfully configured using IxExplorer, IxAutomate (previously IxScriptmate), the Tcl API, the C++ API, or other tools. The generated Tcl script can be used to re-create a port setup as the basis for a new Tcl test. ScriptGen may be used on both Windows-based and Unix-based computers.

ScriptGen generates a complete Tcl program into an output file. All aspects of a port's configuration is reflected in the output.

NOTE Port ownership can affect ScriptGen's file creation, in the following manner:

If the first port is explicitly owned by a user, then all ports in the set of ports to be scripted must either be owned by that user or be 'unowned.'

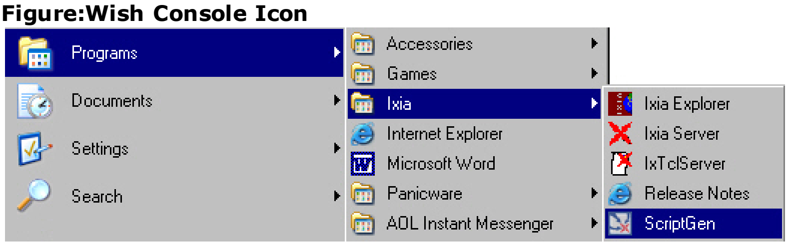
If the first port is 'unowned,' then all ports in the set must be 'unowned.'

Invoking ScriptGen

Windows

To use ScriptGen, use the Windows Start menu for the Ixia group, as shown in *Figure:Wish Console Icon*

