Xgig Analyzer

Version 7.3

User's Guide

Xgig Analyzer

Version 7.3

User's Guide

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

Notice

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

Copyright/Trademarks

Copyright release

Terms and conditions

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

Third Party License Agreements

LZ4 - Makefile

You can contact the author at:

- LZ4 source repository: https://github.com/Cyan4973/lz4

- LZ4 forum froup: https://groups.google.com/forum/#!forum/lz4c

CONTENTS

PART ONE: Using Xgig Analyzer

Chapter 1 Introduction

PART TWO: Using Xgig TraceControl

Chapter 2 About Xgig TraceControl

Chapter 3 Getting Started with Xgig TraceControl

PART ONE: Using Xgig Analyzer

Chapter 1

Introduction

In this chapter:

- The Xgig Systems
- Xgig Blades
- Connecting the Xgig Analyzer to a Target System
- Xgig Analysis and Control Software
- New Features
- Getting Help

The Xgig Systems

The Xgig Family of Distributed Systems for Monitoring, Analysis, and Testing are multi-purpose systems designed for engineering, field service, and network operations personnel. Xgig platforms can be rack-mounted at your data center or strategically located anywhere in your network. For Fibre Channel, Gigabit Ethernet, PCIe/NVMe, or SAS/SATA applications, Xgig chassis contain a set of hardware analyzer blades that attach through SFP or XFP transceivers to the circuit or device under test and software programs for hardware control and data analysis. For detailed information about each of the Xgig systems, refer to the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* on the product USB memory drive.

The Xgig Analyzer software features data capture, real-time performance reporting, protocol analysis, and error rate measurements. The software automatically extracts and decodes the data correctly. The software displays the data in several formats for statistical analysis. Extensive find, hide, and filter capabilities speed up the job of protocol analysis.

Xgig Blades

Blades within an Xgig chassis perform application-specific tasks. The Multi-Function Blade ports can support a variety of different functions depending on the license for the blade. Possible functions include analysis, traffic modification, and traffic generation.

Each blade consists of four major elements: serial gigabit connection, real-time performance measurement, filter and trigger, and capture to memory. Xgig blades ensure both accurate data collection and transparency on the link. The blade has sophisticated triggering and filtering to isolate error conditions in the data. Pre-capture filtering can expand the capture time to minutes.

For detailed information about each type of Xgig blade, refer to the *Xgig Blade Hardware Guide,* the *Xgig5000 Blade Hardware Guide,* or the *Xgig1000 Hardware Guide* on the product USB memory drive.

Xgig Fixed-Port Systems

An Xgig fixed-port system is a self-contained bench setup Xgig system. These systems are available as either fixed-function (Analyzer) or multi-function. All ports, connectors, and controls found on an Xgig chassis containing Xgig blades are present on these systems. The multi-function system ports can support a variety of different functions depending on the license for the system ports. Possible functions include analysis, traffic modification, and traffic generation.

Xgig fixed-port systems consist of four major elements: serial gigabit connection, real-time performance measurement, filter and trigger, and capture to memory. Xgig fixed-port systems ensure both accurate data collection and transparency on the link. The system has sophisticated triggering and filtering to isolate error conditions in the data. Pre-capture filtering can expand the capture time to minutes.

For detailed information about Xgig fixed-port systems, refer to the *Xgig Family Hardware Guide* or the *Xgig1000 Hardware Guide* on the product USB memory drive.

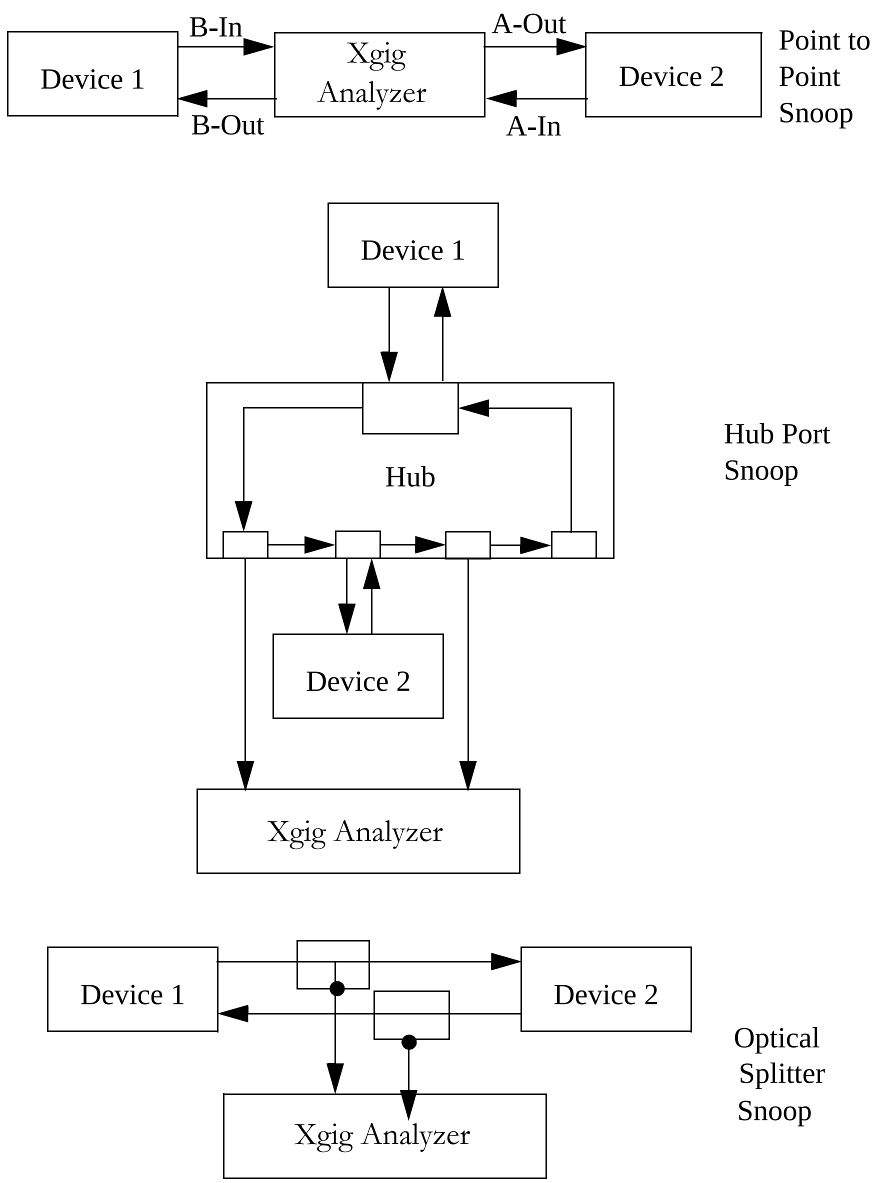
Connecting the Xgig Analyzer to a Target System

There are three methods for placing an Xgig analyzer in a Fibre Channel or Gigabit Ethernet system, as shown in Figure 1. These are:

- Point-to-point
- Hub Port Snoop
- Optical Splitter Snoop

Refer to Appendix B, "Connection and Wiring Examples" for examples of the physical wiring for connecting analyzer ports.

Figure 1: Placing the Analyzer in a Target Network System



With the point-to-point connection, the Xgig is placed in a series, between the source and destination. If the analyzer is configured for analog passthrough, a small amount of jitter, with an acceptable eye opening, is added to the signal as it passes through the analyzer. If the Xgig is configured for digital retiming at the front end, any jitter in the incoming signal is corrected, but idle characters may be added or dropped from the traffic.

The transmit port of a hub is active at all times. A hub port is in bypass mode until a signal is returned to the receive connection. This property of a hub can be used to passively snoop a network.

Connect only the transmit port of the hub to the receive port of the analyzer. The analyzer captures the data while the hub port remains in bypass mode. With the analyzer connected to one port on the hub, you can remove or reconnect the analyzer without disturbing the links under test.

Another alternative is the Optical Splitter Snoop or Fiber Tap. This alternative allows you to connect or remove the analyzer without disturbing the links under test. This is valid only for Fibre Channel or Gigabit Ethernet.

If you cannot interrupt the network and you need maximum versatility for sniffing at different configuration points, consider using the Viavi Snoop GBIC or a Viavi Fiber Tap. This product provides an additional pair of ports for simultaneous transparent monitoring of either Gigabit Ethernet or Fibre Channel links without causing any link loading or down time of the system under test.

Xgig Hardware to Xgig Analyzer Software Connection

For Xgig, the analyzer blade(s) resides in a different system from your Xgig client software. You must have an Ethernet connection between the Xgig chassis and the system running your Xgig client software. For Xgig1K and Xgig5K chassis, you may control the chassis using the USB connection if it is supported by your Xgig client software.

Xgig Access Through a Firewall

In general, Xgig client software should be able to access an Xgig Chassis that lies behind a firewall. Ports must be open as described in the following table to permit operation across a firewall for Xgig applications:

Table 1: Requirements for Xgig Access Through a Firewall

Application	TCP/UDP	Port Direction	Server Application on Port
Administration Web Pages	80 (HTTP)	Out	Apache Web Server
Administration Web Pages	21 (FTP)	In	None
Xgig Analyzer	2000 or 52000 or ...	In/Out	Xgig Analyzer Server
Xgig Maestro	2000 or 52000 or ...	In/Out	Xgig Maestro Server
Xgig Maestro	6000	In/Out	Xgig Maestro Server
Xgig Maestro	135 (DCOM)	In/Out	Xgig Maestro Server

The main TCP port number used to communicate with an Xgig chassis is port 2000. If your IT department blocks the TCP port 2000 on the network, you can still change it to 52000 or any other number of your choice. However this change must be done on all client computers and all Xgig chassis on your network at the same time, otherwise some chassis won't be visible and accessible from some clients.

On the client side, you can change the default TCP port 2000 by selecting **Edit Xgig TCP Port** from the **Start** menu. A dialog appears where you can type in a value for the TCP port. Click **Apply** to change the port. You can also change the TCP port for the most recently used chassis by clicking the chassis name(s) in the Most Recently Used Chassis section of the dialog. Again, you must update all the clients and chassis on your network at the same time; otherwise the Xgig applications will not see some chassis.

For sites where Xgig Maestro is not used, it is suggested that the DCOM port remain closed.

Network Address Translation (NAT) is not supported. An Xgig Chassis protected by a firewall that uses Network Address Translation (NAT) cannot be accessed from Xgig clients outside the firewall.

Finally, client-initiated chassis upgrades do not work across network firewalls since they use random TCP port numbers between the client and the chassis. The Xgig client installers automatically open the Windows Firewall for the syncgroupupgradeutil.exe and probeupgradeutility.exe, but again, network firewalls will prevent the client-initiated chassis upgrades from succeeding. In that case, you should always upgrade your chassis from the chassis Administration web page.

Xgig Analysis and Control Software

The Xgig Analyzer software is a suite of four programs for controlling hardware capture and analyzing the data. The first three programs are described in this book. Refer to the Xgig Expert help system for information on Xgig Expert.

Xgig TraceControl 

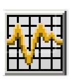
Xgig TraceControl configures and runs the protocol analyzer to capture data. Using the Xgig TraceControl, you can set the payload filter and trace size, select the capture and trigger criteria, and start/stop the capture of data.

Xgig Performance Monitor 

Xgig Performance Monitor displays real time performance and error parameters passing through the analyzer. Use the Xgig Performance Monitor to monitor the performance of each channel and detect errors. You can vary the update rate to suit your measurement and all meters scale automatically. Both the instantaneous, average, and maximum rates are plotted on the screen.

Xgig TraceView 

Xgig TraceView displays the data captured by the analyzer. Xgig TraceView will either show data currently in trace memory or open a file containing saved data. Xgig TraceView displays traces, searches and filters the traces, and extracts portions of the trace. You can export the traces to a delimited format that can be used by other databases and spreadsheets.

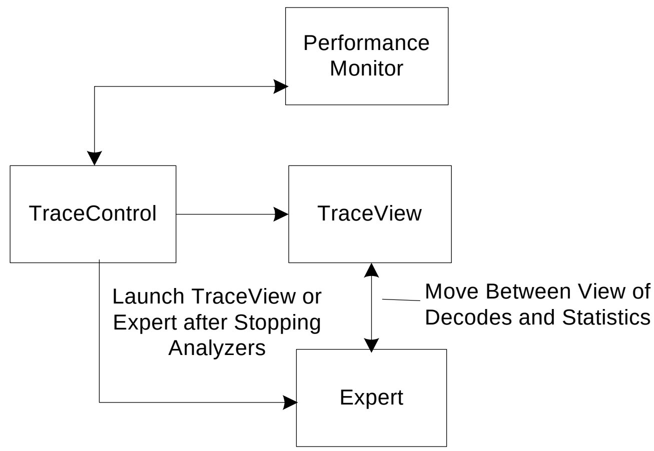
Xgig Expert 

Expert is an analysis tool for Fibre Channel, FCP-SCSI, Gigabit Ethernet, FCoE, IP, TCP, iFCP, FCIP, SAS, SATA, PCIe/NVMe, AHCI, and iSCSI traffic. Xgig Expert automatically identifies protocol violations and errors within the trace as well as providing a rich set of metrics for performance and behavioral analysis. Traces from Gigabit Ethernet topology, Fibre Channel topology (Arbitrated Loop, Public Loop, Switch Fabric, etc.), and SAS/SATA topologies are supported and automatically analyzed when opened.

Software Road Map

The diagram below shows how the Xgig suite of programs are interrelated.

Figure 2: Xgig Client Applications Road Map



Xgig Software Limitations

Domains that contain ports on different chassis when Xgig chassis are cascaded are called inter-chassis domains. Intra-chassis domains refer to domains where all ports are on the same chassis. A Sync Group can have up to 8 locked inter-chassis domains. There is no limit on the number of unlocked domains, except that each port must belong to only one domain at a time. Also, the number of intra-chassis domains is only limited by the number of port-pairs on the chassis.

If you perform a soft reboot of the Xgig chassis, all ports will be disconnected.

Xgig Expert performance is related to several factors – the size of the trace, the number of ports in the trace, and the CPU speed and memory capacity of the computer running the Xgig Expert client. You can improve performance by manipulating any of these variables. Reducing the size of the trace information or reducing the port count in the trace will improve Xgig Expert's performance. Increasing the processing power and memory of your client PC will also improve performance. Although Xgig Expert will eventually process extremely large traces (e.g., 32 GB) with extremely large port counts (e.g., 64 ports), opening such traces will take many hours.

If you need to open large-file/high-port-count traces, it is recommended that you add as much memory and CPU speed to the client system as possible. It is also recommended that you make sure you do not include more ports than are needed or make traces larger than needed when using Xgig Expert.

Installation

Below is an overview of the installation process. For system requirements and complete installation instructions for the Xgig Analyzer software, refer to the *Xgig Analyzer Software Installation Guide*.

The general steps are outlined below:

1. Check to make sure your system meets the system requirements for installing Xgig Analyzer software.
2. Install any new hardware in your Xgig chassis. Refer to the documentation that comes with the new blade.
3. Installation requires the removal of older versions of software. Remove all older versions of GTX, IBT, Expert, or Xgig software before installing the new version.
4. Install the new Xgig Analyzer software on your PC system.
5. If the new version requires an upgrade to the Xgig chassis, you will receive a separate USB memory drive to upgrade the software on the Xgig chassis. Xgig remote analyzer system hardware is shipped with all required software installed. However, upgrading to a new version of Xgig Analyzer software may require an upgrade of software at the Xgig system. Refer to the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* for more information on installing software on the Xgig chassis.

New Features

This release of Xgig Analyzer includes the following new features:

- **PCIe specific features:**
    - A new option to capture traces with compression of TS1 and TS2 events.
    - The Xgig can capture the PERST# and CLKREQ# signal transitions and produce the L1 substates in the LTSSM.
    - The Devices And Addresses dialog now draws the PCIe topology in the Topology tab.
    - New equalization presets are available for the SFF 8639 interposer.
    - Detects and support the NVMe Dual Port configuration on the SFF 8639, when the DualPortEn# pin is low.
    - Support the new Right-angle and Left-angle interposers.
    - PCIe Tuning Wizard in TraceControl allowing to change the Equalization settings manually and semi-automatically.
    - NVMe over ROCE/ROCEv2/IBXoE is now decoded when the following TraceView menu is checked:
View/Decode Switches/RDMA Payload Interpretation/NVMe Protocol
    - TraceView LTSSM Boxcar View lists sequences is visited repeatedly, Theay are displayed as a single bubbles listing the states visited and the number of loops.
- O**ther new features:**
    - Xgig-Expert can now skip optional Ethernet headers (like the VnTag) and Fibre Channel headers when present and produce proper metrics.
    - TraceView now has a new Quick Find "Not" option to find anything that does not match the criterion.
    - TraceView now has a new Quick Find "rgn" operator to search for address ranges.
    - New 12G SAS preset for link config#32.

Getting Help

Xgig Online Help

We have included an extensive, online Help system with the Xgig analyzer software. The online Help system contains all the information and instructions for operating Xgig software that is in this guide, plus additional information. See the Xgig Expert help system for additional reference material about Fibre Channel operation and protocols. Press the Help button from within any application to access the online help.

Xgig Hardware Manuals

The *Xgig Hardware Family Guide* explains the hardware and connectors for the legacy models of the Xgig chassis. Refer to this document for information on how to install, configure, upgrade, and administer the legacy Xgig hardware chassis.

The *Xgig Blade Hardware Guide* provides information on ports/LEDs and instructions on how to install or remove the blade for the Xgig chassis.

The *Xgig5000 Hardware Family Guide* explains the hardware and connectors for all models of the Xgig5000 chassis. Refer to this document for information on how to install, configure, upgrade, and administer the Xgig5000 chassis.

The *Xgig5000 Blade Hardware Guide* provides information on ports/LEDs and instructions on how to install or remove the blades for the Xgig5000 chassis.

The *Xgig1000 Hardware Guide* explains the hardware and connectors for all models of the Xgig1000 fixed-port systems. Refer to this document for information on how to install, configure, upgrade, and administer the Xgig1000 chassis.

The *Xgig1000 Interposers Hardware Guide* explains the connectors and hardware for all models of the Xgig1000 interposers. Refer to this document for information on how to install and connect these devices.

Decode Improvements

Decode improvements implemented in each release are documented in the file named `CurrentProtocolVersions.txt` in the CurrentProtocols folder located in the installation folder.

Technical Assistance

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

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

PART TWO: Using Xgig TraceControl

Chapter 2

About Xgig TraceControl

In this chapter:

- Introduction to TraceControl

Introduction to TraceControl

Xgig TraceControl is one of four programs in the Xgig Analyzer software suite. Xgig TraceControl provides data capture for Viavi hardware analyzer systems. Use Xgig TraceControl to:

- Configure Viavi analyzers with capture and trigger settings
- Start and stop a capture
- Create sets of hardware analyzer ports for making captures
- Save sets of hardware analyzer ports and configurations for later use
- Save captures to disk for analysis
- Save log of real time statistics

Xgig Analyzer software supports the JXgig family of test/analysis systems. Xgig analyzer software supports up to 64 ports (4 Xgig chassis with 4 blades, each blade with 4 ports) when concatenating Xgig chassis. The maximum number of ports in a domain depends on what types of Xgig, Xgig5000, or Xgig1000 systems you have.

Xgig Analyzer software supports the Xgig family of test/analysis devices. The Xgig, Xgig1000, and Xgig5000 allow you to analyze networks with a variety of protocols, including Fibre Channel, SAS/SATA, Gigabit Ethernet, PCIe/NVMe, and AHCI. The function of ports on blades in a chassis is controlled through TraceControl software.

Chapter 3

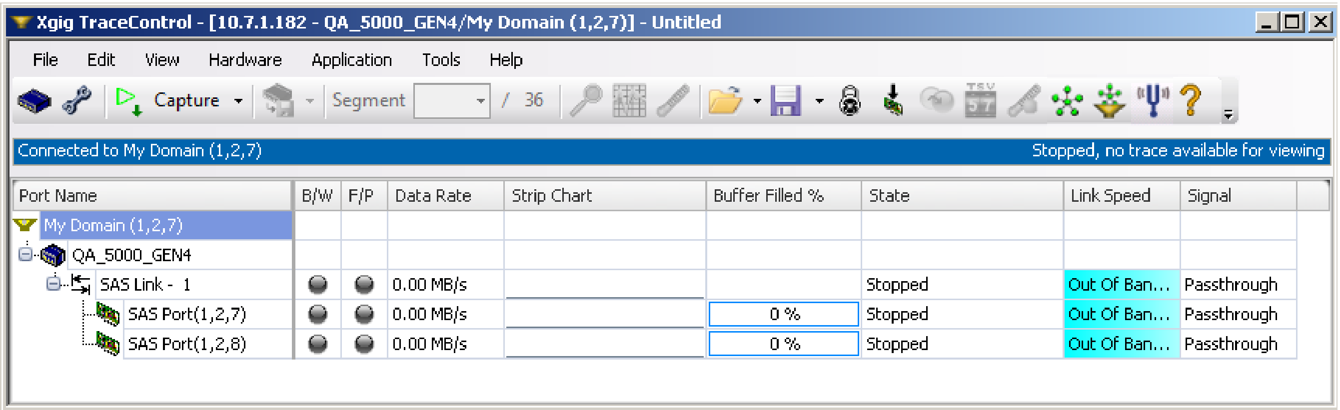
Getting Started with Xgig TraceControl

In this chapter:

Launching Xgig TraceControl

Launch TraceControl by double-clicking on the **TraceControl** shortcut icon on the desktop. The TraceControl main window appears with the **Device Browser** in the left pane.

Figure 3: TraceControl Main Window



As described in the next section, you can create a domain and use the buttons to start and stop a capture. You can then save the resulting trace to a file.

You can set conditions for starting and stopping the analyzer and selecting the type of data the analyzer will capture. For information on setting up what data to capture. See "General Settings" on page 93. For options on starting and stopping the analyzers, See "Capture and Trigger Setup" on page 107.

You must set up the proper domains and configure analyzer blades so you'll get the trace you want. You must load a separate instance of Xgig TraceControl software to start a simultaneous capture for another domain. For more information on domains, See "Domains, Links, and Sync Groups" on page 30.

Customizing the Menu Bar

You can customize the menu bar in TraceControl in several ways. Click the arrow icon at the right edge of the menu bar, and select either **Show or Hide Buttons** or **Customize**. Clicking **Show or Hide Buttons** opens a list of available menu items. You can click any of the items' icons to show or hide them. Clicking **Customize** opens a dialog that allows you to show or hide each icon in addition to moving icons up or down in the list to determine in what order they appear in the menu bar. You can also access the list of menu items by selecting **View, Customize Toolbar.** Note that the Surveyor button is hidden by default when you first install the client application. Use the Show/Hide feature to display it.

Secure Login for Xgig Chassis

An Xgig chassis may be password protected to prevent access by unauthorized users. Password protection is set through the Xgig Web Utility for each Xgig chassis. If the Xgig chassis you are attempting to access is password protected, you are required to provide the password. The following login screen will appear. Enter the password to continue; the account name is always Administrator.

Figure 4: Xgig Analyzer Login

Login is only required once from any of the Xgig Analyzer applications or Xgig Maestro running on the same Xgig Analyzer PC client machine. For example, if you login through TraceControl, you will not be asked for the password again when you access the same Xgig chassis sync group through Xgig Performance Monitor. To make sure you are completely logged off from all Xgig chassis, you must close all Xgig applications.

For login, the settings of a master Xgig chassis in a sync group prevail for all chassis in the sync group. If the master has authentication turned off and a slave(s) has authentication turned on, then the sync group as a whole has authentication turned off. The settings for the master Xgig chassis also prevail for the password; the password of the master Xgig chassis will be the password of any attached slave. See “Xgig Blade and Port Numbering” on page 45 and the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* for more information on master, slaves, and sync groups.

Port Status View

The TraceControl main window displays a status of all ports for the current domain. If no domain has been created the window is blank.

When you first open Xgig TraceControl, no domains have been created, so no domains are shown. When you open Xgig TraceControl after creating a domain, the last used domain is selected. To create a domain, press the **Create Domain** button or select **Create Domain** from the **Hardware** menu.

At the top of the **Port Status View** is a status bar. This bar provides the following information: the state of your connection to the domain, any warnings about the status update being stopped, and the capture duration.

The Port Name column lists the name of all ports and chassis within the domain. The domain is displayed in a tree structure with the domain as the root of the tree. Ports are listed within chassis. Ports are shown in the order of their physical presence in the Xgig chassis.

The software LEDs (B/W and F/P) only update while the ports are connected in TraceControl. If you disconnect and then reconnect to a domain, the port LEDs will be reset.

The port status fields shown in the TraceControl main window are defined below. Note that you can change the order of the columns by dragging and dropping them. All columns shown in Performance Monitor's List View can be added to Port Status view. To add/remove columns, select **View, Customize Columns, Add/Remove Columns**. You can also right-click a column header and select **Add/Remove Columns**. To restore default columns, select **View, Customize Columns, Restore Default Columns**.

Port Name

The name identifying the port. If the port has been given a user-defined name, the user-defined name will appear in this column. See "Default Port and Domain Labels" on page 44 for information on port naming. Note that when you rename a port, the status update pauses, and a warning message appears in the status bar above the **Port Status View**.

B/W

The color of a software "LED" light indicates the Byte/Word status for the port. The colors have the same meaning as in Performance Monitor. If the ports are not locked, port LEDs are shown gray. See Table 2 for descriptions. A tooltip showing the status or errors for a port appears when you curse over the LED.

F/P

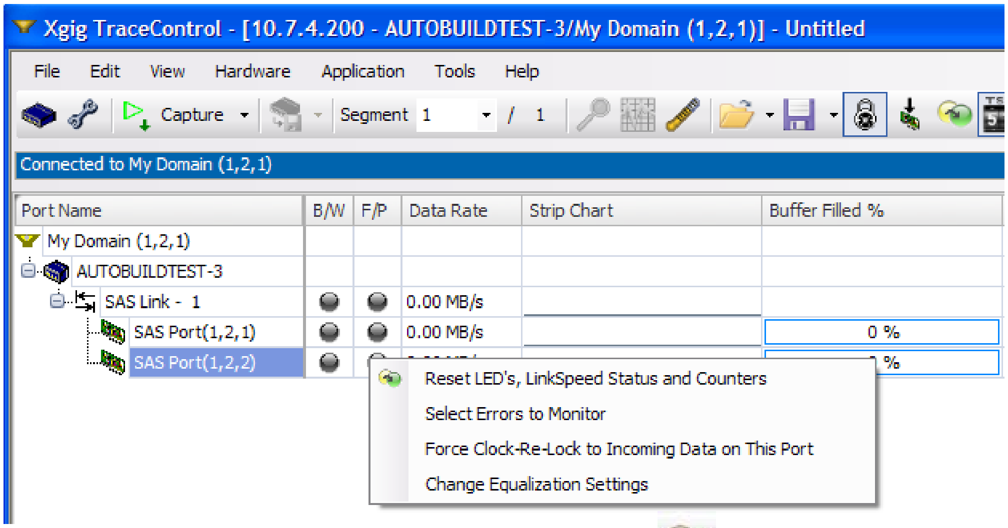
The color of a software "LED" light indicates the Frames/Packets status for the port. The colors have the same meaning as in Performance Monitor. If the ports are not locked, port LEDs are shown gray. See Table 2 for descriptions. A tooltip showing the status or errors for a port appears when you curse over the LED.

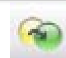
Table 2: Word and Frame Status LEDs for Ports

Byte/Word LED	**Reason**
Black	No signal or no light, often a result of a disconnected cable
Red	Signal with errors, for example, illegal characters, running disparity violations, CRC mis-match
Yellow	Had an error in the past, currently no errors
Green	Good signal, legal characters, proper disparity, good CRC if present
Frame/Packet LED	**Reason**
Black	No SOF ordered set recognized
Red	SOF with CRC mismatch error
Yellow	Had a CRC error in the past, currently no errors
Green	Good CRC and recognized SOFs are present

If you wish to reset ports or change the errors being monitored, right-click one of the **B/W** or **F/P** LED for the port. From the context menu, you have four options, as shown in Figure 5.

Figure 5: Options for Selecting Errors and Resetting Ports in Port Status View



- **Reset LED's, Link Speed Status, and Counters** 
  A reset clears all errors, resets the software LEDs in TraceControl for the ports, resets the Link Speed Status, the counters, and the columns. You can also reset LEDs by using the button in the toolbar shown above.

- **Select Errors to Monitor**
  This option brings up the dialog for configuring TraceControl options. The following tabs are available for setting errors to monitor, the **Frame Errors**, **Phy Errors**, **PCIe Errors**, and **SAS/ SATA Errors** tabs. Select the errors to monitor from these tabs as described in "TraceControl Options" on page 88.

- **Force Clock Re-lock to Incoming Data on This Port**
  This option will only appear when an 8G blade FC port or 6G blade SAS/SATA port is clicked. When the Clock Detection Recovery (CDR) loses its lock on the incoming data signal, the link speed cell will turn red and display the message **CDR Loss of Lock**. This menu item forces the re-locking of the clock to incoming data on the corresponding port. If the ports are not locked or capturing, this menu will be grayed out.

  For optical 8G blade FC ports, if this option fails to re-lock the signal, clean the fiber optic connections and check the signal.

- **Change Equalization Settings**
  This option opens the Blade X Equalization Settings web page. You will be prompted to enter the user name and password for the chassis web page. The default user name is **JDSU** and the default password is **JDSUsnt**. If the defaults have been changed, check with your system administrator for the correct user name and password. See "Equalization" on page 69 for more information.

- **Tuning**
  This option is only available for 12G SAS blades. It allows you to tune ports manually using a link tuning preset, find the best link tuning preset for ports, or automatically tune ports. See "Tuning for 12G SAS" on page 61 for more information.

Data Rate
Gives the current data rate for each port.

Strip Chart
Shows a view of the data rate for the port over time. The strip chart shows a red bar when errors occur.

Buffer Filled %
The percentage of the hardware buffer that is filled with data. This field turns blue if the hardware buffer has filled during the capture. An arrow marker appears in the field if the hardware buffer has filled and wrapped during capture. For multiplexed ports, the Buffer is split into upper and lower regions to show the amount of data filling up individually for logical link 0 and logical link 1. This field is not used for ports in a link.

State
Shows the state of each port within the current configuration, Pre-Armed, Armed, Pre-Triggered, Postfilling, or a custom Advanced Triggering state. If a capture is available, the length of the capture will be displayed in the status bar below the menu bar.

Link Speed
Shows the link speed for each port. Ports in the same pair will always share the same link speed. The link speed is set as part of the configuration for each port. If auto-negotiation is used, the auto-negotiation is displayed. See “Link Speed” on page 95 for more information.

If the port goes into an OOB (SAS/SATA only) state, the link speed will display **Out of Band in progress** and the background color of the cell will turn into a light blue. After the OOB has completed, the cell will be yellow. You can reset the background color by selecting **Reset LED’s, Link Speed Status**, **and Counters** from the **View** menu.

When the 16GFC analyzer detects training frames and patterns on the link, it displays the message “Training in progress” in the signal column and turns the cell into a light blue. When the analyzer comes out of the training, the cell turns yellow to indicate that there has been training frames. You can reset the background color by selecting **Reset LED’s, Link Speed Status, and Counters** from the **View** menu.

Signal
Shows the signal regeneration method, Retiming, Passthrough, or Passthrough(Mux) for the link. See “Signal Regeneration” on page 99 for more information.

Link Width
Shows the width of the link for PCIe ports, i.e. x1, x2, x4, or x8. This only applies to PCIe ports.

Scrambling
Shows if scrambled data is turned on or off for each port. See “Fibre Channel Link Speeds” on page 96 for information on setting up scrambled data for the port. Scrambling applies to 16G FC ports and PCIe ports. However, the scrambling status for PCIe ports is not shown in Port Status view.

FEC Columns
There are three FEC columns, all of which are hidden by default.

- **FEC Mode -** Indicates which FEC mode the port is set to
  To show this column, right-click a column header, and select **Add/Remove Columns** > **Data Transmission Columns**.

- **FEC Locked -** Indicates whether the port was able to detect the FEC and lock into it
  To show this column, right-click a column header, and select **Add/Remove Columns** > **Data Transmission Columns**.
- **FEC Parity Err -** This is an error counter for errors detected by FEC.
  To show this column, right-click a column header, and select **Add/Remove Columns** > **Phy Error Columns**.

CDR
The CDR (Clock Data Recovery) column is hidden by default. See "CDR (Clock Data Recovery)" on page 105.

Note that the running time of the capture is provided in the right corner of the status bar.

Link Monitoring in Port Status View

When ports are aggregated into links, links appear as a separate row within the status view. The same status fields (columns) are used for a link, but some fields have a slightly different meaning and some are not used.

Port Name
The name identifying the link. If the link has been given a user-defined name, the user-defined name will appear in this column.

B/W, F/P (LEDs)
See the table below for the definition of LED colors for links. The LEDs for links are slightly different than for individual ports as it indicates a status for the entire link. A tooltip showing the B/W or F/P status or errors for a link appears when you curse over the LED.

Table 3: Word and Frame Status LEDs for Links

Byte/Word LED	Reason
Gray	Ports in link are not locked
Black	No signal or no light for all ports
Red	At least one port in the link has a signal with errors; for example, illegal characters, running disparity violations, CRC mis-match
Yellow	At least one port in the link has had an error in the past, currently no ports have errors
Green	All ports free of errors. At least one port in the link has a good signal, legal characters, proper disparity, good CRC if present
Frame/Packet LED	**Reason**
Black	No SOF ordered set recognized for all ports
Gray	Ports in link are not locked
Red	At least one port in the link has an SOF with CRC mismatch error
Yellow	At least one port in the link had a CRC error in the past, currently no errors for all ports in the link
Green	All ports free of errors. At least one port in the link has a good CRC and recognized SOFs are present

Data Rate
Shows the current data rate for the link. The data rate the sum of the data rates for all ports in the link.

Strip Chart
Shows a view of the data rate for the link over time. The value displayed over time is the sum of the data rates for all ports in the link. The strip chart shows a red bar when errors occur.

Buffer Filled %
This field is not used for links.

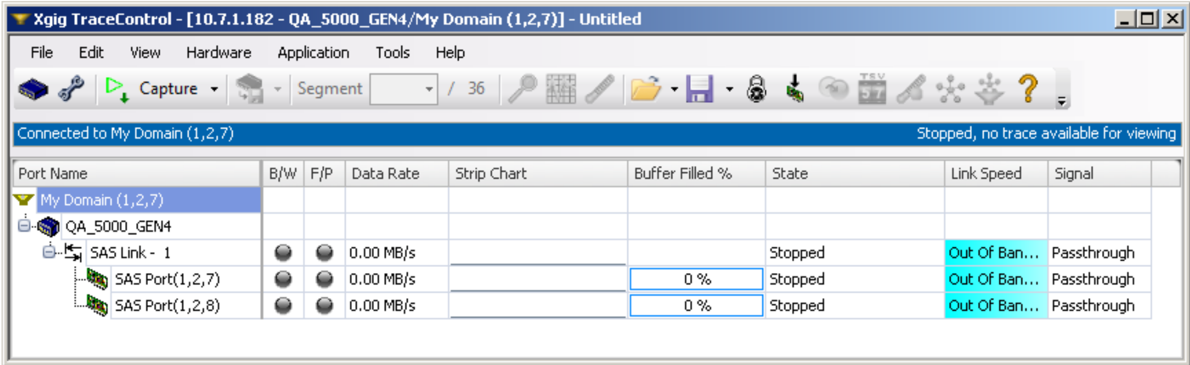
State
Shows the state of the link within the current configuration, Pre-Armed, Armed, Pre-Triggered, Triggered, Postfilling, Capture Available, or a custom Advanced Triggering state. If no configuration is applied to the ports, this field is blank. Capture Available indicates that a trace has completed, any traffic summary information has been generated, and the trace is ready to be viewed in TraceView. If a capture is available, the length of the capture will be displayed in the status bar below the menu bar. When different ports have different states, “mixed” is displayed.

Link Speed
Shows the link speed for all ports if the link speed is the same. If the link speed is not the same for all ports, this field displays **mixed** to indicate mixed data speeds within the link. If auto-negotiation is used, the auto-negotiation is displayed.

If one of the ports goes into an OOB (SAS/SATA only) state, the link speed will display **OOB in progress** and the background color of the cell will turn into a light blue. After the OOB has completed, the cell will be yellow. You can reset the background color by selecting **Reset LED’s, Link Speed Status, and Counters** from the **View** menu.

Signal
Shows the signal regeneration method, Retiming, Passthrough, or Passthrough(Mux) for the link. If the signal regeneration is not the same for all ports, this field displays **mixed** to indicate mixed signal regeneration within the link.

Figure 6: Link Monitoring in Port Status View



SFP and Power Monitoring in Port Status View

Some optional columns are available in the status view to obtain general information about SFPs and to monitor the transmit and receive power for ports. These columns only display if you select them by customizing the columns as described above. The default is to not display SFP diagnostic fields.

The columns shown under **SFPs** only contain information for optical SFPs only. N/A is shown for SAS or copper SFPs, or the field may be blank.

The columns shown under **40G SFPs** are for optical 40G SFPs. A set of diagnostic status fields are available for each of the four 40G ports in an Xgig1000 chassis.

Power levels can indicate if signal levels are not strong or have degraded due to the optical-electrical-optical pass-through process when the signal is passed through multiple analyzers or taps.

SFP diagnostic status fields take some time to show values. Allow at least 5 seconds for values to display in these columns, especially if you have many ports in the domain.

SFP RxPower

Shows the current power level for the receive port on the SFP. If no power level is reported by the SFP, this field will show **N/A**.

SFP TxPower

Shows the current power level for the transmit port on the SFP. If no power level is reported by the SFP, this field will show **N/A**.

SFP Make

Shows the vendor name of the SFP for each port. If no vendor is reported by the SFP, this field is blank.

SFP Model

Shows the model number of the SFP for each port. If no model number is reported by the SFP, this field is blank.

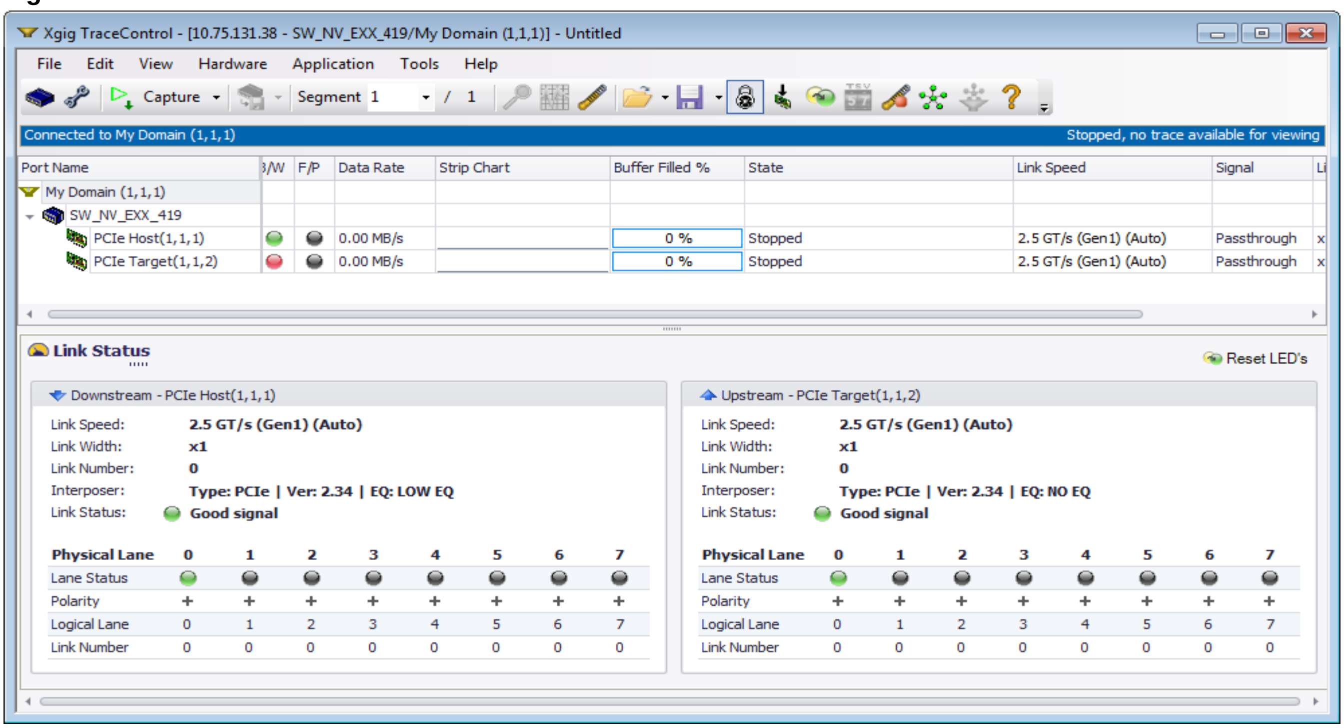
Error Monitoring in Port Status View

Some optional columns are available in the status view to obtain information about different types of errors, for example, frame errors, phy errors, SAS/SATA errors, PCIe errors, etc. These are the same errors that you can select to monitor in Performance Monitor using the Preferences menu under the Options tab. These columns only display if you select them by customizing the columns as described above. The default is to not display errors in Port Status view.

Link Status View

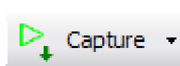
The **Link Status** panel shown in TraceControl's main window is a duplicate of the **Link Status** panel on the **Lane Control** tab of TaceControl's **Configuration Manager**. See "Lane Control" on page 136 for details about the information shown on this panel.

Figure 7: Link Status View



Capturing Traffic

To capture traffic and create a trace, follow the steps below.

Starting a Capture 

Create a domain of ports to use. See "Creating a New Domain" on page 47 for information on creating domains. Using the pull-down arrow, captures can be started in different modes for buffer segmentation. See "Segment Capture Options" on page 139 for more information.

Press the **Start** button. Xgig TraceControl displays a window showing the progress of the capture for all analyzer ports in the domain. The percentages should change if data streams are present. If there is no movement, check the following:

- Make sure that the link speed is set properly for all analyzer ports. An analyzer port with the wrong link speed will not collect data.
- Make sure that you have configured any filters in the **Configuration Editor** correctly. Filters can be set up that eliminate all data.
- Make sure that you have configured any triggers in the **Configuration Editor** correctly. Triggers can be set so the module immediately triggers.

If there appears to be nothing wrong with the analyzer configuration, check that you really are seeing traffic on the link using the Xgig Performance Monitor.

Trigger/Stop Xgig Captures from the Command Line

A utility exists to Trigger or Stop captures at the Xgig chassis from the command line of remote clients. The domain being triggered/stopped needs to be created using TraceControl. However, the utility does not have to be installed or run on the same machine as TraceControl. See Appendix D, “Xgig Chassis Trigger/Stop from the Command Line” for complete information.

Stopping a Capture Stop

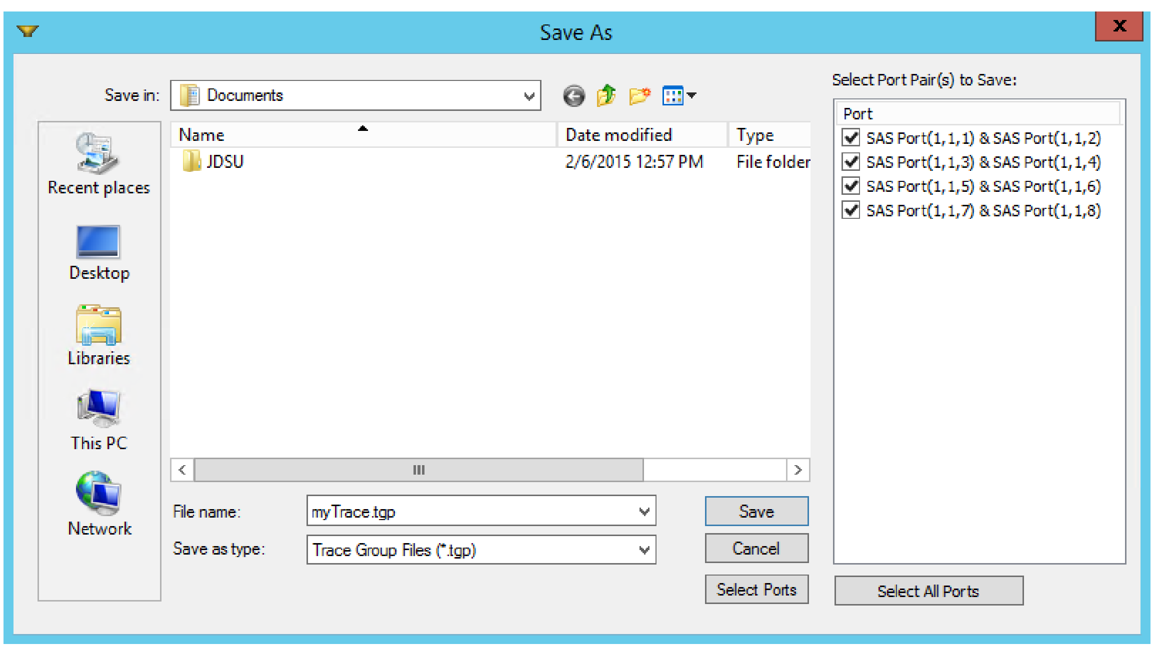
After starting, you may manually stop the capture if the trigger condition does not occur.

After stopping, you can view traffic within the hardware buffer by launching TraceView.

Saving a Trace to a File

After stopping a capture, you can save the trace to a file name and path of your preference by clicking the **Save Trace** button in TraceControl’s main window menu bar or by selecting **Save Trace…** from the **File** menu. You can choose to save the trace data from all ports or just selected ports.

Figure 8: Save As Dialog Box

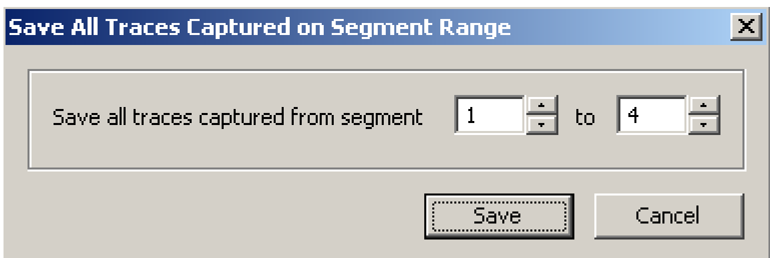


To save selected ports, click the **Select Ports** button below the **Save** button which displays the **Select Port Pair(s) to Save** list box. A dialog box is displayed to allow you to specify the name of the saved trace files.

When the trace files are saved, a sub-directory is also created with the same name followed by "**`.tgd`**" and the trace files are saved into that sub-directory. As an example, if you name the trace file "**`MyNewTrace`**", a sub-directory named "**`MyNewTrace.tgd`**" is added to the directory where you chose to save the files. Saving the trace files to a sub-directory allows you to copy or zip the sub-directory to share all of the required files for the complete trace with your associates. The following restrictions are imposed when saving a trace file:

- No other directory with a ".tgd" extension is allowed in the selected path.
- Once a trace file has been saved in a directory, no other trace file with the same name can be saved into that directory. If a the same name exists, an error message is displayed asking you to select a different path or a different name.

To save multiple segments, select **Save Traces from Segment Range...** from the **File** menu. A dialog box appears to select the range of segments to save. Then, another dialog box appears to allow you to specify the name of the saved trace file(s).



When saving a range of segments, the end segment number cannot exceed the number of segments available in the current capture buffer segment configuration. If a segment in the specified range does not contain data, the segment is not saved. An information message will display at the end of the save operation to notify you that some segments were not saved. If the option **Do not show this warning again** is checked in a previous appearance of this message, the message will not display. For each segment, the trace name is appended with an identifier indicating the segment number (_seg1, _seg2, etc.).

For example, assume you are saving segments 1 through 4, and segment 3 does not have any capture data. The trace name you have provided is **`newtrace`**. The following saved trace files will be created:

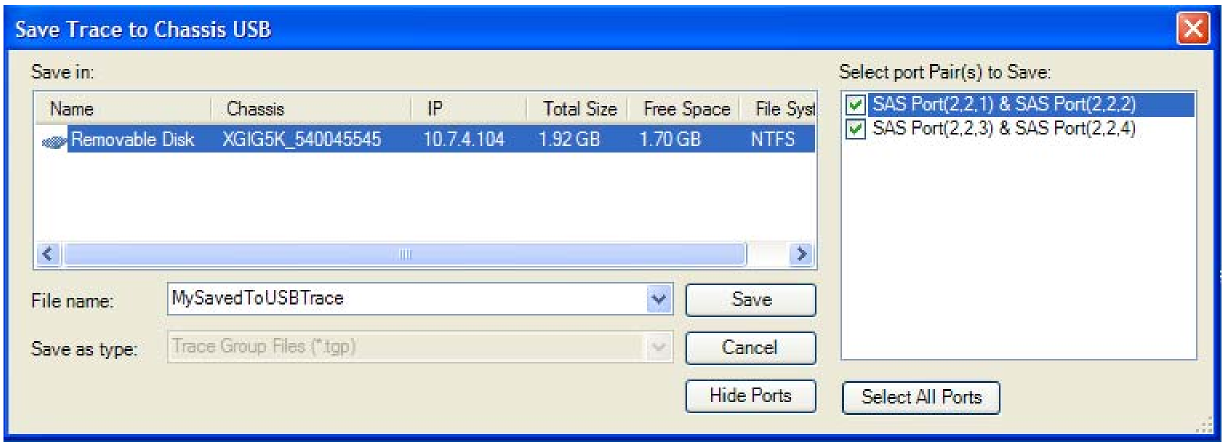
`newtrace_seg1.tgp`	and will be saved in a subdirectory named **`newtrace_seg1.tgd`**
`newtrace_seg2.tgp`	and will be saved in a subdirectory named **`newtrace_seg2.tgd`**
`newtrace_seg4.tgp`	and will be saved in a subdirectory named **`newtrace_seg4.tgd`**

If you are using an Xgig5000 or an Xgig1000, and you have a USB device connected to the chassis, the following options are available for saving traces. **Save Trace to Chassis USB...** and **Save Traces from Segmented Range to Chassis USB...** These options are identical to those discussed above. The only difference is the Save As dialog. The "Save in" list view shows all connected USB drives within the sync group. This allows you to save a capture on any chassis in the sync group even though the ports do not reside in that chassis.