Figure:Wish Console Icon

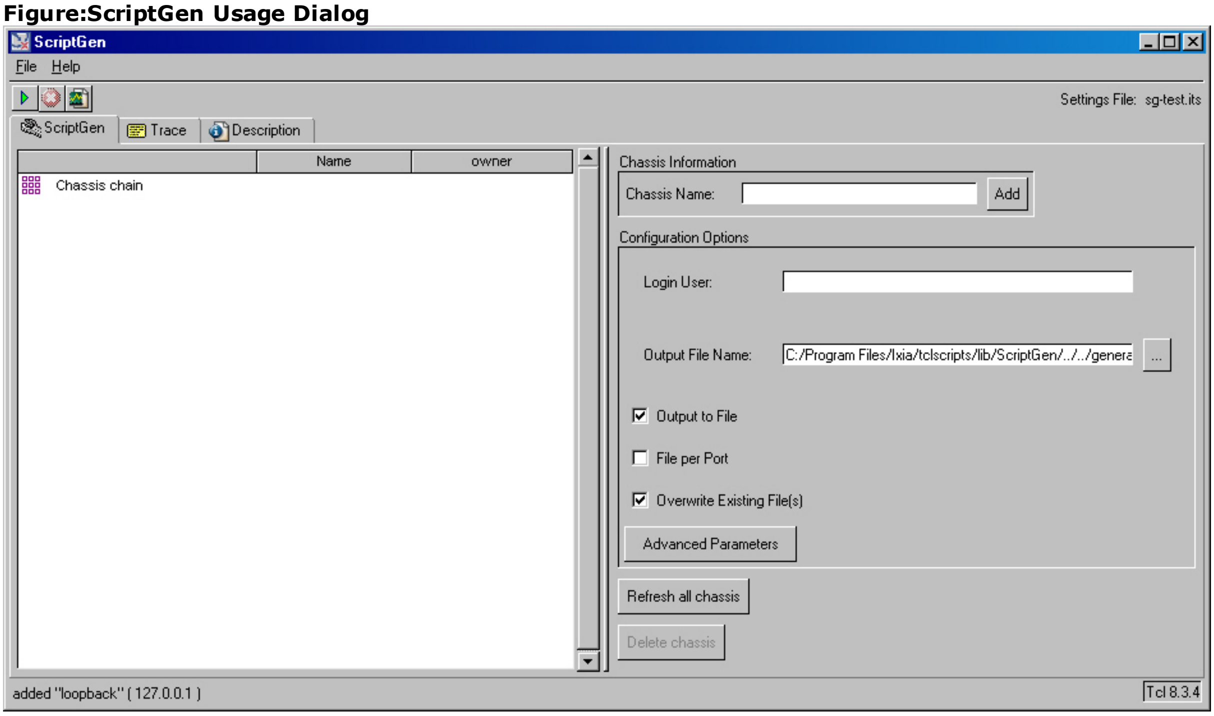


Unix Systems

On Unix systems, the Wish Console must be used and is usually started by invoking *wish* in the *Ixia/bin* directory, then sourcing *ixSgMain.tcl* in the *Ixia/scriptgen* directory.

Either method brings up the *ScriptGen* dialog, shown in *Figure:ScriptGen Usage Dialog*.

Figure:ScriptGen Usage Dialog

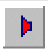


Using the *ScriptGen* dialog to create Tcl scripts is described in the following sections:

- *Adding a Chassis*
- *Creating a Script for a Port*
- *Trace Tab*
- *Description Tab*

The fields in this dialog are described in *Table:ScriptGen Usage Dialog Fields*

Table:ScriptGen Usage Dialog Fields

Section	Field	Usage
		Starts the process of generating the output script based on the other settings in this dialog. For information on how to create a script for a port or selection of ports, *Creating a Script for a Port*.
		Stops the script generation process.
		Verifies a generated script for accuracy. The results of the verification appear in the *Trace* tab.*Trace Tab* for more information on the *Trace* tab.
Chassis Information	Chassis Name	Enter the chassis name or IP address to be added for ScriptGen
	Add	Adds the chassis entered in the field above.
Configuration Options	Login User	Enter the user login name for the chassis. If this option is not used, then only ports on the chassis that are not owned are scripted. If a login is used, then only ports owned by that login name and unowned ports are scripted.
	Output File Name	The name of the output file to generate the output

Section	Field	Usage
		into. The name of the .tcl file should be changed for each port used.
	Output to File	If selected, the output is saved to the file indicated in *Output File Name*. Output always goes to the *Trace* tab.
	File per Port	If selected, the output for each port is saved as a separate file. The file name is an amalgam of the name indicated in the Output File Name and the chassis, slot, and port.
	Overwrite Existing Files	If selected, the saved file or files will overwrite any files with the same name. If not selected, the output will not be saved, and a warning displays in the *Trace* tab.
	Advanced Parameters	This button opens the *Advanced Parameters* dialog. *Advanced Parameters* for more information.
	Refresh all chassis	Selecting this button refreshes the view of the chassis in the tree on the left side of the dialog.
	Delete chassis...	Selecting this button deletes the selected (selected) chassis in the tree on the left side of the dialog. If only one chassis is selected, the name of the chassis appears in quotes after Delete Chassis.

Menu Functions

There are several menu options available under the File menu *Figure:ScriptGen Menu Options* shows the options.

Figure:ScriptGen Menu Options

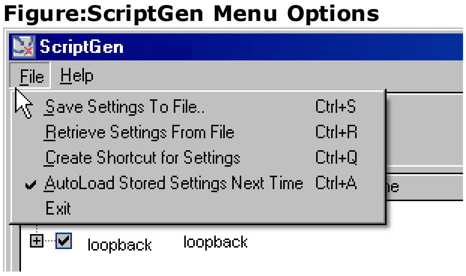


Table:Option Descriptions describes the menu functions. Note that the functions involve the configuration settings for the ScriptGen application, not the created Tcl scripts.

Table:Option Descriptions

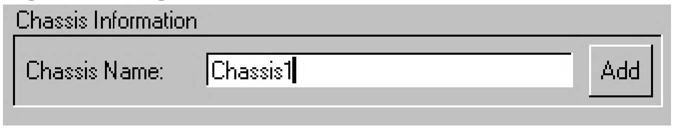
Selection	Usage
Save Settings To File...	Saves the configured ScriptGen settings to a specified file.
Retrieve Settings From File...	Retrieves a ScriptGen configuration from a selected file.
Create Shortcut to Settings	Creates a shortcut to a ScriptGen configuration.
Auto Load Stored Settings Next Time	Automatically loads the last configuration when opening ScriptGen. A check next to this options indicates that it is active.

Selection	Usage
	This option is selected by default.
Exit	Exits ScriptGen and closes the *ScriptGen* dialog.

Adding a Chassis

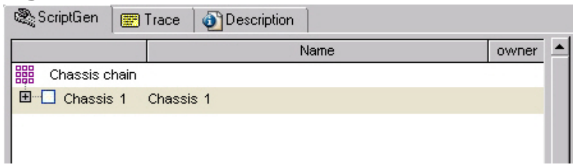
After opening the *ScriptGen* dialog, the chassis of the port that is to be scripted must be added. Enter the chassis name or IP address in the *Chassis Name* field, as shown in *Figure:Adding a Chassis*.

Figure:Adding a Chassis



Once the chassis name is entered, select the *Add* button. When the chassis is added, it will appear in the tree in left window as shown in *Figure:Added Chassis*.

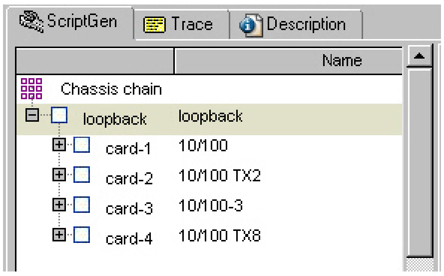
Figure:Added Chassis



Chassis in a chain must be added to ScriptGen in the same order they appear in the chain.

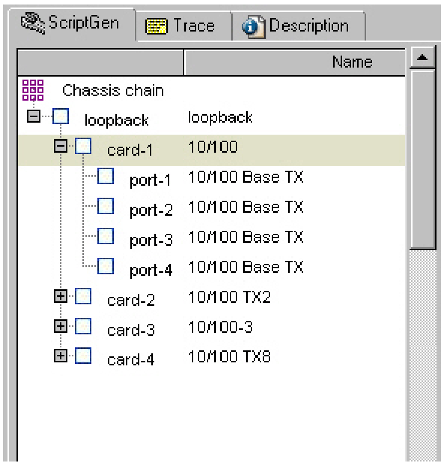
Double-click the chassis to expand the tree and view the modules in the chassis, as shown in *Figure:Expanded Chassis Tree (Modules)*.

Figure:Expanded Chassis Tree (Modules)



Double-click a module to further expand the tree and view the ports in the module, as shown in *Figure:Expanded Chassis Tree (Ports)*.

Figure:Expanded Chassis Tree (Ports)

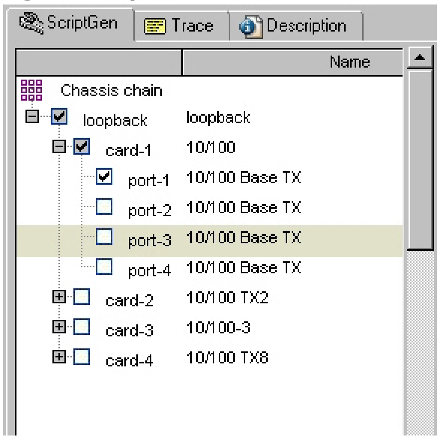


Creating a Script for a Port

To create a script for a port:

1. Expand the chassis tree on the left side of the *ScriptGen* dialog and select the port or ports for which a script will be created by clicking the empty box to the left of the port. A check mark appears, as shown in *Figure:ScriptGen Ports*.

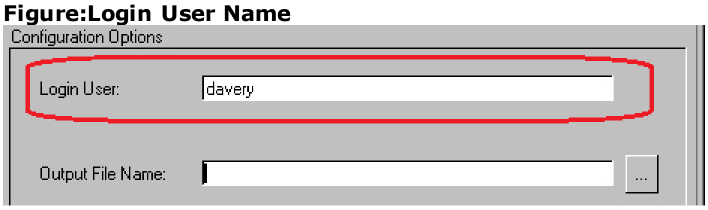
   Figure:ScriptGen Ports

   More than one port can be selected for scripting by clicking several ports in the chassis. All ports in a module can be selected by clicking the module box.