The dialog shows the volume name of the drive, the chassis name where it is connected, the IP address of the chassis, the total size of the drive, the space available for saving, and the file system of the drive.

Note: If your external USB drive prompts for a HW installation, it will not be usable on the Xgig chassis. Only those drives that will operate with the standard USB storage class system drivers without prompting for a HW install will operate on the chassis.

Figure 9: Save Trace to Chassis USB



The **Show Ports** button opens the Port Selector list like the regular Save As dialog does.

PCapNg Files Format Option for Save

TraceControl supports traces being saved as PCapNg (PCAP Next Generation) files so that they can be used by applications other than Xgig Analyzer. Only Ethernet files can be saved to the PCapNg format. These files are saved with the .pcapng file extension.

Surveyor Format Options for Save

Gigabit Ethernet captures can be saved as Surveyor format files. Our Surveyor application can be used to open and view the decodes. To save the trace in Surveyor format, use the **Save As type:** box in the Save As dialog box and select **Surveyor Histogram Files (.hst) or Surveyor Capture Files (.cap)** as the file type.

When saving as a .cap file, TraceControl may save the trace as multiple files. More than one .cap file is created when the total number of bytes converted exceeds 512MB. Subsequent files will have a similar file name as the first converted file with a number in the file name. For example, if you save a trace as temp_GE.cap where the trace contains 1250MB, the save results in three files named in the following format:

```
temp_GE.cap
temp_GE_0536870928.cap
temp_GE_1073741864.cap
```

Launching Other Applications

You can launch Xgig TraceView, Xgig Performance Monitor, and Xgig Expert from the Xgig TraceControl window. Simply click these program icons in the TraceControl toolbar, or select an application from the **Application** menu.

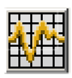
Xgig TraceView 

Once the Trace Buffer contains data or a trace file is saved, Xgig TraceView can be launched to view the decode of events contained in the analyzer hardware buffer or the trace file. Select the **Xgig TraceView** icon.

Xgig Performance Monitor 

The Xgig Performance Monitor application displays ongoing analyzer hardware buffer activity. Once the link speed is set for all analyzers, Xgig Performance Monitor can be launched. Select the **Xgig Performance Monitor** icon.

See “Link Speed” in the Port Status View section above for information on setting the link speed.

Xgig Expert 

Once the Trace Buffer contains data or a trace file is saved, Xgig Expert can be launched to view expert information for the trace. Select the **Xgig Expert** icon.

Surveyor 

If Surveyor is installed on the client computer, Xgig TraceControl can convert a GigE capture and launch Surveyor to view the converted capture. The **Surveyor** icon is hidden by default when you install the client application. To display it, use the Show/Hide feature as described above.

Domains, Links, and Sync Groups

A Sync Group is a single chassis or multiple chassis that can be time-synchronized. The Sync Group can be controlled as a single entity through Xgig Analyzer software. A Sync Group can be established with multiple analyzer chassis if the chassis are properly concatenated using the Cascade ports on the chassis.

A domain is a logical set or subset of ports that belong to the same Sync Group. A domain must contain an even number of hardware analyzer ports. Thus, a logical domain is an even number of analyzer ports between 2 and 64. The actual maximum number of physical ports is determined by the number of chassis concatenated together, the number of blades in each chassis, and the port density of each blade. The physical maximum is four chassis, with four blades, with four ports on each blade, for a maximum port count of 64.

Links are an aggregation of port-pairs. Port-pairs are a logical subset of a link, and links are a logical subset of domains. It is not required to use links; they are only required when you need to group more than one port-pair to carry the data for a single physical address, such as in wide-port SAS. SAS ports can be configured as a wide port that lets multiple SAS connections (typically four) be treated as one SAS address. In Xgig Analyzer, the multiple port-pairs that comprise the wide port SAS data pipe are configured into a link, which allows analysis of the four ports as a single data stream. Links are available for all protocols. For SAS links, all ports in a link must reside on the same blade. For FC, ports from different 4G and 8G blades can be grouped together. For GE, ports from different 10G blades can be grouped together.

The Sync Group Domain(s) area lists all the domains that have been created using the TraceControl and Maestro programs (even those created by other users). When you first open TraceControl, no domain exists.

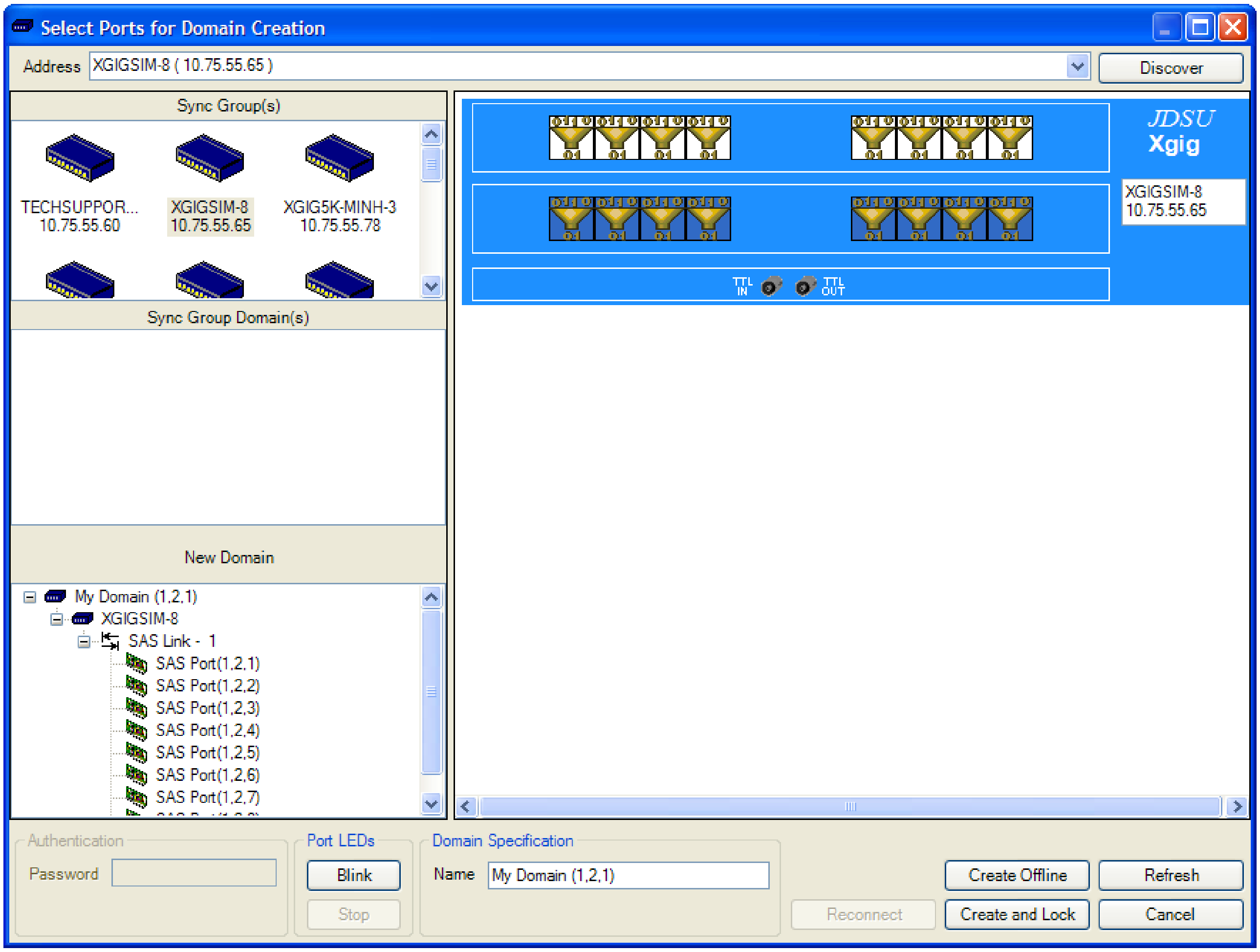
Traces are started and stopped for a domain, not for a port. Configuration can be performed on an entire domain, an individual port, or a collection of ports. Ports within a domain can look for different events to capture, and can be set to trigger by different events. However, all ports within a domain have the same trigger mode and are triggered at the same time by the trigger event.

Configuration files can only be saved for domains, not for individual analyzer blades or ports.

Select Ports for Domain Creation Dialog Box

Ports are selected for a domain using the **Select Ports for Domain Creation** dialog box. Press the **Create Domain** button on the toolbar to bring up the dialog. The dialog indicates the type, availability, and status of ports. It also allows you to name the domain or blink the front panel LEDs of ports on an Xgig chassis. The three areas on the left of the dialog can be resized as needed by clicking the splitter bar between the areas to make them different sizes.

Figure 10: Select Ports for Domain Creation Dialog



Discover Chassis on Different Subnets

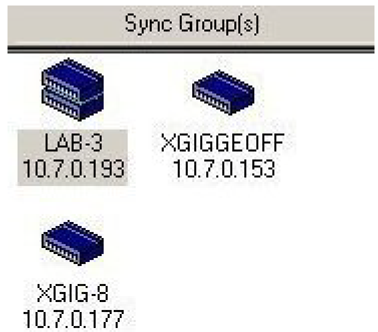
To select Sync Groups on a different subnet, enter the IP Address or DNS name in the Address field and press Discover (top of the dialog). The specific Sync Group you requested and all other Sync Groups on the same remote subnet will be added to the left panel.

If you are an Administrator on a Microsoft Windows system with Windows Firewall enabled and you open the Select Ports for Domain Creation dialog box of TraceControl for the first time, the firewall will prompt you to unblock `xgig-tracecontrol.exe`. Click **Unblock** to add `xgig-tracecontrol.exe` as a firewall exception to allow the other Sync Groups in the same subnet to be discovered. If you are a Standard User, you will need the Computer Administrator to unblock `xgig-tracecontrol.exe`. This also applies to the corresponding “discovery” dialog box of TraceView `(xgig-traceview.exe)`, Performance Monitor (`xgig-performance monitor.exe`) and Expert (`xgig-expert.exe`).

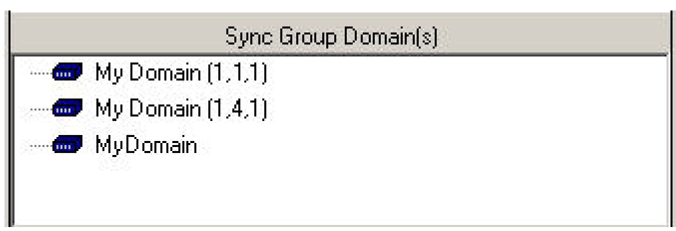
For Microsoft Windows Server operating systems, Windows Firewall must be disabled to allow the other Sync Groups in the same subnet to be discovered irrespective of whether you are an Administrator or a Standard User.

Sync Groups, Domains, Links, and Ports

All Sync Groups discovered on the local subnet are displayed in the upper left panel. When you select a Sync Group, its chassis, blades and ports display in the right panel showing all available ports. If multiple chassis are cascaded to form a Sync Group, the name and address of the master chassis within the Sync Group displays in the Sync Group(s) area. The addresses of slave chassis cascaded to the master do not display. However, you can use the name or address of a slave chassis in the Address field described above to discover a Sync Group on a subnet.



The **Sync Group Domain(s)** area lists all the domains that have been created using the TraceControl and Maestro programs (even those created by other users). Only one domain can be selected and used per TraceControl application. Once you select a domain and lock ports, if the domain contains ports within another domain in the list that are not locked, that domain is deleted. Users can create a maximum of eight domains in a Sync Group. Each domain within the Sync Group is shown as a hierarchical structure, showing all chassis, all links, and all ports that comprise the Domain.

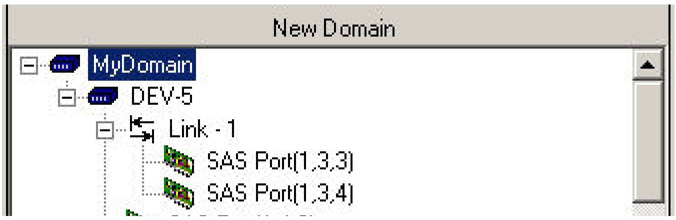


The **New Domain** area lists a domain that is being created without being connected (or locked) to the hardware. Click a port-pair in the Port Viewing and Selection area to start the process. Only one domain can be created in this area per TraceControl application. Once you select the domain and lock ports, the domain will be added to domains that are stored on the Xgig chassis and will appear in the **Sync Group Domain(s)** area.

The new domain within the Sync Group is shown as a hierarchical structure, showing all chassis, all links, and all ports that comprise the Domain. Chassis are automatically added to the domain hierarchical structure by selecting ports from that chassis. You can add more ports to a chassis by selecting ports (port-pairs) in the Port Viewing and Selection area. Click a chassis to add all ports within the chassis to the domain.

Links are an aggregation of port-pairs. FC and GE port-pairs are included in a domain without being assigned to a link. However, you can drag FC or GE port pairs into a link. TraceControl assigns newly added SAS/SATA ports to new or existing link according to a formula, as described in the note on page 35.

Add links by right-clicking the chassis and choosing **Add Link**. Ports can be added to a link by dragging the ports on a blade to the link on that blade, from the **New Domain** area. Links can be renamed by right-clicking on the link and selecting **Rename Link**.



Important: It is not required to create wide links (more than one port-pair in a link) unless you need to aggregate ports into a single address, such as for wide-port SAS.

Other context menu options are available for link manipulation in the **New Domain** area.

Create one link per blade
Select a chassis with SAS ports from the New Domain area, and right click this option. Ports from the same blade that span more than one link are moved to occupy a single link

To move a port-pair on a blade to a different link, drag-and-drop the SAS port-pair to the desired link.

Create one link with all ports
This option is available when the FC or GE ports in the same chassis are similar to each other, for example, they are all 1G GE.

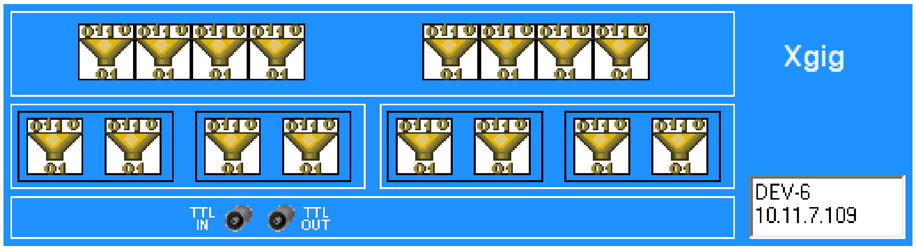
Port Viewing and Selection

The dialog box displays an icon for each port, arranged as they physically exist within the Xgig chassis. To select a port, click the port. Ports are always selected in pairs, so the port and remaining port of the port-pair are selected. Click ports again to remove them from the domain.

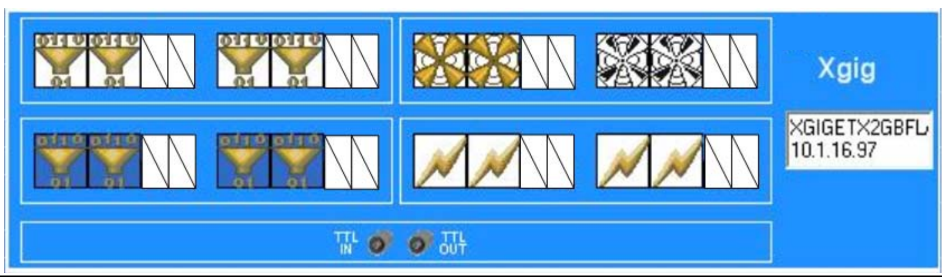
Selected ports have a blue background; unselected ports have a white background. Note that you must also have the appropriate license purchased to use a port for a specific protocol. See “Licensing for Xgig Multi-Function Blades” on page 44.

The icons change as the selection, availability, and type of each port changes. Ports are shown individually but have the same status for each port in a port-pair. See “Chassis, Blade, Port, and TTL Selection” on page 40 for information on the display of port icons.

Ports for the Xgig 3 and 6 Gigabit SAS/SATA Wide-Port/4x blades and the Xgig5000 12G SAS blade display somewhat differently. Ports are grouped into two banks of four. The first port in the left bank is logically associated with the first port in the right bank to form a port-pair. Port-pairs on the blade can be selected individually as narrow links or together as part of a wide link.



Note: The 6 Gigabit SAS/SATA Multi-Function System (Xgig-LXP) and the 6 Gigabit SAS/SATA Multi-Function blade each have four ports although eight ports are shown in the chassis view as in the Wide-Port 4x blades, and the port pairs are arranged in the same pattern as the Wide-Port 4x blades. The four non-operational ports are displayed as blank with a diagonal line through them as shown below.



40G ports are made from eight 10G ports merged into 40G functionality and displayed as two ports.

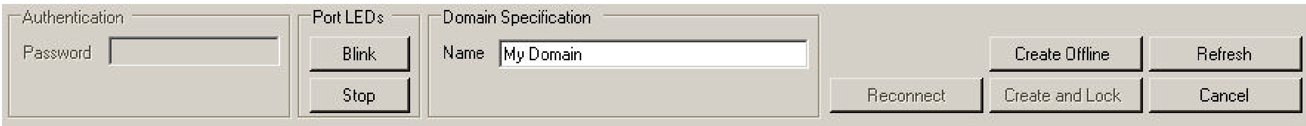
When you select a wide-port/4x blade or any combination of ports in a wide blade, all of the selected ports are put into a wide link. Click the wide-port/4x blade to add all ports in the blade as a wide-port link to the domain.

When you click the chassis to select all of the ports, ports in each wide-port/4x blade are placed into a single, separate wide-port/4x link. If there are other SAS ports in the selected chassis, these ports will be placed into another single wide link.

Note: The ports in the **New Domain** area are synchronized to the port selection in the **Port Viewing and Selection** area. Make sure you have selected all ports in the **Port Viewing and Selection** area before customizing links, as the links return to the default configuration when you modify the port selection. Every time the port selection changes in the **Port Viewing and Selection** area, the **New Domain** tree gets re-populated with chassis, links, and ports, and the links are recreated using a default algorithm.

The algorithm for creating the default configuration for links is as follows:
1.SAS/SATA, FC, and GE ports are grouped together consecutively into links of up to 8 ports.
2.Within each domain, links are named consecutively **Link - 1**, **Link - 2**, etc.
3.SAS links are named **SAS Link - 1**, **SAS Link - 2**, etc.

Dialog Buttons and Naming a Domain



If you are not logged into the Sync Group that contains the resources in the domain, use the **Password** field to login. Login is only required if the Sync Group is password protected. When you create a domain, the domain is given a default name based on the first port in the domain. Provide a unique name by typing in the name in the **Name** field.

Important: It is good practice to use a name other than the default for a domain, especially in a network environment where many users may access the Xgig chassis. A user-defined name will allow you and other users to quickly identify domains. This can be critical to protecting captures when running TraceControl in disconnected mode. See "Persistent Domains (Running Disconnected)" on page 49 for more information on running captures disconnected from TraceControl.

The following buttons are available:

- **Blink**
  Causes the LEDs for the selected ports to blink. LEDs will blink for forty seconds or until the stop button is hit.
- **Stop**
  Causes the LEDs to stop blinking.
- **Reconnect**
  Reconnects TraceControl to the blade hardware and brings up the TraceControl main window to display a status of all ports for the current domain.
- **Refresh**
  Updates the status of blades and ports in the right panel and available hosts in the left panel.
- **Create Offline**
  Establish the new domain without locking the ports for use. This allows you to create a new domain, even if the ports included in the domain are locked by another user.
- **Create and Lock**
  Exit and establish the new domain, applying a lock to all port-pairs selected for the domain.
- **Cancel**
  Exit without establishing the new domain.

Controlling the Chassis using a USB Connection

As a alternative to controlling the chassis using an Ethernet connection, Xgig Analyzer supports controlling the chassis by connecting the computer to a chassis using a USB cable.

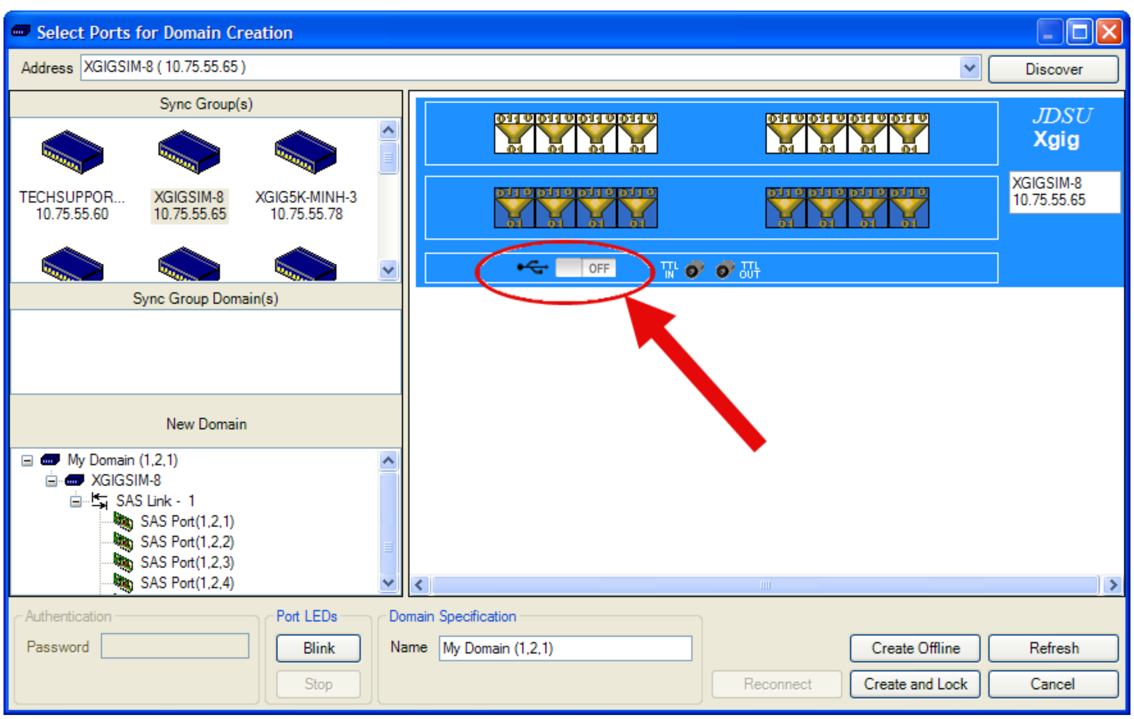
Note: This feature is currently only supported for use by the Xgig Analyzer software. Xgig Maestro software products do not currently support this feature.

Note: To control the chassis using a USB connection, you must upgrade the chassis software to the most recent software version. Refer to "Chassis Software Upgrade" on page 52 for instructions on upgrading the software.

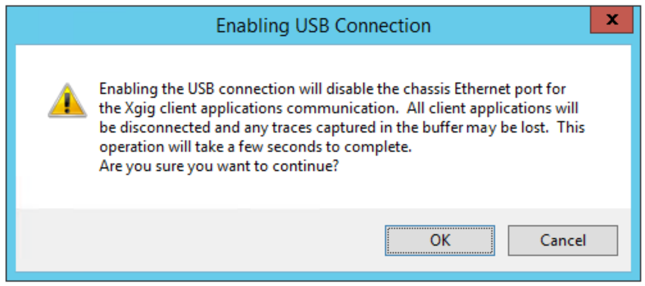
Using a USB cable (Type A to Type B connectors), connect the host computer to the Xgig chassis front panel USB connector. Attach the cable's Type A connector to the computer; attach the cable's Type B connector to the chassis.

With Xgig Analyzer started and a USB cable connected from the computer running Xgig Analyzer to the chassis, once the Analyzer client detects a chassis connect to the USB port, a switch is displayed in the Select Ports for Domain Creation window as shown in Figure 11. Select this switch to turn the USB connection on.

Figure 11: USB Switch in the Select Ports for Domain Creation Window



When the switch is selected to turn the USB connection on or off, a Sync Discovery on the chassis is triggered destroying all the domains and restarting all the server applications. An information box is displayed advising you that the current chassis port will be disabled, all client applications will be disconnected, and any traces captured in the chassis buffer will be lost. You must select the **OK** button to complete the control port change.

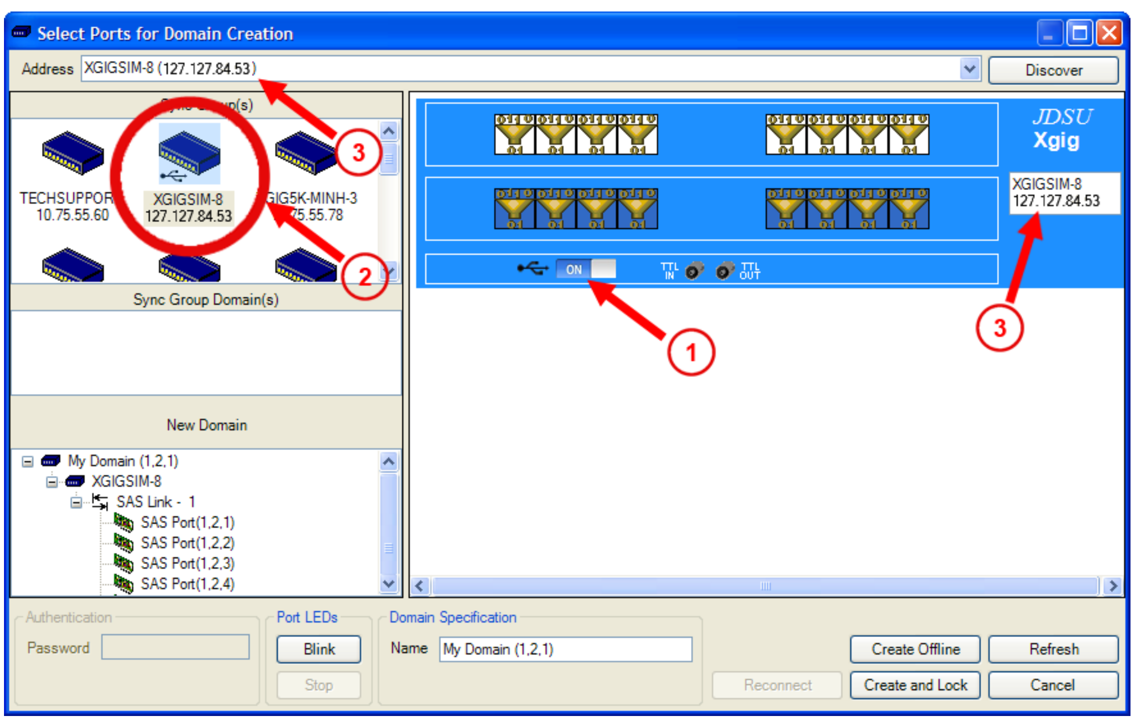


If ports on the chassis are locked by another application, a message will be displayed asking to unlock all ports before changing the USB mode.

Refer to Figure 12 to see that once the switch is on (1) and the USB connection has been established with the chassis, the connected device icon in the Sync Group(s) pane of the Select Ports for Domain Creation window changes to reflect that it is connected with the USB. Note the icon now displays the USB symbol (2).

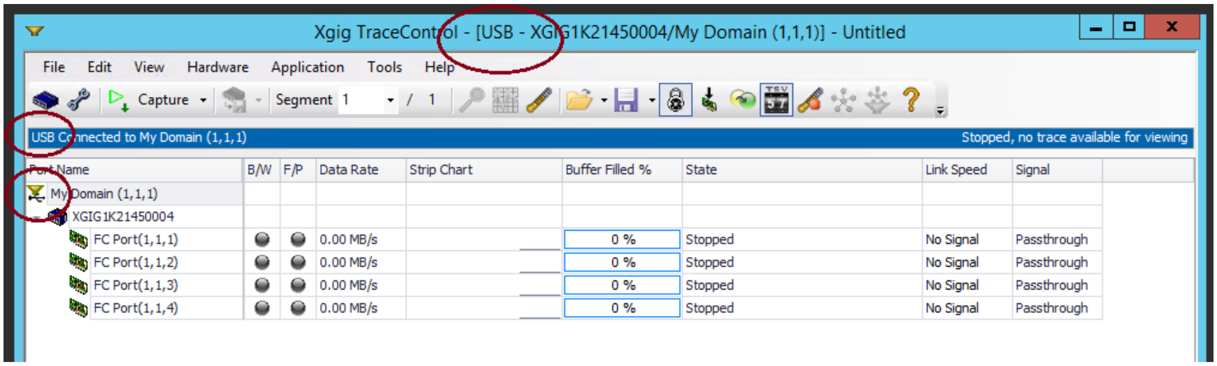
Also, previously, the label for the icon displayed the IP address, however, it now displays a number starting with “127.127.” to show that it is a USB identifier (2). This number is also shown in the address bar and in the pane with the USB switch (3).

Figure 12: Select Ports for Domain Creation Window with USB Connected



The TraceControl window also displays indications that the chassis is connected via USB as shown in Figure 13.

Figure 13: TraceControl Window with USB Connected

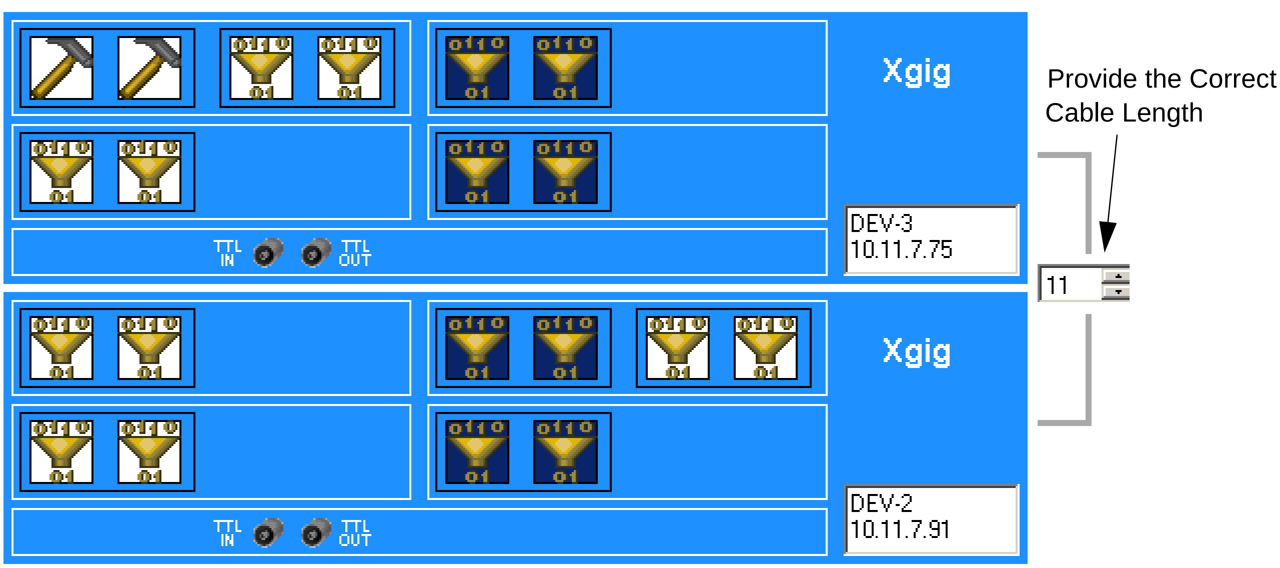


You can click the **Connect** button to reconnect in USB mode as well. If the chassis is no longer in the USB mode, it will try to set it after warning you if there are captures still in the buffer. Note that if the USB cable is disconnected or the client computer is shutdown, the chassis will go back into Ethernet mode.

Because the Xgig Web Utility is not supported over USB, you need to use the Xgig remote administrator. Refer to your chassis hardware guide.

Setting Cable Lengths for Interconnected Chassis

You can specify the length of the sync cable(s) between chassis if you are required to use sync cables other than the ones provided with a chassis. Chassis can only sync using straight through RJ-45 cables and the Cascade In and Out ports on the Xgig chassis. The minimum value is 1 foot and the maximum value is 100 feet. If authentication is enabled, you must provide the Xgig password prior to setting the cable length. Providing the proper sync cable length(s) is essential to ensure that the captures are properly time-aligned.



Chassis, Blade, Port, and TTL Selection

The dialog box displays an icon for each port, arranged as they physically exist within the chassis. The icons change as the selection, availability, and type of each port changes. Ports are shown individually but have the same status for each port in a port-pair. You can also select **TTL In** and **TTL Out** to set actions for external triggering.

Port, Blade, and Chassis Description

When you pass the cursor over a port, blade, or chassis, a “tool tip” displays information about the port, blade or chassis. Also, if you right-click any port or blade, a **Port Description** or **Blade Description** button appears, and when you right-click a chassis, a **Chassis Description** context menu item appears. Clicking this button or menu option opens a dialog box containing all the information about that port, blade, or chassis.

Port Types

- **Analyzer Port** 
  Indicates that the port-pair is configured to operate as a Fibre Channel Analyzer, Gigabit Ethernet Analyzer, SAS/SATA, or PCIe Analyzer port. Right-click or pass the mouse over the port to see if the port is for Fibre Channel, Gigabit Ethernet, SAS/SATA, or PCIe.
- **Jammer Port** 
  Indicates that the port is configured to operate as a Jammer port. Jammer ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a Fibre Channel, Gigabit Ethernet, or SAS/SATA Analyzer port.
- **BERT Port** 
  Indicates that the port is configured to operate as a BERT port. BERT ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a Fibre Channel or Gigabit Ethernet Analyzer port.
- **Generator Port** 
  Indicates that the port is configured to operate as a Generator port. Generator ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a SAS/SATA Analyzer port.
- **Target Emulator Port** 
  Indicates that the port is configured to operate as a Target Emulator port. Target Emulator ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a SAS/SATA Analyzer port.
- **Load Tester Port** 
  Indicates that the port is configured to operate as a Load Tester port. Load Tester ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a Fibre Channel or Gigabit Ethernet Analyzer port.
- **Delay Emulator Port** 
  Indicates that the port is configured to operate as a Delay Emulator port. Delay Emulator ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a Gigabit Ethernet Analyzer port.

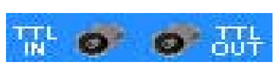
- **Unknown Port**
  Indicates that the floating Jammer license dongle has been removed, and the Jammers have been terminated. In this case, the port icons turn white to indicate that the ports have changed to an unknown state. From this state, the ports can be configured to operate as any other licensed function.

Port Selection and Other Indicators

- **Selected** (port icon background is Blue) 
  Indicates the port is selected as part of the domain. You can select a port that is locked or has triggered and assign it to a domain. However, you may not be able to lock the port or start a capture if the port is locked by another user.
- **Unselected and Unlocked** (port icon background is White) 
  Indicates the port is not selected as part of the domain and is not locked by another user.
- **Locked** (lock appears in the port icon) 
  Another user or another instance of TraceControl owns the port-pair. The port-pair is unavailable for capture.
- **Port Triggered** 
  Indicates that data received on this port has triggered the ports of the domain.
- **Port Locked and Triggered** 
  Indicates that data received on this port has triggered the ports in another user's domain. The port is locked by another user.
- **License Missing** 
  Indicates that the license key for this port is invalid or missing. The port is not usable until a proper license key is entered. The licensing for different functions is entered using the Xgig Web Utility. See "Licensing for Xgig Multi-Function Blades" on page 44 for more information.

Xgig Port Selection by Chassis or Blade

Ports are displayed within blades, and blades are displayed within chassis. Port-pairs are the unit that is added to the domain selection. As a shortcut for all Xgig chassis, you can select a chassis and add all its ports to the domain by clicking on the logo above the chassis name. You can also click the blade area surrounding ports to add all the ports in the blade to the domain.

Select TTL In or TTL Out 

Each chassis in the Port display has a **TTL IN** and a **TTL OUT** port, representing the TTL In and TTL Out ports on the chassis. A physical connection to pass trigger information between two systems must be established using a BNC cable for Xgig or an MCX cable for Xgig5000 and Xgig1000 to use this feature. To use the chassis as the sending device, you must connect the TTL Output port of the chassis sending the external trigger to the receiving device. To use the chassis as the receiving device, you must connect the TTL Input port of the chassis receiving the external pulse to the external sending device.

Caution: Improper connection of BNC or MCX input and output cables can cause serious damage to the system. Please double-check to make sure that the TTL Input port and/or TTL Output port of a chassis are properly connected to other Viavi devices or blades.

Select TTL Out

Select the TTL OUT icon for the chassis sending the trigger. If the cabling is correct as described above, the selected chassis will send the pulse when the trigger condition is met for the current domain. At least one port-pair of the current domain must be on the chassis cabled to send the external TTL pulse. Check the TTL Out check box inside the overview pane of the **Capture and Trigger Setup** tab to activate TTL Out.

Select TTL In

Select the TTL IN icon for the chassis receiving the trigger. You can set the action to occur in the **Capture and Trigger Setup** tab in the **Configuration Editor** window. At least one port-pair of the current domain must be on the chassis cabled to receive the external TTL pulse. For TTL IN, the configuration for all the ports in the domain are re-initialized to stop capture after trigger. Check the TTL In checkbox in the overview pane of the **Capture and Trigger Setup** tab to activate TTL IN.

Important: Selection of the chassis to send/receive a TTL pulse is a function of the proper connection of the BNC cables for Xgig or MCX cables for Xgig5000 or Xgig1000 as well as selection of the TTL OUT or TTL IN port in the TraceControl software. For domains that span multiple chassis, a trigger condition for ANY of the ports in the domain will cause the TTL pulse to be sent, as long as one of the port-pairs of the domain exists on the chassis that is cabled to send the pulse. For domains that span multiple chassis, an incoming external pulse will stop ALL of the ports in the domain, as long as one of the port-pairs of the domain exists on the chassis that is receiving the pulse.

Changing Port Functions

For Xgig Multi-Function Blades, except the 6G SAS/SATA blade and the 10G blade, you can change the function of a port on the blade if you have a license for multiple functions. The following functions are currently supported:

- Fibre Channel Analyzer
- Gigabit Ethernet Analyzer
- SAS/SATA Analyzer
- PCIe Analyzer
- Fibre Channel Jammer
- Gigabit Ethernet Jammer
- SAS/SATA Jammer
- Fibre Channel BERT
- Gigabit Ethernet BERT
- SAS/SATA Generator
- SAS/SATA Target Emulator
- Fibre Channel Load Tester
- FCoE Load Tester

- Gigabit Ethernet Delay Emulator

The 3G and 6G Xgig SAS/SATA blade supports SAS/SATA Analyzer and Jammer. The 6G Xgig SAS/SATA blade also supports SAS/SATA Generator and Target Emulator functionality. The 8G Fibre Channel blade only supports Fibre Channel Analyzer, BERT, Load Tester, and Jammer functions. The 10G blade only supports Fibre Channel Analyzer, Gigabit Ethernet Analyzer, 10GigE Load Tester, and 10GigE Jammer.

The following are supported on the Xgig5000:

- The 10G IO blade supports Ethernet Analyzer and Load Tester functions.
- The 12G SAS blade supports SAS/SATA Analyzer, Jammer, and Generator functions.
- The 16G FC blade supports FC Analyzer, Jammer, and Load Tester functions.

The Xgig1000 12G SAS blade supports SAS/SATA Analyzer, Jammer, and Generator functions.

The Xgig1000 4 Port and 8 Port 10G/16G systems support the Analyzer, Jammer, and Load Tester functions at 10.3125 Gbps in the 10 Gigabit Ethernet protocol. Analyzer and Load Tester are supported in Analog Passthrough and Digital Retime. Jammer is supported in Digital Retime only. These systems also support the Analyzer, Jammer, and Load Tester functions at 4.2500, 8.5000, or 14.0250 Gbps in the Fibre Channel protocol.

The Xgig1000 8+2 Port 10G/16G/40G system’s eight SFP ports support the Analyzer, Jammer, and Load Tester functions at 10.3125 Gbps in the 10 Gigabit Ethernet protocol. Analyzer and Load Tester are supported in Analog Passthrough and Digital Retime. Jammer is supported in Digital Retime only. The SFP ports also support the Analyzer, Jammer, and Load Tester functions at 4.2500, 8.5000, or 14.0250 Gbps in the Fibre Channel protocol in Analog Passthrough or Digital Retime. The two QSFP ports support the Analyzer function at 41.2500 Gbps in the 10 Gigabit Ethernet protocol in Analyzer Passthrough only.

The Xgig1000 2 Port 10G/40G system’s two QSFP ports support the Analyzer function at 41.2500 Gbps in the 10 Gigabit Ethernet protocol in Analyzer Passthrough only. The two QSFP ports can be used as eight SFP ports at 10.3125 Gbps by using two one-to-four break out cables (one for each QSFP port) with male QSFP and female SFP connectors. See the *Xgig1000 Hardware Guide* for more information.

The Xgig1000 PCIe system has two CXP ports (16 lanes), which support the Analyzer function at 2.5, 5.0, and 8.0 GT/s in the PCIe protocol in Analog Passthrough only. This system supports a trace buffer of 32GB upstream and 32GB downstream per port.

From TraceControl, only Analyzer functions can be used. In the display, ports that have a Jammer, BERT, Generator, Target Emulator, Delay Emulator, or Load Tester function will display, but will not be available for use. Xgig ports with another function can be changed to an Analyzer function if the port is not locked by another user and the blade has the proper license.

To change a port function:

1 Select the port you want to change by right-clicking it.

2 From the **Use Port(s) as...** menu, select the function type you want. If only one function type is available for this port, only one type will be shown.

3 The list will contain only those functions that have been licensed for the port.

Caution: The change in function does not complete until you create and lock ports in a domain.

Note: When selecting a port function for two ports on an FPGA in an Xgig1000 10G/16G or 10G/16G/40G system, a dialog will appear asking you to choose port functions for the other two ports on the FPGA as all four ports for an FPGA are loaded at once. The dialog box only appears when there are two or more port functions licensed for a particular port. You may choose from one of the following: Ports 1,2 as Jammer Fibre Channel with Ports 3,4 as Analyzer Fibre Channel; Ports 1,2 as Jammer Ethernet with Ports 3,4 as Analyzer Ethernet; or Ports 1,2 as Analyzer Ethernet with Ports 3,4 as Analyzer Fibre Channel.

You may check the **Do not prompt again** check box, and the software will remember your last selection. When this check box is checked, a **Prompt For Unused Port Functions** option will be present in the port context menu.

Licensing for Xgig Multi-Function Blades

The licensing for different functions is set up using the Xgig Web Utility. From TraceControl, you can only change the function of a port if the blade and port-pair has a license for multiple functions. If a blade or port-pair does not have the ability or the license to change functions, the options and menus in TraceControl described above will not be available.

For all Xgig, Xgig5000, and Xgig1000 blades, there is a blade license key and, if required, a license key for each port-pair. The port-pair license key allows specific functions for each port-pair. The port-pair license is only assigned if port-pairs within the blade are licensed for different functions. If all port-pairs on the blade have the same functions, only the blade license key is assigned and used.

The proper licenses are assigned and stored on the blade using the Xgig Web Utility. If the blade is moved to a different chassis, its blade and port-pair licenses, and therefore its ability to change functions, remains the same. In other words, the licenses “follow” the blade and are not associated with the chassis.

Default Port and Domain Labels

Default names are provided for both ports and domains. For ports and domains, the default name includes a unique port designation in the form (X,Y,Z). The meaning of **X**, **Y**, and **Z** are defined below.

X For all Xgig systems, Chassis Number

Y For all Xgig systems, Blade Number

Z For all Xgig blades, Port Number within the blade

Domain Names

Domains are given default labels in the format My Domain(X,Y,Z). The chassis/blade/port designation will be the first port in the domain configuration. This provides a unique ID for the domain. It is suggested that domains be renamed by the user.

You can rename a domain by double-clicking on the domain name or by selecting **Rename Domain** from the **Edit** menu.

Domain Name Examples:

My Domain(1,1,1)	Default name assigned to a new domain whose first port is Chassis 1, Blade 1, Port 1
John's Test	Renamed domain

Port Names

Ports are given labels in the format AA Port(X,Y,Z) where AA is function of the blade (for example, FC for Fibre Channel). The function indicator and the chassis/blade/port indicator cannot be modified.

You can rename a port by double-clicking on the port name or by selecting **Rename Port** from the **Edit** menu. To return a port name to the default, right-click the port name and select **Set Default Port Name**.

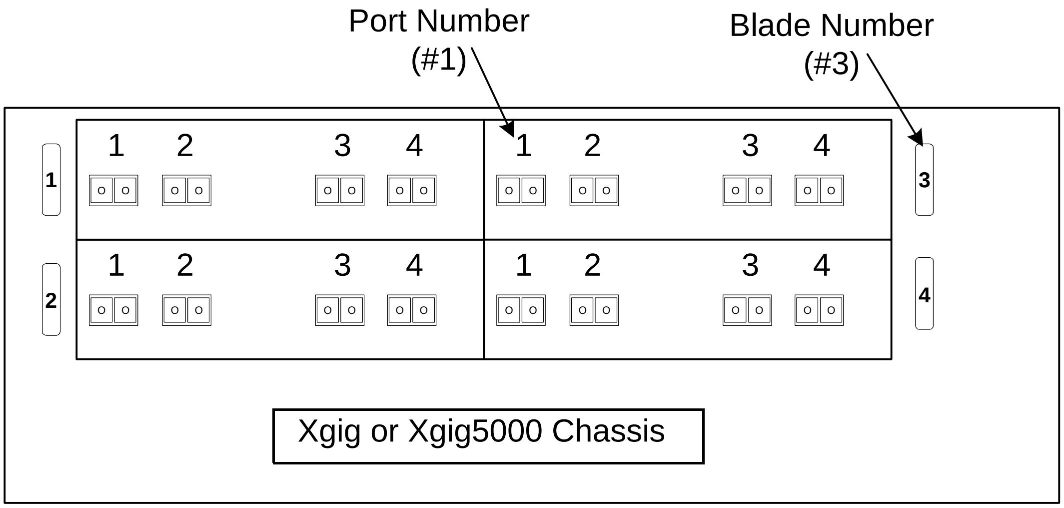
Xgig Port Name Examples:

FC Port(1,3,4)	Fibre Channel; Port 4 on Blade 3 in Chassis 1
GE Port(3,2,2)	Gigabit Ethernet; Port 2 on Blade 2 in Chassis 3
FC Port(1,3,2)	Fibre Channel; Port 2 on Blade 3 (single chassis)
GE Tims(2,1,1)	Gigabit Ethernet; Port 1 on Blade 1 in Chassis 2 renamed “Tims”

Xgig Blade and Port Numbering

The diagram below shows how blades and ports are numbered for the chassis. Blades are numbered by physical slot number in the chassis. For example, if no blade exists in slots 1 or 2, the blade in slot 3 is still numbered as blade 3.

Figure 14: Xgig Analyzer Blade Port Numbers

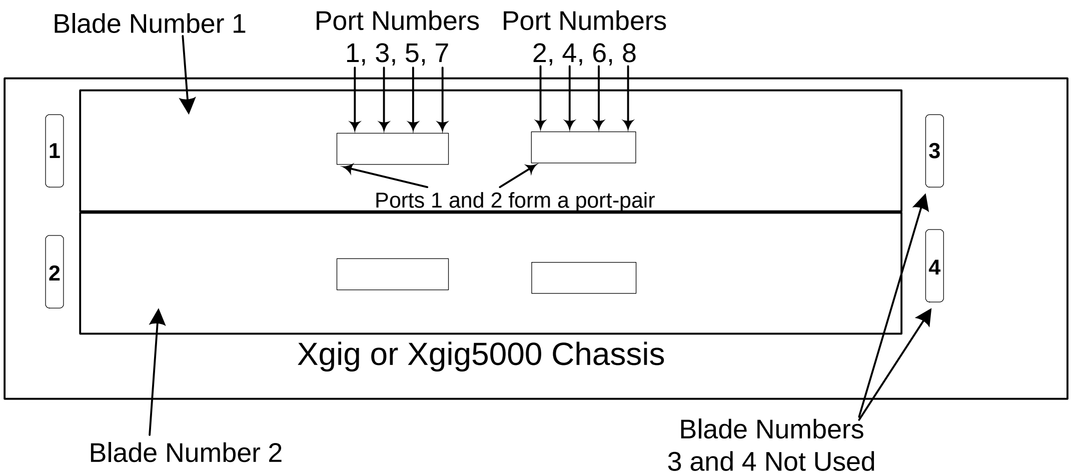


The Xgig 3/6 Gigabit SAS/SATA Wide-Port/4x blade and the Xgig5000 and Xgig1000 12G SAS blades use the same numbering scheme to identify chassis, blade, and port – for example, (1,1,3). The blade occupies two slots; a blade in the upper two slots is numbered as blade 1, and a blade in the lower two slots is numbered as blade 2. Blade numbers 3 and 4 are not used.