2. If desired, enter the login name for the chassis, as shown.

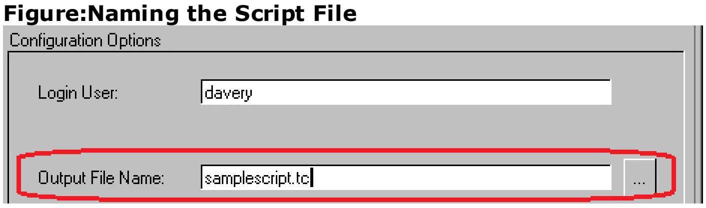
   Figure:Login User Name

   If this option is used, then only ports owned by the login name entered and unowned ports are scripted.

3. Enter the file name for the script in the *OutPut File Name* field, as shown.

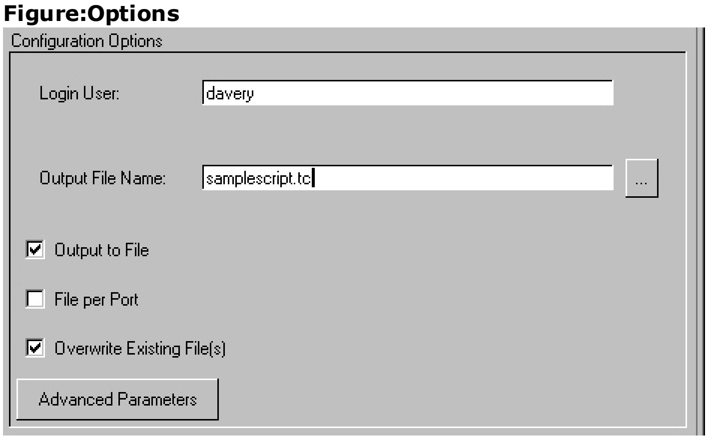
Figure:Naming the Script File



The '...' button (...) can also be used to browse to a specific file.

4. Beneath the *OutPut File Name* field, set the other configuration options for script generation, which include *Output to File*, *File per Port*, *Overwrite Existing File(s)*, and *Advanced Parameters*, as shown.

Figure:Options



Refer to *Invoking ScriptGen* for more information regarding these options. The *Advanced Parameters* button is described in *Advanced Parameters* below.

5. When conditions have been accurately configured, select the *Run* icon ( ) to initiate the generation of a script or scripts.

NOTE

Port ownership can affect ScriptGen's file creation, in the following manner:

If the first port is explicitly owned by a user, then all ports in the set of ports to be scripted must either be owned by that user or be 'unowned.'

If the first port is 'unowned,' then all ports in the set must be 'unowned.'

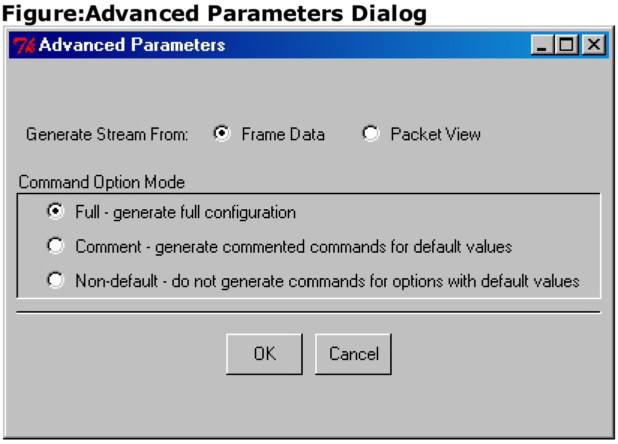
NOTE

When using ScriptGen with Port Groups, ports from different chassis chain that are in the same Port Group cause the ScriptGen option to fail. Likewise, ports from chassis that have the same chassis ID will cause the ScriptGen option to fail.

Advanced Parameters

The *Advanced Parameters* button opens the *Advanced Parameters* dialog, shown in *Figure:Advanced Parameters Dialog*.

Figure:Advanced Parameters Dialog



The controls for this dialog are explained in table.

Figure:Advanced Parameters Configuration

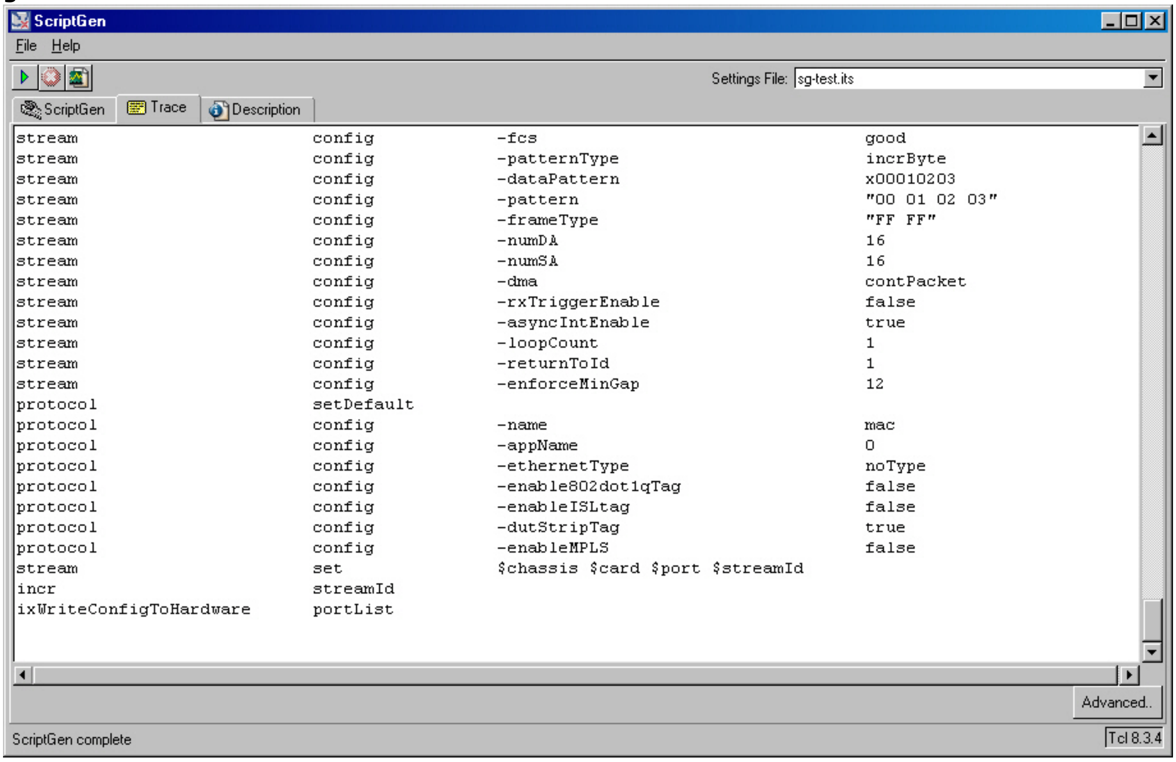
Section	Field/Control	Usage
Generate Stream From		Sets from where to generate the scripted stream. The default is Frame Data.
	Frame Data	Generates the scripted stream from Frame Data controls.
	Packet View	Generates the scripted stream from the Packet View.
Command Option Mode		Sets how much of the default information should be included in the script.
	Full	Generates a script that includes all control information, whether it is default configuration or not. NOTE Use Full option if port configuration is important. Other than Full option may result in configuration that is not complete.
	Comment	Generates a script that includes all control information, but all default configuration is set as a comment. Commented information does not affect card, port, or stream behavior.
	Non-Default	Generates a script that only includes non-default configuration information.