For the Xgig 3/6 Gigabit SAS/SATA Wide-Port/4x blade and the Xgig5000 and Xgig1000 12G SAS blades there are only two physical ports on the blade, and the two ports together compose a 4x wide link. You can only see individual port numbers within the wide link (numbered 1 through 8) through Xgig software; a single physical port on the blade has no direct correspondence to the single logical port number. In the Domain Creation dialog, the first port in the left bank is logically associated with the first port in the right bank to form a port-pair. For example, port number one in the left connector is paired with port number two in the right connector to form a port pair.

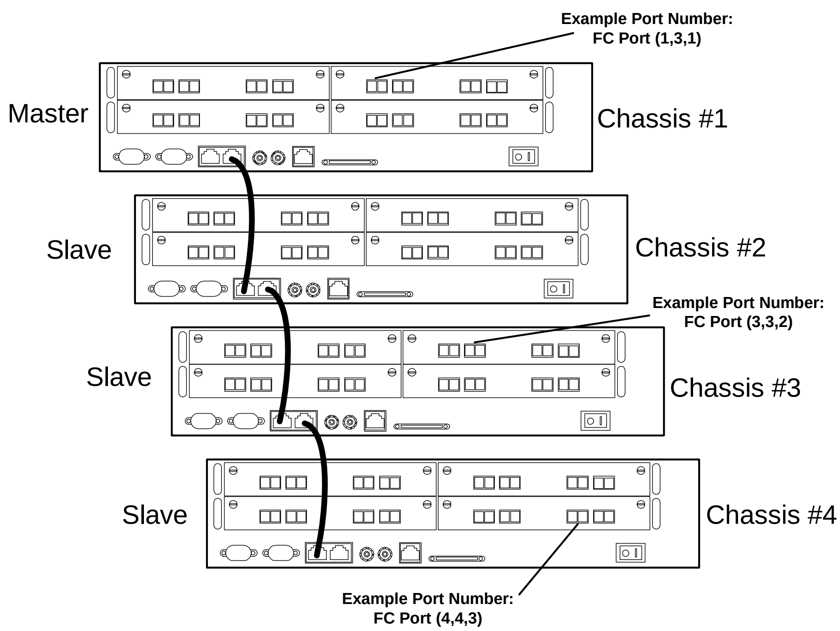
When you use the eight ports on a 10G blade as 40G ports, only two ports are shown. These ports are numbered 1 and 2.

Figure 15: Xgig Analyzer Blade Port Numbers, Wide-Port/4x Blade



Chassis are numbered consecutively as they are cabled in the cascade, beginning with the master as number one. Figure 16 shows how chassis are numbered.

Figure 16: Xgig Chassis Numbering



Creating a New Domain

A new domain establishes a set of ports for capturing traces. Domains must exist in the same Sync Group. If you require another domain, you can launch another instance of TraceControl and create a domain in that instance.

To create a new domain:

1 Click the **Create Domain**  button or select **Create Domain...** from the **Hardware** menu.

2 Select a Sync Group from the area on the top left. If a remote chassis is not listed and on another subnet, enter the name (if a DNS server is present) or IP address of the chassis in the IP Address field and press **Discover**. Once the remote chassis appears in the **Sync Group(s)** area, select it.

3 In the window showing all ports/blades/chassis for the Sync Group, click all ports you want for the domain. All ports added will display in the New Domain area. The New Domain area shows the domain as a hierarchical structure, showing all chassis, all links, and all ports that comprise the domain.

   If you use any Xgig chassis in a multi-user environment where some users may have active domains that are disconnected, check the domains in the **Sync Group Domain(s)** area of the dialog. Select each domain and see if any of the ports are part of another domain. You can elect to use any ports in another domain that are not locked for use. However, these ports may contain data or be active as a disconnected domain.

4 Skip this step unless you need to create links that aggregate more than one port-pair.

   Create any links you want for the new domain. Select a chassis in the New Domain area, and right-click **Add Link**. After the new link is created, drag-and-drop all ports onto the link name. Ports will now appear as a subset of the link in the New Domain area display. Duplicate link names are not allowed, and the maximum length of a link name is 64 characters.

5 Enter the name of the new domain in the **Name** field at the bottom of the window. A default name is supplied.

6 Click **Create and Lock** to connect the domain and load the configuration settings to the hardware. Click **Create Offline** to create the domain and not load the configuration settings or lock the ports in the domain.

Locking Ports for Use 

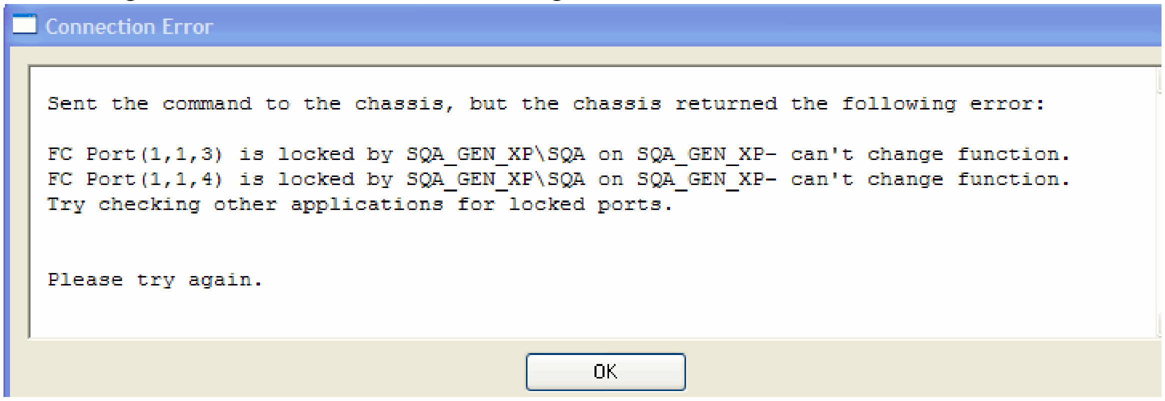
Locking all analyzer ports in a domain for exclusive use occurs when you start a capture, when you press the **Lock** button on the toolbar, when you apply hardware settings, or when you click the **Create and Lock** button in the **Select Ports for Domain Creation** window. If another user has started or locked any ports in the domain, you will not be able lock the ports and an error message will appear. The error message will let you know the exact ports that are in use. You can also select **Lock Ports** from the **Hardware** menu to lock ports.

You can start a capture for the current domain if all ports in the domain are not locked by other users. The start operation will automatically lock the ports for exclusive use.

When ports are locked, the lock icon in the TraceControl main window, shown above, appears depressed and “Connected to [domain name]” appear below the menu bar, for example, “Connected to My Domain (1,2,1)”. When the ports are not locked, the text “Not Connected to the Domain” appears below the menu bar.

If you try to lock or start a domain that contains ports that are already locked, you will receive an information message. This is also the way to get information about who is locking the ports you are trying to select.

Figure 17: Connection Error Message



Port Indicator LEDs

Hardware blades in remote chassis come with LEDs that can flash to identify each port on the blade. When you select specific ports in the **Select Ports for Domain Creation** dialog box, you can match these ports to the physical hardware ports. Use the Port LEDs **Blink** button in the dialog or select **Blink Chassis LEDs** from the **Hardware** menu to cause all the LEDs to flash for the port pairs you have selected in the dialog.

Persistent Domains (Running Disconnected)

Once created and applied to the hardware, a domain on a sync group (remote chassis) will continue to exist if you lose network connection, exit the TraceControl application, or connect to another domain with no ports in common. There are two primary reasons for persistent domains:

- You can continue (reconnect) with any capture or other activity being performed for a domain in the event that the network connection is lost between the client PC and Xgig Chassis.
- You can switch client systems and still be able to work with the same domain.

Although capture operations continue to run while disconnected from the TraceControl application, the ports in the domain are no longer locked for exclusive use. Another user can lock the ports and use them for another purpose. If your remote analyzer(s) are in a network environment with many users, it is recommended to run captures while connected, ensuring that you get the capture you want. You can also use the password capabilities to set up an Xgig chassis for your exclusive use to guarantee that captures continue to run when you disconnect from the chassis.

When running disconnected in a network environment, it is strongly suggested that you name domains clearly. This allows other users to see that domains have been created for ports, and may prevent them from being allocated for other purposes. Also, if other users lock the ports and use the same default domain name, you may not have the capture data you expect when you reconnect to the Xgig chassis.

When you reconnect to an unlocked existing domain on an Xgig Sync Group, any modifications to port configurations made prior to the reconnect will be discarded.

In the Port Status View, the software LEDs (B/W and F/P) only update while the ports are connected in TraceControl. If you disconnect and then reconnect to a domain, the port LEDs will be reset.

To disconnect and reconnect to a domain:

1 Create a domain of ports to use. Name the domain so that other users can clearly see that ports are for exclusive use. See “Creating a New Domain” on page 47 for information on creating domains.

2 Apply the domain to the hardware using the **Apply Hardware** button. If desired, press the **Start** button to start the capture. Note that domains can be disconnected and then reconnected in any state. You do not need to start a capture before disconnecting from a domain.

3 Disconnect from the domain by shutting down the TraceControl application or by selecting another domain within TraceControl that has no ports in common with the first domain.

4 You can reconnect to the domain from the same client PC or from another client PC running TraceControl.

   a If you are re-launching TraceControl from the same client PC, the last domain started should reappear in TraceControl. Reconnect by pressing the **Lock/Unlock Ports** button.

   b The **Start** button will also reconnect to the domain. However, reconnecting using the **Start** button will cause the analyzer to restart the data capture if the analyzer is already capturing. Any data currently within the ports of the domain will be overwritten. It is recommended to use the **Lock/Unlock Ports** button to reconnect, as this reconnects to the domain without performing any actions.

   c If you are reconnecting to the domain from within the same session of TraceControl, reconnect using the **Select Ports for Domain Creation** dialog box. Press the **Create Domain** button to bring up the dialog and select the name of the domain from the **Sync Group Domain(s)** list. Press the **Reconnect** button to reconnect to the domain.

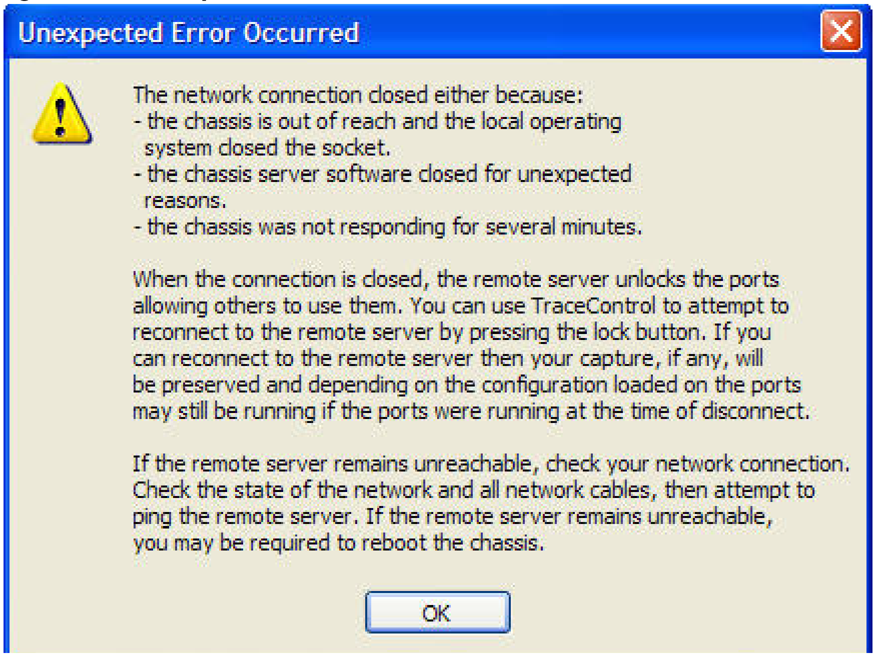
   d If you are reconnecting from a different client PC, launch TraceControl and reconnect using the **Select Ports for Domain Creation** dialog box. Press the **Create Domain** button to bring up the dialog and select the name of the domain from the **Sync Group Domain(s)** list. Press the **Reconnect** button to reconnect to the domain.

Network Connections

Remote analyzers do not require a persistent Ethernet LAN connection between the local Xgig Analyzer software and the remote hardware to operate properly. The remote analyzer will continue to run if you lose network connection or exit the TraceControl application.

If the network connection is lost, you will receive the following message.

Figure 18: Unexpected Error Occurred



You may receive this message when using Microsoft Windows operating systems if you do not have the power options set correctly. Make sure the power options for Windows are set to High Performance.

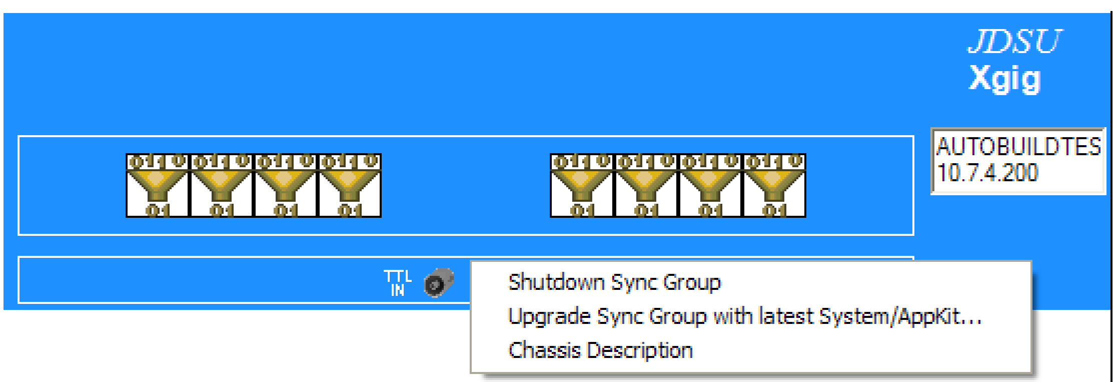
If you receive this message, ping the chassis to see if you get a response. If the ping is successful, try to reconnect to the ports in the domain. If unsuccessful, look for cabling problems at your local system and then within the network; make sure the chassis is physically connected to the network.

If you can ping the chassis but cannot lock the ports, and the ports are not locked by another user, as a last resort you may have to reboot the chassis. A reboot will result in loss of any capture data within any of the ports on the chassis.

Chassis Upgrade and Maintenance Options

Chassis software upgrade and chassis shut down are available from the Domain Creation Dialog of TraceControl. Right-click a chassis, and select the option from the context menu. You can also shut down a Sync Group and get a description of the chassis by using the context menu.

Figure 19: Chassis Context Menu from the TraceControl Domain Creation Dialog



Chassis Software Upgrade

If the selected chassis is compatible with the client, the **Domain Creation Dialog** will display the ports for the chassis and a context menu (see Figure 19) with an option for upgrading the chassis. Right-click a chassis and select **Upgrade Sync Group with latest System/Appkit...** from the context menu to start the software upgrade. If the chassis selected for upgrade is part of a Sync Group that includes multiple chassis, all chassis in the Sync Group will be upgraded.

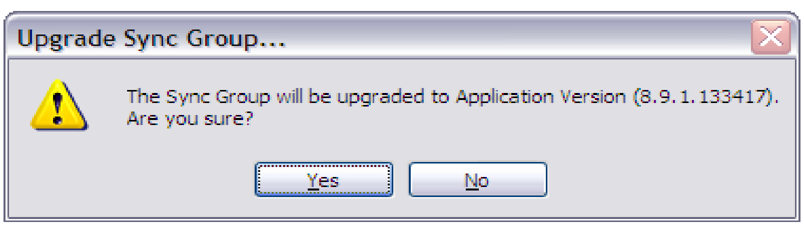
If you are an Administrator on a Microsoft Windows system with Windows Firewall enabled and you upgrade the chassis for the first time, the firewall will prompt you to unblock `ProbeUpgradeUtility.exe` and `SyncGroupUpgradeUtil.exe`. Click **Unblock** to add these 2 programs as firewall exceptions to allow the upgrade to happen. If you are a Standard User, you will need the Computer Administrator to unblock these 2 programs. Otherwise, the upgrade will fail after a timeout of 6 minutes.

For Microsoft Windows Server operating systems, Windows Firewall must be disabled for the upgrade to happen irrespective of whether you are an Administrator or a Standard User.

The upgrade process will set up a temporary FTP server and upload the correct system and application files to the chassis. The latest system and application files for the chassis were copied to your client during Xgig Analyzer client software installation and these files must be on your client PC for the upgrade to complete. During client software installation, these files were copied to the directory **\Chassis** within the Xgig Analyzer Client installation directory.

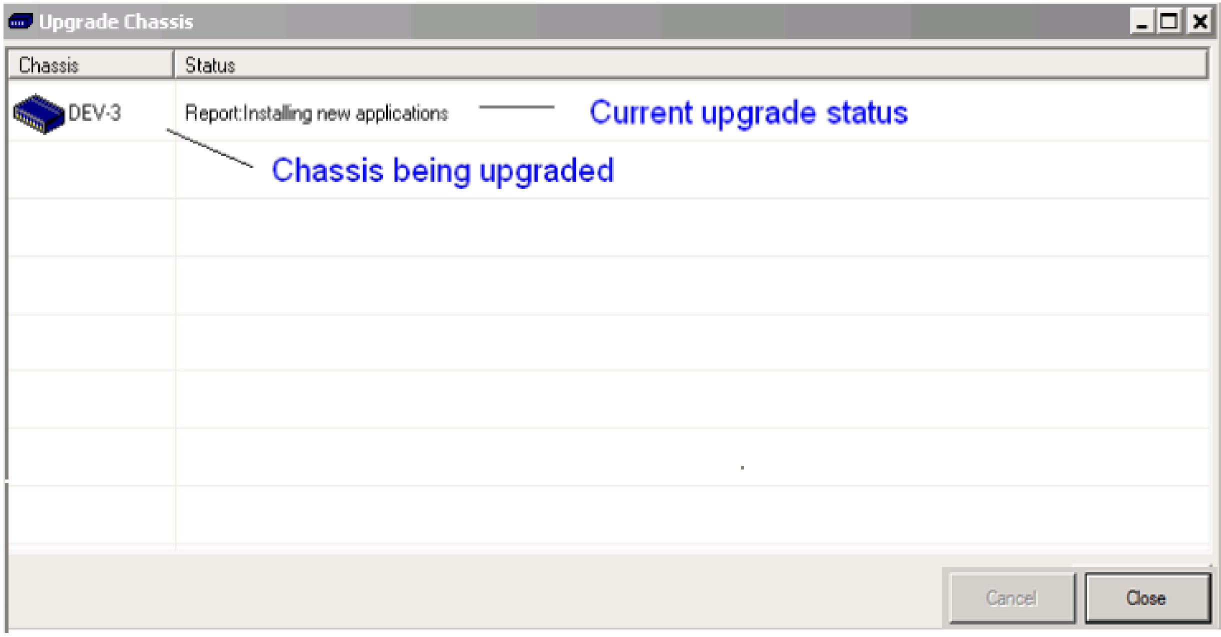
A confirmation message will appear showing the new version numbers before the upgrade starts. Note that the chassis application files can also be re-installed or downgraded if the files in the **\Chassis** directory are at the same or lower level than the currently installed files. The confirmation message will indicate if application files are being re-installed or downgraded.

Figure 20: Confirm Version Numbers Message for Upgrade



During upgrade, the **Upgrade Chassis** screen appears showing upgrade progress. The system resets itself during the upgrade process, so there is a time delay between when the Application Kit software is upgraded and when the System software is upgraded. The status of the upgrade process is shown in the **Upgrade Chassis** dialog box.

Figure 21: Upgrade Chassis Screen



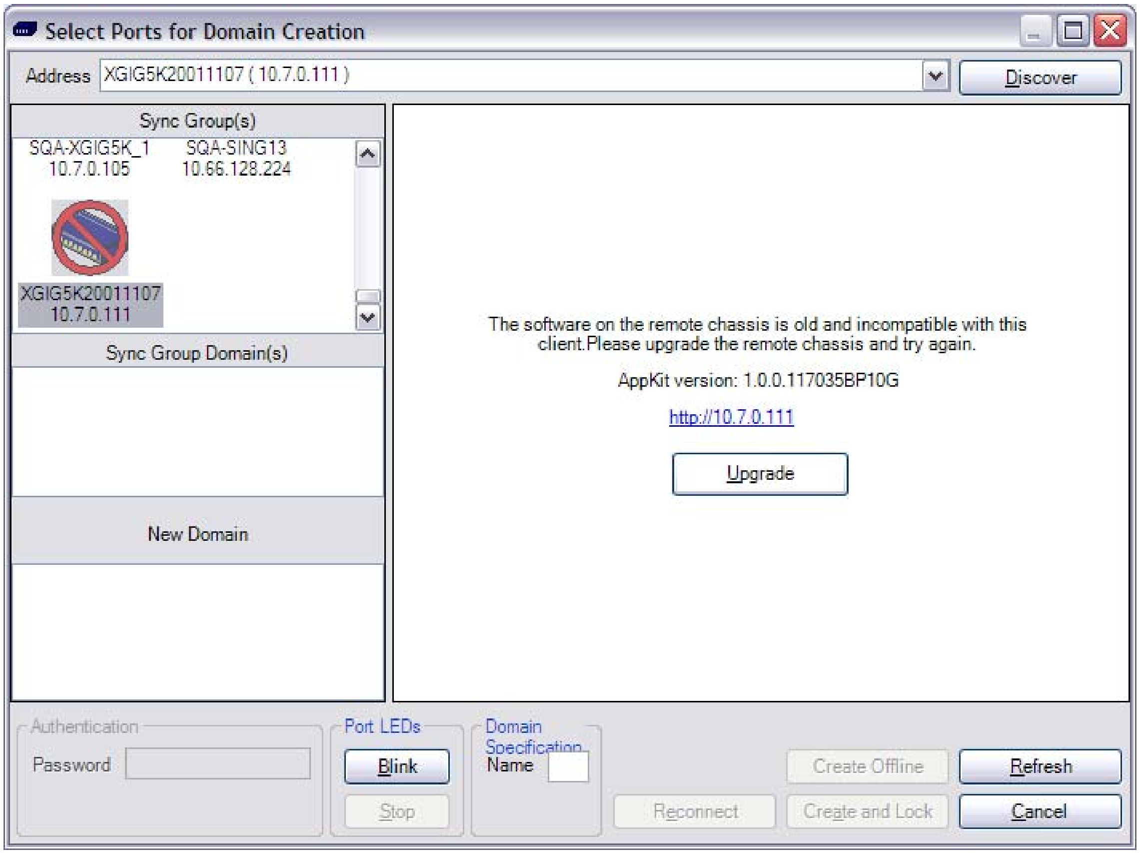
The upgrade process will take several minutes; it may take longer, depending on network performance and if you are updating multiple chassis in a Sync Group. If the upgrade process takes too long, you can click the **Cancel** button to cancel the process. A dialog will appear with a hyperlink to the chassis upgrade logs and another hyperlink to the `UpgradeLog-CHASSIS_IP_ADDRESS.txt` file. When all the chassis have downloaded their new files, the FTP server software is disabled and removed from the client. When the process is completed, click the **Refresh** or **Discover** button when the Sync Group is in an operational state.

Upgrading Chassis that are Not Compatible with the Client

If the chassis is incompatible with this version of TraceControl but you can upgrade using the application files on the client, the **Domain Creation Dialog** displays an incompatibility message, the Appkit version in the chassis (if it is recognized), a web link to the chassis, and an **Upgrade** button. Click the **Upgrade** button to upgrade the chassis software. Refer to the section above for details about the upgrade process from the client.

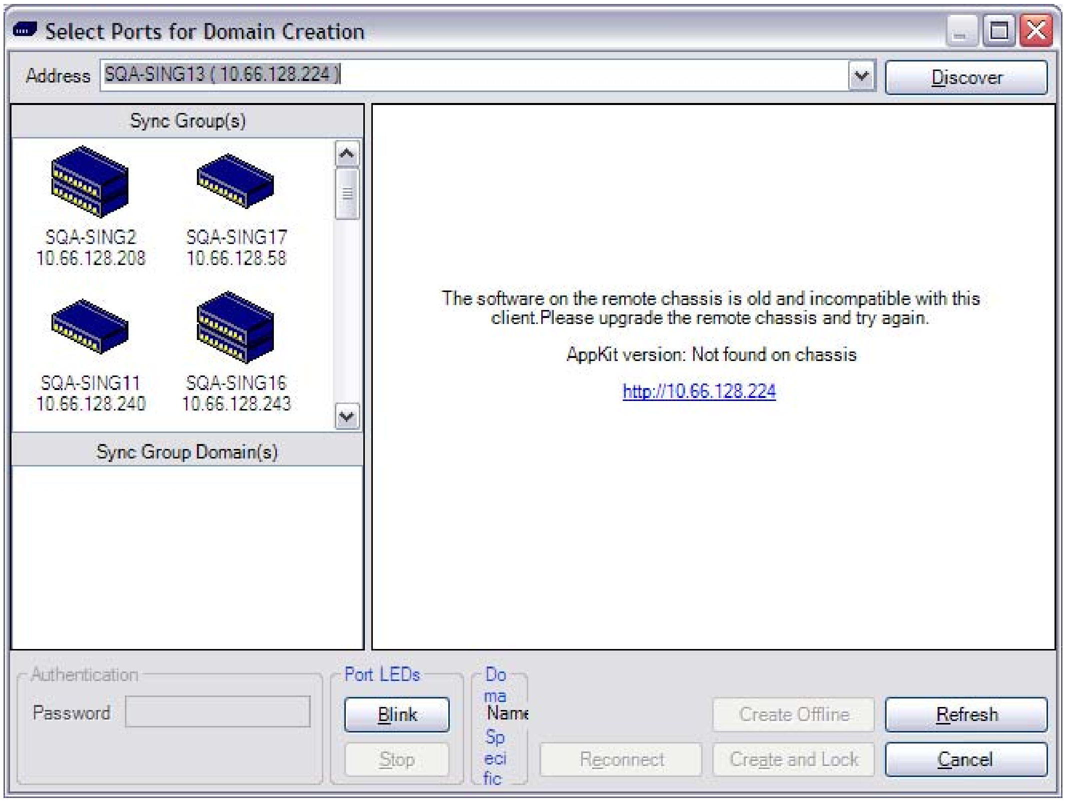
Note: Analyzer client version 6.0 breaks compatibility with Application Kits older than version 9.0 and vise versa.

Figure 22: Incompatible Chassis, Upgrade Supported from TraceControl



If upgrading a Sync Group that has Application Kit software version lower than 3.2, you cannot upgrade the chassis from TraceControl software. The **Domain Creation Dialog** does not display the port selection area for the chassis, but instead displays an incompatibility message and a web link to the chassis so you can use the Xgig Web Utility to perform the upgrade.

Figure 23: Incompatible Chassis, Upgrade Not Supported from TraceControl

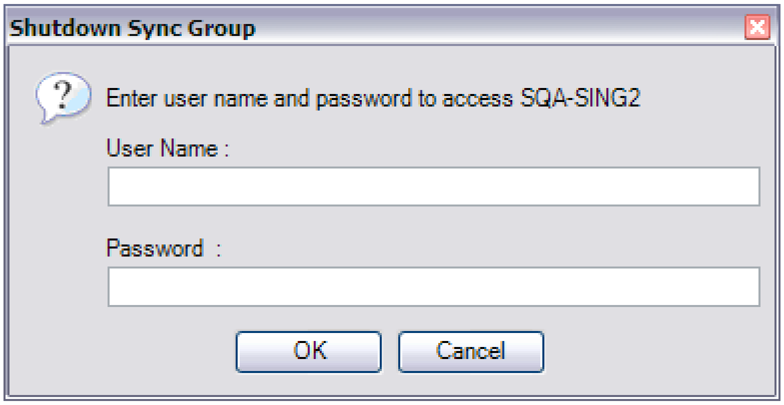


Chassis Shutdown

Shutting down of chassis can be carried out using TraceControl. This operation is performed for a Sync Group, so all chassis (master and all slave chassis) in the Sync Group will be shut down. The shutdown is required before removing power to the chassis for maintenance or other reasons.

Right-click any chassis in the **Domain Creation** dialog and use the context menu to select the **Shutdown Sync Group** option (see Figure 19). After clicking on the context menu, you are prompted for the chassis administrative user name and password. The user name and password entered in the shutdown prompt is applied to all chassis in the Sync Group. If there are chassis in the Sync Group that have user names and passwords that are different, you are prompted again for user name and password of those particular chassis. You need to enter the correct user name and password for all chassis in the Sync Group to complete the shutdown.

Figure 24: Chassis Shutdown, System Security Dialog

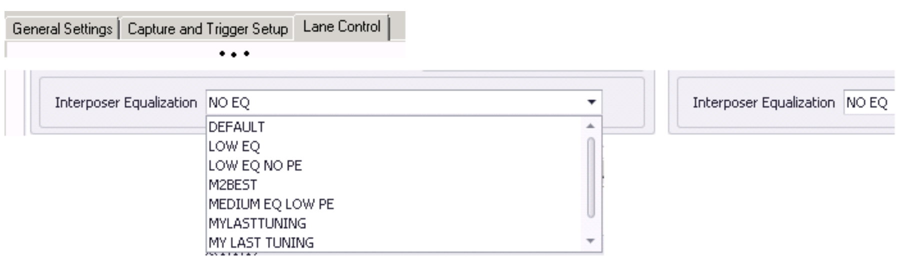


You must wait more than one minute before you can remove power from the chassis once the shut down message is sent from TraceControl to the chassis.

PCIe Tuning Wizard

TraceControl provides several Interposer Equalizations to suit different hosts and devices. When your host/device cannot reach the Gen3 speed, or when there are errors on the link, you can try each Interposer Equalization in the Lane Control panel to find the best one for your system. It is important to reboot the DUT every time you change any Interposer Equalization because the equalization affects both the thru path between the host and the target, and the tap path towards the Xgig Analyzer. Changing the equalization on the thru path changes the link characteristics and the Host/Device must be retrained in the Gen3 LTSSM Recovery Equalization phase, which happens during reboots.

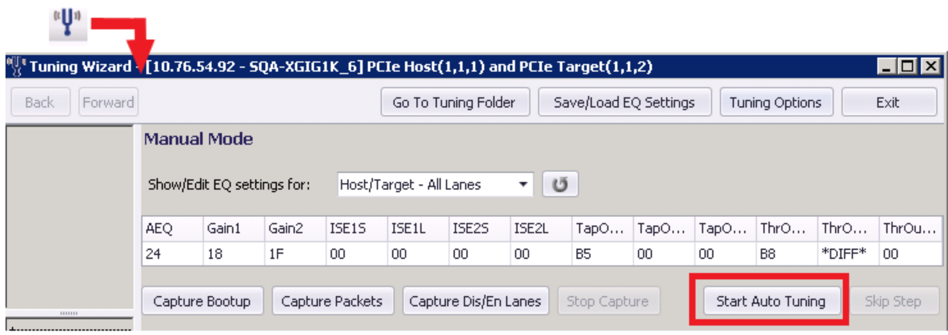
Figure 25: Interposer Equalization List



TraceControl has a Tuning Wizard which can find the best equalization from the list or beyond by trying additional settings. Once it finds good settings, you can save them to a new preset that will appear in Lane Control's Interposer Equalization list for a future use.

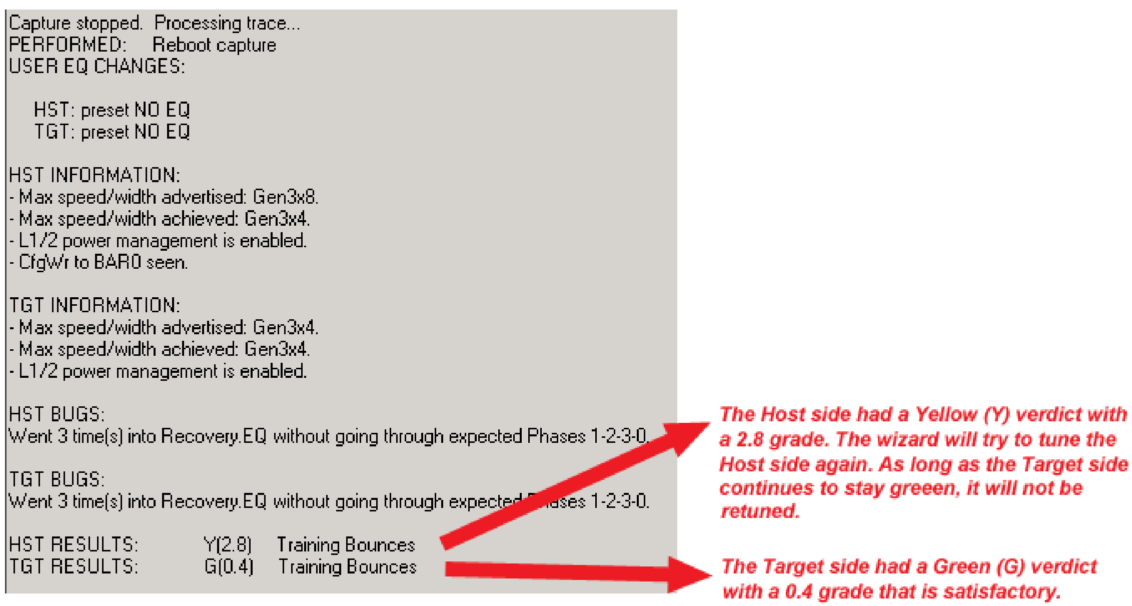
To launch the tuning wizard, click on TraceControl's Tuning Wizard toolbar button and then click **Start Auto Tuning**.

Figure 26: Launching the Tuning Wizard



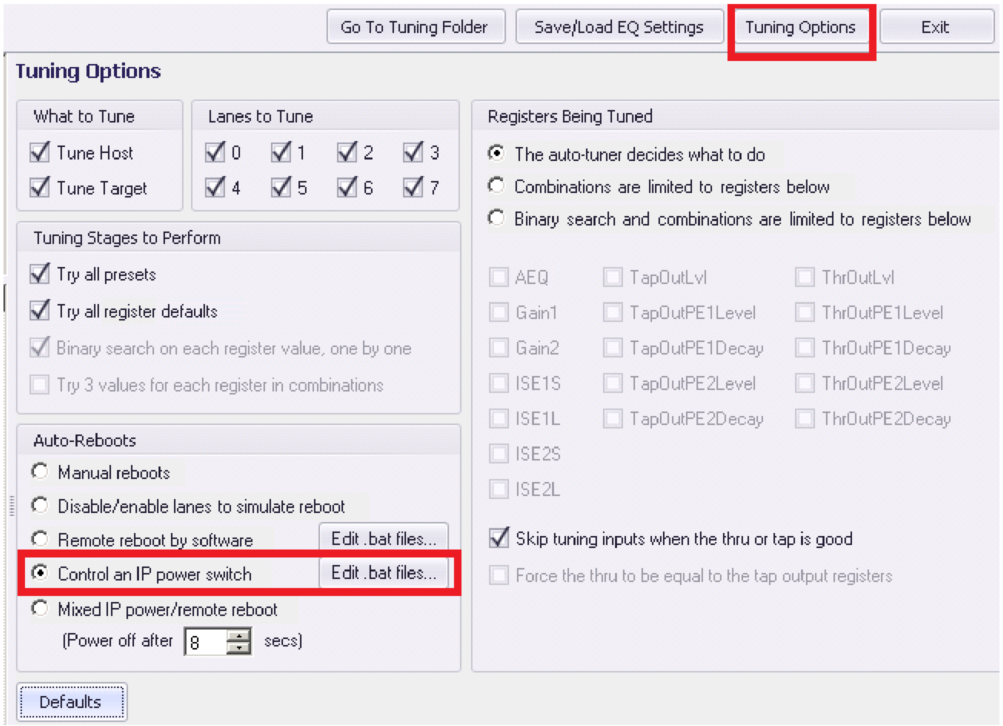
The wizard automatically tries different presets and settings and prompts you to reboot the DUT in the log at the bottom left corner of the wizard. Rebooting the DUT repeatedly is all you will have to do when using the wizard, and it will prompt you when needed in the log on the bottom left corner. TraceControl automatically captures and triggers on each boot-up. It stops the capture and processes the trace to determine if the link is good. During the tuning process, it reports useful information on the host/target, reports bugs, and produces an equalization verdict and grade for each side.

Figure 27: Tuning Report



Tuning a system may require from 10 to more than 500 DUT reboots, depending on how difficult the tuning is. For this reason, it is highly recommended that you automate the DUT reboots and run the wizard overnight. To do this, click the **Tuning Options** button and select one of the auto-reboot options.

Figure 28: Auto-Reboot Options Window



There are 4 options to automatically reboot a system:

Disable/enable lanes to simulate reboot - Instead of rebooting the DUT, this option switches off/on all the interposer lanes for one second. Some host computers detect the inadvertent Electrical Idle state and they re-initiate the full LTSSM state machine from the Gen1 Configuration phase through the Gen3 Recovery.Equalization phase, which is what is needed for tuning. This option is only useful for host computers capable of doing it, when L0s/L1 power management is disabled and when the target drive is not the primary partition. You can test if a host supports this by hitting the **Capture Dis/En Lanes** button on the wizard main panel. If TraceControl triggers within a few seconds and goes to “PostFilling” in the State column” (look at TraceControl’s main window for this), you can hit the **Stop Capture** button. It is successful! The log will show “PERFORMED: Reboot capture” upon success. Redo this test three times in a row to confirm that it works. From there you can select this Auto-Reboot option in the “Tuning Options” panel and then hit the **Start Auto Tuning** button.

Remote reboot by software - This option consists of sending a command over the LAN to reboot the DUT. The wizard calls the batch file RemoteReboot.bat to do this. The file is accessible by clicking the **Edit .bat files…** button. By default, that batch file calls RebootWin.bat, capable of rebooting any Microsoft Windows DUT, given that you provide the IP address, login information and you carefully follow all the steps described at the top of RebootWin.bat to enable this feature on the DUT. This option will not work if the target drive is the primary partition as the tuning process will transition into states that will prevent the DUT from booting, and the DUT will not be able to act upon the remote reboot requests. Once you finished editing the RemoteReboot.bat/RemoteWin.bat files, double-click on them three times in a row to make sure they work. Once this works, you can select this Auto-Reboot option in the “Tuning Options” panel and then hit the **Start Auto Tuning** button.

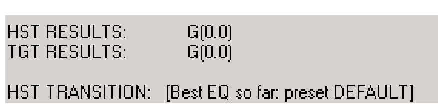
Control an IP Power switch - (This is the best and preferred method.) This option controls an IP Power switch over the LAN to power off/on the DUT. Once the DUT is on and the first packet is seen on the PCIe bus, a capture is taken and the DUT is automatically powered off again after 8 seconds (configurable). That technique allows powering on/off computers without damaging the operating system as it is powered off before the operating system is fully loaded. The wizard calls the batch files IPPowerOff.bat and IPPowerOn.bat to do this. The files are accessible by clicking the **Edit .bat files…** button. By default, the files call into IPPower9258.bat, which is capable of controlling an IP Power 9258 switch (cheap and widely available). You need to specify the IP address, login information and port number used on the IP Power switch. The switch uses DHCP and must be on the SAME SUBNET as the computer where TraceControl runs. You must first download and run the ipedit.exe software (http://www.aviosys.com/downloads.html) to discover the IP9258 switches on your network and retrieve the IP address (you can also use an IP scanner if you run into troubles http://angryip.org/download/#windows). When the IPPower9258.bat file is ready, double-click on the IPPowerOff.bat and IPPowerOn.bat files to make sure they work. Once they work, you can select this Auto-Reboot option in the "Tuning Options" panel and then hit the **Start Auto Tuning** button.

Mixed IP power/remote reboot - This is a mix of the two prior options, so it requires you to make both of them work before you can use this one. This is a last resort option if you find out that repeated short 8 second captures used in "Control an IP Power switch" are not leading to an error-free link.

Once you hit **Start Auto Tuning**, the wizard will perform from 10 to over 500 reboots overnight until it finds error-free settings. Once it has found an error-free setting in an 8-second capture, it will try a 2-minute capture error-free (if an IP Power switch is used, it tries 16 eight-second error-free captures in a row instead). If the 2-minute capture(s) is not error free, then the wizard continues and tries other settings. Once we have an error-free 2-minute capture, then the wizard displays a pop-up dialog box requesting you to start packet traffic on the DUT.

The packet captures the run for two minutes after you clicked **OK**. 10,000 packets are required, error-free, to declare success; otherwise, the wizard will try other settings again. Upon success, the log shows the final grade and final EQ settings applied.

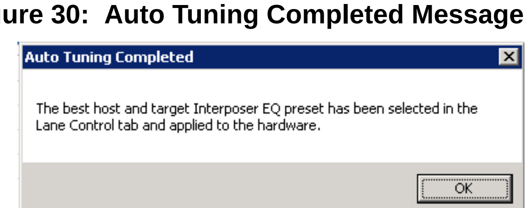
Figure 29: Successful Test Results



Note: Sometimes, while the wizard is busy writing the best settings to the interposer, a "Server Busy" message indicating that the "action cannot be completed" may be displayed. If this happens, just dismiss the message.

Then the wizard displays a final message that the Auto Tuning has completed.

Figure 30: Auto Tuning Completed Message

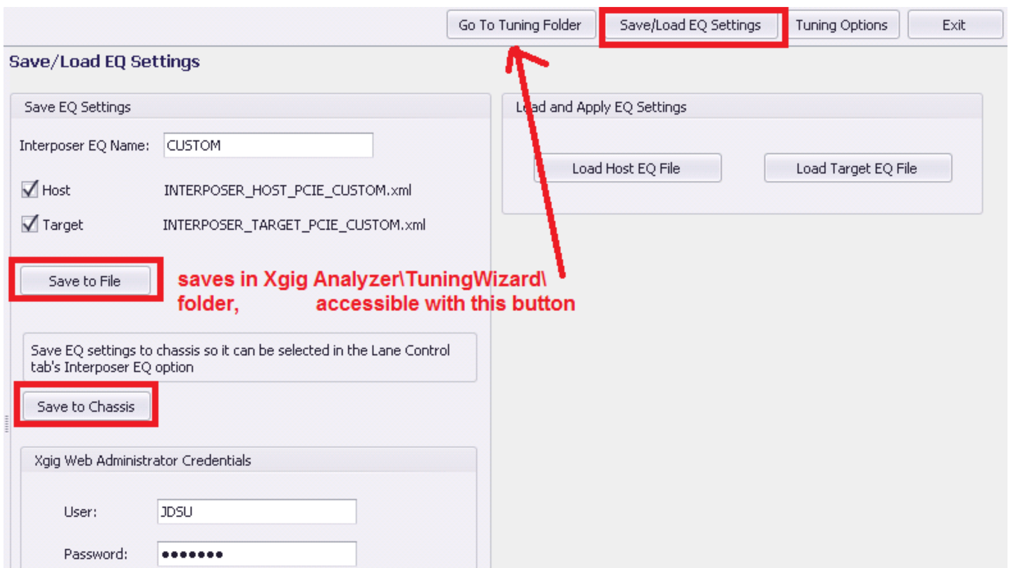


Note that while the wizard is tuning, you can stop/pause auto-tuning at any time by clicking **Stop Auto Tuning**. At that point, the wizard stops and re-applies the best settings on the interposer. You can resume the auto-tuning where it left by clicking **Start Auto Tuning** again.

If you are satisfied with a certain level of errors in the best settings, or if you want to try some manual captures or settings, click **Stop Auto Tuning**, and do what is required, but leave the Tuning Wizard dialog box displayed. While the Tuning Wizard is displayed, you can still access TraceControl's main window and take captures, open TraceView, etc.

Before exiting the Tuning Wizard, you should save the best settings of your session to a file with a proper name identifying the Host/Target environment. You should save locally on your PC and on the chassis with the **Save To File** and the **Save to Chassis** button.

Figure 31: Save EQ Settings

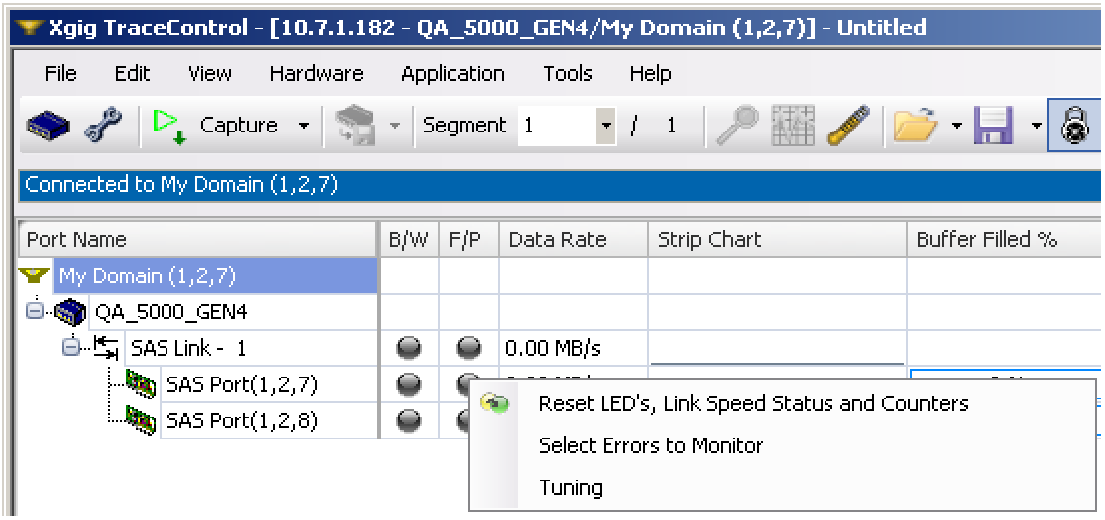


The wizard automatically saves the best settings in the "MY LAST TUNING" preset on the chassis and in the TuningWizard\ folder. However, it is recommended that you save it again using a meaningful name. Newly-saved files on the chassis are only available in TraceControl's Lane Control tab after you reboot the chassis. Furthermore, the chassis files will be deleted when you upgrade your chassis, so it is important that you save the file locally on your computer so it can uploaded it again.

Finally, if you experience problems or if you are not able to get satisfying results out of the auto-tuning session, email a copy of your PCIeTuningSession.xml file to our Technical Support team at techsupport-snt@viavisolutions.com. This file is constantly updated while tuning so you can even send it while auto-tuning is running. The next time you open the tuning wizard, it will be overwritten, so make sure you copy it before you open a new Tuning Wizard session again.

Tuning for 12G SAS

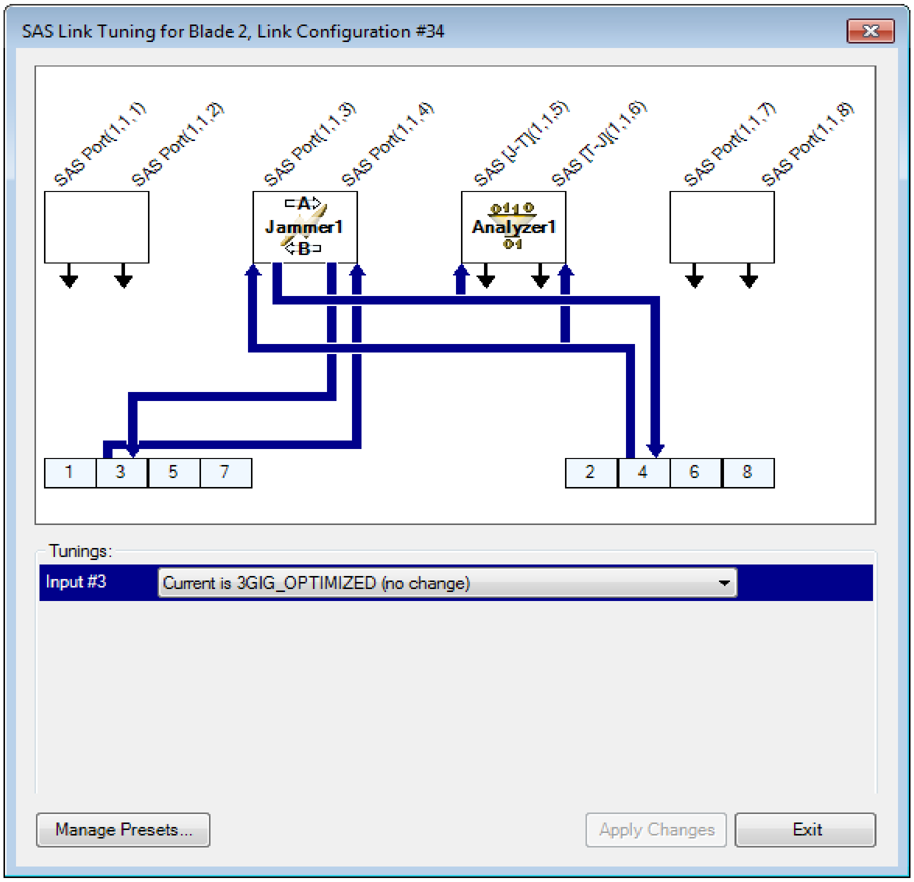
This option is for 12G SAS only. If two blades are being used, the user must tune each blade independently by launching the SAS Link Tuning dialog twice. In TraceControl, create a domain and lock all ports to be tuned. Right-click the software LEDs at the port level shown in the domain created for the 12G SAS blade or system, and click Tuning from the context menu to open the SAS Link Tuning dialog.



This option is for 12G SAS only. Click **Tuning** to open the **SAS Link Tuning** dialog. If two blades are being used, you must tune each blade independently by launching the **SAS Link Tuning** dialog twice.

The new **12G SAS Link Tuning** dialog introduces a new concept of port groups. It still focuses on the tuning of a single 12G blade, but the ports on the blade are aggregated into port groups. The port groups are named "Input #n" or "Output #n", referring to ports on the mini-SAS connectors. The dialog shows the port group for the selected configuration and allows you to load a preset tuning, auto-select the best preset, or auto-tune.

The top portion of the **12G SAS Link Tuning** dialog displays the lane steering diagram for the current link configuration. It is the same dialog as visible inside the Discovery dialog's Link Configuration, except that the wire colors uniquely identify port groups.



Use the drop-down menu to select a tuning method. You can choose from the following options:

- Auto-select the best preset
- Auto-tune
- Change to [preset name]

Auto-select the best preset

To automatically select the best preset, select **Auto-select the best preset** from the Tunings drop-down menu. Then, click the **Apply Changes** button. The software selects the best preset from the list of saved presets and applies that tuning preset to the hardware. This selection is based on the preset with the lowest bit error rate (BER). When the preset selection is complete, a dialog is displayed showing the selected preset.

The **Save** area is reserved for future use.

Click the **Back** button to close the dialog and returns to the **SAS Link Tuning** dialog where the name of the preset selected is shown as the current tuning.

Click the **Exit** button to close the dialog and return to the **TraceControl** window.

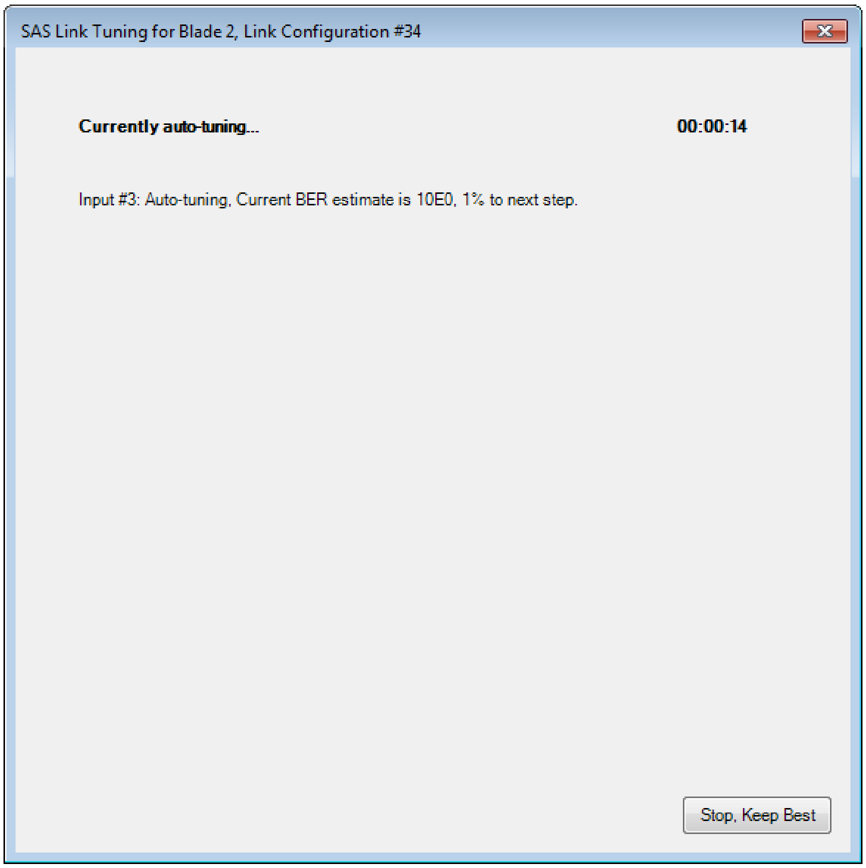
Auto-tune

Auto-tuning in Trace Control is supported by the following configurations:

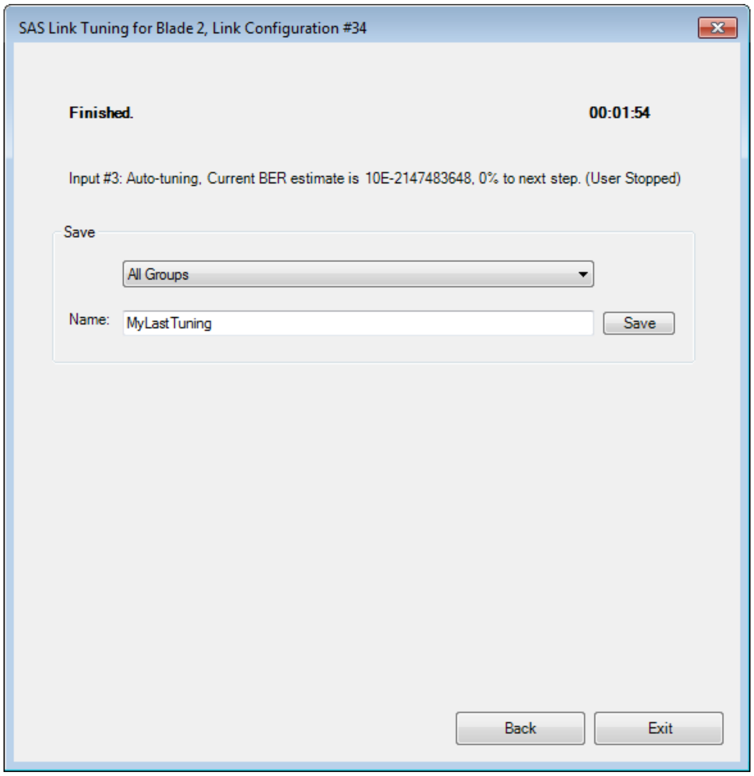
#31 – A,A,A,A	#32 – A-J-A,A	#34 – J-A
#35 – G-A	#41 – G-J-A,A	#49 – G-A,G,G
#55 – G-A, G-A		

Before starting the auto-tuning process, try applying the best preset. If you are not sure which one is best, perform the Auto-Select the best preset process. This may shorten the time it takes to auto-tune. To auto-tune all the ports in the configuration loaded on the hardware for the ports you have selected, select **Auto-tune** from the Tunings drop-down menu. Then, click the **Apply Changes** button to begin the auto-tuning process. Note that when a configuration is selected in the **Discovery** dialog, auto-tuning will tune all the ports in that configuration regardless of whether the other ports in the configuration are locked or not.

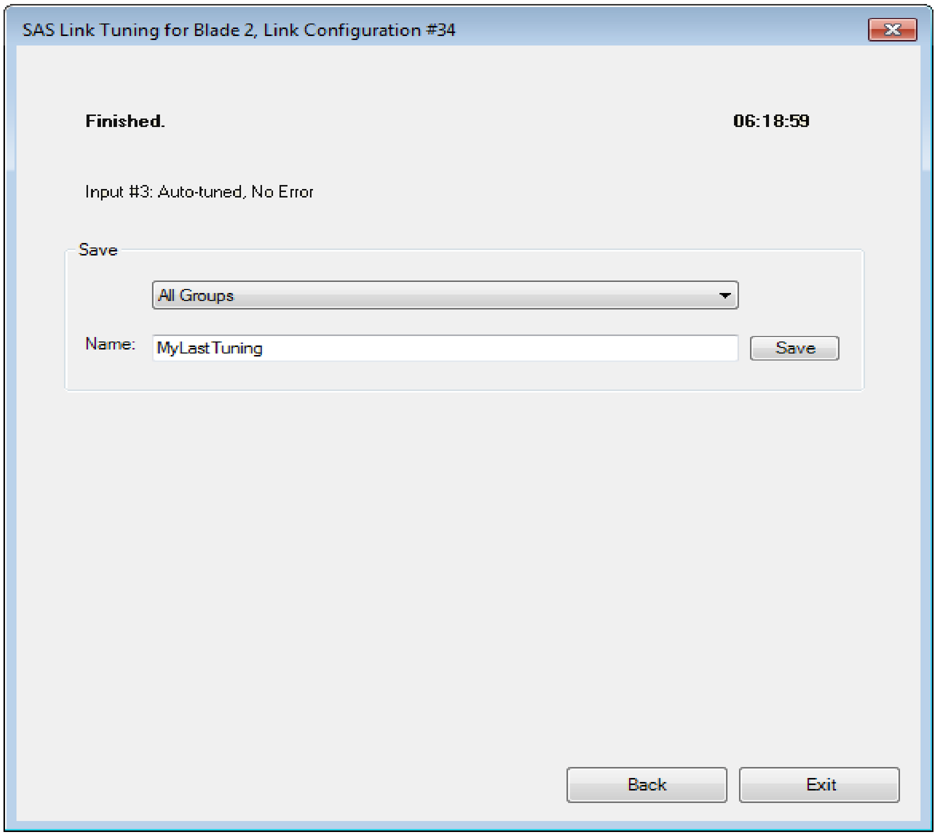
A dialog appears showing the tuning progress. It includes the duration of the tuning and the bit error rate (BER).



The auto-tuning process concludes only when the ports are error free for the longest of a series of intervals. This may take six hours or more. You can stop the auto-tuning process at any time and keep the best settings found thus far by clicking the **Stop, Keep Best** button.
In this case, the dialog shown below appears.



When the tuning is done, the dialog displays the finished page with the final status and the duration of the tuning.



In the **Save** area, the group and the name of the tuning is displayed. The group is provided by default and is not editable. The default name of the auto-tuning is ***MyLastTuning***. You can change the name by typing another name into the text field. When you enter a new name, a **Save** button is displayed. Click the **Save** button to save the auto-tuning with the new name.

Click the **Back** button to close the dialog and returns to the **SAS Link Tuning** dialog.

Click the **Exit** button to close the dialog and return to the **TraceControl** window.

Change to [preset name]

To load a preset on the ports in a configuration, click **Change to [preset name]** from the Tunings drop-down list. Then, click the **Apply Changes** button. The software applies the tuned settings of the preset configuration hardware and returns to the **TraceControl** window.

In addition to the default settings, the tuned settings that you have saved after auto-tuning are also available.

The **Manage Presets...** button opens a dialog allowing you to delete or rename presets.

All the presets are listed in the right column. The left column shows the port groups affected by each preset. You cannot rename or delete the factory provided presets, nor any preset currently in use.

As a side note, a client application could be killed or lose network connectivity while an auto-tuning is performed on an Xgig blade. In that case the auto-tuning will continue running on the chassis until it finishes by itself. However the tuning dialog always checks for in-progress auto-tunings when it comes up and prompts to cancel them.

Xgig Tuning and Equalization

Tuning and Equalization are procedures to optimize ports on the 6G SAS/SATA blades and systems for your environment. When you connect the Xgig SAS Analyzer or Jammer in a new environment (for example, after changing devices or cable length) we recommend that you run the Tuning procedure below. If, after Tuning, the Analyzer or Jammer detects excessive signal integrity issues, go on to adjust the Equalization settings. For more information about Tuning and Equalization, see "Technical Overview of Tuning and Equalization" on page 72.

Tuning

Tuning is used to fine-tune the sampling position in the data stream. The tuning function optimizes the Xgig ports for the particular devices and channel in use, and maximizes the receiver margin to ensure signal interoperability. Always perform Tuning after Equalization settings have changed.

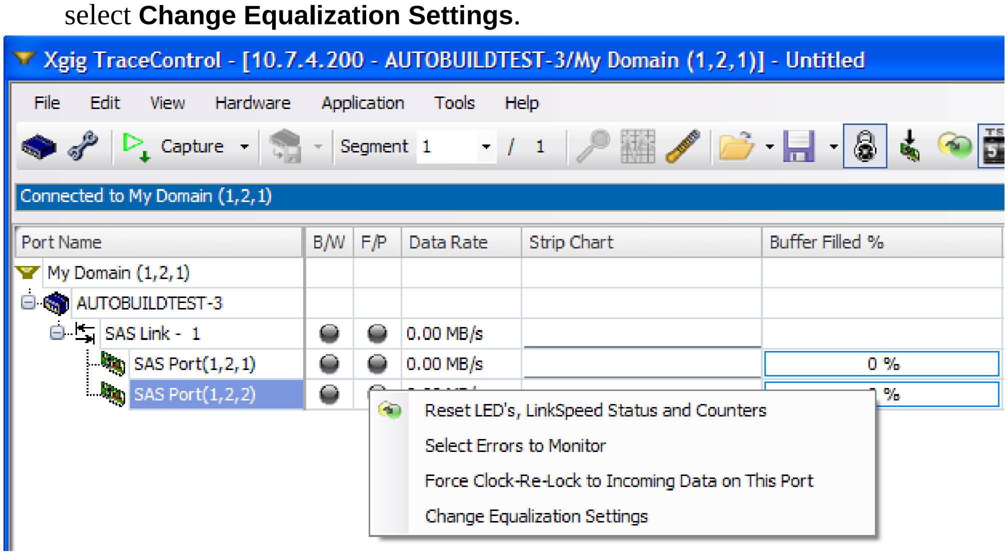
Tuning can only be performed when the Analyzer ports are in **Analog Passthrough** mode. Digital retiming would initiate an OOB sequence which would cause the user's devices to temporarily stop sending traffic needed by the tuning algorithm.

Requirements for Tuning

1. All port-pairs to be tuned must be exchanging traffic in both directions. All ports will be tuned at their respective data rate.
2. Use high link utilization, if possible.
3. If possible, use a stress pattern such as unscrambled CJTPAT; however, this is not required.

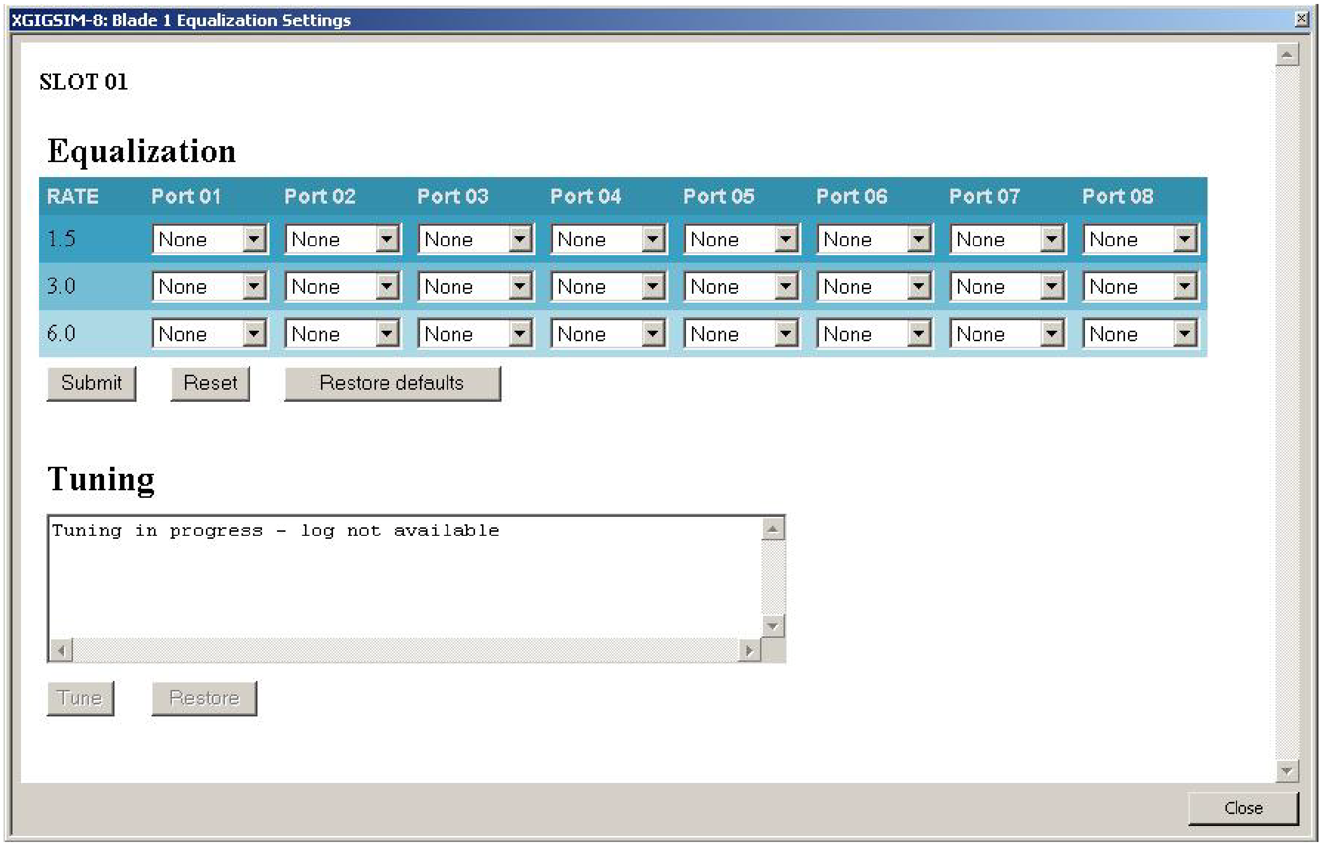
Initiate Tuning

1. Set up and connect all ports to be tuned so that they are exchanging traffic in both directions.
2. In TraceControl, create a domain and lock all ports to be tuned. Right-click the software LEDs at the port level shown in the domain created for the 6G SAS/SATA blade or system, and select **Change Equalization Settings**.



3 You will be prompted to enter the user name and password for the chassis web page. The default user name is **JDSU** and the default password is **JDSUsnt.** If the defaults have been changed, check with your system administrator for the correct user name and password.

4 To start tuning, press the **Tune** button on the **Blade X Equalization Settings** web page. If you have not selected all the ports on the blade to be included in the domain, the unselected ports will be grayed out and therefore will not be tuned when you click the **Tune** button.



5 The tuning process optimizes the receiver. This process takes a variable amount of time and can last up to 30 seconds. During tuning, the TraceControl LEDs will flash red while the optimal parameters are determined for the receiver. Upon completion of a successful tune, the LEDs will turn yellow. A page will display showing Tuning has started for the blade/ports and the Equalization page automatically returns after a brief period. The Tuning result is shown on the Equalization page.

6 Manually reset the TraceControl software LEDs. Right-click the LEDs and select **Reset LED's and Link Speed Status** from the menu. You can also reset the LEDs by clicking on the **Reset LED's, Link Speed Status, and Counters** button in the toolbar.

The optimized settings will take effect immediately. If you press **Apply Configuration** or start a capture in TraceControl, the newly optimized settings will be used.

Notes for Tuning

1 The optimized values determined by Tuning become invalid if any of the following is true:

a The blade is moved to a different chassis or slot

b The blade is replaced

c A cable is changed

d Device is replaced (drive, HBA, expander, etc.)

e Device transmitter settings are changed (for example, de-emphasis is increased)

2 Upon completion of tuning, if some ports still receive errors, follow the instructions below to modify the equalization on that particular port and attempt to tune again. If problems persist, shorten the cables or adjust the emphasis and/or amplitude settings on the transmitter, if possible.

3 Settings persist across an Xgig chassis reboot or power cycle.

Restore Tuning Defaults

To restore the original factory settings for tuning, press the **Restore** button on the web page. The restore function will also cause all link rates to return to the original factory settings. The tuning process will automatically apply both the Tuning results and the latest Equalization settings at the end of the tuning process.

Equalization

The general rules for choosing the appropriate Equalization setting are listed below. The suggested settings for Equalization for each port and speed are provided in Table 4. Note that the legend below Table 4 shows the precise meaning of cable lengths and de-emphasis settings at the input device.

1 At data rates of 1.5000 Gbps and 3.0000 Gbps the equalization setting can be left to **None**.

2 The Equalization process is performed for the selected ports on a blade. All locked ports are selected by default, but you can choose to unselect any of those ports. If Equalization is not required for a particular port at a particular speed, make sure it is set to **None**.

3 At 6.0000 Gbps, you may need to change the equalization setting. Situations where equalization settings should be changed include when the transmitting device has low or no emphasis, or where a long cable is used. See Table 4 for a list of the suggested settings for equalization based on de-emphasis of the signal and the length of the cable.

4 Always perform the Tuning procedure after you have completed Equalization. In the unlikely event you believe the analyzer is receiving false errors after performing both Equalization and

Tuning, you should attempt Equalization at the higher and lower settings from the current setting. Re-tune whenever you change Equalization settings.

Table 4: Recommended Equalization Settings

Case / Equalization Settings	None	Low	Medium	High	Notes
1.5000 Gbps Operation	♦				Frequency components not high enough to need equalization in normal use.
3.0000 Gbps Operation	♦				Frequency components not high enough to need equalization in normal use.
6.0000 Gbps Operation, Short Cables, No De-Emphasis			♦		Frequency components close to the source may need medium equalization as the channel will attenuate high frequencies.
6.0000 Gbps Operation, Long Cables, No De-Emphasis				♦	Frequency components far from the source may need high equalization as the channel will significantly attenuate high frequencies.
6.0000 Gbps Operation, Short Cables, Low De-Emphasis		♦			Frequency components close to the source may need low equalization as low de-emphasis and cable may cause the channel to mildly attenuate high frequencies.
6.0000 Gbps Operation, Long Cables, Low De-Emphasis			♦		Frequency components far from the source may need medium equalization as the low de-emphasis and long cable may cause the channel to moderately attenuate high frequencies.
6.0000 Gbps Operation, Short Cables, High De-Emphasis	♦				Frequency components close to the source may not need equalization as high de-emphasis and short cable may normalize the signal.
6.0000 Gbps Operation, Long Cables, High De-Emphasis		♦			Frequency components far from the source may need low equalization as high de-emphasis and long cable may cause the channel to mildly attenuate high frequencies.

Low De-Emphasis < 3dB
Medium De-Emphasis = 3dB
High De-Emphasis > 3dB

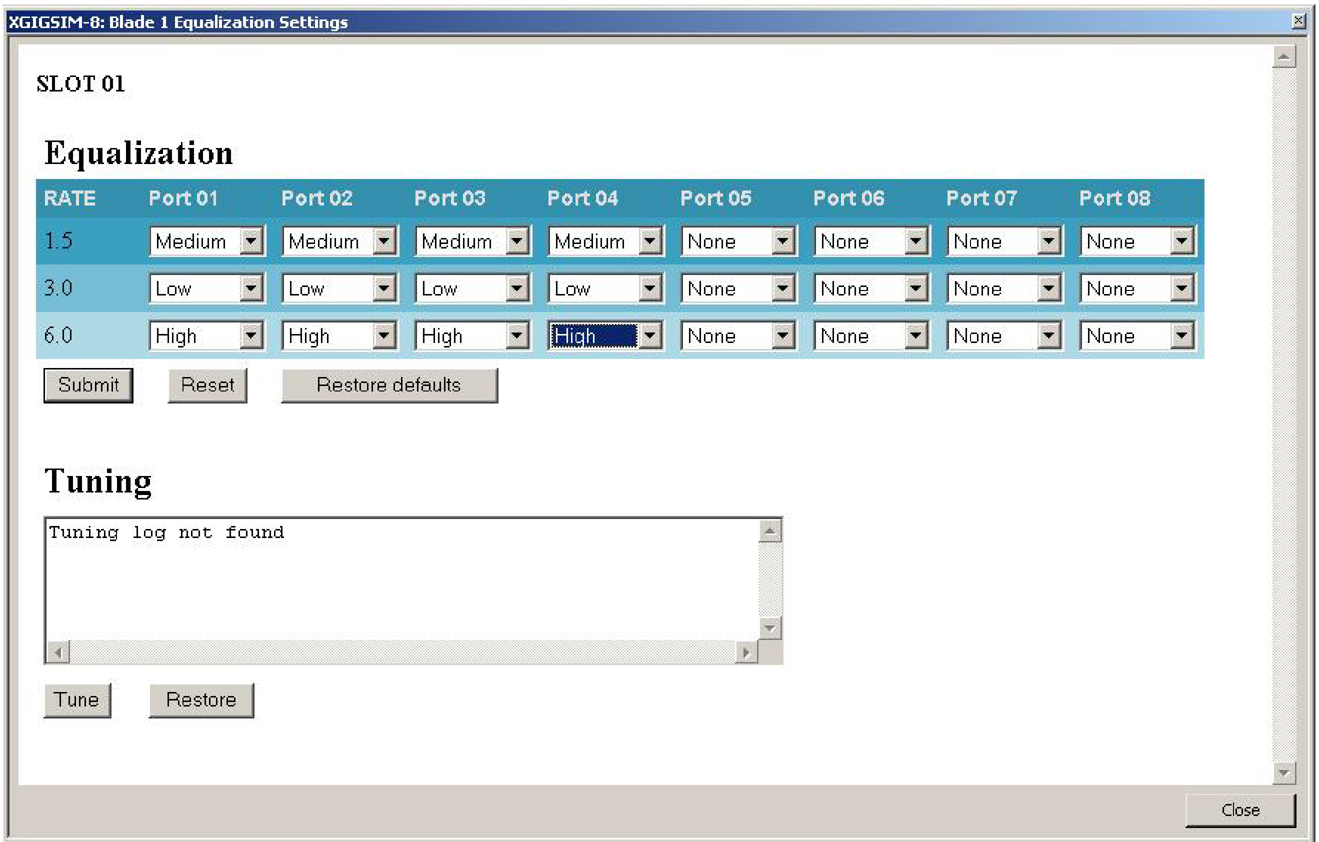
Short cable = 0.5m to less than 2.0m
Long cable = 2.0m to 3.0m

Steps to Apply Equalization

1 In TraceControl, right-click the port level LEDs shown in the domain created for the 6G SAS/ SATA blade or system, and select **Change Equalization Settings**.

2 You will be prompted to enter the user name and password for the chassis web page. The default user name is **JDSU** and the default password is **JDSUsnt**. If the defaults have been changed, check with your system administrator for the correct user name and password.

3 A web page will appear with drop down boxes for each port at all speeds, 1.5000 Gbps, 3.0000 Gbps, and 6.0000 Gbps. An example of the web page is shown below. The Xgig chassis name appears in the title bar, and the slot number for the chassis is displayed at the top of the web page. If you have not selected all the ports on the blade to be included in the domain, the unselected ports will be grayed out and therefore not configurable in the web page.



4 Press the **Submit** button after the appropriate settings have been selected from the drop-down boxes. This results in an update on the chassis with your requested settings, but does not update the hardware. A page will display showing the settings you have selected. Press **Go Back** to return to the Equalization page.

5 Perform the Tuning procedure. Whenever you press the **Tune** button, the tuning process will automatically apply both the Tuning results and the latest Equalization settings at the end of the tuning process.

Once the equalization setting(s) have been submitted, the settings will persist across an Xgig chassis reboot or power cycle. Unless a device is replaced or the transmitter settings are changed, the Equalization and Tuning settings will remain valid. If a device is replaced or the transmitter settings are changed, then the Equalization and Tuning settings should be reset.

Press **Reset** to refresh the web page to the currently stored settings.

Restore Equalization Defaults

To restore the original factory equalization settings, press the **Restore defaults** button. The restore process will automatically apply the factory default Equalization settings and the latest Tuning results at the end of the Tuning process.

Technical Overview of Tuning and Equalization

Given the challenge of extreme serial bit rates for 6.0Gbps SAS/SATA and the state of current 6.0Gbps SAS/SATA components, manual Equalization and Tuning procedures are required to ensure that you receive reliable results. These procedures may become unnecessary in the future as SAS-2 devices evolve and signal quality and jitter issues are resolved, but at present they are the best way to achieve optimal results.

Tuning is used to fine-tune the sampling position in the data stream. In addition to the intrinsic parasitics found in a copper channel, there are additional interoperability challenges with the high serial bit rates for 6.0Gbps SAS/SATA. These include jitter sources, transmitter voltage levels, and slew rate, to name a few. A user-initiated tuning function optimizes the Xgig ports for the particular devices and channel in use. The tuning process maximizes the receiver margin to ensure signal interoperability.

The copper channel used in SAS/SATA, consisting of traces, vias, connectors, and cables, has low-pass filter characteristics. This means higher-frequency components in the serial bit stream will have their voltage amplitude attenuated in comparison to low-frequency components in a pattern. To compensate for this phenomenon, the SAS-2 specification requires the use of de-emphasis at the transmitter and equalization at the receiver. De-emphasis reduces the low-frequency signal. Equalization attempts to correct any lingering differences between high and low frequencies at the signal destination.

Equalization is required for all SAS-2 devices; however, most current SAS-2 devices, including the current version of the 6G SAS/SATA blade or system, do not have auto-equalization circuitry. This means that equalization settings are selected for the ports when the blade is shipped, and the settings need to change based on the environment they are used in. The primary variables for setting equalization are the length of the cables and amount of de-emphasis from the source.

See Figure 32 for contrasting examples showing how Equalization is required to ensure signal integrity when there is no de-emphasis. The first example shows no de-emphasis at the source, signal degradation, and the need for a moderate equalization setting to ensure signal integrity. The second example shows how de-emphasis at the source can eliminate the need for changing the Equalization setting. See Figure 33 for an example of how the use of long cables slightly increases the need for Equalization.

Figure 32: SAS Signal Characteristics, With and Without De-Emphasis at Source

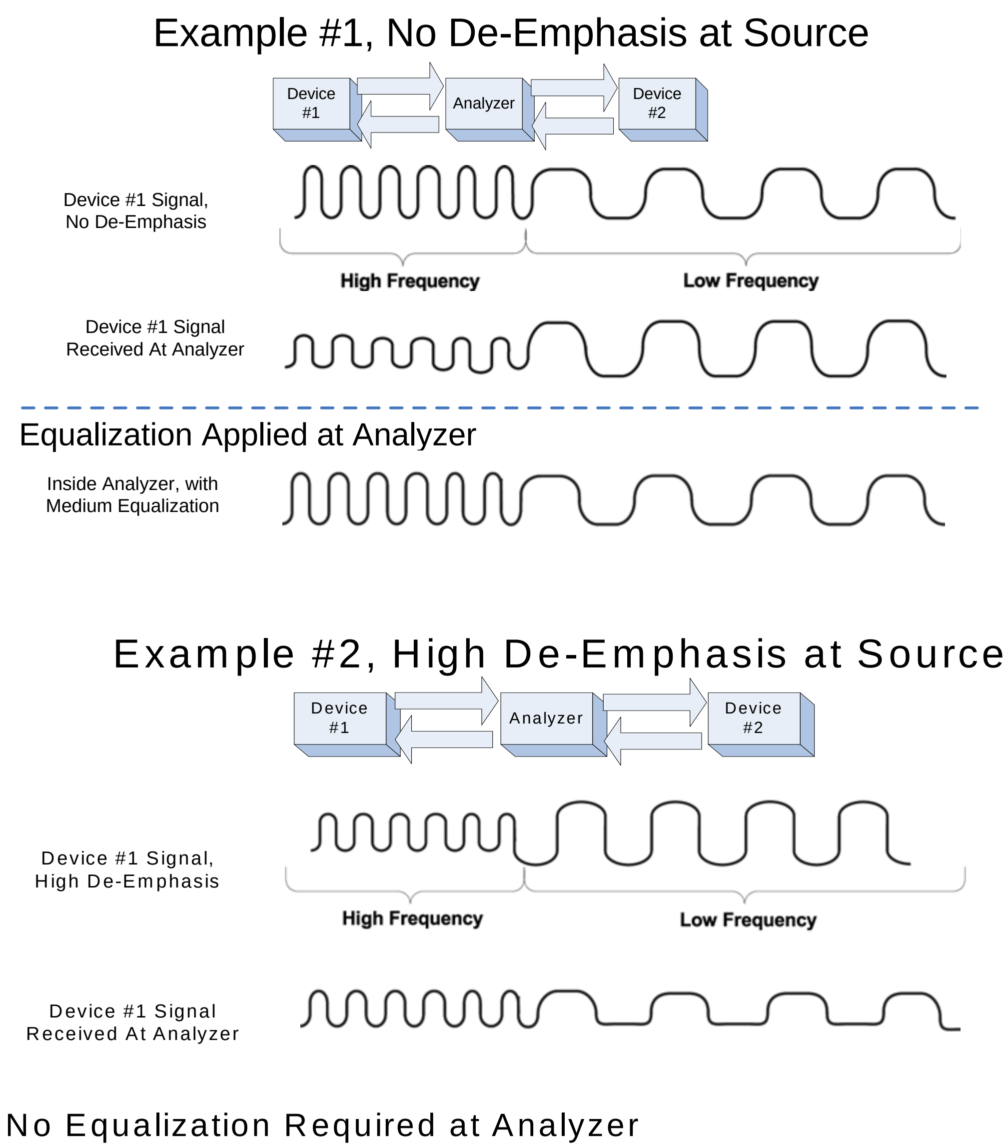
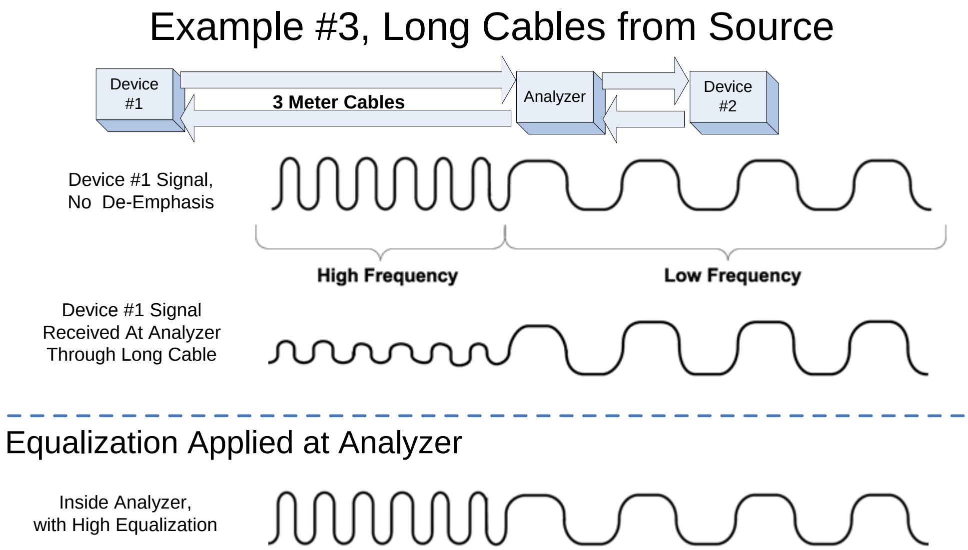


Figure 33: SAS Signal Characteristics Using Long Cables



Note that only 6.0Gbps devices are allowed to have 3M cables, and all devices at lower speeds are restricted to 0.5M (or possibly 1M).

Chapter 4

Xgig TraceControl Capture Configuration

In this chapter:

- Configure Ports or Domains
- Configuration Editor
- General Settings
- Capture and Trigger Setup
- Segment Capture Options

Configure Ports or Domains

You must configure all ports in a domain before starting a capture for the domain. If you do not set the configuration for an analyzer blade, it inherits the default configuration values.

All ports in a domain are divided into state machines. For SAS/SATA, each link is a state machine. For FC and GE ports, each port pair is a state machine. You can add a link for FC or GE ports. For SAS/SATA, all ports in a link must reside on the same blade. For FC and GE, ports in a link may reside on multiple blades within the same chassis. All ports in a state machine transition in sync. See “General Settings” on page 93 for more information.

You can apply the configuration of the current state machine to all state machines for that protocol. If you have a domain with different port types, you must configure ports for each protocol separately. See “Triggering with Mixed Ports” on page 133 for more information on configuring a domain with different port types.

The configuration is loaded to the hardware when a capture is started or when the **Apply Configuration** button is clicked. Ports must be locked by the user to upload (apply) a configuration to hardware.

Click the Configuration button to bring up the TraceControl Configuration Editor. Below is an overview of the type of information you can define for an analyzer configuration.

- **Size Options: Number of Segments, Trace Size, Frame Length, Post Trigger Fill**
  Set the number of buffer segments, the trace size (per segment), the maximum number of bytes in a frame/packet to capture, and the position of the trigger point within the capture buffer. The **Number of Segments** and the **Trace Size** fields are interrelated. Setting the value of one will determine the value for the other, based on the total memory available. See “General Settings” on page 93 for complete information on these fields and buffer segmentation.
- **Signal Regeneration**
  The signal can be passed through, or the signal can be boosted and digitally retimed. The signal attenuation is no more than 4dB for analog passthrough.
- **Link Speed**
  You must set/check the link speed for each port. Auto speed negotiation options are available for SAS/SATA and for 16G FC ports of the Xgig1000 chassis.

Important: If your network requires you to change link speeds, you should verify that the link speed is correct even if you have loaded a configuration file.

- **Transceiver Options**
  For 8G blades, select the transceiver options, either **High** for all speeds or **Standard** for the industry standard. For 16G blades, select the transceiver options, either **High** for 16G fixed speed or **Low** for auto and all other speeds.
- **FCoE CRC Checking**
  Fibre Channel over Ethernet (FCoE) is the proposed mapping of Fibre Channel over selected full duplex IEEE 802.3 networks.

- **Scrambling**
  This setting applies only to the 8G and 4G Fibre Channel ports. It allows you to specify whether the capture will include scrambled data.
- **FEC (Forward Error Correction)**
  This setting applies only to 16G Fibre Channel ports with the Link Speed set to 14.0250 Gbps and 10GigE ports on the 2 port 10G Multi-function Xgig blade. It allows you to specify whether FEC is enabled in the link or not. It also has an **Auto** option that detects FEC automatically.
- **Capture and Trigger Setup Tab**
  From the **Capture and Trigger Setup** tab, set what traffic to capture and what traffic to ignore and select how you want the analyzer to trigger.
- **TTL In/Out**
  From the **Capture and Trigger Setup** tab, you can enable or disable the use external trigger input/output ports.
- **Output Signal Voltage**
  From the **General Settings** tab, you can select either high or low output voltage for Xgig SAS/SATA ports.
- **Traffic Summary Data**
  From the **General Settings** tab, you can specify whether to generate post-traffic summary data.
- **Options for this State**
  From the **Capture Options** tab in the Capture Filter Editor, you can capture the granularity of Out-of-Band Signaling and set other options related to SAS/SATA, FC, or GE captures.

Clock Sync

The clock on the all Xgig chassis is synchronized with your local system by using the Clock Sync operation from the Xgig Web Utility. See the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* for more information on the Xgig Web Utility. Synchronizing the clock ensures that timestamps in any captured data will match your system clock. Synchronization is only required the first time you use the chassis or, if another user has reset the chassis clock.

Note that if you perform a Clock Sync operation after you have started a capture operation, the capture will not use the updated timestamps from the Clock Sync operation. Subsequent captures will use the new timestamps.

Applying the Configuration to Hardware 

A TraceControl configuration controls starting and stopping analyzers, specifies capture filters, and other conditions such as frame size. All configuration information specified in the TraceControl Configuration window is applied to the hardware.

Press the **Apply Configuration** button to load the configuration to the hardware. If you start a capture before you apply the configuration, this step is automatically taken before the capture starts. You can also select **Apply Changes to Hardware** from the **Hardware** menu to load the configuration to the hardware.

If applying the configuration may result in any loss of data, you will receive a warning message.

Saving a Configuration

A TraceControl configuration file controls triggering analyzers, specifies capture filters, and other conditions such as frame size. All configuration information specified in the Configuration Editor is saved with the configuration. You can restore the configuration by loading the configuration file at a later time.

If you have already saved the configuration, use the **Save Configuration** option from the **File** menu to save updates to the configuration.

To Save a New Configuration File:

1. Select **Save Configuration As…** from the **File** menu, or click the **Save Configuration**  button in the TraceControl main window menu bar, and select **Save Configuration As....** The **Save As** dialog box appears.
2. If needed, use the dialog box to navigate to the folder where you want to store the configuration file. Configuration files can be stored in any location.
3. Name the Xgig TraceControl configuration file and press **Save**.

Saving a Configuration to TC API

To save a TraceControl configuration in a format that can be loaded by the TraceControl API, select **File > Export Configuration to TC API**. This saves the file with a `.tccapi` extension. Files with this extension can be loaded into the TraceControl API. For more information about the TraceControl API, see the TraceControl API Help system.

Loading a Configuration

Loading a configuration file reads the contents of the configuration file and displays it in the TraceControl window for all analyzer ports in a domain. It does not load the configuration to the hardware; the configuration is downloaded to the hardware when you start the capture. Configuration files for TraceControl must have an extension of `.tcc`.

A configuration can be loaded into a domain.

1. Select **Load Configuration Into Existing Domain…** from the **File** menu, or click the **File**  button in the toolbar, and select **Load Configuration Into Existing Domain…**. The **Open** dialog box appears.
2. If needed, use the dialog box to navigate to the folder containing the configuration file. Configuration files can be stored in any location.
3. Select the TraceControl configuration file and press **OK**. The configuration will be loaded for all the analyzer ports in the domain.

To load the default configuration into an existing domain, select **Load Default Configuration** from the **File** menu.

If you are applying a configuration file that results in ambiguous mappings, the software makes some assumptions about the mappings you want. For example, if you are applying a configuration with four ports to a domain with two ports, the first two ports from the configuration are applied and the others are ignored. As another example, if you are applying a configuration with two ports to a domain with four ports, the configuration for the first two ports are copied and the other ports in the domain are given the default configuration.

Note: When loading a configuration created using Analyzer 4.6 or earlier, the software may need to alter the settings to conform to the new format but will maintain the existing functionality as much as possible.

Create a Domain and Load a Configuration File

You can use a configuration file to create a domain and load the configuration file in one operation.

To Create a Domain and Load a Configuration File:

1. Select **Load Configuration…** from the **File** menu, or click the **File**  button in the toolbar, and select **Load Configuration...**. The **Open** dialog box appears.
2. If needed, use the dialog box to navigate to the folder containing the configuration file. Configuration files can be stored in any location.
3. Select the Xgig TraceControl configuration file, and press **Open**. The domain specified in the configuration file will appear in the domain tree.

Working with Surveyor

If Surveyor is installed on the client computer, Xgig TraceControl can convert a GigE capture and launch Surveyor to view the converted capture. The picture below shows the TraceControl buttons for launching other applications with the Surveyor button enabled. The button is enabled only when Surveyor is installed. The button is hidden by default when you first install the client software. You must use the Show/Hide feature to display it.

The capture is converted and saved to a local .hst file before opening with Surveyor. The **TgpToHst** dialog box will display after pressing the Surveyor button; TraceControl will save one or multiple .hst files, and launches Surveyor. The .hst file(s) are saved in a folder specified on the Surveyor tab of the **Tools > Options** dialog box. The .hst files are saved for the domain, for each port-pair, and/or for each port as specified in the Surveyor tab of the **Tools > Options** dialog box. See “Surveyor Conversion Options in TraceControl” on page 80 for information on how to use the dialog to select Surveyor conversion options.

An example is shown below of the files created when converting a Gigabit Ethernet capture of a domain with four ports using all conversion options.

Surveyor Base File Name = C:\Conversions\Temp
All converted files are located in C:\Conversions

Conversion for the entire domain:
Temp - Domain.hst

Conversion for port-pairs:
Temp - PortPair 0,1.hst
Temp - PortPair 2,3.hst

Conversion for ports:
Temp - Port 0.hst
Temp - Port 1.hst
Temp - Port 2.hst
Temp - Port 3.hst

When saving a domain .hst at the same time as port or port-pair .hst files, the Surveyor opens the domain .hst. When saving multiple ports or port-pairs as .hst files, Surveyor only opens the first port or port-pair, but it is possible to open the other ports or port-pairs with the **File > Open** menu within Surveyor.

The **Base Capture File Name** that you set for saving the Surveyor capture sets the file names and location used for ALL TraceControl to Surveyor conversions. If you want to save a converted capture, it is suggested that when the capture opens in Surveyor that you save it using a new file name. Subsequent conversions from TraceControl will attempt to convert using the same **Base Capture File Name**. Subsequent conversions could therefore overwrite previously converted Surveyor captures.

If the file with the Base File Name for the domain is currently open in the Surveyor application, you will not be able to perform another conversion from TraceControl. An error message will appear, indicating that the file is in use by another application.

Surveyor Conversion Options in TraceControl

Select **Tools > Options...** to bring up the dialog for configuring Surveyor conversion options within TraceControl. The **Surveyor** tab sets options for how TraceControl captures will be converted and saved when you hit the Surveyor button to open a capture. Only Gigabit Ethernet capture data in TraceControl can be converted. If there is a mix of FC and Gigabit Ethernet in a trace, only the Gigabit Ethernet data is converted.

Select the **Base Capture File Name** for all conversions to Surveyor. Use the Browse button to navigate to a location and name the base file.

Select the type of conversion. All three types may be selected.

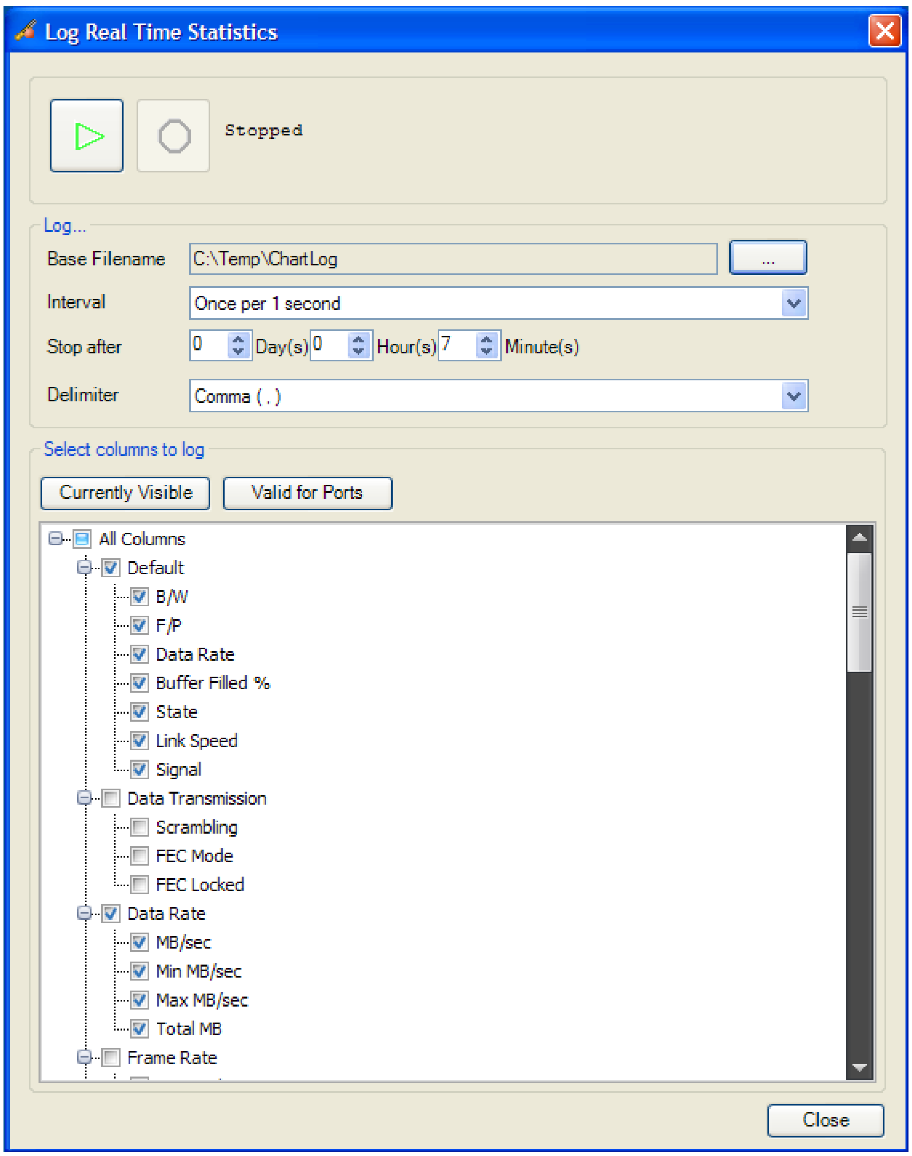
- **Convert by Domain**
  The entire domain is converted into a single Surveyor .hst file.
- **Convert by Port Pair**
  Each port pair in the domain is converted to a separate Surveyor .hst file.
- **Convert by Port**
  Each port in the domain is converted to a separate Surveyor .hst file.

Log Real Time Statistics

Real time TraceControl data can be saved to a .csv file. The .csv files can be directly imported into Microsoft Excel. In the **Log Real Time Statistics** dialog box, you specify the interval at which data points are saved, how many hours TraceControl will continue to save log files, and the .csv file delimiter type. You can also select which columns to log. A separate log file is saved for each port and each link in the current domain in TraceControl.

To open the **Log Real Time Statistics** dialog box, click the **Log Real Time Statistics**  button in the toolbar, or select **Tools**/**Log Real Time Statistics** from the menu bar. Use the start and stop buttons at the top of the dialog box to start and stop the logging process.

Figure 34: TraceControl Real Time Statistics Logger



Base Filename (and Location)

Data is saved as one file per port or link with the start date, start time, and port or link name appended to the base file name. The file name format is: <basefilename> _<day_month_year_hour.minute.second>_<Port_Name or Link_Name>; for example, **ChartLog_28_02_07_13.07.22_FC Port(1,1,1)**. All statistics in current domain in TraceControl will be saved to the file, one file for each port or link.

Stop after

Sets the overall time, in number of days, hours, and minutes, for which information will be written to log files. For example, if the **Interval** is set to 1 minute and **Stop after** is set to 2 hours (120 minutes), 120 log entries will be written to each single-port log file.

Interval

Sets the interval for gathering and writing data to the log file. Data for each interval shows in Microsoft Excel as another row. Options available are once per 1, 5, 20, or 30 seconds, 1 minute or 1 hour.