Trace Tab

The *Trace* tab page records and displays the actions of ScriptGen. When a script is created, it is displayed in the *Trace* tab. The *Trace* tab also displays error messages and warnings.

The *Trace* tab page is shown in *Figure:Trace Tab*.

Figure:Trace Tab



Advanced Trace Options

Clicking the *Advanced* button displays the *Trace Settings* dialog. The *Trace Settings* dialog is shown in *Figure:Trace Settings Dialog*.

Figure:Trace Settings Dialog

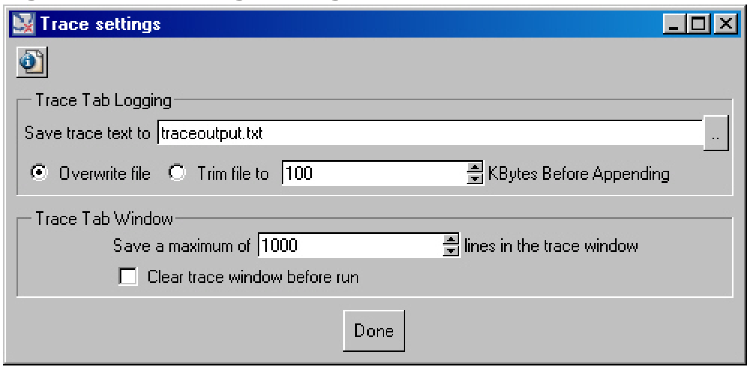


Table:Trace Settings describes the fields in the *Trace Settings* dialog.

Table:Trace Settings

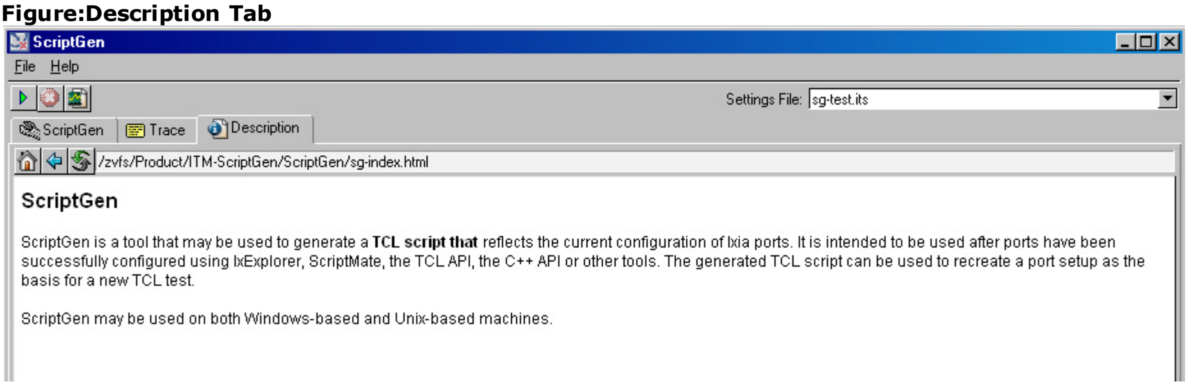
Group	Field	Usage
Trace Tab Logging	Save trace text to	Allows to select the name and destination of the *Trace* tab capture file.
	Overwrite file	Overwrites the *Trace* tab capture file each time a new test is run. Information from the previous test is lost.
	Trim file to	Trims the old file size to the set level, then appends new test Trace information to the file contents.

Group	Field	Usage
Trace Tab Window	Save a maximum of	Limits the size of the *Trace* tab information that is displayed. The oldest entries in the tab are removed when the line cap is reached.
	Clear trace window before run	Clears the *Trace* tab of all previous test information when a new test is run. If not selected, new test information is added to previous test information.

Description Tab

The *Description* tab provides a basic description of the function of ScriptGen. It is shown in *Figure:Description Tab*.

Figure:Description Tab



[This page intentionally left blank]

Index

G

J

S

V

W

X