Delimiter

Delimiters provided are comma (,) , semicolon (;) , or tab (\t). The delimiter specifies the character(s) inserted in the .csv file to determine the end of a value and the beginning of a new value. Delimiters are interpreted by Microsoft Excel when the .csv file is imported. Comma is the default choice for the delimiter, which is also the default delimiter used by Microsoft Excel.

Select Columns to Log

You can select which columns to log by clicking the check boxes in the tree displayed. Clicking All Columns at the top of the tree selects all TraceControl columns that are available for logging. You can click the **Currently Visible** button to log all columns that are currently displayed in the TraceControl's main window. You can also click the **Valid for Ports** button to log all the columns that are relevant to the type of ports in the domain.

An example .csv file shown in Microsoft Excel for a single port is shown in Figure 35. Note that for display purposes not all entries are shown.

Figure 35: Example .CSV Log File

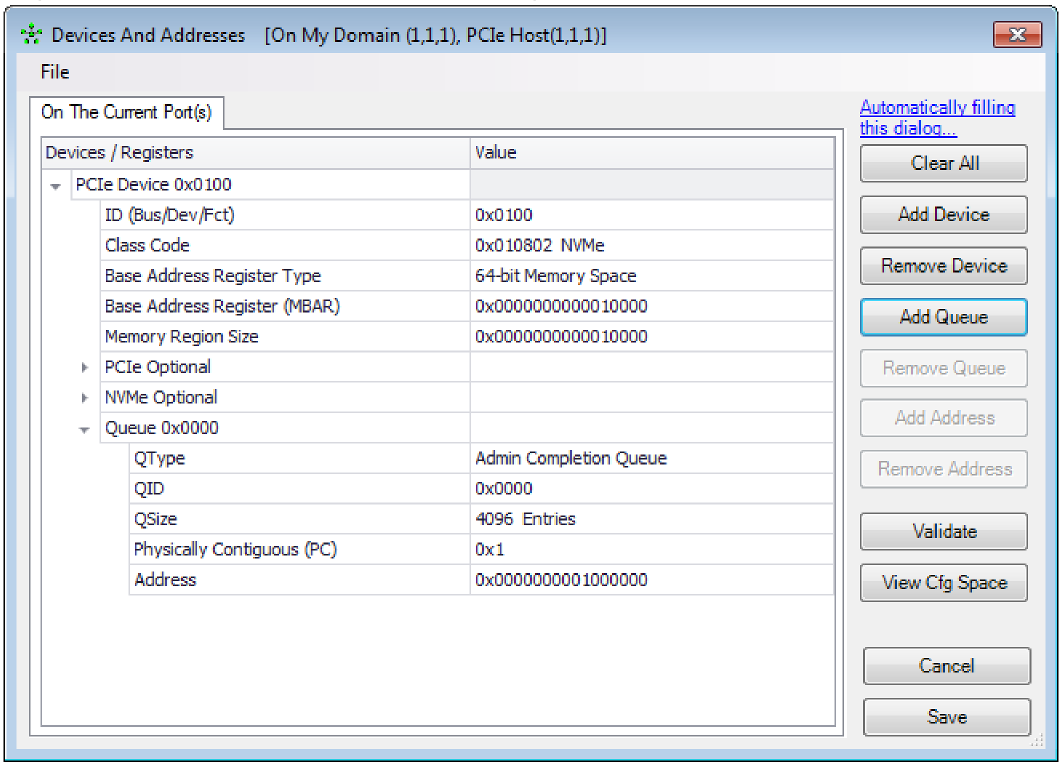
	A	B	C	D	E	F	G	H	I	J	K	L	
1	Time	B/W	F/P	Data Rate	Buffer Fille	State	Link Speec	Signal	MB/sec	Min MB/se	Max MB/s	Total MB	CRC
2	19:14:54	GREEN	GREEN	1484.33 M	99%	Stopped	14.0250 G	Retiming	1484.33	1483.22	1485.53	90569.84	
3	19:14:55	GREEN	GREEN	1484.39 M	99%	Stopped	14.0250 G	Retiming	1484.39	1483.22	1485.53	92842.78	
4	19:14:56	GREEN	GREEN	1484.39 M	99%	Stopped	14.0250 G	Retiming	1484.39	1483.22	1485.53	94350.35	
5	19:14:57	GREEN	GREEN	1484.76 M	99%	Stopped	14.0250 G	Retiming	1484.76	1483.22	1485.53	95765.14	
6	19:14:58	GREEN	GREEN	1484.44 M	99%	Stopped	14.0250 G	Retiming	1484.44	1483.22	1485.53	97272.69	
7	19:14:59	GREEN	GREEN	1484.39 M	99%	Stopped	14.0250 G	Retiming	1484.39	1483.22	1485.53	98780.25	
8	19:15:00	GREEN	GREEN	1484.39 M	99%	Stopped	14.0250 G	Retiming	1484.39	1483.22	1485.53	100287.8	
9	19:15:01	GREEN	GREEN	1484.39 M	99%	Stopped	14.0250 G	Retiming	1484.39	1483.22	1485.53	101702.6	

PCIe Device and Address Mappings

The PCIe Analyzer remembers the devices and address mappings from a prior boot-up sequence in order to analyze and decode future traces. You can manually enter all the devices and addresses in the **Devices And Addresses** dialog. Expert automatically generates those mappings when it processes a boot-up sequence. To open the dialog, click the **Devices And Addresses** button in TraceControl's toolbar, or select **Devices and Addresses** from the **Tools** menu. This button is enabled when you lock PCIe ports.

The **On the Current Port(s)** tab in the **Devices And Addresses** dialog shows the mapping stored in a file on the chassis. If there are multiple chassis in a domain, the contents of this tab is always the information for the first port pair listed in the domain. The contents of this tab can also be retrieved from any PCIe chassis in the domain.

Figure 36: Devices And Addresses Dialog



When a capture stops, TraceControl copies the device mapping from the first domain port into the pre-capture.devices file for the domain so that every capture's pre-capture.device file is initialized from TraceControl's domain device mapping.

The devices and addresses mapping is mandatory for TraceView and Expert to decode any protocols over PCIe, such as NVMe or SATA-AHCI. The information is exchanged during the boot sequence between the host and the devices. It may change from one reboot to the next.

You can fill the device mapping in two ways. First, you can click the “Automatically filling this dialog” hyperlink at the top of the dialog. When you do, a popup appears instructing you how to fill the dialog automatically. Second, you can enter the information manually. The buttons on the dialog's right-hand side allow you to add or remove devices, queues, and addresses.

If you are adding information manually, you should add every PCIe or AHCI device found in the capture and provide the Device ID, Class Code, and the Base Address Register (BAR) information for the address ranges used in the capture.

When the device is of Class Code 0x010802 (NVMe), you should also create the NVMe queues that are used in the trace and verify that the Memory Page Size (MPS) and Sector Size are set correctly. The NVMe queues have an ID, type, and size. Likewise, when the device is of Class Code 0x010601 (SATA-AHCI), you should create the SATA-AHCI queues.

The regular Submission and Completion queues can be Physically Contiguous or not, while the Admin queues are always physically contiguous. When physically contiguous, a queue has only one starting address. When non-contiguous, the queue uses a PRP List, and you need to enter the starting address of every memory page covering the queue (not the address of the PRP List itself, but all the addresses inside the PRP List).

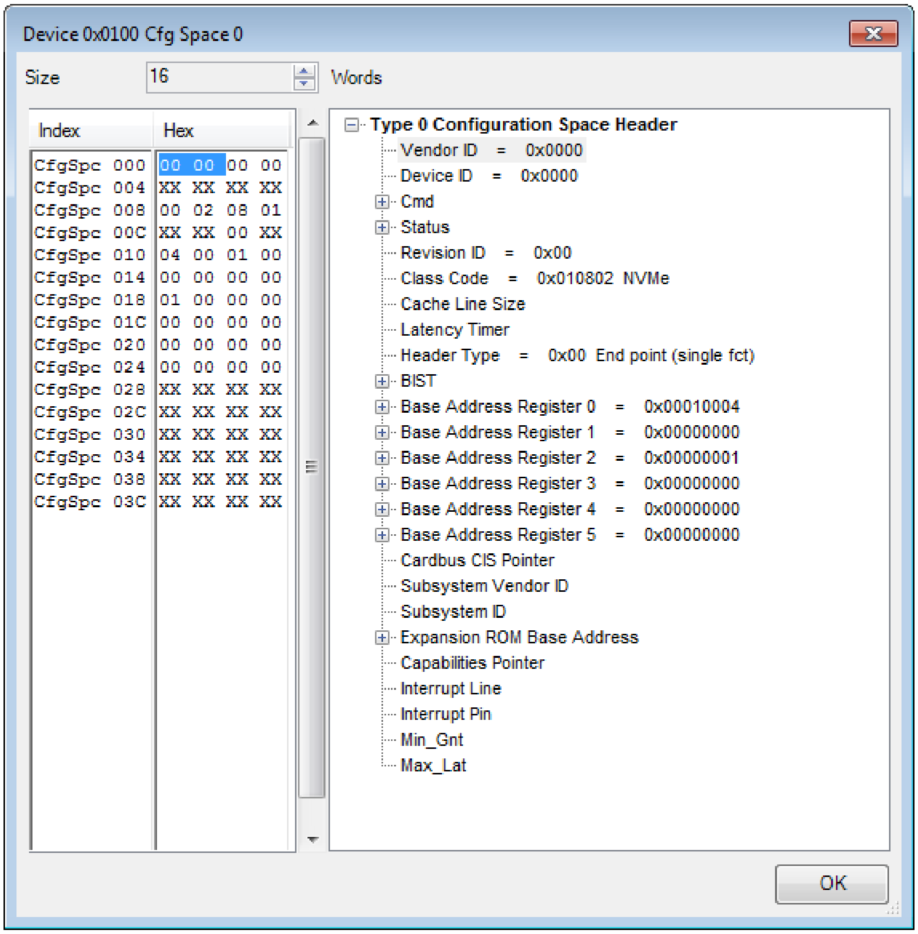
There are several optional settings in the dialog that improve expert's analysis, annotations and decodes for the capture.

- **PCIe Device/Vendor ID**: This combination uniquely identifies a PCIe device worldwide
- **Revision ID, Header Type**: Informational only for this release
- **Expansion ROM Base/Size and Additional BARs**: Used by Expert to identify the target device of a packet routed by address
- **MSI Interrupts**: Addresses for each MSI interrupt sent by the device
- **MSI-X Interrupts**: Addresses for each MSI-X interrupt sent by the device
- **TC to VC Mapping**: Traffic Class to Virtual Channel mapping as found in the Virtual Channel Capability of the device
- **NVMe Version**: Informational only for this release

Once you have finished editing the device mapping, you can click the **Validate** button to check the consistency and reports issues. This process ensures that all the memory regions do not overlap, the device ids are unique, and the queue ids and types are appropriate. TraceControl performs the validation when you click the **Save** button.

To view the Configuration Space for each device, click the **View Cfg Space** button.

Figure 37: Configuration Space Dialog



This can be useful when the device mapping was automatically populated by Expert. Expert stores the data for every successful CfgRd/CfgWr transaction for the entire configuration space accessed during a boot-up sequence (up to 4KB). When a DWORD contains XX XX XX XX, it means that it was not accessed during that capture.

Click the **Save** button in the **Devices And Addresses** dialog to save your changes to the device mapping.

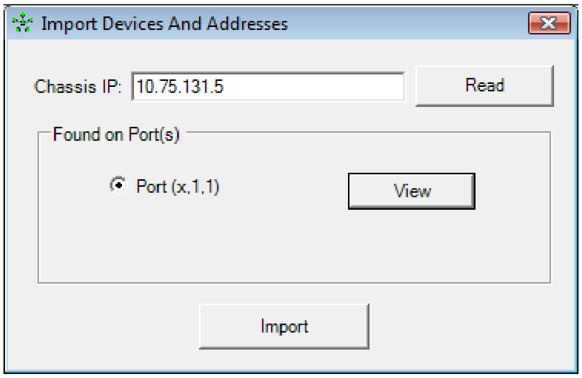
Click the **Export To File...** button to save the mappings to a *.devices* file on the local hard drive for future use. Once you export the devices and addresses to a file, you can import that file into the **Devices and Addresses** dialog in the future.

Exporting/Importing Device Mappings

To export or import device mappings, use the selections in the File menu in the **Devices And Addresses** dialog.

When you click “Import From File...”, the **File Open** dialog appears. When you click “Export To File”, the **File Save** dialog appears. When you click “Import From Chassis Ports” the following dialog appears.

Figure 38: Import From Chassis Ports Dialog



Type the IP address of a chassis in the “Chassis IP” field, and click the **Read** button to read all the mappings for all the port pairs on that chassis.

Click the **View** button to open the **Devices And Addresses** dialog in read-only mode, to view the port's mappings.

When you click the **Import** button, the **Import** dialog closes, and the original dialog is filled with the new devices and addresses, copied from the port selected.

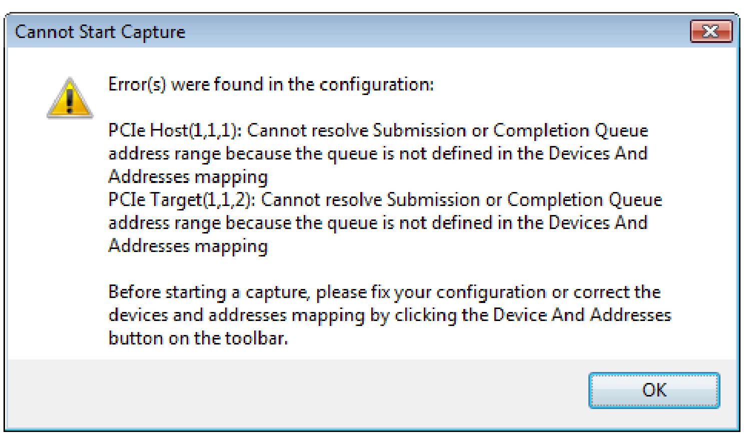
Detecting Insufficient Device Mappings In TraceControl

TraceControl's configuration files may contain NVMe-specific filters and triggers, for example “Trigger on a NVMe Write command”. Each NVMe trigger or filter element needs to be matched in a specific PCIe address range, as specified in the **Device And Addresses** dialog. TraceControl resolves the PCIe address range for each NVMe element when you do one of the following.

- lock the domain ports
- start a capture
- edit a configuration on locked ports

TraceControl shows errors messages when it is unable to resolve the address ranges between a configuration file and the PCIe devices and addresses mapping.

Figure 39: Insufficient Device Mappings Error



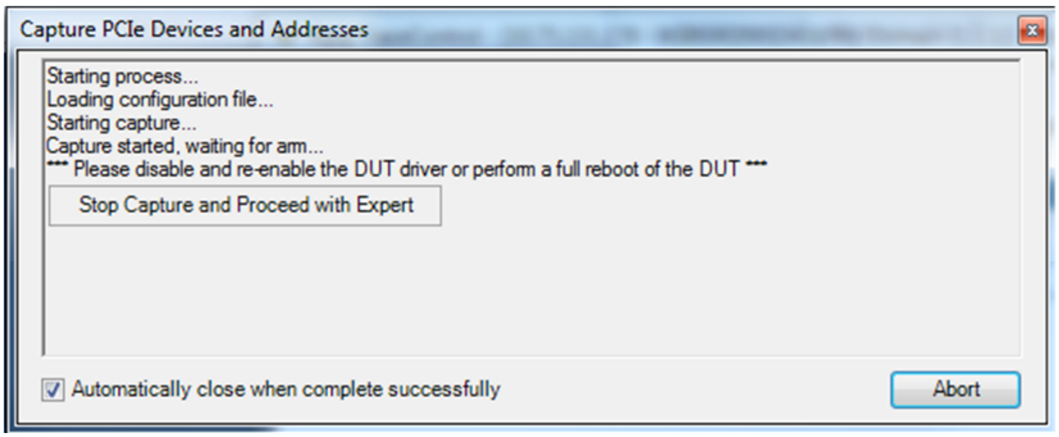
Capture PCIe Devices and Addresses

Capturing the boot-up sequence is critical for PCIe/NVMe to generate the device mapping file and queue addresses for decoding NVMe.

Clicking the **Capture PCIe Devices and Addresses** button  in TraceControl's toolbar or selecting **Capture PCIe Devices and Addresses** from the **Tools** menu provides an automated way of capturing the boot-up sequence. This button is enabled when you lock PCIe ports.

Upon clicking the button or menu selection, TraceControl starts a capture and prompts you to reboot or re-load the PCIe driver. The status dialog box shown in Figure 40 is displayed to display the status of the process at every stage. Use the **Abort** button to end the process.

Figure 40: Capture PCIe Devices and Addresses Dialog Box

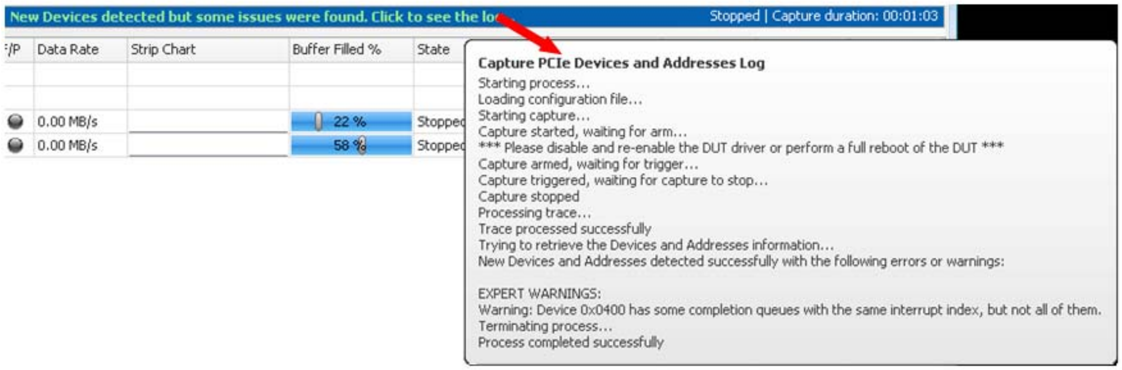


The automated Capture PCIe Devices and Addresses process does the following:

- Loads the appropriate configuration file
- Starts a capture on the current segment
- Waits for the capture to arm, trigger and stop (or stops automatically 30 seconds after it is armed)
- Runs Expert on the captured trace
- Retrieves the Device Mapping file generated by Expert
- Loads the new detected device mapping in TraceControl
- Reports errors and/or diagnostic messages if the capture did not contain all or insufficient boot-up information

When the Capture PCIe Devices and Addresses dialog closes, the result of the process is shown in the TraceControl status bar. The last log that was produced by the button "Capture Devices And Addresses" can always be seen by clicking the message in TraceControl's blue status bar (see Figure 41). The message will disappear when you click on any button.

Figure 41: Capture PCIe Devices and Addresses Log Screen



TraceControl Options

Select **Tools > Options** to bring up the dialog for configuring TraceControl options.

Dialog Box Options

The **Dialogs** tab is used to enable or disable the display of certain warning dialog boxes. Select **Always overwrite the hardware settings with the configuration** to use the port/domain configuration regardless of the settings that already exist in the hardware.

If you do not check this box, you will receive a warning dialog box, **Configuration Mismatch with Hardware Settings**, whenever the hardware link speed or signal regeneration settings for the configuration do not match currently existing settings for the hardware. The dialog box gives you the opportunity to use the settings already loaded to the hardware or verify that your link speed/ signal regeneration settings are correct. If you do not want to see this dialog to double-check your settings, you can disable the dialog display.

Select **Enable configuration editing during capture** if you want to be able to modify configuration files during capture. Note that this does not change the configuration for the capture. When this option is checked, you can save the configuration you are editing during a capture.

Select **Include non-overlapped data in saved trace** to enable saving non-overlapped data. Once turned on, this setting will be in effect until explicitly turned off. By default, this checkbox is unchecked.

Frame Errors

Select the **Frame Errors** tab from the **Options** dialog box to select the specific frame errors to be monitored by Port Status View LEDs. Jabbers, Fragmented Frames, and FCoE Embedded CRC errors will be gray if no Gigabit Ethernet port is being monitored.

Check the box for all error types to be included. Unselected error types are not used in determining the value of status LEDs for a port. See “Frame Errors Tab” on page 184 for a description of all Frame Errors.

Phy Errors

Select the **Phy Errors** tab from the **Options** dialog box to select the specific physical errors to be monitored by Port Status View LEDs**.** Errors are grayed out if they are not supported for the ports being monitored. This does not apply to Loss of Sync (LOS) errors.

Check the box for all error types to be included. Unselected error types are not used in determining the value of status LEDs for a port. For example, if CV errors are not selected, and the only errors detected for a port are CV errors, the status light for that port will remain green.

SAS/SATA Errors

Select the **SAS/SATA Errors** tab from the **Options** dialog box to select the specific SAS/SATA errors to be monitored by Port Status View LEDs. These options will be gray if there are no SAS/SATA Analyzer ports currently being monitored.

Check the box for all error types to be included. Unselected error types are not used in determining the value of status LEDs for a port. See Table 30, “Traffic Summary SAS/SATA Error Counters,” on page 343 for a description of all SAS/SATA Errors.

PCIe Errors

Select the **PCIe Errors** tab from the **Options** dialog box to select the specific PCIe errors to be monitored by Port Status View LEDs. These options will be gray if there are no PCIe Analyzer ports currently being monitored. See Table 14, “PCIe Errors,” on page 204 for a description of all the PCIe errors.

Check the box for all error types to be included. Unselected error types are not used in determining the value of status LEDs for a port.

Chart Options

The options on the **Charts** tab control the color display of the **Strip Chart** in the **Port Status View** as well as scaling options for the strip chart. You can also access the **Charts** tab by right-clicking the **Strip Chart** field for any port or link in TraceControl’s main window.

Color Options

Select the color for the strip chart graph using the **Chart** button, and select the background color for the strip chart using the **Background** button. The default graph color is green with a white background.

Scaling Options

These options control the scaling display of the **Strip Chart** in the **Port Status View**. The scaling can be done by port-pair/link or domain. If the scaling is set to domain, the scale for the strip chart graph will be the same for all ports. If the scaling is set by port-pair/link, the same scaling is applied to all ports in a link. If ports are not part of link, the same scaling is applied to both ports in a port-pair.

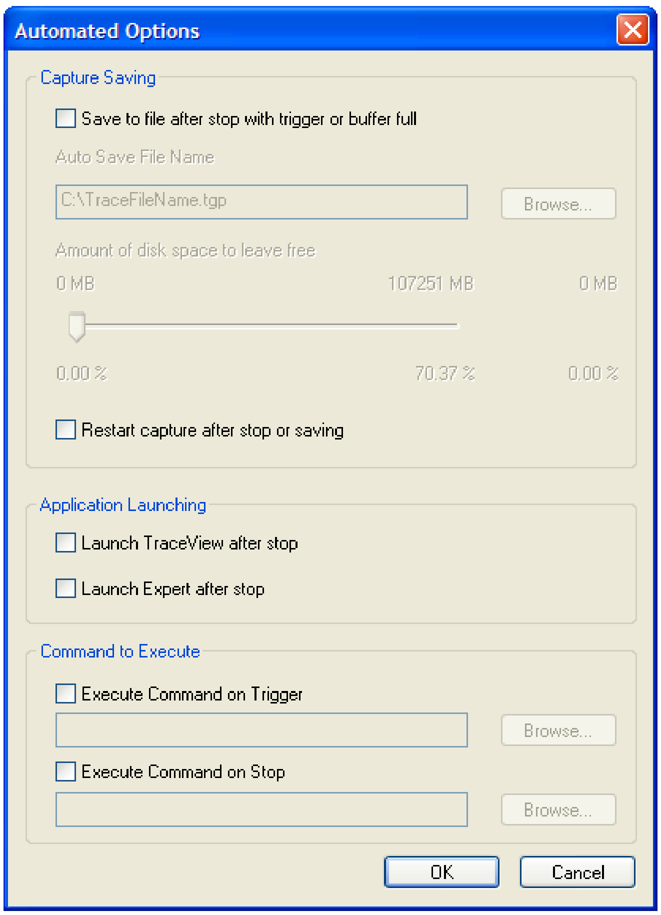
Surveyor Options

See “Working with Surveyor” on page 79 for information on setting the options for converting traces to Surveyor format.

TraceControl Automated Options

Select **Tools > Automated Options...** to bring up the dialog for configuring TraceControl automated options. Automated options control what actions TraceControl will take when a capture is triggered or completed. Automated options are not available for the following trigger modes, Stop When Stop Button is Clicked and Advanced with no Triggered state.

Figure 42: TraceControl Automated Options



Autosaving the Capture to a File

Check the **Save to file after stop with trigger or buffer full** option to auto save the capture to a file. Use the **Browse** button to choose a directory location and a file name for the saved file.

You can restart the capture after the save is complete. To restart the capture, check the **Restart capture after stop or saving** option. You can also select the **Save to file after stop with trigger or buffer full** option. The **Restart capture after stop or saving** option is still available if you do not select the **Save to file after stop with trigger or buffer full** option.

Since the restart option will continue to save capture files after the capture stops, it may eventually leave no disk space. Set the slider bar in the **Amount of disk space to leave free** area to protect a percentage of your total disk space. The default is to not save any disk drive space on the volume where you are saving the capture files.

Successive capture files are given the name of the first capture file with _DD_MM_YYYY_hh.mm.ss appended to the filename, where _DD_MM_YYYY_hh.mm.ss is the timestamp of the capture; for example, TraceFileName_16_02_2006_14.56.04.

Restarting capture and the application launch options are mutually exclusive. If you set the restart option, you will not be able to launch another Xgig application automatically.

Application Launch After Capture

Other Xgig applications can be automatically launched after the capture is stopped. Use the check boxes in this section of the dialog to control how other applications will behave when capture is stopped. If the **Save to file after stop with trigger or buffer full** option is used, the application will process the trace file saved for the capture. If the **Save to file after stop with trigger or buffer full** option is not used, the newly-launched application will process the contents of the Xgig buffer.

- **Launch TraceView after stop**
  Launches the TraceView application after capture is complete. TraceView or Expert may be launched automatically, but not both.
- **Launch Expert after stop**
  Launches the Expert application after capture is complete. TraceView or Expert may be launched automatically, but not both.

The application launch options and capture restart are mutually exclusive. If you choose to automatically launch another Xgig application, you will not be able to automatically restart the capture.

Command to Execute

This option allows you to select an application, script, or batch file to execute upon trigger or capture stop of the domain. You can use this option to start an application that sends email, start other devices, or log information to a file. Note that the command can include parameters passed to the script, for example, `my_script.bat arg1 arg2`.

Configuration Editor

The Configuration Editor is where you configure ports and define capture filters and trigger conditions. This editor has two tabs. The **General Settings** tab displays a summary of the settings for all the ports in a domain. Use the **General Settings** tab to set the values and options for all hardware and data settings for all ports in a configuration.

For the purposes of triggering, all ports are divided into state machines. For PCIe, FC, and GE ports or links, each port pair is a state machine. For SAS/SATA each link is a state machine. For SAS/SATA, all ports in a link must reside on the same blade. FC and GE links can reside on multiple blades. All ports in a state machine transition in sync.

The **Capture and Trigger Setup** tab allows you to define capture filters and transitions for state machines. It provides a graphical representation of the state machine and capture filter and transition editors. You can only edit one state machine at a time. The State Machine drop-down menu in the Trigger Setup window allows you to choose which state machine you want to edit. The **Apply to all port pairs** button applies the current configuration to all port pairs/links. You can use the **Apply to other port pairs** button to access a dialog where you can choose other port pairs or links to apply the current capture and trigger settings to. Click **Apply** to apply the current configuration to the selected port pairs. A configuration for a state machine cannot be applied to state machines of another protocol. For example, if a domain contains two FC port pairs on a 4G blade, one GE port pair, and a SAS/SATA link, selecting **Apply to other port pairs** while editing the state machine for a 4G FC ports pair will pop up a dialog showing the remaining 4G FC port pair available for selection.

Note: The only protocols that allow a state machine to be applied to blades of another type are FC and SAS/SATA. 2G, 4G, or 8G FC configurations can be applied to one another’s state machines. 2G, 4G, or 8G FC configurations can be applied to a 16G FC state machine, but a 16G FC configuration cannot be applied to other FC state machines. 10G FC cannot be applied to an FC blade of another speed.

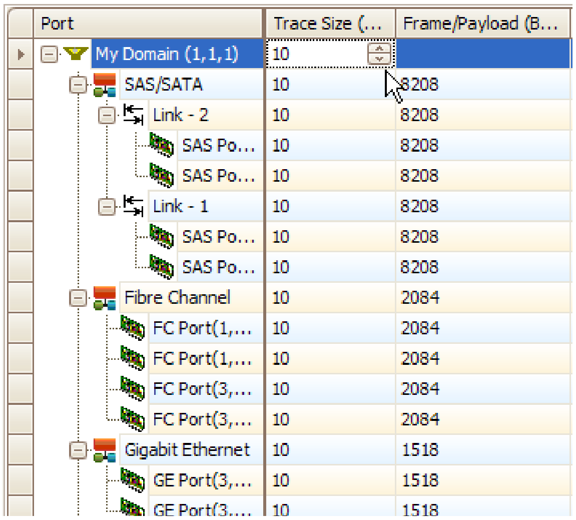
3G SAS configurations can be applied to 6G and 12G SAS/SATA state machines, but 6G and 12G SAS/SATA configurations cannot be applied to a 3G SAS/SATA state machine.

General Settings

The **General Settings** tab of the Configuration Editor displays the configuration settings for all ports and allows you to define the hardware and data settings for each port individually, for a link, or for an entire domain.

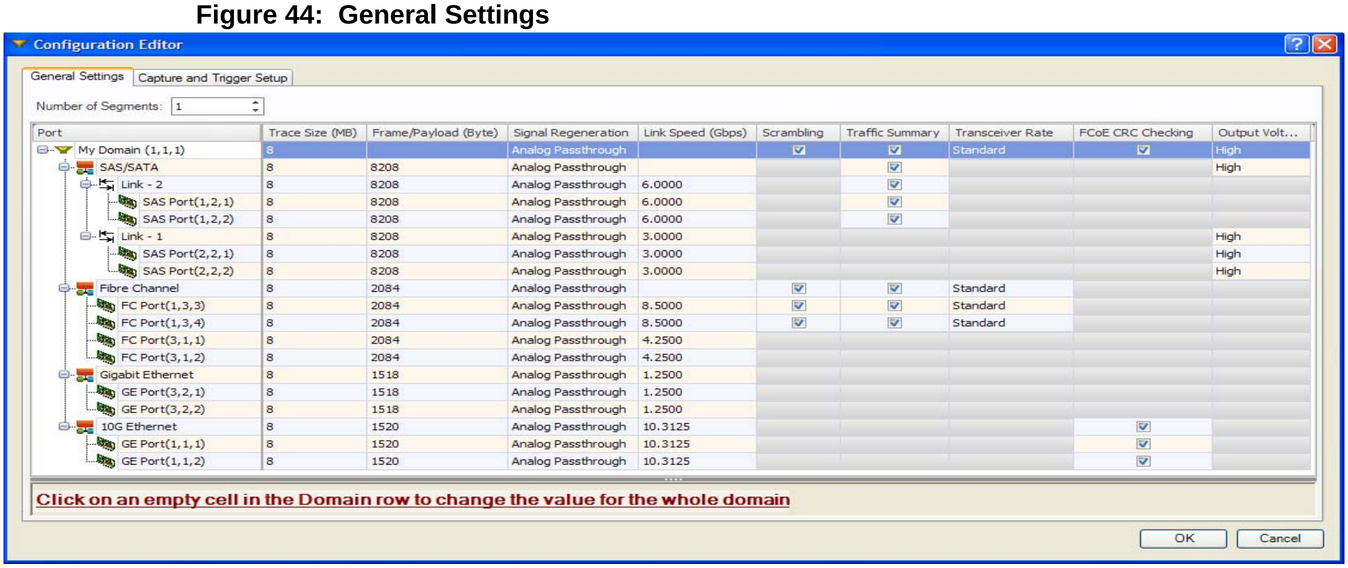
Click a port to edit its settings. Click the cell corresponding to a link or the whole domain to edit those values. The domain and link rows are either blank until you click them, or if all ports have the same value, that value is displayed.

Figure 43: Set Value for All Ports in a Domain



Not all fields are editable for all ports. However, all settings for all ports are shown to provide a clear view of all ports in the domain. When using mixed ports, some columns may be available for some ports but may not apply to others. Fields that do not apply to a port are grayed out for that port.

Figure 44: General Settings



Use this tab to configure the following:

- Link Speed (applies for all ports in a link for SAS/SATA, FC, GE. and PCIe or port pair for FC and GE. If there is no link, settings are applied to the port pair.)
- Signal Regeneration (applies for all ports in a link for SAS/SATA, FC, or GE or port pair for FC and GE. If there is no link, settings are applied to the port pair.)
- Traffic Summary (applies per link/port pair)
- Frame/Payload size (applies per port)
- Number of Segments (applies for the whole domain)
- Trace size (applies per port)
- Scrambling (applies for an FC port pair)
- FEC (Forward Error Correction) (applies per 16G FC or 10GigE port including 40G on Xgig1000)
- CDR (Clock Date Recover) (applies per 10GigE port pair for 40G Xgig1000 only)
- Transceiver Rate (applies per port)
- FCoE CRC Checking (applies per port)
- Output Voltage (applies per port)

At the bottom of the **General Settings** window, there is a description field that provides a description of the column selected along with some additional details about the setting such as whether the setting is per port or per link/port pair or any other restrictions. Whenever a setting is edited, additional constraints may be applied due to interdependency of some settings.

Link Speed

The link speed and signal regeneration options allow the analyzer hardware to perform correctly in your environment. The link speed must match the rate of your circuit under test and signals may have to be retimed in some environments.

You must ensure that the link speed (data rate) is set properly before you start a capture or use the Performance Monitor program. If you only use one speed on your network, you can set the speed one time and not be concerned about checking the link speed when you start a capture operation.

Note: If your network requires you to change link speeds, you should verify that the link speed is correct even if you have loaded a configuration file.

The link speed is set for a port-pair or all the ports in a link. You cannot set the link speed for only a single port.

If you try to capture with the wrong link speed, you will notice red status for the B/W or F/P LEDs in Port Status view.

The link speed setting for the analyzer ports affects the behavior of Xgig TraceControl and Performance Monitor. If the link speed is set incorrectly in Xgig TraceControl, the Xgig TraceControl and Performance Monitor will display red status LEDs and LOS traffic status for the ports configured in the Xgig TraceControl.

To select the link speed, follow these steps:

1. Place the cursor in the **Link Speed (Gbps)** field.
2. Select a rate or **Auto**. For example, select the **2.1250 Gbps** option from the **Link Speed** pull-down menu in the **General Settings** tab to set the link speed.

Note: The Auto speed setting only detects link speed when the analyzer is idle. Once a capture is started, the auto-detect feature does not change the current analyzer speed if the link does change. The data rate will be fixed by the analyzer during capture.

Gigabit Ethernet Link Speeds

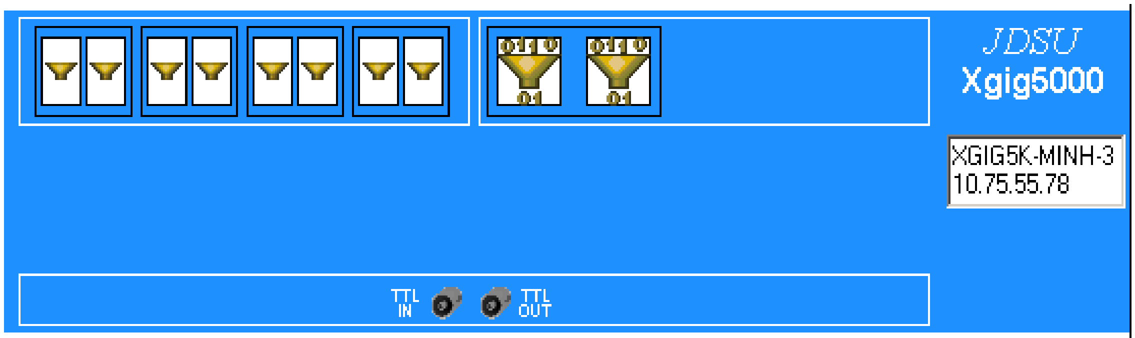
The link speed for the Xgig 1G Gigabit Ethernet blade is fixed at 1.2500 Gbps; no link-speed options will appear for domains with Xgig Gigabit Ethernet ports.

Using the Xgig5000 10G 8 Port Gigabit Ethernet Blade as a 40G Analyzer

The link speed for the Xgig5000 10G 8 Port Gigabit Ethernet blade can be changed to 40G. However, at 40G, this blade only supports the Analyzer function. The speed for this blade cannot be changed in the Link Speed settings in the Configuration Editor. The **40G Analyzer** setting must be selected in the **Select Ports for Domain Creation** dialog box. To use the Xgig5000 10G Ethernet blade as a 40G Analyzer, follow these steps.

1. From TraceControl's **Select Ports for Domain Creation** window, discover an Xgig5000 chassis containing an 8 port 10G Ethernet blade. This blade must be licensed for 40G Analyzer.

Figure 45: 10G Ethernet Blade Showing Eight Ports



2 Select any port in the blade.

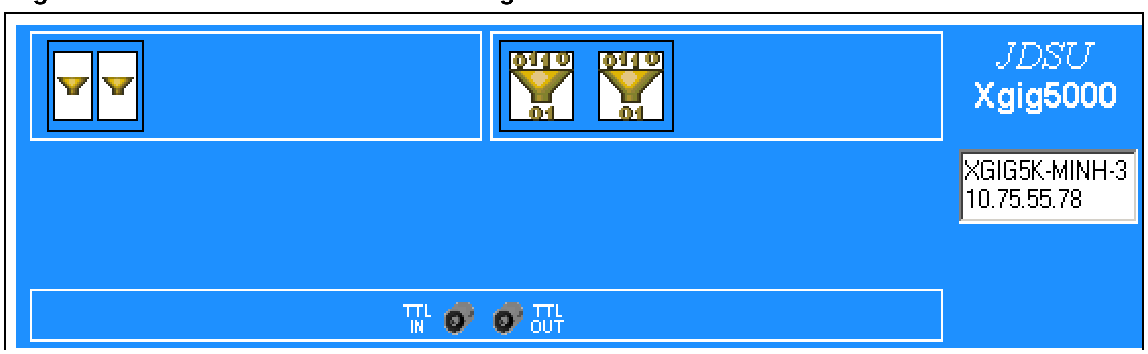
3 Right-click on the selected port, and select **Use Port(s) as.... > 40G Ethernet**.

4 Click the **Create and Lock** button at the bottom of the window.

5 All eight ports are locked as one 40G port pair, and only two ports are now shown.

Notice in the **New Domain** window, whenever the ports are being used as 40G, the ports are shown as only two ports in a single port pair.

Figure 46: 10G Ethernet Blade Showing Two 40G Ports



Fibre Channel Link Speeds

For Fibre Channel, the link speed can be set to the highest rate supported by the blade containing the ports, or a supported lower rate. Available rates for Xgig Fibre Channel are 1.0625 Gbps, 2.1250 Gbps, 4.2500 Gbps, or 8.5000 Gbps. For example, the Xgig 2 Gigabit Multi-Function blade ports can be set to 1.0625 Gbps or 2.1250 Gbps; however, higher rates are not supported.

The Xgig 8 Gigabit Fibre Channel blade fully supports 2.1250 Gbps, 4.2500 Gbps, or 8.5000 Gbps rates when equipped with SFP+ optical transceivers that support the 8.5000 Gbps rate. However, the 1.0625 Gbps rate does not work to specification when using the same SFP+ transceiver. To support a 1.0625 Gbps link speed on this blade, use SFPs that support a maximum rate of 4.2500 Gbps.

The Xgig5000 16G FC blade supports a link speed of 4.2500, 8.5000, or 14.0250 Gbps.

The Xgig1000 systems with 16G FC functionality support a link speed of 4.2500, 8.5000, or 14.0250 Gbps. It also includes an Auto option for ports used in Analog Passthrough. This is the default setting. The auto-detect option automatically detects the link speed when the analyzer is idle. Once a capture is started, the auto-detect feature does not change the current analyzer speed if the link does change. The data rate will be fixed by the analyzer during capture.

SAS/SATA Link Speeds

For 3G SAS/SATA blades, the link speed can be set to **1.5000 Gbps**, **3.0000 Gbps**, or **Auto**. For example, select the **3.0000 Gbps** option from the pull-down menu to set the link speed to 3.0000 Gbps.

For 6G SAS/SATA blades and systems, the link speed can be set to the highest rate supported by the blade containing the ports, a supported lower rate, or one of the **Auto** selections. The Xgig 6G SAS/SATA Wide-Port/4x Blade, the 6G SAS/SATA Narrow blade, and the LX and LXP fixed-port systems support 1.5000 Gbps, 3.0000 Gbps, and 6.0000 Gbps. For example, select the **3.0000 Gbps SAS** option from the **Link Speed** pull-down menu to set the link speed to 3.0000 Gbps. These blades and systems also have an auto-detect option, which will automatically detect the idle link speed between 1.5000 Gbps, 3.0000 Gbps, and 6.0000 Gbps.

The Auto options available for 6G SAS/SATA blades and systems are **SAS 6/3/1.5G & SATA 3/1.5G** and **SATA 6/3G.** For the **Auto** options, no actual negotiation or handshake takes place between the analyzer and any external device – the blade ports merely detect the data speed from the speed negotiation sequence happening on the idle link. The **Auto** options can automatically determine the idle link speed only if the Xgig ports see the link initialization activities that take place (for example, OOB and speed negotiation events). If link initialization sequence does not happen while an **Auto** option is set, the blade will retain its existing speed. For example, select the 1.5000 Gbps option for the Link Speed in the TraceControl Configuration window to set the link speed to 1.5000 Gbps. Then select the **Auto (SAS 6/3/1.5G & SATA 3/1.5G)** option for the Link Speed. If no link initialization happens, the speed of the blade will still be 1.5000 Gbps. The auto-detect option automatically detects the link speed when the analyzer is idle. Once a capture is started, the auto-detect feature does not change the current analyzer speed if the link does change. The data rate will be fixed by the analyzer during capture.

For 12G SAS blades, the link speed can be set to the highest rate supported by the blade containing the ports, a supported lower rate, or one of the **Auto** selections. The Xgig5000 12G SAS Wide Port blade and the Xgig1000 12G SAS blade support a link speed 3.0000, 6.0000, or 12.0000 Gbps. These blades and systems also have an auto-detect option, which will automatically detect the idle link speed between 3.0000 Gbps, 6.0000 Gbps, and 12.0000 Gbps.

The Auto options available for 12G SAS blades are **Auto (SAS 12/6G)**, **Auto (SAS 12/6/3G)**, and **Auto (SAS 6/3G)**.

Choosing an Auto Option for 12G SAS Blades

When you set the Link Speed to **Auto (12G/6G/3G)**, the analyzer is able to auto-detect any of these three data rates. In the 3G and 6G cases, the analyzer uses oversampling to detect the data rate. 12G traffic is captured directly. 6G traffic is oversampled 2x, and 3G traffic is oversampled 4x. This setting provides flexibility if you do not know the data rate of the link under test. However, note that if the traffic is at a 3G data rate, then oversampling by 4x can cause false bit errors. In this case, it is better to change the Link Speed to **3G** fixed or **Auto (SAS 6/3G)** and reinitialize the link under test.

When you set the Link Speed to **Auto (12G/6G)**, the analyzer is able to auto-detect either 12G or 6G data rates. In the case of 6G, the analyzer uses oversampling to detect the data rate. 12G traffic is captured directly. 6G traffic is oversampled 2x, and 3G traffic is not detected. This setting provides flexibility if you do not know whether the data rate of the link under test is 6G or 12G. However, note that if the traffic is at a 6G data rate, then oversampling by 2x may not be ideal. If the analyzer shows bit errors, then try setting Link Speed to **6G** fixed or **Auto (SAS 6/3G)**.

When you set the Link Speed to **Auto (6G/3G)**, the analyzer is able to auto-detect either 6G or 3G data rates. In the case of 3G, the analyzer uses oversampling to detect the data rate. 6G traffic is captured directly. 3G traffic is oversampled 2x, and 12G traffic is not detected. This setting provides flexibility if you do not know whether the data rate of the link under test is 3G or 6G. However, note that if the traffic is at a 3G data rate, then oversampling by 2x may not be ideal. If the analyzer shows bit errors, then try setting Link Speed to **3G** fixed.

For the **Auto** options, no actual negotiation or handshake takes place between the analyzer and any external device – the blade ports merely detect the data speed from the speed negotiation sequence happening on the link. The **Auto** options can automatically determine the idle link speed only if the Xgig ports see the link initialization activities that take place (for example, OOB and speed negotiation events). If link initialization sequence does not happen while an **Auto** option is set, the blade will retain its existing speed. The auto-detect option automatically detects the link speed when the analyzer is idle. Once a capture is started, the auto-detect feature does not change the current analyzer speed if the link does change. The data rate will be fixed by the analyzer during capture.

PCIe Link Speeds

For PCIe, the link speed can be set to the highest rate supported by the blade containing the ports, or a supported lower rate. Available rates for Xgig PCIe, in GT/s, are 2.5 (Gen1), 5.0 (Gen2), and 8.0 (Gen3). You can also select **Auto**, and the Xgig will select the correct speed based on the device under test, and if it cannot, it will default to 8.0 (Gen3).

Link Speeds for 10G Multi-Function Blades

No link-speed options will appear for ports on 10 Gigabit Multi-Function blades including the Xgig5000 10G Ethernet blade; the speed is fixed at 10.3125 Gbps for Gigabit Ethernet and 10.5187 Gbps for Fibre Channel and cannot be changed.

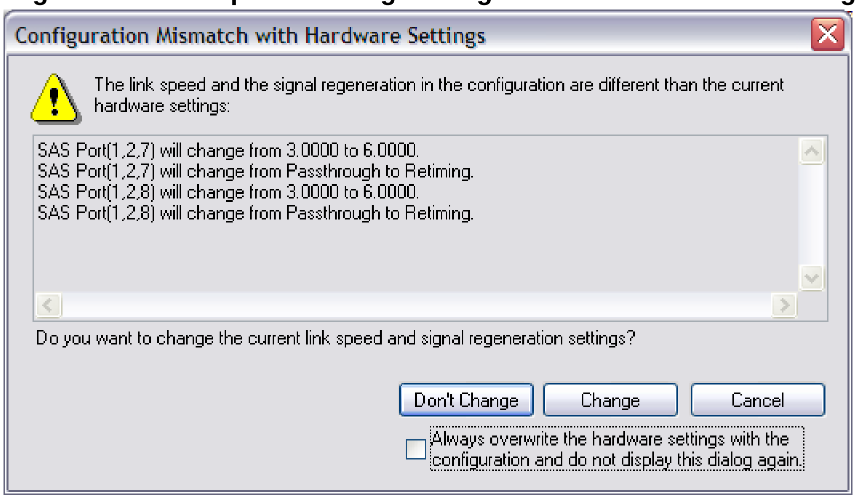
Changing the Link Speed

A warning message appears when the new settings are different than the current hardware settings. Press **Change** to proceed with the signal regeneration or link speed change and send the new configuration to the hardware. If you press **Don't Change**, the configuration in the software will be updated to reflect the current setting for the hardware. Check the **Always overwrite the hardware settings with the configuration and do not display this dialog again** to avoid receiving this warning message in the future. Use the **Options** dialog in the **Tools > Options** menu to directly set the option for this dialog box.

Warning: Changing the link speed when the signal is digitally retimed may cause data loss.

Important: When changing the link speed from 3.0000 Gbps to the “Auto SATA 6/3G” setting, a link error may occur during the speed change, and TraceControl LEDs will briefly flash red.

Figure 47: Link Speed and Signal Regeneration Mismatch Warning



Signal Regeneration

Digital signals that are received and passed through the analyzer are weakened very slightly by the optical-electrical-optical pass-through process. For most applications, the slight reduction in signal strength will not be a factor. However, for some applications, especially where the signal is passed through multiple analyzers, the reduction in signal strength can affect throughput.

To select the signal regeneration mode, follow these steps:

1. Place the cursor in the **Signal Regeneration** field.
2. Select an option.

Analyzer configuration in TraceControl gives you the option to retime/regenerate the signal at its optimum level.

Select the **Digital Retime** option in the TraceControl Configuration Editor to retransmit the signal using the analyzer's clock. Jitter is eliminated and fill characters are added or deleted in compliance with the specification of the network data.

The default option is **Analog Passthrough**. The received signal is buffered and retransmitted unmodified. The signal is amplified and link jitter is increased by <100psec. An **Analog Passthrough Multiplexed** option is available for Analog Passthrough when analyzing SAS/SATA. See “Multiplexing for SAS/SATA” on page 100.

Digital retiming is currently supported in FC, GE and SAS/SATA Analyzer ports. For SAS/SATA Analyzer ports, Digital Retime is only available for the 6G Wide-Port and Narrow Blades and the LX and LXP fixed-port systems. The Xgig5000 16G FC blade only supports Digital Retime. However, the Xgig1000 systems with 16G FC functionality support Digital Retime and Analog Passthrough, and the Xgig1000 PCIe system supports Analog Passthrough only.

The signal regeneration option is set for each port-pair or link.

Warning: Changing the signal regeneration from Analog Passthrough to Digital Retime may cause loss of data on the network.

When you have a configuration that is different from the current hardware settings, a warning message appears. Press **Change** to proceed with the signal regeneration or link speed change and send the new configuration to the hardware. Check the **Always overwrite the hardware settings with the configuration and do not display this dialog again** box to stop receiving this warning message. Use the Options dialog in the **Tools > Options** menu to directly set the option for this dialog box. See Figure 47 above.

Multiplexing for SAS/SATA

Multiplexing is only supported for analog passthrough in SAS/SATA. To analyze multiplexed signals, select the ports that have multiplexed signals and choose the **Analog Passthrough Multiplexed** option from the **Signal Regeneration** drop-down menu. This option is only available for the 6G SAS/SATA blades and systems.

SAS/SATA Multiplexing in the analyzer context means that the analyzer ports will be able to correctly interpret and decode the signal when two logical links exist within a single physical link (port-pair). The Dwords for each logical link are interleaved on the wire.

The logical links within a multiplexed signal can be analyzed as with any other link within the analyzer. For example, you can trigger or search on the data contained within a single logical link that is being transmitted within a multiplexed signal. Domains within TraceControl are still comprised of physical ports selected in the **Domain Creation Dialog** box.

Setting the **Analog Passthrough Multiplexed** option affects the **Trace Size** and **Number of Segments** options. Multiplexed signals are separated into two logical links, and therefore require twice the number of buffer segments and half the buffer size per logical port.

If multiplexing is enabled for a state machine, the ports appear in the **Ports Selection for Current Template** section of the Capture Filter and Transition Editors with a zero or a one following the port name to indicate the logical link. You can select or deselect the checkbox for a link to choose which logical link you want to trigger on.

Multiplexing options are available in Template Editor for SAS/SATA frames and primitives when you drag them into the condition boxes in the Capture Filter and Transition editors. See the “Template Editor” on page 146 for complete information.

Traffic Summary

The Traffic Summary data provides metrics for errors, OOB events, speed negotiation events, primitives, connections, transactions, ordered sets, and frames that can be used during analysis. Traffic Summary data is only supported for analog passthrough for 6G and 12G SAS/SATA and 8G and 16G FC blade ports. Check the **Traffic Summary** box for a link or port pair to generate the data. Note that you can also turn off Traffic Summary generation for all ports by clicking the TSV button in TraceControl’s main window menu bar so that it is not depressed. You can enable Traffic Summary generation for all ports that support Traffic Summary data generation by clicking the TSV button so that it is depressed.

Selecting **Traffic Summary** with the Signal Regeneration set to **Digital Retime** is not supported for SAS/SATA, and you will receive an error. However, **Digital Retime** Signal Regeneration is supported for FC. See “Using the Traffic Summary Pane” on page 336 for complete information on Traffic Summary data in TraceView.

Important: If Traffic Summary View is enabled in TraceControl and the analyzer is stopped manually, the link will be disrupted for a short time by an operation where TSV updates a file on the blade. This may cause errors.

Payload/Frame Size

The Configuration Editor window shows a field to set the length of the payload/frame to capture. This field allows you to truncate payloads/frames. Truncating payloads/frames can reduce the size of trace when you are not interested in portions of the data.

This field displays differently depending on the analyzer hardware being used. For Fibre Channel, the hardware can capture from 0 to 2144 bytes of payload. The first 28 bytes of header information is always captured for Fibre Channel, so setting the **Frame/Payload Size** to 0 will still capture 28 bytes of every frame. The length specified in this field has no effect on non-frame data such as ordered sets or errors.

For Gigabit Ethernet, the hardware can capture from 4 to 16384 bytes. The Frame Size value does not include the CRC or GE End, which are always captured with a frame.

For SAS/SATA, the hardware can capture from 4 to 16392 bytes in even multiples of four. The Frame /Payload size value includes the SOF, but not the CRC or the EOF.

For FC, the hardware can capture in even multiples of four.

For 10Gbps Ethernet, the Payload Size is in even multiples of four.

For PCIe, the hardware can capture from 20 to 8188 in even multiples of four. The default value is 4192.

If a payload/frame contains less data than specified in field, the entire payload/frame/packet is captured.

To specify the frame length, follow these steps:

1 Place the cursor in the **Payload/Frame** field.

2 Use the arrow keys to select a size, or enter a value in the field.

Number of Segments and Trace Size

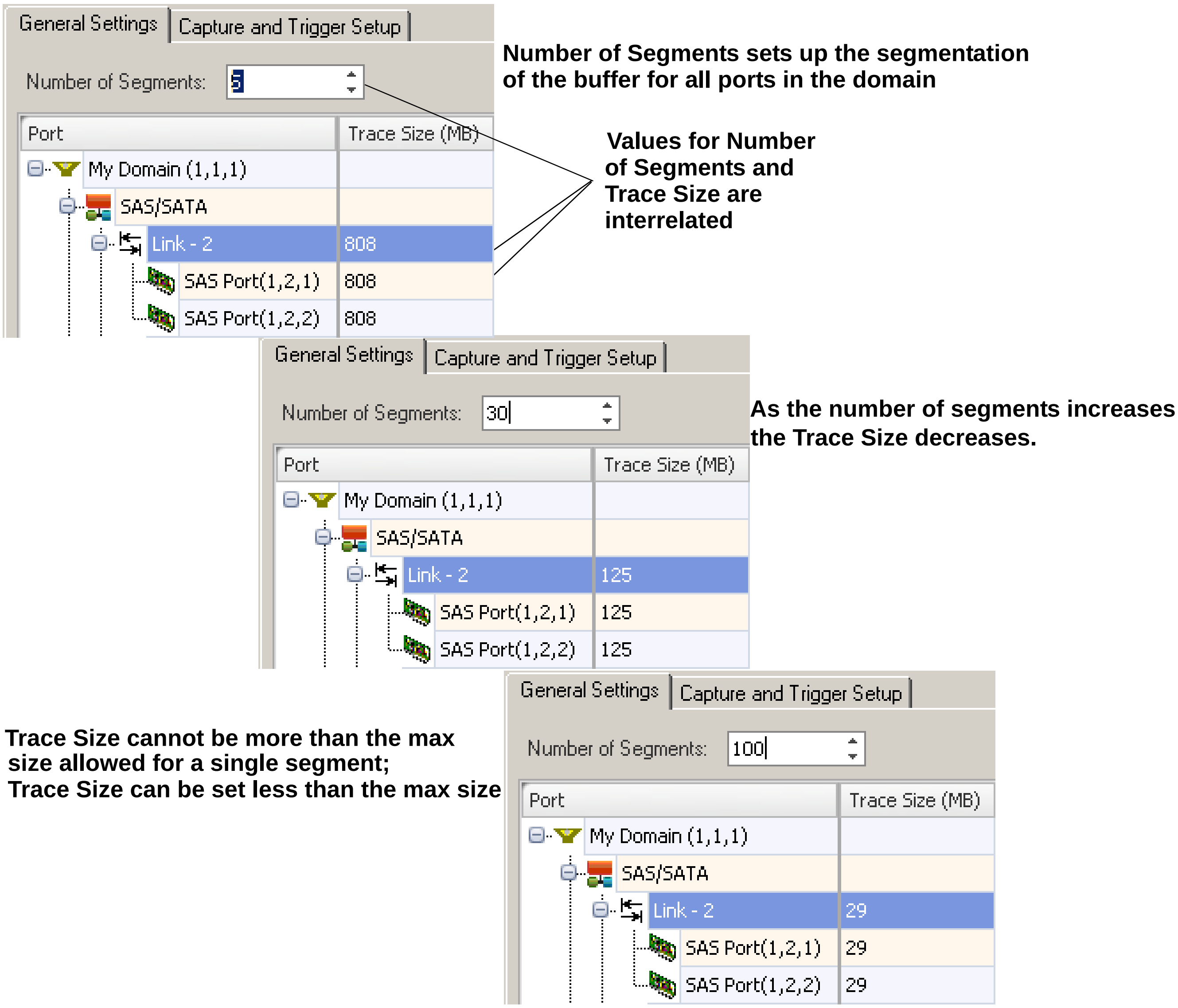
The **Number of Segments** and the **Trace Size** fields are used in buffer segmentation. The sequence of how segments are filled when capturing events is determined by the option used when you start the capture.

The hardware capture buffer on Xgig Analyzer blades can be divided into different segments. Buffer segmentation allows you to perform multiple captures within a single capture buffer. Time between trigger and restarting capture is minimized allowing you to avoid missing critical events when capturing multiple sections of information. See “Segment Capture Options” on page 139” for information on selecting a segment and segment capture modes.

The **Number of Segments** and the **Trace Size** fields are interrelated. Setting the value for **Number of Segments** determines the value for the **Trace Size**. The trace size is adjusted based on the available memory.

For example, if you select 4 as the value for **Number of Segments** and the total memory available for that port is 2GB, the **Trace Size** value will be set to approximately 500MB (note that exact value may vary slightly due to the header size).

Figure 48: Number of Segments and Trace Size



The total capture buffer memory can be divided into equal segments by specifying the number of segments or the size of each segment, and segments are numbered from 1 to **n**. The maximum number of segments is 128. The minimum size for traces is 2MB.

This same relationship between the fields exists when analyzing multiplexed SAS/SATA ports (Signal Regeneration is set to **Analog Passthrough Multiplexed**). However, since the ports contain two logical links, the maximum trace size will be half of what it would be for non-multiplexed ports. For example, if you select 4 as the value for **Number of Segments** and the total memory available for a multiplexed port is 2GB, the **Trace Size** value will be set to approximately 245MB (note that exact value may vary slightly due to the header size). The **Number of Segments** option sets the number of segments per logical link. In the case above, you have 4 segments for each logical link:
(4 segments X 2 links X 245MB Trace Size = Approximate total port memory size).

Once you have set the **Number of Segments** for the domain, you can reduce the **Trace Size** for individual port-pairs by selecting them and setting the value of **Trace Size**. For example, if the maximum Trace Size is 500MB for all non-multiplexed ports in the domain based on the Number of Segments set to 4, you can select a port-pair within the domain and set the Trace Size to 100MB.

Number of Segments

The number of segments can be set from 1 to 128. If the number of segments is set to one, a single capture buffer is used that includes all available memory. To set number of segments, follow these steps:

1. Place the cursor in the **Number of Segments** field.
2. Use the arrow keys to select the number of segments, or enter a value in the **Number of Segments** field.

All ports within a domain will have the same number of segments.

Trace Size

A trace size can be set from 2MB to the maximum memory available for the segment. To set the trace size, follow these steps:

1. Place the cursor in the **Trace Size** field.
2. Use the arrow keys to select a trace size, or enter a value in the **Trace Size** field.

You can have different trace sizes for different ports that are part of the same domain.

Scrambling

This setting applies only to the 8G Fibre Channel ports and PCIe ports. It allows you to specify whether the capture will include scrambled data. For Fibre Channel, select the ports, and check the **Scrambling** checkbox to enable scrambling. For PCIe ports, the **Scrambling** checkbox is on the **Lane Control** tab, and this setting is enabled by default.

When capturing data using analyzer ports on the new 8G Fibre Channel blade, you can set the link speed so that the capture will include or not include scrambled data. By default, scrambled data is turned on for 8.5000 Gbps captures and turned off for lower-speed captures. You must set the **Link Speed** to 8.5000 (Scrambling Off) to turn off the data scrambling feature for 8.5000 Gbps link speed. You must set the **Link Speed** to the 2.1250 (scrambling On) option to turn on the data scrambling feature for 2.1250 Gbps link speed.

When capturing data using analyzer ports on the Xgig1000 with 16G FC functionality, you can set the link speed so that the capture will include or not include scrambled data. By default, scrambled data is turned on for 8.2500 Gbps captures and turned off for 4.2500 Gbps captures.

If you toggle between the scrambling and the non-scrambling mode for the same link speed, you will not get a warning message since scrambling does not affect the data path but only how the data is written to the buffer.

FEC (Forward Error Correction)

This setting only applies to 16G Fibre Channel ports with the **Link Speed** set to 14.0250 Gbps, 10GigE ports on the 2 port 10G Multi-function Xgig blade, and 10GigE ports at all speeds on Xgig1000 systems. It allows you to specify whether FEC is enabled in the link or not. You can also set this option to **Auto**, and the Analyzer software will automatically determine whether or not the link contains FEC traffic and will capture the traffic either way. This is the default setting.

CDR (Clock Data Recovery)

This setting only applies to the 10GigE ports on the 40G Xgig1000 chassis. The CDR cleans the signal output after passing through the analyzer. This is similar to a Digital Retime, but the signal is not completely re-created. It is just cleaned and re-clocked. The default setting is off.

Note: If you are using copper cables, turning the CDR setting on prevents the training signals from passing through the analyzer. If you want training signals to come through when using copper cables, turn this setting off.

Transceiver Rate

This option is enabled only if it applies to the transceiver used by the hardware ports you have selected. For other transceivers, this option is grayed out.

For 8G Blades Only

The **Transceiver Rate** option sets how the transceiver reacts to the fiber-optic light source. The default industry standard setting may introduce errors when switching speeds. Switching rates to lower rates may introduce momentary errors during the switching process in the downstream data, even in **Analog Passthrough** mode. Errors introduced in the switching process can be avoided in **Analog Passthrough** mode by selecting the **Set rate select to “High” for all speeds**. The two options available are described below.

- **Standard -** Use industry standard setting (Rate select set “high” for the maximum supported speed by the transceiver and “low” for all other speeds).
  This setting is industry standard, and is typically used in most environments. However, this setting may result in momentary errors when speeds are switched between higher and lower speeds. A warning is displayed when the above condition is detected when you are trying to switch speeds.
- **High -** Set rate select to “high” for all speeds (Results in lower light sensitivity at speeds below the maximum supported by the transceiver).
  This setting is recommended if you experiencing momentary errors when switching port speeds. This setting will eliminate switching errors, but results in lower light sensitivity for speeds below the maximum rated speed for the transceiver. If the incoming signal is not strong, errors that result from signal attenuation may occur if this setting is used.

For 16G Blades Only

This option is only applicable to ports supporting a maximum speed of 14.0250 Gbps.

The Transceiver Rate option sets how the transceiver reacts to the fiber-optic light source. Setting the option to **High** may introduce momentary errors during the switching process from 16G to a lower rate in the downstream data, even in Analog Passthrough mode. Errors introduced in the switching process can be avoided in Analog Passthrough mode by selecting the rate select to **Low** for all speeds. The two options available are described below.

- **High** - Set rate select to “high” for the 16G fixed speed, and low for auto and all other speeds.
- **Low** - Set rate select to “low” for all speeds.
  This setting will eliminate switching errors and is the default setting.

You should use the **High** option at 14.0250 Gbps if you are experiencing errors on the link at this speed. However, note that if the link speed between your devices changes to 8G or below errors will be introduced on the link even in Analog-passthrough mode. In this case, change the setting to **Low**.

FCoE CRC Checking

Fibre Channel over Ethernet (FCoE) is the proposed mapping of Fibre Channel over selected full duplex IEEE 802.3 networks. Different versions of the protocol have different formats and different specifications for calculating the FCoE’s embedded FC-CRC value. This option allows the Xgig hardware to calculate the FCoE embedded CRC value based on the latest version of the protocol or disable calculation of this value.

Checking the check box enables selects the latest draft of the T11 standards committee specification as of this Xgig Analyzer release. Unchecking the check box disables FCoE embedded CRC calculation. When the FCoE embedded FC-CRC calculation is disabled, the analyzer will not perform any actions (for example, Trigger, Arm, or Rollback) on the embedded FC-CRC values. Also, Performance Monitor will no longer count FCoE embedded CRC error events. This check box is checked by default.

Output Voltage

These settings specify output signal voltage for Xgig 3G SAS/SATA ports.

- **High -** Standard Operation (800 - 1300 mV) (default)
  High voltage should be used for all standard SAS operations and for all standard SATA operations with later versions of SATA.
- **Low -** Margin Testing (500 - 800 mV)
  Low voltage should only be used for testing the margins cases of signal propagation or for early versions of SATA. Early versions of SATA only support a short cable length and specify this lower voltage range for signaling.

Capture and Trigger Setup

The **Capture and Trigger Setup** tab is where you define your capture filters and your transitions to capture the information you are looking for. This window consists of two panes, the overview pane and the editor pane. The editor pane has two editors, the Capture Filter Editor, which is active when you are working with a state and the Transition Editor, which is active when you are working with a transition. Use the editors to filter out the data you do not want. The overview pane lists all the capture filters and transition settings you have defined for each state or transition.

Overview Pane

The overview pane shows the entire capture as elements arranged in a flow chart. It shows the state(s) of a capture, their associated transitions, and the flow between the elements. All the states are color-coded. A state and all the transitions originating from it are the same color. Transition lines are the same color as the destination state. Depending on the trigger mode you have selected, the overview pane will contain the following elements:

- States
- Transitions
- Destination indicators
- Transition Lines
- TTL selection
- Domain Triggered
- Post Trigger Fill %
- Terminators

Figure 49: Configuration Editor

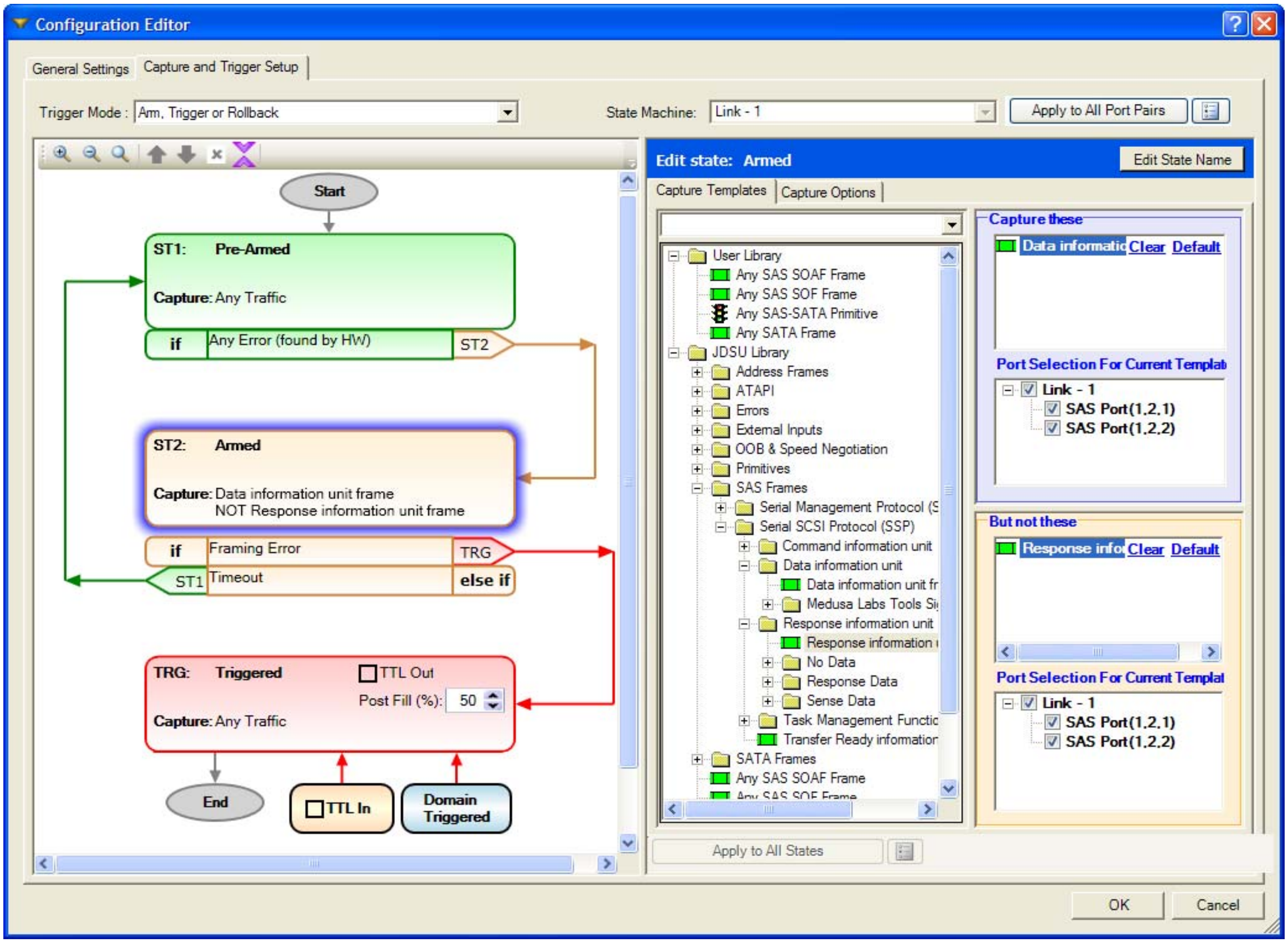
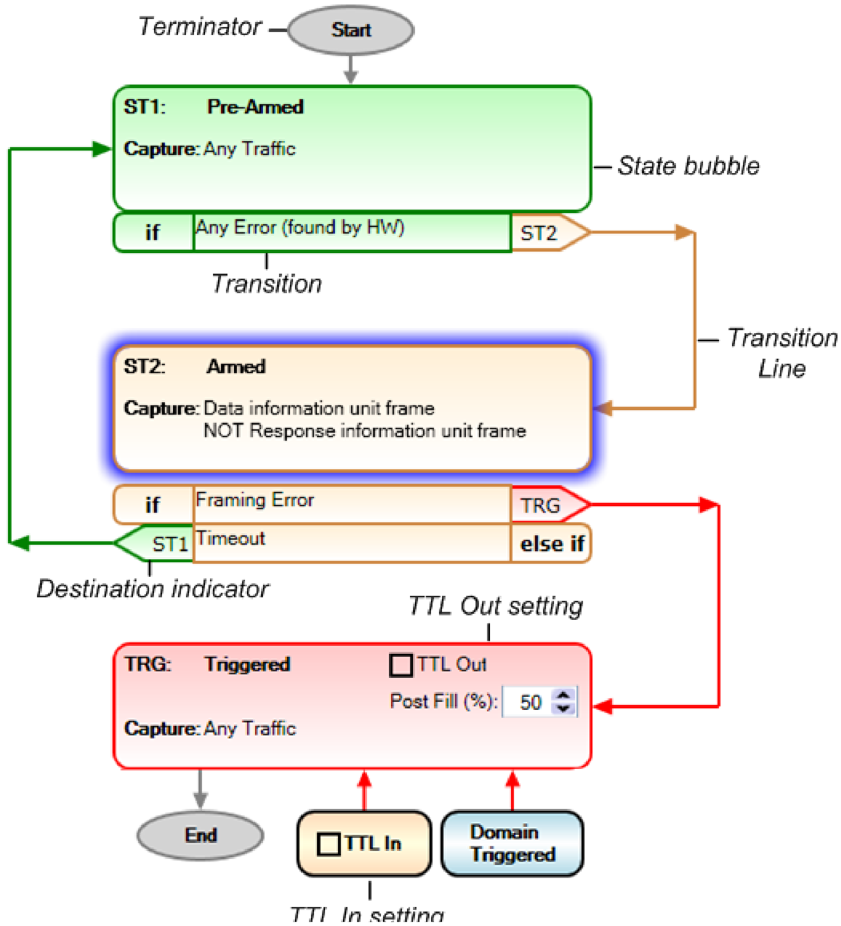


Figure 50: Overview Pane



States

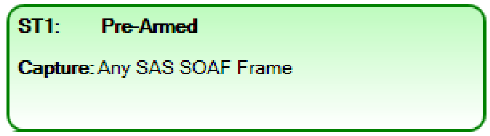
Depending on the trigger mode you have chosen, the overview can contain the following states:

- Pre-Armed
- Armed
- Pre-Triggered
- Triggered

When creating new states, TraceControl copies the capture settings from the state it is coming from into the newly created state. In case of a non-advanced trigger mode for example, going from **Stop When Buffer is Full** to **Arm and Trigger** copies the capture settings from the first state to the **Armed** state.

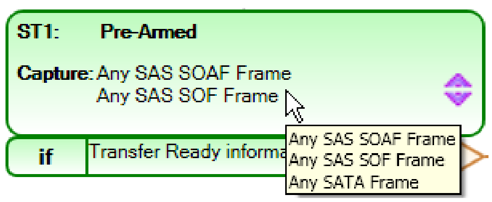
The Advanced triggering mode for 6G SAS/SATA, 12G SAS, and PCIe allows you to define additional states. See “Multi-State Triggering” on page 126 for more information.

Each state is represented by a bubble. States contain an identifier such as ST1 or TRG followed by a name. You can change a selected state's name by clicking the button next to the state's name field near the top of the editor window. This opens the **Edit State Name** dialog where you can type the new name.

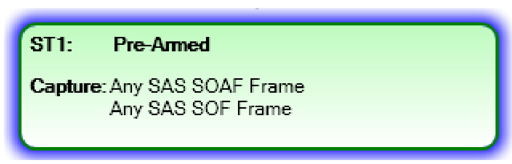


The state bubble also contains the name of the template(s) for the traffic it is capturing. These are the templates you have dragged from the **Available Templates Browser** into the **Capture These/ But Not These** panes of the Capture Filter Editor. When a state is highlighted, the Capture Filter Editor is shown in the right pane. See "Capture Filter Editor" on page 111 for more information.

As you drag templates from the **Available Templates Browser** to the Capture Filter Editor, the template names appear in the state bubble as a list. If there are more than two items in the list, a collapse/expand icon appears. Click this icon to expand the list. If a list of two or more items is collapsed, a tooltip containing the names of all the items appears when you curse over the capture section of the state bubble.



When you click a state or transition bubble, a halo appears around it to indicate it is selected.



Transitions

Each state has a transition, except the Triggered state. The transition is the same color as its originating state, as are the transition line and the destination indicator.

As you drag templates from the **Available Templates Browser** to the Transition Editor, the template names appear in the transition bubble as a list. If there are more than two items in the list, a collapse/expand icon appears. If a list of two or more items is collapsed, a tooltip containing the names of all the items appears when you curse over the capture section of the transition bubble.

When a transition is highlighted, the Transition Editor is shown in the right pane. See "Transition Editor" on page 118 for more information.

Destination Indicators

Destination indicators originate from a transition and indicate the direction of the flow to the destination state. If the destination state is below the current state in the flow chart destination indicator is on the right, otherwise it is on the left. If it is on the left "if / else if" is displayed on the right. The destination indicator has the same color as the destination state and has a label with that state's identifier.

Transition Lines

Transition Lines connect transitions to their destination states. Each transition line is the same color as its destination state.

TTL Selection

The TTL In and TTL Out selections allow you to trigger across devices. TTL Out is used to trigger another Xgig device. TTL In allows the current Xgig device to be triggered by another Xgig device. See "Triggering Across Devices" on page 134 for more information.

Domain Triggered

The Domain Triggered box indicates that there may be another port pair that could trigger, and in doing so, would trigger the current capture.

Post Trigger Fill

Post Trigger Fill defines where in the buffer the trigger should be located. For example, 25% post fill tells the hardware to set the capture window where 3/4 of the buffer contains data that occurred before the trigger and 1/4 contains the data that occurred after the trigger.

To set the post trigger fill:

1 Place the cursor in the **Post Fill (%)** field.

2 Use the arrow keys to select a post trigger fill percentage, or enter a value in the **Post Fill (%)** field.

The post trigger fill value increments corresponding to memory chunks of 512KB. For smaller capture sizes, not all percentages are available; the post trigger fill value will round up or down so the percentage fits on a memory boundary. For example, a 5MB capture can have a post trigger fill value of 80% or 90%, but not 85%. 5% of the 5MB capture is 256KB, which is smaller than the 512KB limit for the post trigger fill increment.

Terminators

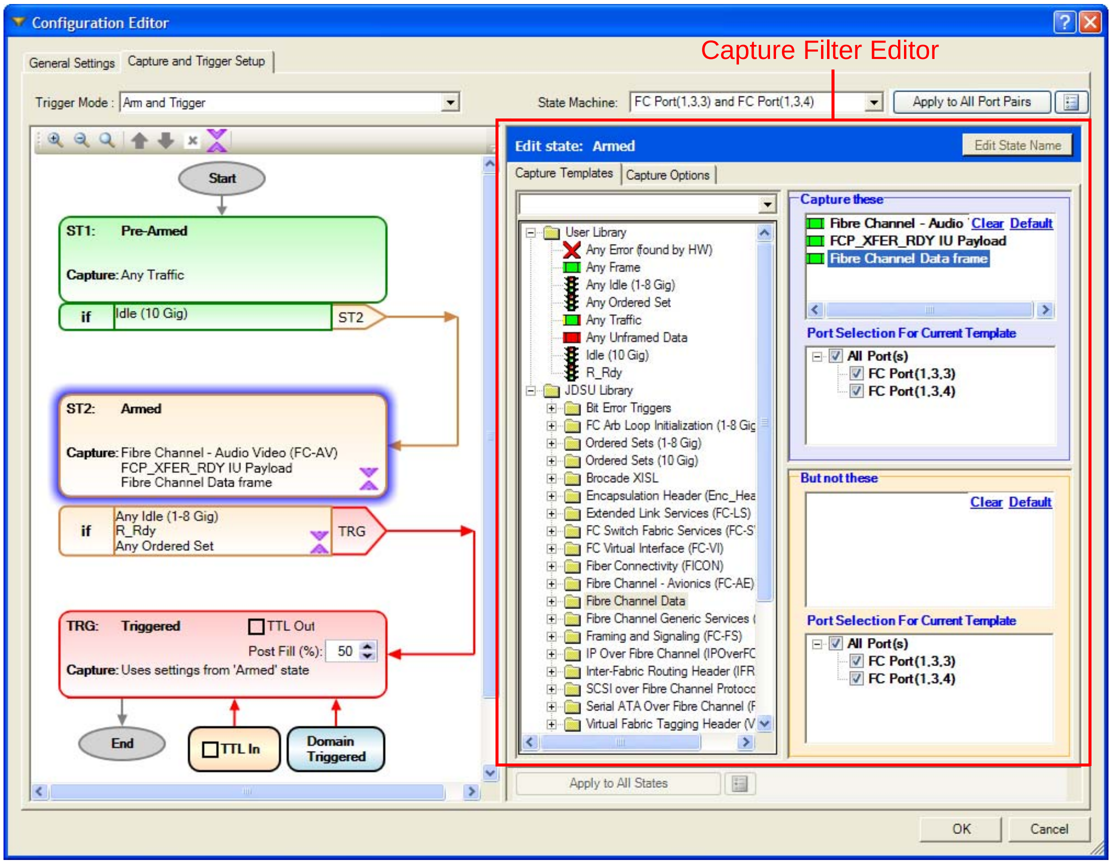
Terminators indicate the start and the end of the capture.

Capture Filter Editor

The Capture Filter Editor on the **Capture and Trigger Setup** tab is shown when you highlight a state. Use the Capture Filter Editor to specify the particular types of frames, ordered sets, or primitives you want to capture with the Xgig Protocol Analyzer.

Create capture filters by selecting a state bubble and dragging templates from the **Available Templates Browser** into the **Capture These/But Not These** panes of the editor. The **Available Templates Browser** is the area to the left of the configuration area that contains a tree structure of all available templates. See “Available Templates Browser” on page 310 for more information. As you drag the templates into the panes, the template names appear within the selected state bubble.

Figure 51: Capture Filter Editor



If the trigger mode is set to a type of trigger that allows three-state or multi-state (Advanced) triggering, you can specify different capture filters for different states.

Note: Multi-state triggering is only available for 6G SAS/SATA, 12G SAS, and PCIe. This option is not available in a mixed-port environment. All ports in a domain must be 6G SAS/SATA, 12G SAS, or PCIe for the Advanced Triggering option to be present in the Trigger mode menu. See “Multi-State Triggering” on page 126 for more information.

The Capture Filter Editor contains two panes. Drag templates into the **Capture These** pane to capture only the events that match any of the conditions in the pane. Data will be captured if any one of these conditions are met. Drag templates into the **But Not These** pane to exclude the events that match the all of the conditions in the pane. These two panes also have “Clear” and “Default” links in the upper, right corner to clear the contents of the panes or restore the list of templates to the default.

The **Ports Selection for Current Template** sections of the panes indicate which ports are in the current state machine. You can select or un-select individual ports to include in the configuration. You can select any combination of ports in the **But Not These** section. However, only 6G SAS/ SATA, 12G SAS, and PCIe allow you to have both the **Capture These** and the **But Not These** populated for any one port.

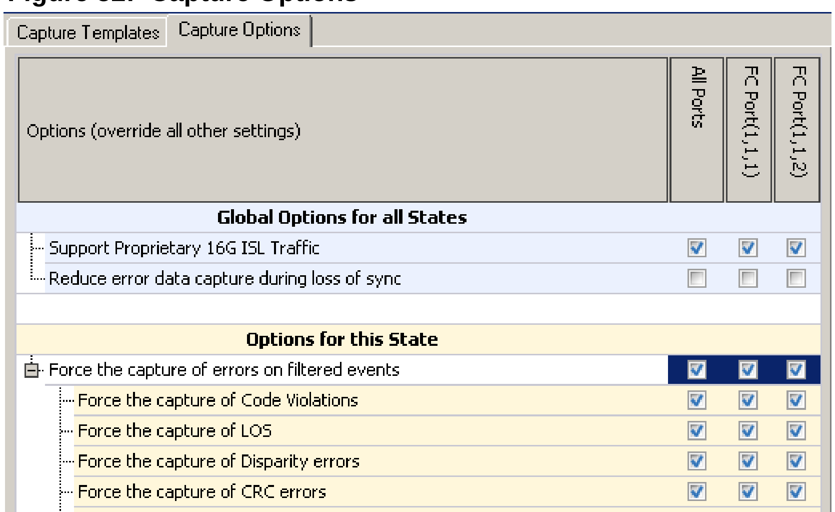
User-defined templates can be created for capture filters. Double-click a template to bring up the Template Editor. Selection and creation of templates works exactly the same way as in Xgig TraceView.

If you want to apply the capture filters in one state to all states, use the **Apply to All States**. First, highlight the state with the templates to want to apply and then click the **Apply to All States** button. The capture filters in the selected state are now listed in all states.

Capture Options

A **Capture Options** tab appears in the Capture Filter Editor for configuring capture options for all protocols. The options displayed will be different based on the protocol. Some options are global for all states while others can be set per state.

Figure 52: Capture Options



Capture Options Listed Alphabetically

The capture options are listed alphabetically in the remainder of this section.

Capture EI (when seen on all lanes)

When checked, this option forces the hardware to capture Electrical Idle (EI) when present in all lanes. Trace View shows an EI event with a repetition count. The intention is that if the DUT is in ASPM mode, you will see an EI event in Trace View when the DUT goes in L0s state instead of nothing if the errors are filtered out. The setting is set by default.

Capture Sideband Signal

This selection allows you to set up a PCIe signal to capture on. To trigger the analyzer on TTL Input, check the TTL In check box outside the trigger state bubble. Also, a sideband cable is connected from the interposer's External Trigger port to the TTL In port on the Xgig chassis.

Capture CLKREQ# - Sets Xgig Analyzer to capture the CLKRQ# signal transitions.

Capture PERST# - Sets Xgig Analyzer to capture the CLKRQ# signal transitions.

Capture PEWAKE# - Sets Xgig Analyzer to capture the PEWAKE# signal transitions.

Compress identical training frames in sequence

This option is for 16G FC traffic. Enabling this option allows compression into one rep-count event for all identical training frames coming in sequence. The training pattern is discarded in this case. Only the 32-bits of information is captured for each training frame instead of the full 36-bytes of Manchester data. You can use this option to significantly reduce the size of a transmitter training trace. This option cannot be enabled if a Training Pattern template is used as a capture filter in any state. When you use this option, TraceView's **Inspector** view only displays 32-bits of data per training frame instead of 36 bytes. However, the decodes in the **Interpretation** column are the same. This option is selected by default.

Data Compression Mode

This option is for PCIe traffic. It defines how the analyzer compresses non-frame data. The default setting is to **Compress to a count of Dwords**.

- **Store each individual Dword**
  Captures the data without any compression.
- **Compress to a count of Dwords**
  Stores identical subsequent data as a repetition count.
- **Compress to a count of Dwords including SKP, TS1 and TS2**
  Compresses the data to a repetition count as the previous setting but also compress to a single count the SKP, TS1 and TS2 even if their data can vary.

Exclude duplicate UpdateFC DLLPs

When checked, the hardware filters out of the capture any duplicate UpdateFC DLLPs that are repeated over time. The setting is set by default.

Exclude TS1/TS2, SKP and EIEOS when repeated TS1/TS2 are detected

When checked, the hardware filters out of the capture any duplicate TS1/TS2 ordered sets that are repeated over time. Duplicate SKP and EIEOS ordered sets are also filtered out.

Force the capture of errors on filtered events

The “Force the capture of” errors are listed below:

Table 5: “Force the capture of” Errors List

Force the capture of Code Violations	Forces capture of all code violations.
Force the capture of LOS	Forces capture of all occurrences of LOS.
Force the capture of Disparity Errors	Forces capture of all disparity errors.
Force the capture of CRC Errors	Forces capture of all CRC errors.
Force the capture of Primitive Errors	Forces capture of all primitive errors.
Force the capture of Multiplexing Alignment Errors	Forces capture of all multiplexing alignment errors.
Force the capture of Frame Errors	Forces capture of all frame errors.
Force the capture of Block Type Errors	Forces capture of all block type errors.
Force the capture of Control Character Errors	Forces capture of all control character errors.
Force the capture of O Code Errors	Forces capture of all O code errors.
Force the capture of Sync Errors	Forces capture of all sync errors.
Force the capture of Reserved Bit Errors	Forces capture of all reserved bit errors.
Force the capture of FCoE Embedded CRC Errors	Forces capture of all FCoE embedded CRC errors.
Force the capture of Bad OOB Pseudo Event	Forces capture of all bad OOB pseudo events.
Force the capture of Primitive Sequence Errors	Forces capture of all primitive sequence errors.
Force the capture of Logical Idle Errors	Forces capture of all logical idle errors.
Force the capture of Unknown OS	Forces capture of all occurrences unknown OS.
Force the capture of OS Errors	Forces capture of all OS errors.
Force the capture of CRC16 Errors	Forces capture of all CRC16 errors.
Force the capture of LCRC Errors	Forces capture of all LCRC errors.
Force the capture of ECRC Errors	Forces capture of all ECRC errors.
Force the capture of Poisoned TLP Errors	Forces capture of all poisoned TLP errors.
Force the capture of Undefined TLP Type Errors	Forces capture of all undefined TLP type errors.
Force the capture of Invalid H0 TLP Type Errors	Forces capture of all invalid H0 TLP type errors.
Force the capture of Message Violation Errors	Forces capture of all message violation errors.
Force the capture of Gen1-2 LOS Errors	Forces capture of all Gen1-2 LOS errors.
Force the capture of Gen1-2 Code Violations	Forces capture of all Gen1-2 code violations.
Force the capture of Gen1-2 Disparity Errors.	Forces capture of all Gen1-2 disparity errors.
Force the capture of Gen1-2 PAD Requirement Violation Errors	Forces capture of all Gen1-2 PAD requirement violation errors.
Force the capture of Gen1-2 Frame Length End Errors	Forces capture of all Gen1-2 frame length end errors.
Force the capture of Gen1-2 Misaligned SOP Errors	Forces capture of all Gen1-2 misaligned SOP errors.
Force the capture of Gen3 Loss of Sync Header Lock Errors	Forces capture of all Gen3 loss of sync header lock errors.
Force the capture of Gen3 Bad Sync Header Errors	Forces capture of all Gen3 bad sync header errors.
Force the capture of Gen3 EDS then Data Block Errors	Forces capture of all Gen3 EDS then data block errors.
Force the capture of Gen3 EDS then Wrong OS Errors	Forces capture of all Gen3 EDS then wrong OS errors.
Force the capture of Gen3 SDS then Wrong OS	Forces capture of all Gen3 SDS then wrong OS errors.
Force the capture of Gen3 No EDS before OS Errors	Forces capture of all Gen3 no EDS before OS errors.
Force the capture of Gen3 Frame Block Errors	Forces capture of all Gen3 frame block errors.

Table 5: "Force the capture of" Errors List

Force the capture of Gen3 Bad STP Errors	Forces capture of all Gen3 bad STP errors.
Force the capture of Gen3 Invalid STP TLP Length Errors	Forces capture of all Gen3 invalid STP TLP length errors.
Force the capture of EDB Errors	Forces capture of all EDB errors.

Ignore errors during Low Power States (Also affects LEDs, Counters, and State Transitions)

When checked, the hardware excludes the errors produced when a DUT goes in and out of a low power state (ASPM mode) from the capture. It will also ignore them for state transition condition, LEDs and error counter columns. The same option can be found on the Lane Control Tab. The setting is set by default.

Ignore errors during SATA Scrambled Primitive Data for Capture and Transition

This option is for SAS/SATA traffic. It specifies that errors that occur during SATA Scrambled Primitive Data are ignored. All errors on Dwords that follow the SATA Primitives, to avoid incoming Disparity Error issues are ignored.

All capture settings that refer to errors will ignore these Dwords as if they were normal scrambled data. Dwords will be captured without displaying errors in the trace. Errors will not be counted nor will they cause a state transition if they are used as transition criteria.

Limit the Force Capture of errors to lane-bound traffic only

This option is for PCIe traffic. It reduces the capture of random errors. This option is checked by default.

Out-Of-Band (OOB) and Speed Negotiation Options

The options in this section specify what OOB and speed negotiation data TraceControl should capture. The default is to capture all events. Possible options are:

- **Capture all OOB & Speed Negotiation events**
  All OOB and speed negotiation data is captured, as well as all other events. This is useful when looking for timing-related problems. This is the default value.
- **Capture only OOB & Speed Negotiation events**
  Primarily only OOB and speed negotiation pseudo events are captured. In addition, this option captures TX training frames when there is a change in the content of the training frame when compared to the previous training frame. No training patterns i.e. TRAIN, TRAIN_DONE or random training data will be captured.
- **Do not capture OOB & Speed Negotiation events**
  All OOB and speed negotiation events and data are ignored.

When using two-state, three state, or multi-state (Advanced) triggering for 6G SAS/SATA and 12G SAS, these options can be selected for different states.

Reduce error data capture during loss of sync

This option is for 16G FC traffic. This option greatly reduces the number of errored primitives captured after a loss-of-sync. It applies to 16G FC only and it is selected by default.

This option is useful when you are capturing the training sequence or during speed negotiation. It is also useful when you physically pull the fiber to create a loss-of-sync event and reconnect it to re-initialize the link.

When this option is enabled, the Xgig hardware waits for 40000 error-free consecutive ordered sets (Idle, NOS, OLS, LR or LRR) or 2 consecutive error-free Training Frame markers to get out of the loss-of-sync state. As a result, it reduces the number of errored events captured after a loss-of-sync.

When this option is disabled, the Xgig hardware synchronizes according to the standard state machine.

Note that this option only affects the capturing of errors after the loss-of-sync occurred. It does not affect the errors captured while going into the loss-of-sync state. If you physically pull the fiber to create the loss-of-sync, it is recommended to start the capture after you pulled the fiber and then reconnect the fiber. Then, you will only capture errors after the loss-of-sync state where this option is in effect to reduce the errors.

SAS/SATA Exclude Options

The options in this section specify if certain SAS/SATA primitives and errors should always be left out of the capture, no matter what is set in the Capture Filter Editor. Force capture Code Violation, for example, means that even if a Frame is set to not be captured, if it has a code violation, an event will be shown in TraceView to show the error. If you un-check these boxes, it does not necessarily mean the primitives are captured.

- **Exclude SATA_HOLD, SATA_HOLDA or SATA_R_IP**
  All SATA_HOLD, SATA_HOLDA or SATA_R_IP primitive sequences are filtered out from the capture.

Note: Captures of SATA_HOLD and SATA_HOLDA primitives are not supported in Digital Retime mode. Use Analog Passthrough mode if you want to capture these primitives.

- **Exclude ALIGNs/NOTIFYs outside OOB and speed negotiation**
  All ALIGNs/NOTIFYs that are outside OOB and speed negotiation are filtered out from the capture.
- **Exclude SAS Scrambled Idle Dwords and SATA_SYNC**
  All SAS Scrambled Idle Dwords and SATA_SYNC primitive sequences are filtered out from the capture.

Support Proprietary 16G ISL Traffic

This option is for 16G FC traffic. Some Proprietary 16G FC inter-switch links make use of ARB ordered sets and nonstandard 64/66B Transmission Words. This option enables the support of one type of proprietary ISL traffic. It is ON by default.

When random Dwords are captured

This option is for 6G SAS/SAT,12G SAS, and PCIe traffic. It specifies how to process random Dwords when random Dwords are captured. The default is to compress random Dwords to a count.

- **Store each individual Dword**
  All random Dwords generated during OOB and speed negotiation are captured and stored individually. Repeat Counts are not used.
- **Compress to a count of Dwords**
  All random Dwords are compressed into Repeat Counts.

Transition Editor

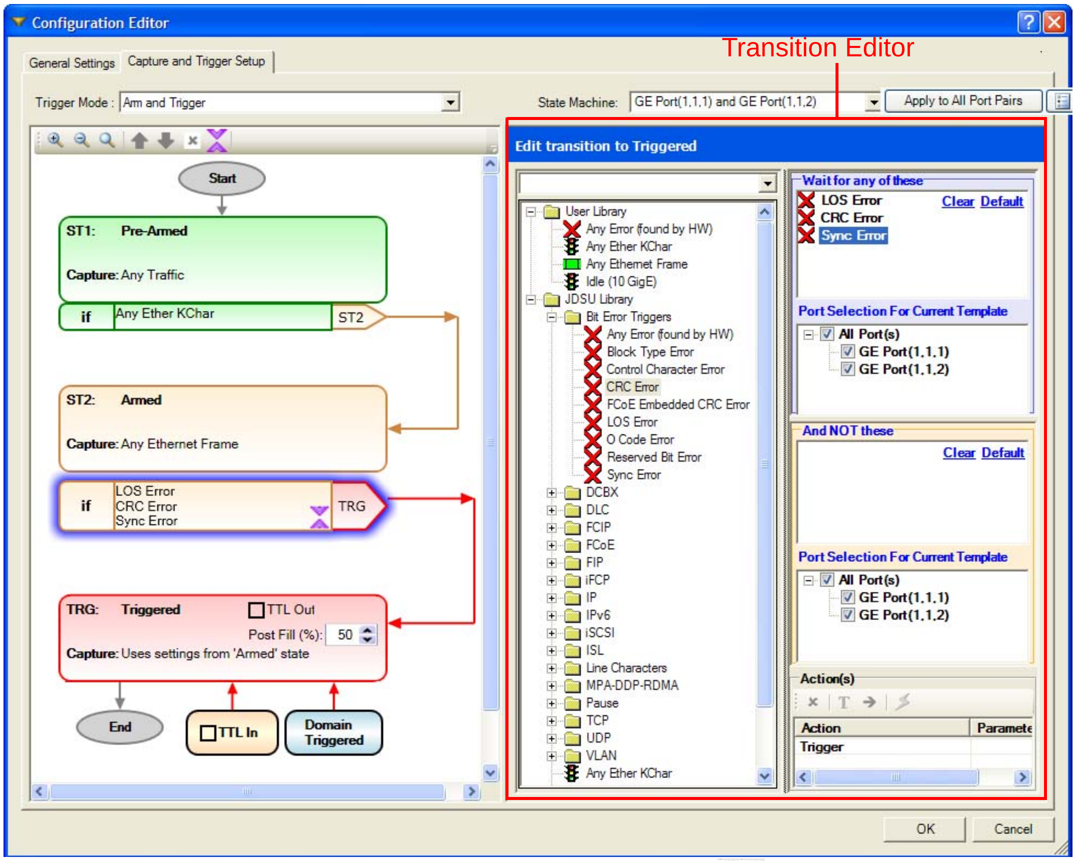
The Transition Editor on the **Capture and Trigger Setup** tab is shown when you highlight a transition. The transition editor allows you to capture the key information that you are looking for. At a minimum, you are directing the analyzer when to stop. There are many options available for determining where to set these stop points, including setting time-outs and counting events. You can direct the analyzer to take certain actions based on the contents of the data it is processing. This includes directing other analyzers to stop.

You can create transitions by using the **Available Templates Browser** to select pre-defined elements. Drag templates from the **Available Templates Browser** into the **Wait For Any Of These/And NOT These** panes to specify the transition from one state to another. The **And NOT These** pane is similar to the **Wait For Any Of These** pane, but the templates dragged here are inverted before they are compared. Only 6G SAS/SATA,12G SAS, and PCIe can use both of the panes. See "Available Templates Browser" on page 310 for more information. As you drag the templates into the pane, the template names appear within the selected transition bubble.

The **Ports Selection for Current Template** sections of the panes indicate which ports are in the current state machine. You can select or un-select individual ports to include in the configuration. You can select any combination of ports in the **Wait For Any Of These** section. However, only 6G SAS/SATA, 12G SAS, and PCIe allow you to have both the **Wait For Any Of These** and the **And NOT These** populated for any one port.

If multiplexing is enabled for a state machine, the ports appear in the **Ports Selection for Current Template** section with a zero or a one following the port name to indicate the logical link. You can select or deselect the checkbox for a link to choose which logical link you want to trigger on.

Figure 53: Transition Editor



To set the trigger condition in the hardware, press the **Apply**  button.

Note: The interface for the **Available Templates Browser** and the **Template Editor** are the same for the Capture Filter Editor and Transition Editor in Xgig TraceControl as well as for the search and find operations within the Xgig TraceView program.

You can set conditions for each state. See the specific examples in this section for information on how these conditions are used with the different triggering options.

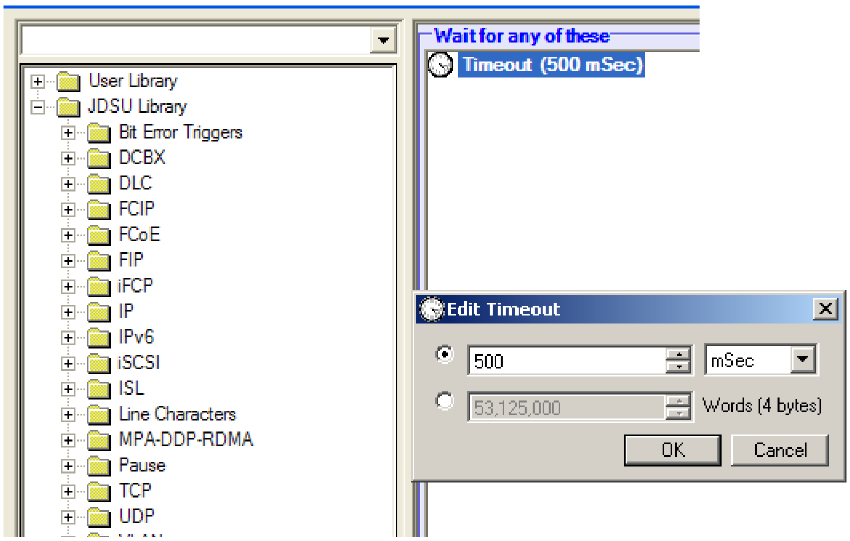
Note: If you define states whose conditions could be met too close together in time on different ports, you may capture unwanted events. For example, avoid the use of general conditions such as “any primitive” where it would cause one condition to be satisfied immediately after another.

Time-out Value

You can use the **Timeout** template in the **Available Templates Browser** when defining transitions in a configuration to set a time-out value when waiting for an event. If the time-out value is enabled when waiting for an event, the analyzer will trigger if the conditions set for the event are met or if the timeout value is reached.

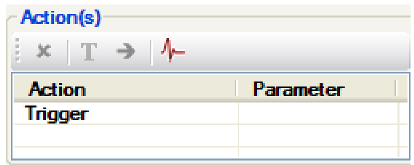
The timeout value can be a time value and/or a Dword value. When you change either value, the other changes to match the new value. To use a time-out, highlight a transition bubble, and drag the **Timeout** template to the **Wait For Any Of These** pane of the Transition Editor. Double-click the **Timeout** icon to set the value. When setting a time as the timeout value, you can choose the scale (nsec, usec, msec, sec) for the value from the drop-down menu. For Dword values, type an 8 byte value. Only one timeout value can be set per state/per port for 6G SAS/SATA, 12G SAS, and PCIe. For 16G FC blades at all speeds, you can set a timeout on arm and trigger/rollback transitions concurrently. Each timeout can have a different value. For other ports, you can only set a timeout on trigger and rollback transition.

Figure 54: Setting the Time-out Value



Actions Pane

The Actions pane in the Transition Editor defines the actions that will be performed during a transition. When a transition is highlighted, the action and its parameter are listed. For example, **Transition To State1**.



The icons in the Actions pane are only available for 6G SAS/SATA, 12G SAS, and PCIe ports. The icons are active when a transition is highlighted. If an action does not apply to the selected transition, the icon for that action is grayed out. The following action icons are available.

Remove Action This button deletes the selected item from the Actions pane.

Trigger This button designates the selected transition as the trigger.

Transition To This button allows you to select another state to transition to or create a new state to transition to.

Pulse Intra Chassis Signal Selecting Intra Chassis Signal #1 or #2 in a link sends a signal that can be picked up by the ports in another link when this transition occurs. To use this option, select a transition bubble, click the **Pulse Intra Chassis Signal** button in the **Actions** pane, and select either #1 or #2. When the transition occurs in the first link, a signal is sent out and picked up by the second link, and the two links transition in sync.

When the Pulse Intra Chassis Signal option is selected for a transition, the Action in the **Actions** pane will read “Pulse Intra Chassis Signal”.

Trigger Modes

There are six trigger modes to choose from in the **Capture and Trigger Setup** tab in the Configuration Editor. Select one of the options from the **Trigger Mode** drop-down menu near the top of the tab. The options are:

- Stop When Buffer is Full (preset trigger condition)
- Stop When Stop Button is Clicked (no trigger condition)
- Trigger (two-state triggering)
- Arm and Trigger (three-state triggering)
- Arm, Trigger or Rollback (three-state triggering)
- Advanced (multi-state triggering)

Note: The Advanced menu item is only available for 6G SAS/SATA, 12G SAS, and PCIe ports. This menu item is not visible for domains with mixed ports. All ports in a domain must be 6G SAS/SATA, 12G SAS, or PCIe for this menu item to be visible.

Stop When Buffer is Full (Preset Trigger Condition)

The **Stop When Buffer is Full** option tells the analyzer to stop capturing when the buffer is full. The flowchart in the overview pane shows one state and a decision box asking whether the buffer is full. If the answer is no, it continues capturing. If the answer is yes, the process stops. There is no trigger.

Stop When Stop Button is Clicked (No Trigger)

The **Stop When Stop Button is Clicked** option tells the analyzer to stop capturing when the **Stop** button is pressed. If the stop button is not clicked before memory is full, the analyzer buffer will wrap around. The flowchart in the overview pane shows one state and a decision box asking whether the stop button has been clicked. If the answer is no, it continues capturing. If the answer is yes, the process stops. There is no trigger. **Stop When Stop Button is Clicked** is the default trigger mode.

Trigger (Two-State Triggering)

The Trigger option has two states, Pre-Triggered and Triggered. The user can enter one transition for the trigger. Once the trigger condition is met, the capture stops unless the post fill option is set. Two-state triggers allow you to stop capture based on an event that occurs in the data stream.

You can select and define the trigger condition in the Transition Editor on the **Capture and Trigger Setup** tab. You may use any or all of the **Bit Errors** as triggers. You can trigger on an ordered set, primitive, or a frame by highlighting the Pre-Triggered state's transition bubble and dragging a template from the **Available Templates Browser** tree into the **Wait For Any Of These/ And NOT These** panes of the Transition Editor. To define a specific frame or frame type that you want to trigger on, you may drag **Any Frame** from the **Viavi Library** folder to the **User Library** folder and double-click it to change its content using the **Template Editor**. Finally, you can rename the template by right-clicking it and selecting **Rename**.

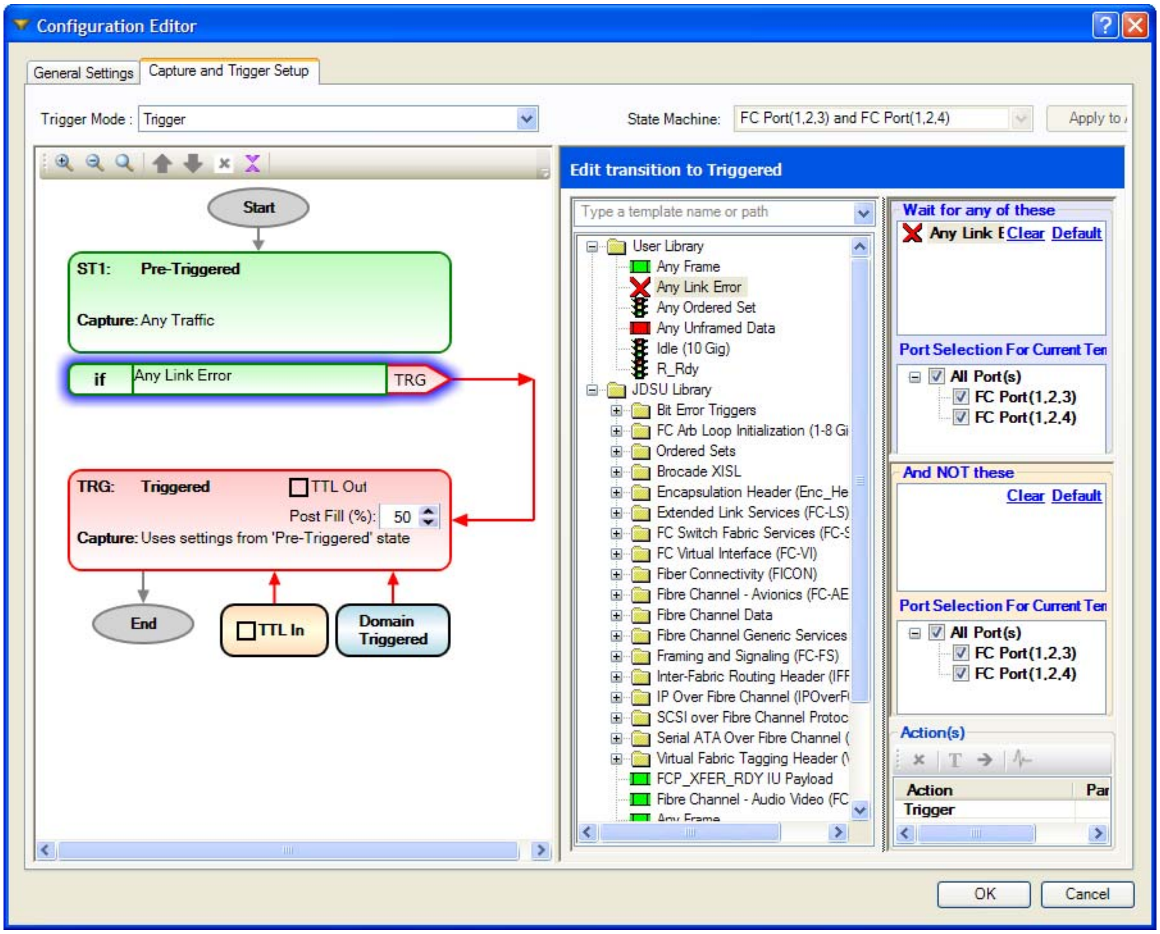
Two-State Trigger Example

In this example, when the trigger condition of **Any Link Error** is encountered in the data stream, the analyzer continues capture until the buffer is full.

The percentage of the buffer containing data immediately after the trigger event is controlled by the Post Trigger Fill setting. If the Post Trigger Fill position is set to 50%, then 50% of the buffer will contain data seen after the trigger event.

Press the **Apply**  button in the TraceControl Status window to load the configuration to the selected analyzer port(s).

Figure 55: Two-State Trigger Example



Three-State Triggering

The Arm and Trigger option has three states, Pre-Armed, Armed, and Triggered. You can define one transition to arm and another to trigger. This allows you to specify a condition for arming the analyzer and a second condition for stopping the analyzer. You can use the **Timeout** template to specify a time-out value for the Trigger.

The Arm, Trigger or Rollback option has three states, Pre-Armed, Armed, and Triggered. The user selects one transition to arm then another to trigger along with an else if transition for the rollback, which resets the capture to Pre-Armed. This allows you to set a condition that causes the Xgig Analyzer to go back to waiting for an Arm condition if the selected rollback event occurs. You can use the **Timeout** template to specify a time-out value for the Trigger or the Rollback Condition. You can use the Timer template for the Trigger or the Rollback but not both.

You can select and define trigger or rollback conditions. You may use any or all of the **Bit Errors** as triggers. You can trigger on an ordered set, primitive, or a frame by highlighting the Arm state’s Trigger or Rollback transition bubble and dragging a template from the **Available Templates Browser** tree into the **Wait For Any Of These/And NOT These** panes of the Transition Editor. To define a specific frame or frame type that you want to trigger on, you may drag **Any Frame** from the **Viavi Library** folder to the **User Library** folder and double-click it to change its content using the **Template Editor**. Finally, you can rename the template by right-clicking it and selecting **Rename**.

Three-state triggering options allow you to specify different capture conditions for pre-armed and armed states. Highlight the Pre-Armed or Armed state bubble, and drag a template from the **Available Templates Browser** tree into the **Capture these**/**But not these** panes of the Capture Filter Editor.

Three-State Trigger Example - Arm and Trigger

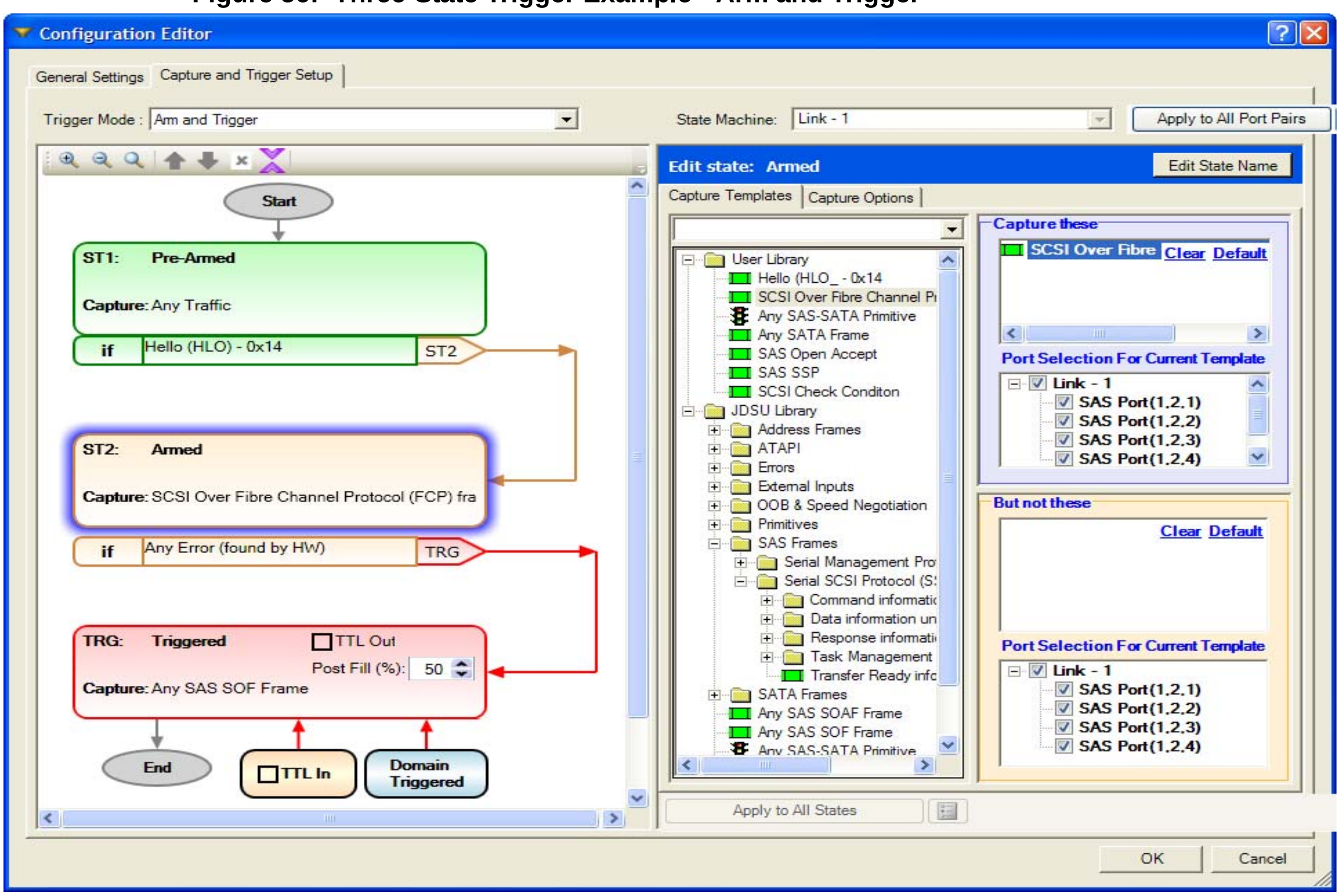
In this example, before the arm the analyzer captures **Any Traffic**. After the Hello command is seen, the analyzer will begin to capture **SCSI over Fibre Channel Protocol (FCP)** traffic. The default setting for the Pre-Armed and Armed states is to capture **Any Traffic**.

The port-pair continues to capture data until the trigger condition is met. When the trigger event of **Any Error (found by HW)** is seen in the data stream, all ports in the domain continue to capture until 50% of the buffer is filled with post-trigger data and then all ports stop.

The percentage of the buffer containing data immediately after the Trigger event is controlled by the Post Trigger Fill setting on the **Capture and Trigger Setup** tab. If the Post Trigger Fill position is set to 50%, then 50% of the buffer will contain data seen after the Trigger event.

Press the **Apply**  button to load the configuration to the selected analyzer port.

Figure 56: Three-State Trigger Example - Arm and Trigger



Three-State Trigger Example - Arm, Trigger or Rollback

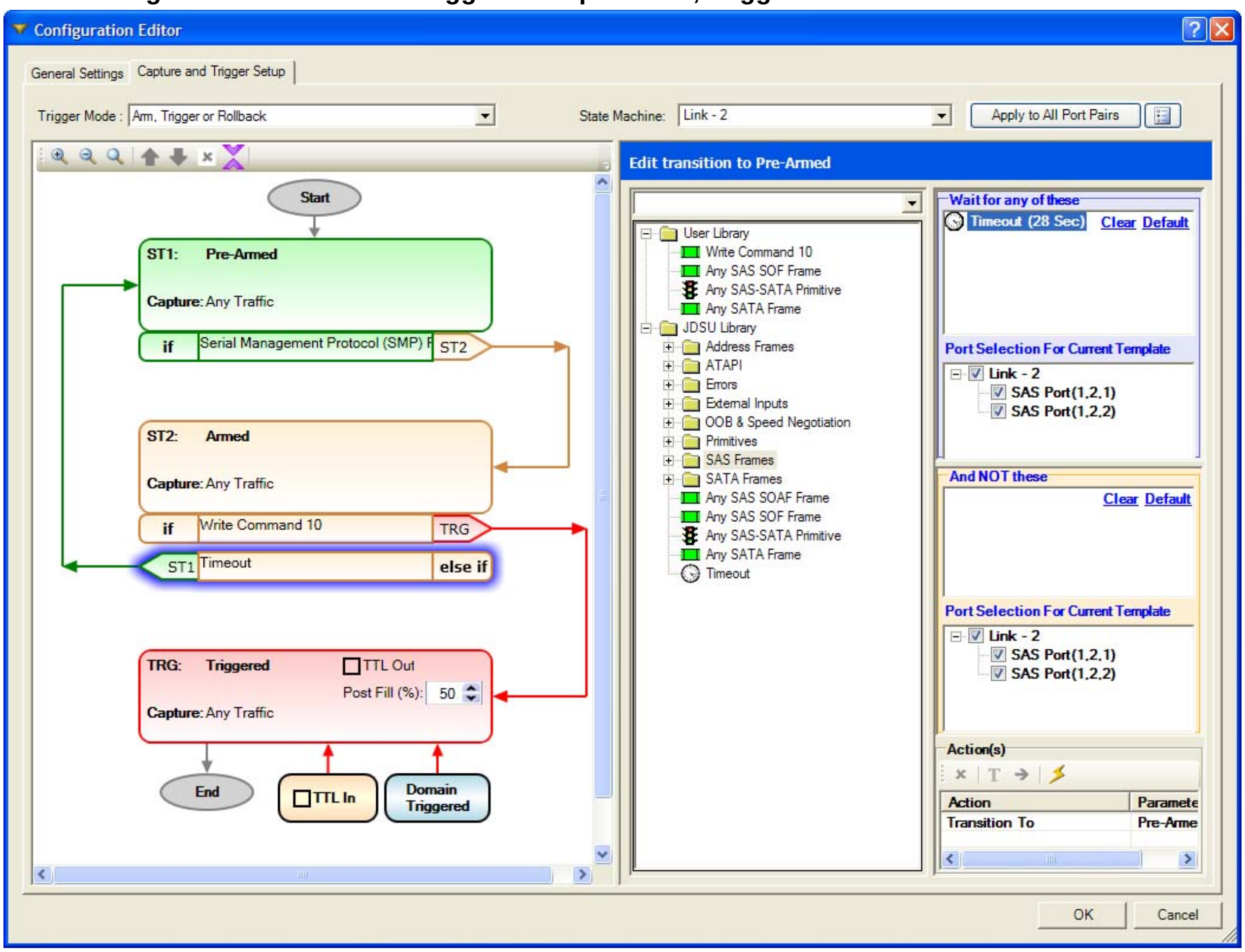
In this example, before the arm the analyzer captures **Any Traffic**. After the SMP Request Frame is seen, the analyzer will continue to capture **Any traffic**. The default setting for the Pre-Armed and Armed states is to capture **Any Traffic**.

The port-pair continues to capture data until either the trigger or rollback condition is met. If the trigger event of **Write Command** is encountered in the data stream, all ports in the domain continue capture 50% more of the trace size and then all ports stop. If the timeout of 28 sec. is reached, the state rolls back to the Pre-Armed state.

The percentage of the buffer containing data immediately after the Trigger event is controlled by the Post Trigger Fill setting on the **Capture and Trigger Setup** tab. If the Post Trigger Fill position is set to 50%, then 50% of the buffer will contain data seen after the Trigger event.

Press the **Apply**  button to load the configuration to the selected analyzer port.

Figure 57: Three-State Trigger Example - Arm, Trigger or Rollback

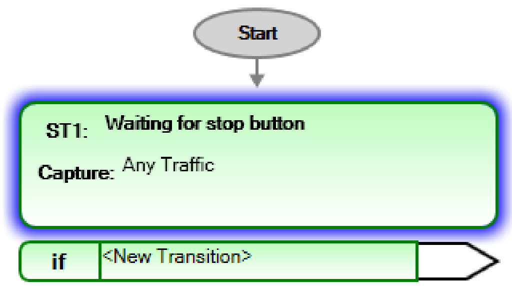


Multi-State Triggering

Multi-state or Advanced triggering is only available and shown in the Trigger Mode drop-down for 6G SAS/SATA, 12G SAS, or PCIe ports. All ports in a domain must be 6G SAS/SATA, 12G SAS, or PCIe in order to use Advanced triggering.

Using Advanced Triggering, you can create complex configurations with multiple levels. You can create states and define capture filters and transitions including rollbacks, triggers, or transitions to other states.

When the Advanced trigger mode is selected, the Overview pane shows a single state and its transition. For Advanced triggering mode, you can define up to 16 states, including the trigger, for 6G SAS/SATA and 12G SAS and up to eight states, including the trigger, for PCIe.

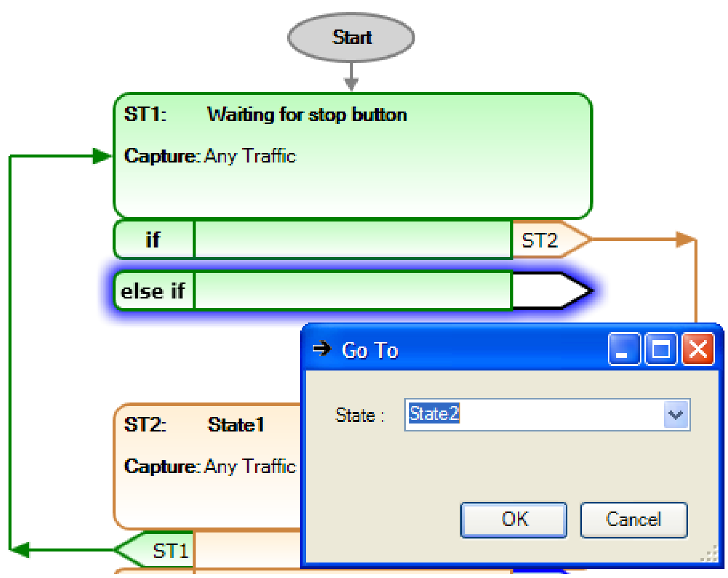


To add a state to the configuration, follow these steps.

1 Click the state’s transition bubble.

2 In the Actions pane, click .

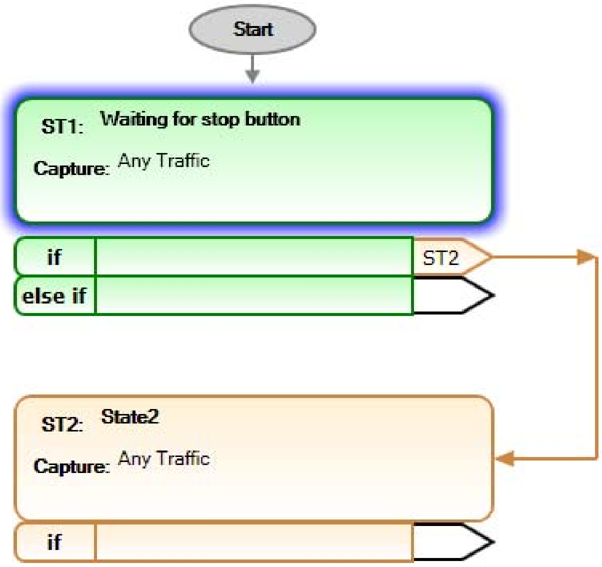
The Go To dialog appears.



3 Type a name in the state field.

4 Click OK.

The new state is created underneath the current state. The new state is a different color as are its transition bubble and transition line. This helps you distinguish it from other states.



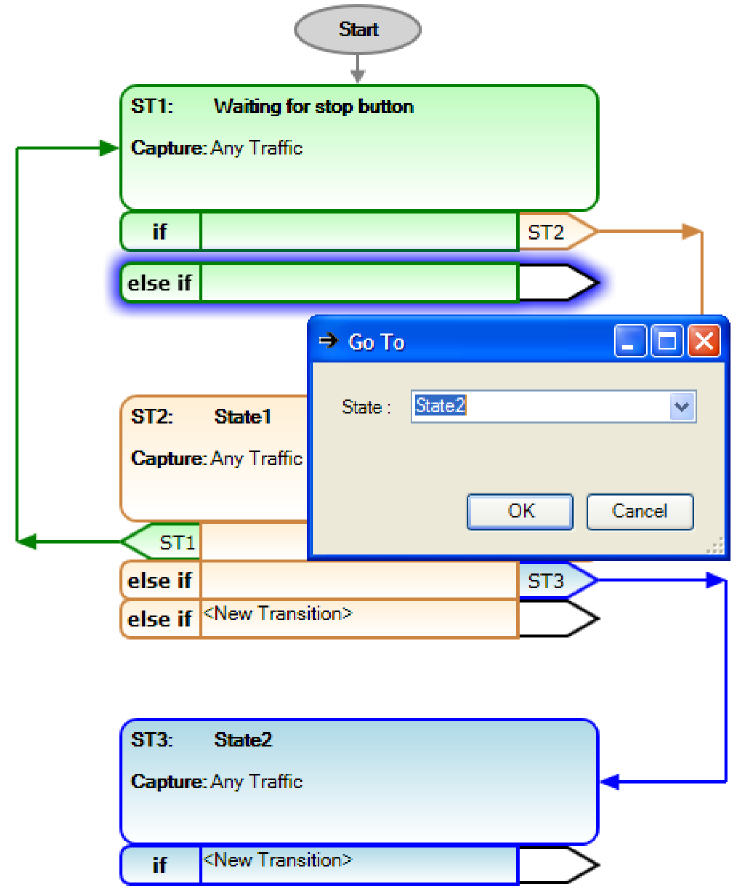
Each state can have a trigger and up to three transitions to other states.

To define a transition from one state to another, follow these steps.

1 Click the transition bubble of the state you want to transition from.

2 In the Actions pane, click .

The Go To dialog appears.

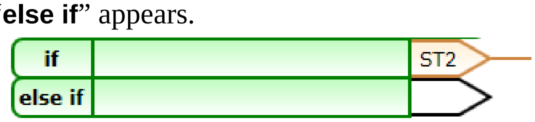


3 Select the state you want to transition to from the drop-down menu.

4 Click OK.

A transition line shows the transition from one state to the other. Notice that the transition line is the same color as the state you are transitioning to. If the state is above the current state, then the transition line is on the left. Otherwise, the transition line is on the right.

Once you define a transition to another state for the transition labeled "if", a new transition bubble named, "**else if**" appears.



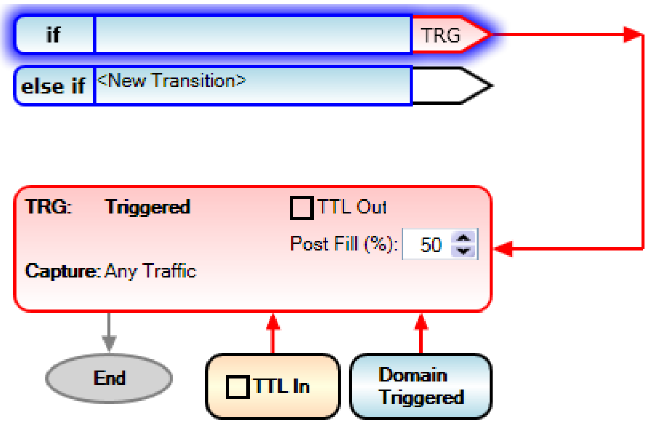
A new "**else if**" transition bubble appears each time you define a transition to another state until you reach the maximum per state of one trigger and three transitions to other states.

To create the trigger, follow these steps.

1 Click the transition bubble of the state you want to transition from.

2 In the Actions pane, click .

The Trigger appears with a transition line from the previous state to the Triggered state. The Trigger and its transition line are always red. The Trigger transition is always the first transition for a state for 6G SAS/SATA and 12G SAS, but it can be moved for PCIe.



To delete a transition, follow these steps.

1 Click the transition bubble for the transaction that contains the action you want to delete (either the trigger or a transition to another state).

The action for that transition appears in the Actions pane.

2 Click the action.

3 Click ✖ to delete the action.

Once you have created several states, you can use the arrows in the menu bar above the Overview pane to move the states up or down. You cannot move the Trigger transition up or down for 6G SAS/SATA or 12G SAS, but you can for PCIe. The Trigger is always the first transition for a state for 6G SAS/SATA and 12G SAS. If you want to zoom in or out, use the zoom and fit to window buttons. To delete an entire state from the configuration, use the ✖ delete icon in the menu bar. Note that this icon is different from the delete icon in the Actions pane, which deletes only the assigned action from a transition. To collapse or expand all the template names in the state and transition bubbles, use the collapse/expand button.

Burst Type Capture

In previous releases of Xgig Analyzer, there was a **Burst Capture Mode**, which allowed you to capture data surrounding an event. While the current software no longer supports **Burst Capture Mode**, it does include features that allow you to create the same burst effect for single burst and continuous burst.

Single Burst

To capture data in a single burst, follow these steps:

1 Select **Trigger** from the **Trigger Mode** drop-down menu. This two-state trigger includes Pre-Triggered and Triggered states.

2 Define the trigger event in the **Transition Editor**.

3 Set the post trigger fill to 100% in the trigger bubble on the **Capture and Trigger Setup** tab.

4 Select **Start Capture on All Segments from Selected to Last** from the TraceControl main window.

When the trigger event occurs, the buffer will be filled with post-trigger data. When the last segment is filled, the capture will stop.

Previous Single Burst Configurations

When using a configuration file that was created with Analyzer 4.6 or earlier using the burst capture feature for a single burst, TraceControl opens the configuration in the **Trigger** trigger mode and sets the post fill to 100%. You must select the Segment Capture Mode manually in the TraceControl main window.

Continuous Burst

To fill the buffer with a series of burst events, follow these steps:

1 Select **Trigger** from the **Trigger Mode** drop-down menu. This two-state trigger includes Pre-Triggered and Triggered states.

2 Define the trigger event in the **Transition Editor**.

3 Select the post trigger fill level you want. The default is 50%.

4 Select **Start Capture on All Segments from Selected to Last** from the Segment select drop-down menu in the TraceControl main window. To continue to wrap until the user clicks the stop button, select **Tools > Automated Options**, then select the **Restart capture after stop or saving** check box.

Previous Continuous Burst Configurations

When using a configuration file that was created with Analyzer 4.6 or earlier using the burst capture feature for a continuous burst, TraceControl uses the **Trigger** trigger mode. You must select the Segment Capture Mode manually in the TraceControl main window. You must also check the **Restart capture after stop or saving** checkbox in the **Automated Options** dialog under the **Tools** menu.

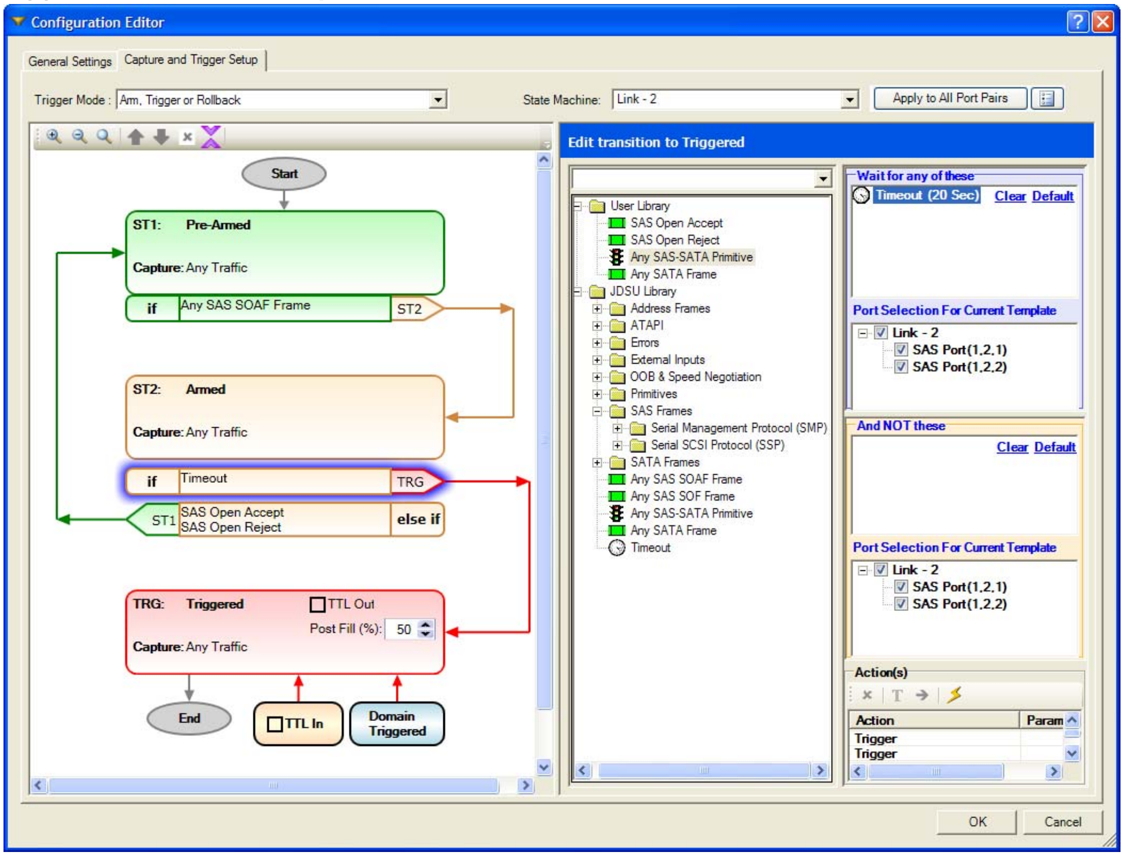
Triggering on Time-out or Within a Window of Time

The **Timeout** template in the **Available Templates Browser** allows you to capture a trace when something on the link is taking too long. Triggering within a window of time allows the user to capture if the trigger event occurs within some time interval after the arm condition. See "Time-out Value" on page 119 for information on time-out options.

Trigger on Time-out Example

In this example, the analyzer will detect an SAS SOAF frame and wait for an Open Reject or an Open Accept. If neither response occurs within 20 sec, the analyzer will trigger, fill up the buffer and stop. If an Open Reject or an Open Accept does occur before the timeout, the analyzer will reset and start looking for the next SAS SOAF frame.

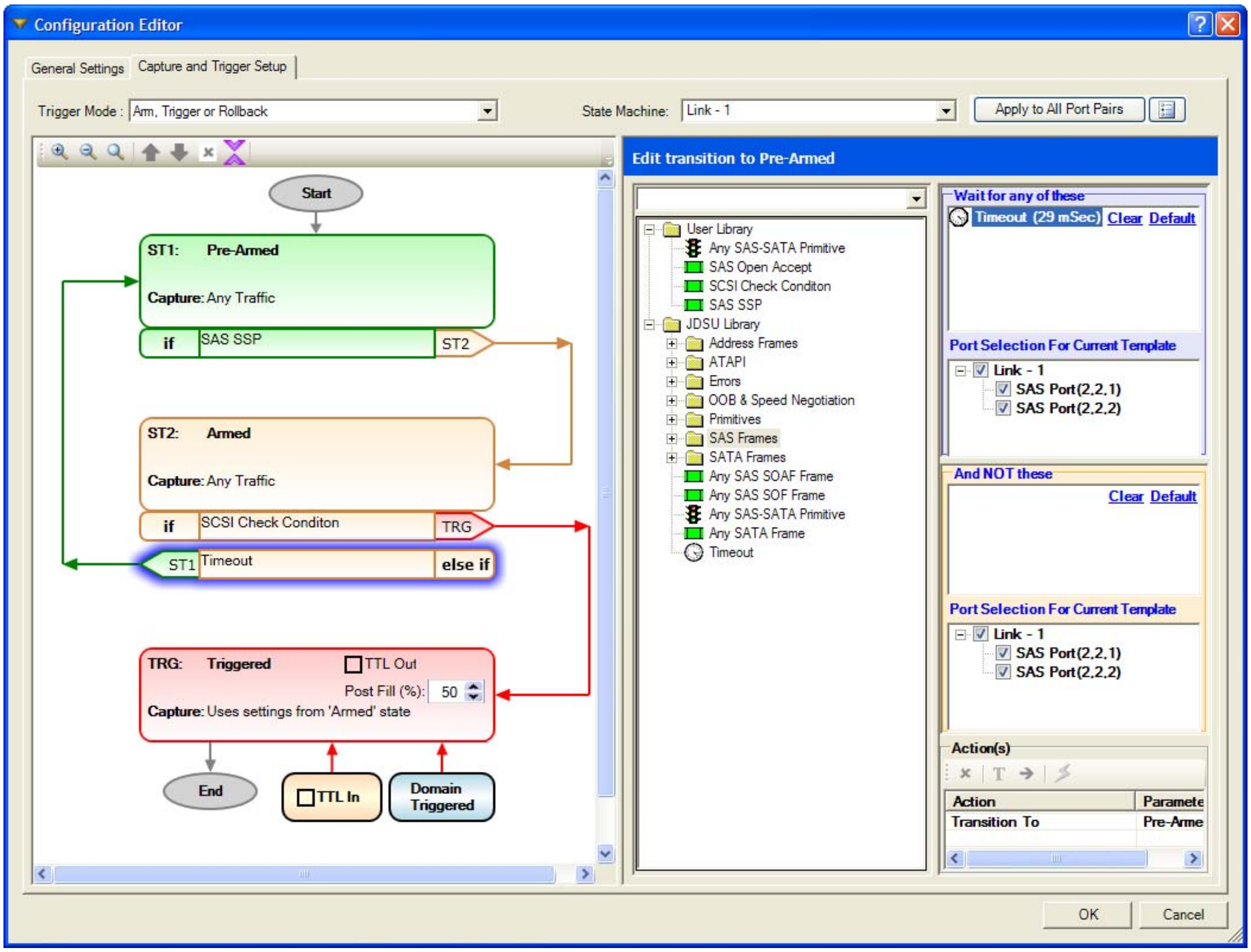
Figure 58: Trigger on Time-out Example



Trigger Within a Window of Time Example

In this example, the analyzer will detect a SAS SSP Command and look for a Check Condition. If the Check Condition does not occur within 29 milliseconds after the Command, the analyzer will reset to looking for a SAS SSP Command. If a Check Condition does occur before 29 milliseconds, the analyzer will trigger, fill up the buffer and stop.

Figure 59: Trigger Within a Window of Time Example



Triggering with Mixed Ports

When any one of the conditions specified in the **Wait For Any Of These/And NOT These** panes of a transition to trigger is encountered in the data stream, the analyzer triggers all ports in the domain and continues capture until the Post Trigger Fill is complete.

Figure 60: Mixed Ports in a Domain

An example is a mixed port domain where the FC ports in one port pair are configured with a trigger. When the trigger condition is encountered in the FC port-pair, all ports in the domain capture until the buffer post-fill operation is complete regardless of their protocol.

Ports are configured by state machine. You can apply the configuration of the current state machine to all state machines for that protocol and blade type by clicking the **Apply to All Port Pairs** button in the **Capture and Trigger Setup** tab.

Note: The only protocols that allow a state machine to be applied to blades of another type are FC and SAS/SATA. 2G, 4G, or 8G FC configurations can be applied to one another's state machines. 2G, 4G, or 8G FC configurations can be applied to a 16G FC state machine, but a 16G FC configuration cannot be applied to other FC state machines. 10G FC cannot be applied to an FC blade of another speed.

3G SAS configurations can be applied to 6G and 12G SAS/SATA state machines, but 6G and 12G SAS/SATA configurations cannot be applied to a 3G SAS/SATA state machine.

To define values for a setting for the ports in link or domain simultaneously, select the link or domain field for that setting (column) in the **General Settings** tab of the Configuration Editor, and choose the value. That value is now applied to all applicable ports for that field. Fields for ports for which the value does not apply are grayed out. For example, in a mixed port domain of FC and GE ports, the Scrambling setting only applies to the FC ports, and the GE ports in that column are grayed out. See "General Settings" on page 93 for more information.

Triggering on Any SCSI Error

A common requirement for a SCSI trigger condition is to trigger on any error, either in the SCSI protocol or at the physical layer. Viavi supplies configuration files that set the conditions to trigger on any SCSI error for either a switch or loop configuration. These configuration files are a composite of many different templates within the Viavi Library. The default configuration files to trigger on any SCSI error are:

- Trigger on Any SCSI Error in Loop.tcc
- Trigger on Any SCSI Error in Switch.tcc

To open either of these configurations, select **Load Configuration...** from the **File** menu and select the configuration file.

Note that within the Viavi Library there is a template that you can apply called **Any Link Error**. This template specifies only physical layer errors (such as CRC errors, Loss of Signal Errors, code violations, and disparity errors). Use one of the configuration file templates listed above to set a trigger on all SCSI errors.

Triggering Across Devices

The Xgig Analyzer can be triggered by or can trigger an external device. Trigger in and out is performed through the TTL ports.

BNC and MCX Trigger Connections

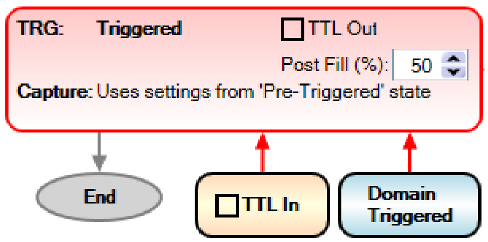
All Xgig chassis have a TTL Input and a TTL Output port. A physical connection between two systems can be established. The Xgig uses a BNC cable. The Xgig5000 and Xgig1000 use an MCX cable.

To use a chassis as the sending device, you must connect the TTL Output port of the chassis sending the external trigger to the receiving device. To use a chassis as the receiving device, you must connect the TTL Input port of the chassis receiving the external trigger to the sending device.

Caution: Improper connection of BNC or MCX input and output cables can cause serious damage to the system. Please double-check to make sure that the TTL Input port and TTL Output port of an Xgig analyzer are properly connected to other analyzer devices or blades.

Xgig as the Output Device

The TTL output can only be sent when the analyzer triggers. Checking the TTL Output checkbox inside the Trigger state bubble will cause the analyzer to send a pulse through the TTL Output port when the trigger condition for the analyzer is met.



See “Select TTL Out” on page 42 for information on using the Domain Creation dialog box to set up the TTL Output pulse.

Xgig as the Input Device

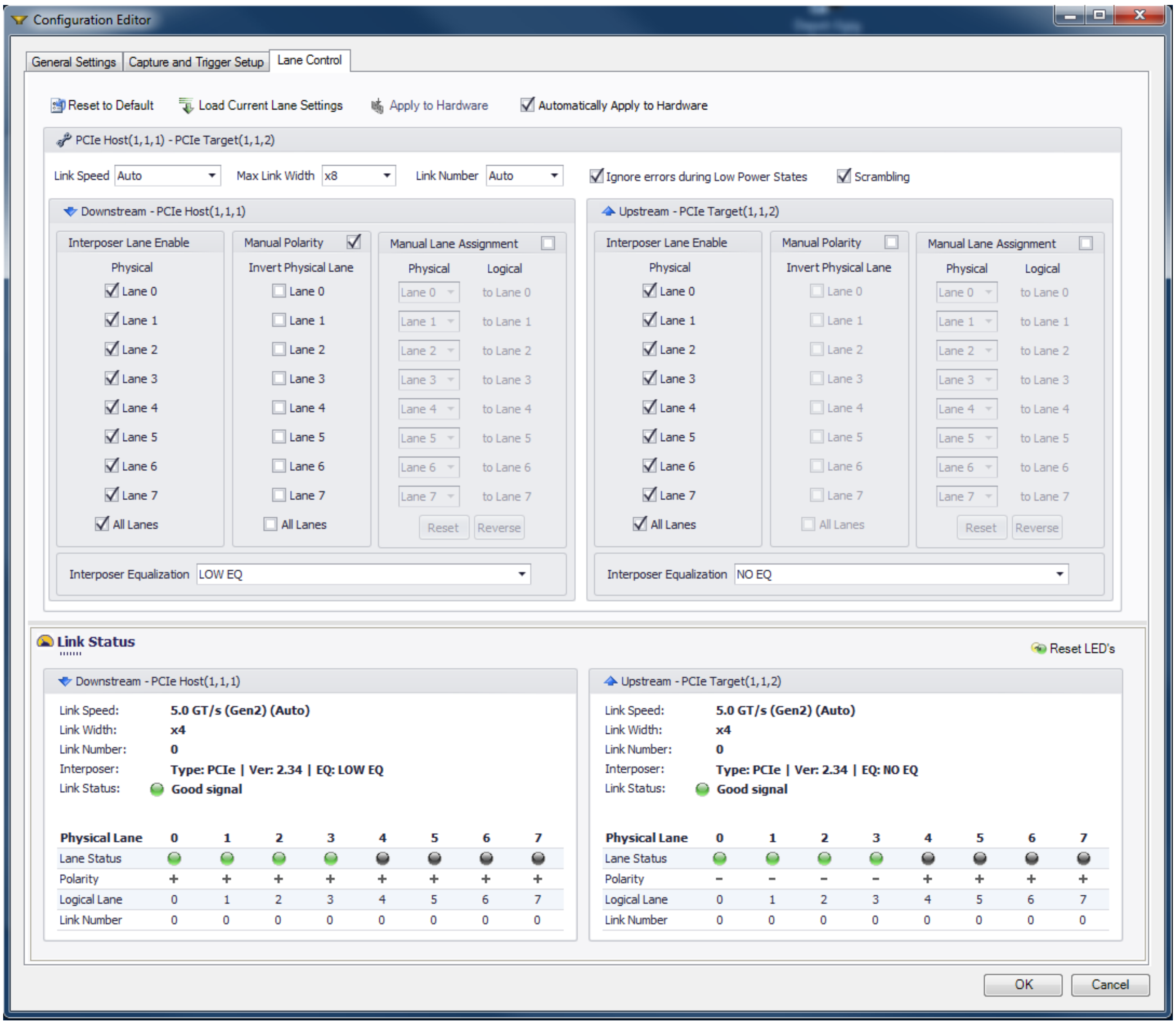
To trigger the analyzer on TTL Input, check the TTL In check box outside the trigger state bubble. See “Select TTL In” on page 42 for information on using the Domain Creation dialog box to set up the TTL Input pulse.

Lane Control

The **Lane Control** tab supports the lane control features for PCIe. This tab is only visible if a PCIe port is in the domain.

The **Lane Control** tab contains two panels. The top panel shows the link and individual lane configuration settings. The bottom panel, labeled Link Status, shows a real-time status of the link and lanes.

Figure 61: Lane Control Tab



The top panel displays the port pair configuration controls side-by-side. If there are more than one port pairs in the domain, they are shown below, and a vertical scroll bar appears. Above the port controls there are three buttons and two check boxes. With the exception of the **Reset to Default** button, they are only enabled if the domain is locked.

The **Reset to Default** button sets all link and lane settings to their default values.

The **Load Current Lane Settings** button retrieves the current hardware settings and loads them in TraceControl.

The **Apply to Hardware** button sends and applies the current link and lane settings to the hardware.

The **Automatically Apply to Hardware** checkbox enables automatic send and apply of the link and lane settings when you modify a value of any settings.

The **Link Speed** drop-down menu is a duplicate of the **Link Speed** drop-down menu in the **General Settings** tab.

The **Max Lane Width** drop-down menu allows you to choose from x1 to x8. This is the maximum lane width the hardware will detect and the default if it does not see any training sequence. Depending on the width value, the number of enabled lane assignment **Physical Lane** drop-down controls will change. The drop-down menu is only enabled on the first port of the pair since both ports have the same setting.

The **Link Number** drop-down menus allow you to manually enter a link number or select **Auto**. Since the hardware supports only one link number, the **Auto** mode takes the lowest value found.

The **Ignore errors during Low Power States** checkbox allows the hardware to exclude from the capture the errors produced when a DUT goes in and out of a low power state (ASPM mode) when enabled. It also ignores them for state transition condition, LEDs and error counter columns. You may adjust the lane settings to get clean Green LEDs. The setting is enabled by default. See “Ignore errors during Low Power States (Also affects LEDs, Counters, and State Transitions)” on page 116.

The **Scrambling** checkbox allows you to specify whether the capture will include scrambled data. This option is enabled by default.

The **Interposer Lane Enable** checkboxes allow shutting down physical lanes when unchecked. This feature is required in order to allow the chassis to interoperate with x1, x2 or x4 PCIe cards installed in the interposer. The motherboard will see all eight lanes as “enabled” because the interposer has all eight lanes populated. If the interposer does not power down lanes that are not present on the card, then the motherboard will try to communicate with PCIe card lanes that do not exist. This is known to cause issues on some Operating System/Motherboard combinations. The default is that all eight lanes are enabled. Please note that turning off a physical lane also shuts down the lane between the host and the device under test.

Note: When supporting Xgig Jammer for PCIe, the interposer row in the Link View displays a message that the port is connected to Jammer and the Lane Enable check boxes and EQ drop-down in the Lane Control tab are disabled on the port that is connected to the Jammer.

The **Manual Polarity** checkboxes allow you to control lane polarity. To manually control lane polarity, check the checkbox. When the box is unchecked, the lane polarity is automatic. In this case, the **Invert Physical Lane** checkbox group below is disabled. These checkboxes give control over the lane polarity. Each of the eight motherboard uplink and downlink PCIe lanes can be independently assigned to have inverted polarity for dealing with devices under test that the auto-detection scheme does not work with. This is a pre-capture configuration option only. The lanes cannot be polarity inverted post-capture. The default is all unchecked.

The **Manual Lane Assignment** checkboxes allow you to assign lanes. To manually control assign lanes, check the checkbox. If the box is unchecked, the lane polarity is automatic. In this case, all the controls in the lane assignment group below are disabled. For automatic lane assignment, the hardware detects the physical to logical lane assignment transmitted during link negotiation for properly functioning devices under test. When you select manual lane assignment, you can manually set the lane mapping using the drop-down menus. Each of the eight motherboard PCIe lanes can be assigned to a single logical uplink or downlink lane for the firmware capture logic in the pre-capture configuration. The lanes cannot be remapped post-capture. The **Reset** button at the bottom of the lane assignment group resets all the lane assignment drop-down menus to a direct mapping of the lanes. The **Reverse** button reverses the mapping of the lanes (physical lane 7 is mapped to logical lane 0 and so on).

The **Interposer Equalization** drop-down menus allow you to select the Interposer EQ file. These menus are populated with the files available on the server. By default, there is no selection and the field is blank. Select a setting from the drop-down menu. This setting is disabled if you are not connected to the domain. The selection is saved in the `.tcc` file.

If the EQ field is blank, the system does not know the current interposer EQ setting. If the EQ field is not blank, then that EQ setting matches what is currently configured on the interposer. The interposer will reload default settings (matching the "default" **Interposer Equalization** drop-down menus) when the interposer is powered up.

The bottom panel shows the **Link Status** view. This panel is shown in the **Lane Control** tab and in the Port Status view in Trace Control’s main window. This panel displays the real-time status of the link and lanes currently detected by the hardware. The top table shows the status related to the link: Speed, Width, Number and Status. The Status LED is the same as the B/W LED in the Port Status view. The LED displays red for the same errors. Text is added to report the errors seen on the link or other information message about the system. The top table also shows the Interposer settings such as interposer type, firmware version loaded on the interposer, and the current equalization selection.

The bottom table in **Link Status** view shows status per physical lane. The Physical Lane row displays the lane number. The Lane Status row has LEDs per lane. The LED is red if there are LOS, Code Violation, Running Disparity, or Logical Idle errors detected for the specific lane. The LED is gray if the ports are not connected or if the lane is shut down by the **Interposer Lane Enable** setting. The LED is black if the lane is in electrical idle. The LED is yellow if there has been error in the past but it is now a good signal. The LED is green if the signal is good. You can mouse over the LED to display a tooltip with the current status for the lane.

The Polarity row displays “+” if the lane has a normal polarity. It displays “-” if the lane polarity is inverted. The Lane LEDs will flash Green (or Yellow) if Electrical Idles and Ordered Sets are detected.

The Logical Lane row displays the logical lane number that the physical lane was assigned to. See the **Lane Assignment** control in the top panel of the tab.

The Link Number row displays the link number assigned to the lane by the host system.

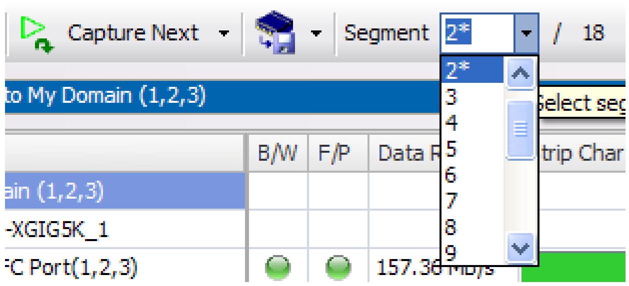
The **Reset LED’s** button resets the previous error flag and turns the yellow LED to a green LED if the signal is good. This setting also applies to the Port Status view LEDs in TraceControl’s main window.

Segment Capture Options

Selecting a Segment

The segment number to start with is specified in the **Use Segment** field in the TraceControl main window. The choices available in the **Number of Segments** field are only updated when the configuration is applied to the hardware. For example, the previous user had 2 buffer segments for the domain. Assume you change the number of segments to be, yet do not apply the configuration to the hardware; the **Use Segment** field will only show that 2 segments are available.

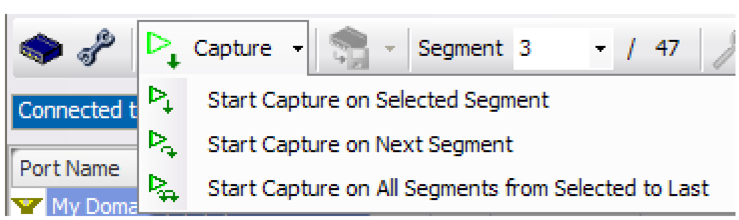
The segment numbers that can be selected in the field is determined by the value of the **Number of Segments** field for the selected domain. If a segment contains capture data, an asterisk will appear next to the number of that segment. For example if you have four segments and segment 2 has data, the drop down list will appear as follows:



The buttons for bringing up analysis applications (TraceView, Expert, or Surveyor) will be grayed out if the current segment does not contain a valid trace. Also, the capture time in the status bar indicates the capture time for the current segment, not the capture time for all segments.

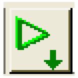
Segment Capture Mode

Different start modes are available when using buffer segmentation. The modes are selected from a drop-down box next to the **Start** button. The **Start** button will appear with a different icon depending on the mode selected. When TraceControl is started, the last mode used for capture will be the current mode. The modes available are described below along with the Start button icon that appears when the mode is selected.

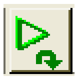


Segments are independent from one another. Each contains one capture with its own start and stop time.

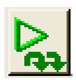
A warning message is displayed before you start a capture that will write data into a segment that has unsaved capture data. A warning message also displays if you change the number of segments in the **Number of Segments** field and the current segments have captured data. If the option **Do not show this warning again** is checked in a previous appearance of either message, the message will not display.

 **Start Capture on Selected Segment**

This capture mode uses the current segment for capture. Once the segment is full, the capture stops. This is the default mode. Note that starting a second capture in this mode will overwrite the data from the first capture in this same segment.

 **Start Capture on Next Segment**

This capture mode works similar to the mode above, but advances the capture to the next segment before starting capture. Once the segment is full, the capture will wrap within the segment or stop, depending on the trigger mode. Note that starting a capture after all segments are full will overwrite capture data, starting with the first segment used for capture.

 **Start Capture on All Segments from Selected to Last**

This capture mode captures in the current segment, and the capture will wrap within the segment until the capture is stopped. After capture is stopped in this segment, TraceControl will automatically switch to the next segment and start a capture again and wait to be stopped. This sequence of captures ends when the last segment has stopped or when the user clicks on the **Stop** button. Note that starting a capture in this mode will overwrite any data in all segments from the current segment to the last segment.

Note that the **Start Capture on All Segments from Selected to Last** mode is not valid when you are in a trigger mode that requires the stop button to be pushed (**Stop When Stop Button is Clicked (No trigger)**. For this condition, the capture is started in the selected segment and you MUST click the **Stop** button to stop the capture, and the **Stop** button will also stop the sequence of captures. If you select one of this invalid combination, a message will appear to notify you that the configuration must be changed.

Examples of Using Segmented Capture Buffer

The examples below will help you see some of uses and advantages of segmenting the capture buffer.

Tracking a Frequent but Intermittent Drive Error

Assume you need to capture all instances of a SCSI Check Condition that occur over time. For instance, a drive may be reporting Medium Errors or Recovered Errors and you want to track down the exact I/O stream and LBA location that caused each one of them. The segmented buffer allows these instances to be captured back-to-back without missing critical events between captures. Without the Segmented Capture Buffer feature, you would need to capture/save/repeat in a script. The time required to save and re-start capture can miss critical instances of the trigger; having segmented buffers absolutely minimizes the time between trigger and re-start capture.

For this application, you might use the **Start Capture on All Segments from Selected to Last** mode and divide the capture buffer into many segments.

Debugging an Intermittent Loss of Sync

As another example, it may be difficult to track down the cause of a SAS/SATA device losing sync (LOS error), especially if such a problem happens infrequently for unexplained reasons. You would likely walk in after a few hours, see that the LOS error had occurred, and the entire trace buffer would be filled with errors. Your first action would probably be to set a trigger for coding and disparity errors to see all the events that led us to the LOS; however, there are also several conditions where a coding/disparity error might cause a LOS, yet these events would not be relevant to your analysis. These errors might happen at rare instances for a variety of reasons, and the system can recover from them by retransmitting the frame – these are not the LOS error you are looking for. You might spend hours taking a trace, only to see later that the error captured has nothing to do with the LOS issue you are trying to correct.

One way to work towards finding the LOS issue would be to segment the buffer. Now you can automatically take several traces over a prolonged period of time for coding/disparity errors. If one of the traces does not demonstrate the LOS condition you are looking for, the next trace on a separate segment might.

Issues that Have Several Symptoms or Several Possible Diagnoses

Sometimes a particular issue seems to have several symptoms, or you might have several hypotheses on its cause based on the result of several unique occurrences. If the error happens infrequently, you can take several traces automatically and see if the events leading up to the error are the same for each instance of the error.

Compare and Contrast Like Events

For example, you may have a problem where a reset event happens at unexpected times. You could segment the buffer to take multiple traces, and capture instances of both scheduled and unscheduled resets. You could then easily compare the different resets within the TraceView decode display.

Chapter 5

Template Browser/Template Editor

In this chapter:

Template Browser

The Viavi and User Template Libraries are located in the **Available Templates Browser** pane in TraceControl's **Configuration Editor**.

Available Templates Browser

The **Available Templates Browser** is a hierarchical display of templates in the Xgig TraceControl **Configuration Editor**. It functions like Windows Explorer, allowing you to view and create a hierarchical structure for templates. You can name, rename, open, or move templates/folders within the **User Library** section. Double-click an editable template to change its contents with the Template Editor. The names of the folders in the Available Templates Library in TraceControl and TraceView are shortened by default. There is a context menu that allows you to display the longer versions of the folder names.

The **Available Templates Browser** is context-sensitive in TraceControl. For example, if you are configuring at SAS/SATA ports, only templates that apply to SAS/SATA ports will display in the Available Templates Browser.

There are templates that are a set of underlying frames/primitives/errors instead of a single frame/primitive/error. These template names start with the word "any". **Any SAS/SATA Primitive** refers to all primitives within the SAS and SATA protocols. For example, **Any SAS Broadcast** refers to any of the SAS broadcast primitives, as there are multiple primitives of this type. Note that the **Any Link Error** template for SAS/SATA includes all SAS/SATA errors except Primitive Sequence Errors. Primitive Sequence Errors have their own template.

There are four types of templates:

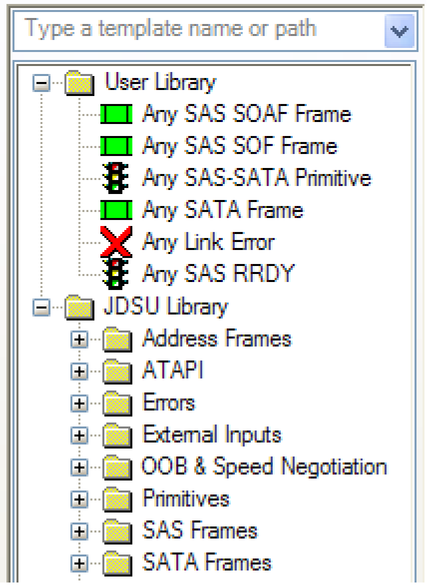
Frames or packets
Frames or packets as defined by the protocol being used.

Primitives, Ordered Sets or Training Frames, Sequences, and Patterns
Control primitives that are sent outside the frame or packet structures within a protocol, for example, ordered set information for the Fibre Channel protocol, and 16G FC training frames, sequences, and patterns.

Errors
Recognized error conditions within the data stream reported by the protocol.

Unframed data
Data that cannot be interpreted as any of the three other types. This is data that does not conform to the physical protocol.

Figure 62: Available Templates Browser Example



Pre-Defined and User-Defined Templates

Two types of templates are available from the **Available Templates Browser**, pre-defined templates and user-defined templates. Pre-defined templates are found in the **Viavi Library** section. User-defined templates are found in the **User Library** section. The **Viavi Library** section is read-only; pre-defined templates cannot be changed or deleted. You cannot move templates into this section, rename templates, change templates, or change the structure. You can drag templates from the **Viavi or User Library** to the **Capture these** and the **But not these** panes when defining the capture settings for a state, and you can drag templates from these libraries to the **Wait for any of these** and the **And NOT these** panes when defining trigger settings for a transition.

User-defined templates are created by the user. They can be identical to the pre-defined templates available in the **Viavi Library**. The **User Library** section can store the templates you use most often, identified by names you create.

You can define unique templates that are not available in the **Viavi Library**. User-defined templates are typically created using a pre-defined template as a starting point. Add the values, patterns, and qualifiers to create a unique template. Double-click any template in the **User Library** section to bring up the **Template Editor.** Use the editor to create and store user-defined templates. Once you have created and saved a user-defined template, you can access it from the **User Library** area of the **Available Templates Browser**.

The templates you create in the **User Library** will also be available from the **Available Templates Browser** in Xgig TraceView. When you create a new template, it is strongly suggested that you copy the template and rename it. This prevents confusion resulting from changing the contents of a template without changing the name.

Creating a New Folder in User Library:

1 Click **User Library**.

2 Right-click to view a pull-down menu. Select **New Folder**.

3 Type a name for the new folder.

Dragging a Template from Viavi Library to User Library:

1 In the **Viavi Library**, select a template. For example, **SCSI Frames**.

2 Drag selected template to the folder you created in **User Library**, and drop it**.**

Apply a Template for Capture or Trigger:

1 Click a state or a transition in the overview pane.

2 Select a template.

3 Drag the template to one of the panes in the Capture Filter Editor, and drop it.

Template Editor

You can create custom templates through the **Template Editor**. Customized templates can be applied as conditions for a capture or trigger setting in the **Capture Filter Editor**. A custom template can be based on a primitive or a frame. Error templates are not editable.

A **Template Editor** dialog box appears when you double-click any template in the User Library section of the **Available Templates Browser**, or, any editable template that has been dragged to one of the panes for a capture or trigger setting. The editor uses the template you have selected as the starting point for creating a new template. There are two template editors, the **Standard Template Editor** and the **LAN Conversation Frame Editor**.

The **LAN Conversation Frame Editor** provides an easier method of including addresses and ports in a template for Ethernet frames. This editor is launched automatically when you double-click the LAN Conversation template, which is only available when using GigE ports.

After you have made all your selections to create the new template, press **OK**. It is suggested that you always rename a new template you create. You can store your new template in any location in the **User Library**.

Standard Template Editor

Creation of templates works exactly the same way as in Xgig TraceView; however, certain functions such as port filters, counter filters, and “match anywhere” filters in Xgig TraceView are not available in Xgig TraceControl. The options in Containing or Qualifiers tabs do not display.

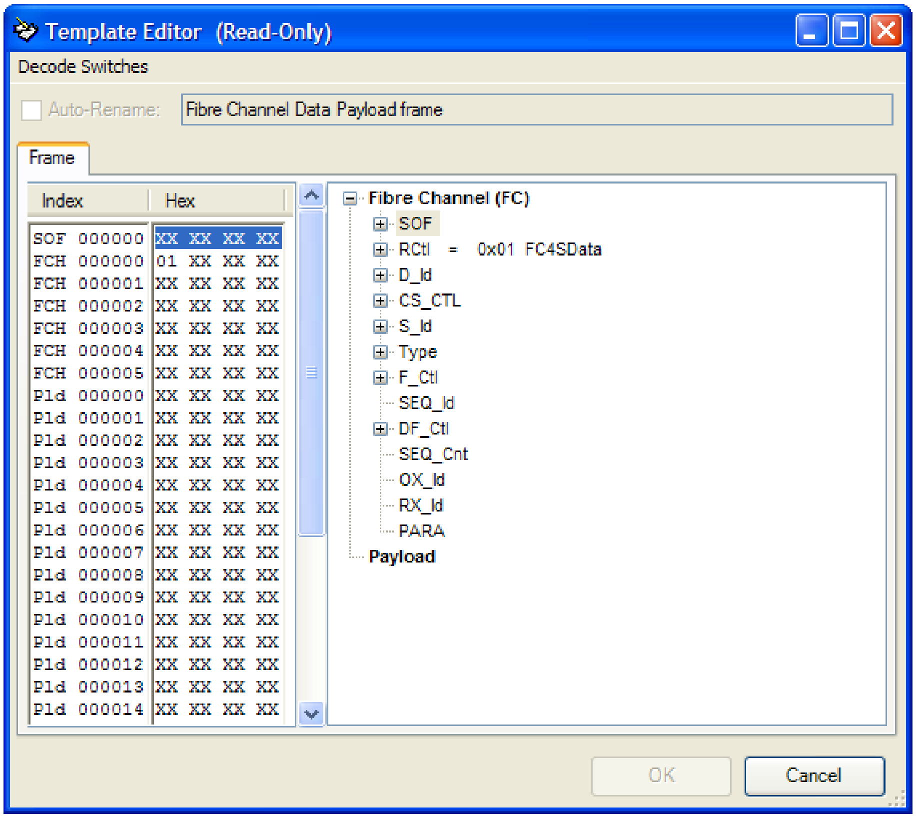
The Template Editor contains an Auto-Rename check box. Enabling this feature allows the Template Editor to generate an appropriate name based on edits the user makes.

For templates used as transitions, the Template Editor provides a counter that allows the user to specify the number of times the event must occur. It is available only for Error, Frame, Primitive and OOB templates for the 6G SAS/SATA, 12G SAS, and PCIe blades and Frame templates for 16G FC blades, at all speeds, in the **Wait for any of these** pane. For example, setting the counter to three on a CLOSE primitive will wait for the third CLOSE primitive before transitioning to the next state.

The types of changes you can make with **Standard Template Editor** to create a new template are:

- **Frame Byte-Pattern Definitions**
  To change the byte contents of the frame template, select the desired field strings on the right from the tree structure. The values in the hex display on the left will change. You can also enter hex values (or Xs for “don't care” bits) directly into the offsets on the left. An example of editing the frame byte-pattern for the Fibre Channel Data Payload frame template is shown below.

Figure 63: Template Editor, Edit All SCSI Frames Template



- **Ordered Set Byte-Pattern Definitions**
  To change the byte contents of a traffic ordered set (FC or GigE), select the type from the pull-down menu. You can also enter hex values (or Xs for “don't care” bits) directly into the fields.

- **Bit-Pattern Definitions**
  Bit level definitions are possible by double-clicking on a byte within a template for a frame, which brings up the Binary Editor. Click the bit in the **Binary Editor,** type in the new value, and click **OK**.

- **Primitives**
  To change the hex values of a primitive, you can either type directly into the field or you can double-click the field, which brings up the **Binary Editor**. To change a bit in the **Binary Editor**, click the bit, and type a new value, then click **OK**.

- **Primitive Group Selection**
  Some SAS/SATA primitive templates (names that start with “**Any**...”) define a group of primitives. The Template Editor allows you to select or de-select individual primitives to exclude or include them in the group.

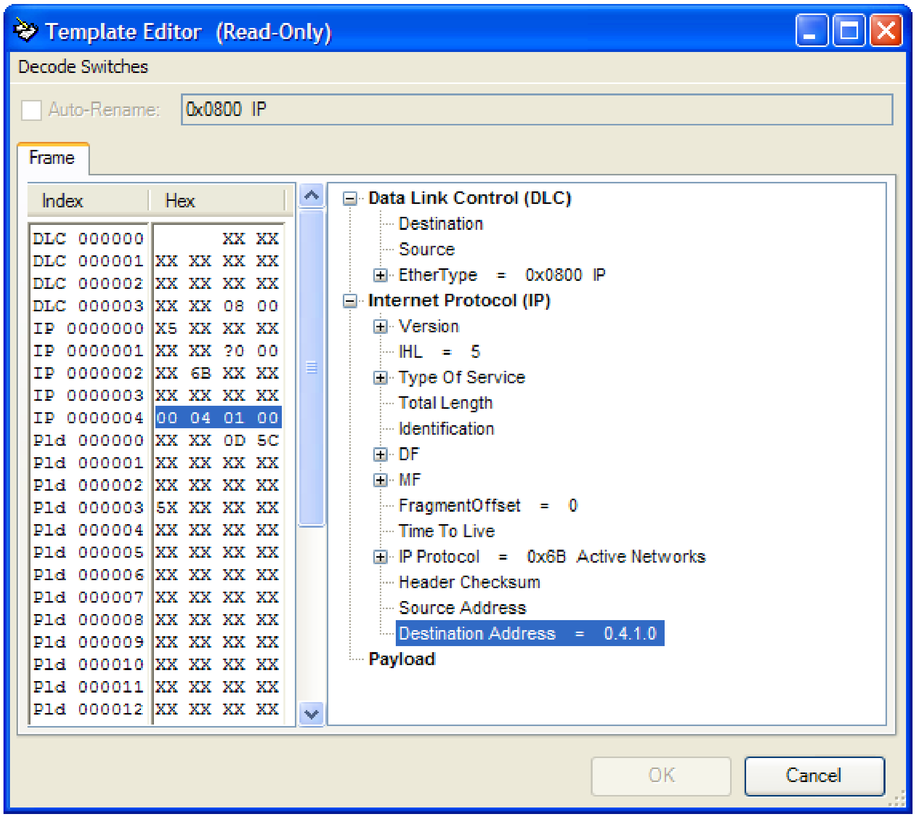
In-Place Field Editing

For editable fields, context menu selections or function key selections allow you to edit the value for field. There are three ways to initiate in-place field editing in the Tree View: press the F2 key, select **Edit** from the context menu, or click the field once to select it, and again to initiate in-place editing. In-place editing can be very useful for fields where the general format is not hexadecimal. For example, IP addresses can be entered in IP dotted notation rather than translated to hexadecimal for direct entry in the byte pattern. Figure 64 shows in-place editing for an IP address.

The context menu displays when you right-click a node in the Tree View. The menu contains some or all of the following options, depending on the current item selected:

- **Edit**
  This menu item is only available on editable fields. Select **Edit** to directly edit the field value in Tree View (the area on the right in the display). The field format can be hexadecimal, decimal, an IP address, etc.
- **Reset**
  This menu item is only available on editable fields with an equals (=) sign and a value associated to them. It allows resetting the value to don't cares (XXXXX) in the match buffer.
- **Description**
  This menu item is available for all fields and displays a detailed description for that field.
- **Font**
  This menu allows you to control the font for that field.
- **Alias**
  This menu allows you to add, delete one or all, or manage aliases for that field.

Figure 64: Example of In-Place Editing to Change the IP Address

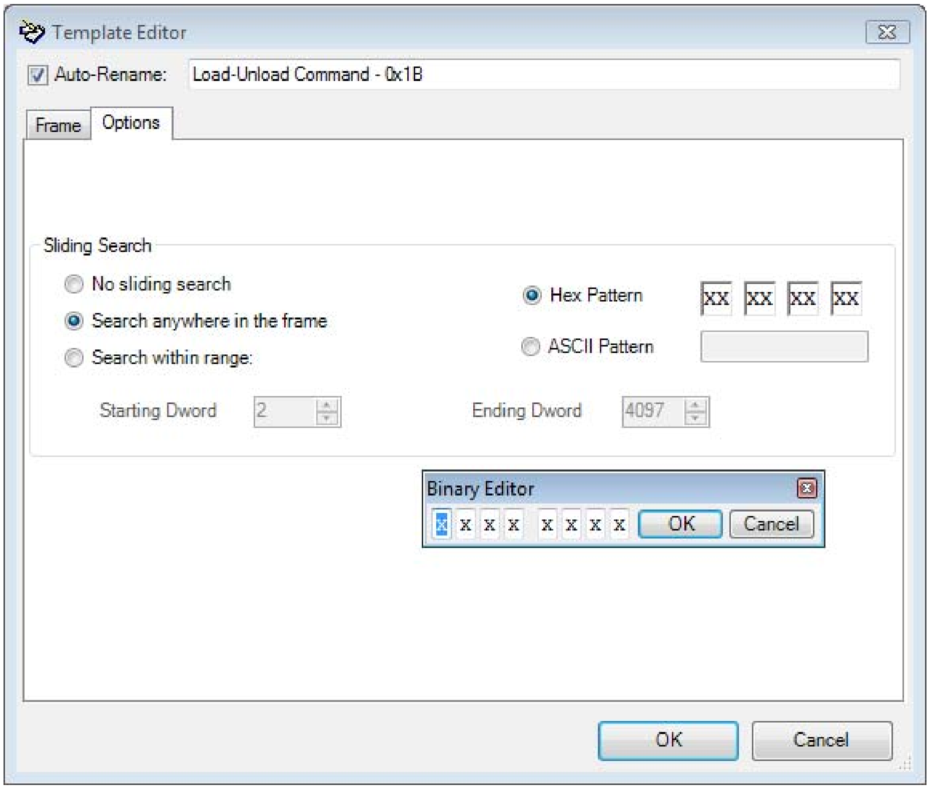


Options Tab

The Options tab is available for 6G SAS/SATA, 12G SAS, or PCIe only, and allows you to perform a sliding search. 6G SAS/SATA blades support a 32 bit search pattern. 12G SAS and PCIe blades support a 64 bit search pattern at all speeds. This tab is only available for Frame templates in the **Wait for any of these** pane in the **Capture Filter Editor**. You can select to search anywhere in a frame or to search within a range of words for a specific hex or ASCII pattern. You can either type a value directly in the hex pattern or double-click a value to open the binary editor. To define an ASCII pattern, type a value into the field.

Note: When using sliding search with a range, the starting Dword default is two, and it cannot be changed to a lower value.

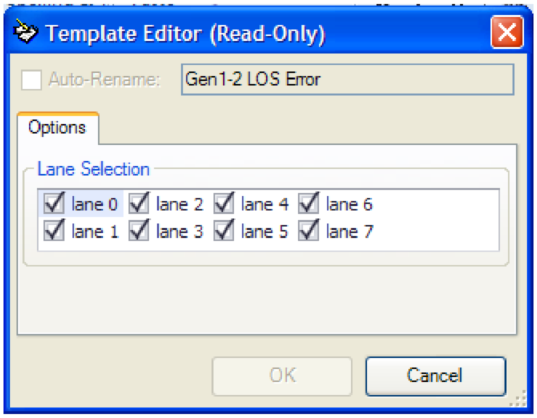
Figure 65: Frame Editor - Options Tab



Per Lane Triggering

The PCIe port supports triggering on specific lanes for OS and Error templates. The Template Editor's Options tab displays the lane selection boxes. By default, all lanes are selected. Although this feature is enabled for all errors, it is useful only for these following errors: Bad Sync Header, Loss of Sync Header Lock, Disparity, Code Violation, LOS, OS Errors, Unknown OS and Logical Idle Errors.

Figure 66: Lane Selection



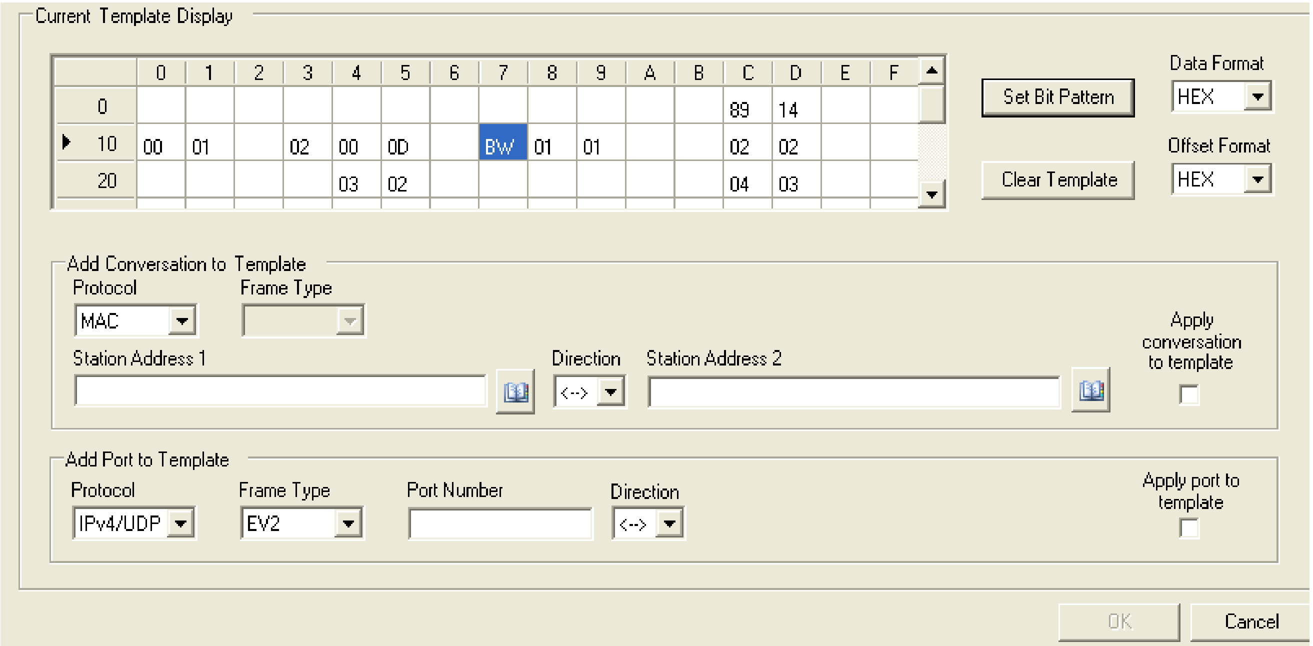
LAN Conversation Frame Editor

The LAN Conversation template in the Available Templates Browser uses the LAN Conversation Frame Editor instead of the Standard Template Editor. The LAN Conversation template is only available for GigE ports. The types of changes you can make with the **LAN Conversation Frame Editor** are:

- **Frame Byte-Pattern Definitions**
  To change the byte contents of the frame template, enter values in the byte display. You can also enter hex values (or Xs for "don't care" bits) directly into the offsets on the left.
- **Bit-Pattern Definitions**
  Bit level definitions for any byte can be specified. Select a byte within a template displayed in the template editor and press the **Set Bit Pattern** button to bring up the bit-level pattern editor. The bit-level pattern editor is a selection box for describing a bit pattern for the selected byte within the template.
- **Add Conversations**
  The area below the byte display table in the **LAN Conversation Frame Editor** dialog box is provided to quickly define and add an address byte pattern to a template.
- **Add Ports**
  The area below the Add Conversation to Template section in the **LAN Conversation Frame Editor** dialog box is provided to quickly define and add a port byte pattern (port number) to a template.

See Figure 67 for an example of the **LAN Conversation Frame Editor** dialog box.

Figure 67: LAN Conversation Frame Editor, Dialog Box Example



Creating Custom Templates

Custom templates can be created adding conversations or port numbers. Enter values directly in the correct offsets in the **Current Template Display** area.

You can edit the template by entering the station you want to select for in the **Add Conversation to Template** area and pressing **OK**.

The small fields in the **Current Template Display** area define the data patterns that comprise a template. The offset defines the position within the packet to start comparing the packet contents with the values in the pattern. If a match occurs, then this portion of the condition is satisfied. The pattern can be specified as a decimal, hexadecimal, or ASCII value.

Use the **Data Format** pull-down box on the right to specify if the pattern is in decimal, hexadecimal, or ASCII. Use the **Offset Format** pull-down box to specify if the column and row headers display in decimal or hexadecimal. Note that although you can display the data in different formats, all formats use a byte boundary. Only byte quantities can be entered or displayed.

Any specific value you create for templates can have “don't care” values. For example, assume you're only looking for `FFFF34` in the first three bytes of the MAC destination address. You could specify the values in your template as `FFFF34XXXXXX`, where X indicates you don't care about the values in the last three offsets. Note that for IPv4 addresses, which uses decimal values, using X characters as partial sub-addresses will cause the complete sub-address to be treated as wildcard. For example, 128.12X.2.2 will be treated as 128.XXX.2.2.

The hex or decimal patterns display in black or magenta. Displays in magenta within the **Current Template Display** area mean that the display does not provide a complete view of the template. The bytes are a macro pattern; for example, the logical OR of two different address patterns that make up a two-way conversation. Note also that many ASCII patterns have no corresponding display character.

Entering Values that Cross Byte Boundaries

Port values are generally understood as decimal numbers. For example, an NFS port is known as decimal 2049. Patterns are expressed as bytes and begin on byte boundaries. It takes two bytes to express a port number. Therefore, for port numbers you must convert the decimal number to a value that can be entered on a byte boundary. The example below shows how to enter NFS port 2049 in the display.

1 Take the port number (2049) and divide by 256. The result is 8 remainder 1. In IP “dot” notation, this could be expressed as “8.1”.

2 Set the Data format pull-down box in the display to Decimal. Values in the Data pattern area will be entered in decimal.

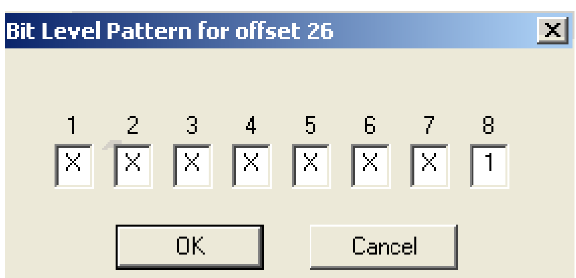
3 Enter 8 in offset 34 and enter 1 in offset 35. Enter 8 in offset 36 and 1 in offset 37. This sets the selection to both the source and the destination port.

If a port number is a decimal value less than 256, then the value of the first byte of the port number is zero, and the second byte is the decimal port number. For example, for HTTP port 80, enter zero in offset 34 and 80 in offset 35.

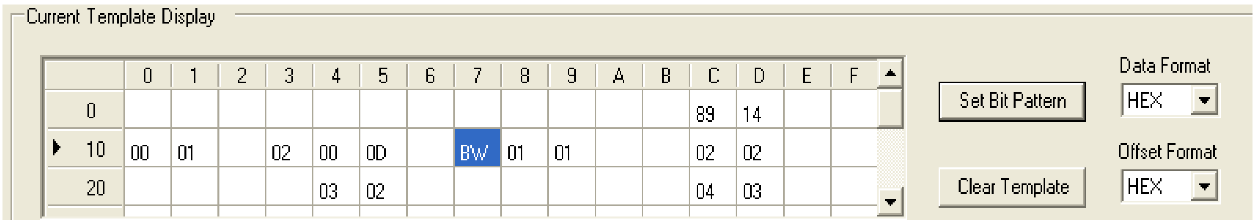
The byte-boundary restriction applies to any other decimal number, such as a number in a data pattern that you want to select for. You must first convert it so the value is expressed using byte boundaries.

Bit-Level Patterns

Xgig TraceControl can create a pattern at the bit level. To set a bit pattern, place the cursor within a byte field in the **Current Template Display** area. Press the **Set Bit Pattern** button. The **Bit Level Pattern** dialog box displays. The dialog box gives the number of the offset you are currently changing in its title bar. Enter any values for each bit that you want to include in the template. Leave values that you do not care about marked with an X. An example **Bit-Level Pattern** dialog box is shown below:



When you view bytes within the **Current Template Display** area, those which have bit-level values applied appear with “**BW**” in the field. This field is shown in blue. If you place the cursor in the byte field and press the **Set Bit Pattern** button, the **Bit Level Pattern** dialog box pops up allowing you to view/change the current bit-level values. A portion of the **LAN Conversation Frame Editor** dialog box with the bit pattern indicator is shown below:



If a bit level filter contains all "X" in either its left portion (first 4 bits) or right portion (last 4 bits) and the Data format selected is HEX, it will be displayed in Current Template Display area as "X" suffixed or prefixed with the hex value of the other portion. For example, if you enter bit pattern "XXXX 0101", it will be displayed as "X5" in Current Template Display area. "X5" is again shown in blue to indicate a bit level filter is in place.

To delete bit-level filtering for a byte, select the “**BW**” in the byte field and press **Delete**. The field must be editable in order to delete the byte.

Creating and Applying a Conversation

The **Add Conversation to Template** area of the **LAN Conversation Frame Editor** dialog box provides a convenient way to add address byte patterns to a template. The area consists of a protocol selection, frame type selection, two station addresses, a direction indicator, and an enable/disable check box. Refer to the table below for field definitions that comprise a conversation.

Table 6: Defining Conversations

Conversation Element	Description
Protocol	FCoE, MAC, IPv4, IPv6, IPX, or Atalk (AppleTalk)
Frame Type	EV2 (Ethernet II), SNAP, 8022 (IEEE 802.2), 8023 (IEEE 802.3), ISL, Q+EV2, Q+SNAP, Q+8022, Q+8023, and ISL+EV2 Frame type applies to network layer addresses only. Use Q+EV2 in conjunction with VLAN as the Frame Type for Ports to select for 802.1Q packets.
Station Address 1	Complete FCoE, MAC, IPv4, IPv6, IPX, or Atalk station address. The station address can be a range of stations (for example, 192.168.0.0/24 or 168.168.10.0/28). See the description below for the meaning of range specifications for station addresses.
Traffic Direction Indicator	`<->` Select all traffic between Station 1 and Station 2 `->` Select only the traffic where Station 1 is the Source Address and Station 2 is the Destination Address `<-` Select only the traffic where Station 2 is the Source Address and Station 1 is the Destination Address
Station Address 2	Complete FCoE, MAC, IPv4, IPv6, IPX, or Atalk station address. The station address can be a range of stations (for example, 192.168.0.0/24 or 168.168.10.0/28). See the description below for the meaning of range specifications for stations addresses.
Apply conversation to template check box	Enable (include) or Disable the conversation as part of the template.

Protocol and Frame Type

The protocol and the frame type are selected from pull-down boxes. Xgig TraceControl automatically restricts you from entering combinations that make no sense.

Station Addresses

Station addresses can be entered directly or by clicking on the **Name** button next to either **Station Address** field. Clicking on either button brings up the Surveyor default host name table to select an address. Note that Surveyor must be installed on the same PC to bring up the name table. The **Name Table** window shows all name and address associations. The entries shown in the Name Table is a default list and will not include those addresses found in the local network. Selecting a name table entry and clicking **OK** will load that name into the currently-selected **Station Address** field.

The station address types are described below.

- FCoE address – 6 hexadecimal digits.
  For example, 5A0009
- MAC address – 12 hexadecimal digits.
  For example, 34FD34AA0001.

- Atalk address - 2 decimal numbers separated by dots. The first can range from 0 to 65534 and the second from 0 to 255. For example 30234.123
- IPX address - IPX address notation accepts 8 hex digits [4 bytes] and 12 hex digits [6 bytes] separated by dot (without ports) or 8 hex digits [4 bytes] and 16 hex digits [8 bytes] separated by dot (with ports) e.g. 34FD34AA.0001000000A1 or 34FD34AA.0001000000A18888.
- IPv4 dot notation address - 4 decimal numbers in the range of 0 to 255, separated by dots. For example, 12.235.96.2.
- IPv6 address - an IPv6 address must be in one of the following formats, in compliance with section 2.2 of RFC 4291 (IP Version 6 Addressing Architecture):
  - Regular representation is a 128-bit address, divided into 16-bit fields of case insensitive hexadecimal, each field separated by colon. An example of this notation is shown below: 2031:0000:130F:0000:0000:09c0:876A:130B
  - Leading zeros in a field are optional. For example 2031:0:130F:0:0:9c0:876A:130B is valid
  - Successive fields of '0' can be represented as "::" but only once in address. For example: 2031:0:130F::9c0:876A:130B is valid. 2031::130F::9c0:876A:130B is not valid.
- It is possible to represent an IPv4 address inside an IPv6 address.
  - IPv6 addresses with an embedded IPv4 address are shown below: 0:0:0:0:0:0:192.168.0.1 or ::192.168.0.1
  - IPv4 mapped IPv6 addresses are shown below: 0:0:0:0:0:FFFF:192.168.0.1 or ::FFFF:192.168.0.1

If no value is entered for a **Station Address** field, all stations are selected. For example, if you set an address for Station 1, no address for Station 2, and set the direction to `->` all packets having Station 1 as the Source Address are selected for, regardless of the Destination Address.

Use wild cards when specifying addresses to select data on more than one station. An `X` used as a character for an address string means that any value will be accepted for that position; for example, `343F4AXXXXXX`.

IP Address Ranges

For addresses in IP dot notation, you can also specify a range of addresses. Ranges are specified by a slash mark and a number after the IP address. The number specifies the number of bits to match within the 32 bits that comprise an IP address (it takes 32 bits to represent an IP address). For example, 192.168.0.0/24 means any address that matches the first 24 bits of the address 192.168.0.0. The larger the number of bits you are matching, the smaller the range of IP addresses that will be selected.

IP range examples:

192.168.0.0/24 – Range starting with 192.168.0.0 and ending with 192.168.0.255.

192.168.0.0/16 – Range starting with 192.168.0.0 and ending with 192.168.255.255.

192.168.0.0/28 – Range starting with 192.168.0.0 and ending with 192.168.0.15.

192.168.0.1/32 – Just one IP address (192.168.0.1) since there are 32 bits in the address.

Traffic Direction Indicator

The direction indicator allows you to select a direction between stations. You can select for packets going from Station 1 to Station 2 (->), Station 2 to Station 1 (<-), or packets in either direction (<->).

Apply Conversation to Template Check Box

To apply the conversation to your template, make sure that the **Apply conversation to template** check box is selected. Enabling the conversation will modify the data patterns used in the template.

A single conversation is defined. If you want to use additional conversations, you can use wild cards as described above.

Creating and Applying a Port Number

Xgig TraceControl provides a convenient way to add a port number to a template. You specify port numbers for the template by filling out the **Add port to template** portion of the **LAN Conversation Frame Editor** dialog box. This area consists of a protocol selection, frame type selection, a port number, a direction indicator, and an **Apply port to template** check box. Refer to the table below for field definitions that comprise a port number selection.

Table 7: Defining Port Numbers

Port Element	Description
Protocol	IPv4/UDP, IPv4/TCP, IPv6/UDP, IPv6/TCP
Frame Type	EV2 (Ethernet II), SNAP, ISL, VLAN Frame type applies to network layer addresses only. Use VLAN in conjunction with Q+EV2 as the Conversation Frame Type to select for 802.1Q packets.
Port Number	Decimal UDP or TCP port number.
Traffic Direction Indicator	<-> Select all traffic where the specified port is the source or the destination -> Select only the traffic where the specified port is the source <- Select only the traffic where the specified port is the destination
Apply Port to Template check box	Include or exclude the port specification as part of the template.

Protocol and Frame Type

The protocol and the frame type are selected from pull-down boxes. Xgig TraceControl automatically restricts you from entering combinations that make no sense.

Port Number

Port numbers can be entered in decimal directly into the **Port Number** field.

Traffic Direction Indicator

The direction indicator allows you to select a direction between ports. You can select packets going to the port (->), coming from the port (<-), or gather packets in either direction (<->).

Apply Port to Template Check Box

To apply the port to your template, make sure that the **Apply port to template** check box is selected. Enabling the port will modify the data patterns used in the template.

Chapter 6

Xgig TraceControl Hints and Tips

In this chapter:

- TraceControl Hints and Tips
- Keyboard Shortcuts

Hints and Tips

Domains/Chassis/Analyzer Ports

- Use the right-mouse button to change the function of Xgig Multi-Function blades.
- Use the right-mouse button to rename domains and ports and to load the default configuration into a domain and ports. Use the right-mouse button to create, change, rename or delete a domain.
- Traces are started and stopped for a domain, not for a port. Configuration is performed for a domain, multiple ports, or for a single port-pair.
- Lock a domain and all its ports by pressing the lock button in the toolbar.
- Only one domain can be created per instance of Xgig TraceControl software.

Capture Traffic

- Configure the ports and domains before you start capture.
- Open a separate instance of Xgig TraceControl software to start a simultaneous capture for another domain.
- Before capture, make sure that the link speed is set properly for all ports. Verify that the link speed is correct even if you have loaded a configuration file.
- Check that you really are seeing traffic on the link using the Xgig Performance Monitor application.
- Set up buffer segmentation to capture multiple captures in the same memory buffer.
- Once started, the remote chassis will continue to run if you lose the connection or exit the TraceControl application. However, the ports in the domain are no longer locked for exclusive use. Reconnect to domains using the **Lock** button.

Trigger

- Highlight a transition bubble to access the Transition Editor. This will give you access to the Available Templates Browser.
- Drag-and-drop templates from the Available Templates Browser to set trigger conditions.
- Drag templates to the **Wait for any of these/And NOT these** panes, and double-click them to set up a custom template. Creating custom templates works as in Xgig TraceView.

Filter Traffic for Capture

- Drag-and-drop templates from the Available Templates Browser to the **Capture Filter Editor**.
- Drag templates to the **Capture these/But not these** panes, and double-click them to set up a custom template. Creating custom templates works as in Xgig TraceView.
- Copy data from TraceView and use it as a filter in TraceControl. Select an event row in the table or a filter template, right-mouse click and then select the **Copy** option. Switch to TraceControl and, one of the panes for the capture or trigger settings. Use the paste option to insert the data as a filter template.

Keyboard Shortcuts

Table 8: Keyboard Shortcuts for TraceControl

Control Key	Description
Ctrl+O	Load Configuration
Ctrl+S	Save Configuration
F3	Apply Configuration to Hardware
F5	Go to Performance Monitor
F7	Start Capture
F8	End Capture
F9	Go to Expert
F10	Go to TraceView
F11	Go to Surveyor
For User-Defined Templates Only …	
Ctrl+O	Open…
Ctrl+C	Copy
Ctrl+X	Cut
Ctrl+V	Paste
Ctrl+D	Go to Create Domain dialog
Del	Delete
F2	Rename
F1	Help

PART THREE:
Using Xgig Performance Monitor

Chapter 7

About Xgig Performance Monitor

In this chapter:

- Introducing Xgig Performance Monitor

Introducing Xgig Performance Monitor

Xgig Performance Monitor is one of four applications in the Xgig Analyzer software suite. It is a versatile monitoring tool which shows performance and error statistics on all analyzer ports being monitored. Xgig Performance Monitor consists of views that provide a quick snapshot of the current running state of the links being analyzed, as well as total statistics over time. The views are:

- **Chart View**
  Presents a view of the port and link information in a line graph with a historical view over time. A **Total** line graph is also available if applicable.
- **List View**
  Brings up a set of table views with monitor data for each port or link. The row for a link displays the sum of all values of each port in the link. The **Total** row shows the sum of values for the chassis. The current view is selected from a tab at the bottom. Table views include data transfer rate in megabytes, data transfer rates in kiloframes, utilization percentage, frame statistics, frame errors, SAS/SATA error counters, PCIe errors, and physical errors.
- **Meter View**
  Presents the current transfer rate and a metered representation of the transfer rate.
- **LED View**
  Indicates the current status of all ports.
- **Summary of Status LEDs (LED Summary View)**
  Indicates the summary status of all ports. The number of ports that are in a particular state is indicated with the status type.

Use Xgig Performance Monitor to monitor performance of each channel and detect errors. You can vary the update rate to suit your measurement.

You can set the protocol of the port (Fibre Channel, GigE, SAS/SATA, or PCIe) from the **Select Ports to Monitor** dialog box in Performance Monitor. You can also set the link speed and the signal regeneration (analog passthrough, analog passthrough multiplexed, digital retime) from the **Hardware > Port Settings** menu of Xgig Performance Monitor.

If you exit and restart Performance Monitor, changes to the position and placement of all view windows are preserved. It is recommended that you have no more than two instances of Performance Monitor running per domain.

Chapter 8

Getting Started with Xgig Performance Monitor

In this chapter:

- Launching Xgig Performance Monitor

Launching Xgig Performance Monitor

Secure Login for All Xgig Chassis

All Xgig chassis may be password protected to prevent access by unauthorized users. Password protection is set through the Xgig Web Utility for each chassis. If the chassis you are attempting to access is password protected, you are required to provide the password. The following login screen will appear. Enter the password to continue; the account name is always Administrator.

Figure 68: Xgig Analyzer Login

Login is only required once from any of the Xgig Analyzer applications or Xgig Maestro running on the same Xgig Analyzer PC client machine. For example, if you login through TraceControl, you will not be asked for the password again when you access the same chassis sync group through Xgig Performance Monitor. To make sure you are completely logged off from all chassis, you must close all Xgig applications.

For login, the settings of a master chassis in a sync group prevail for all chassis in the sync group. If the master has authentication turned off and a slave(s) has authentication turned on, then the sync group as a whole has authentication turned off. The settings for the master chassis also prevail for the password; the password of the master chassis will be the password for any slave chassis in the same Sync Group. See “Xgig Blade and Port Numbering” on page 45 and the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* for more information on master, slaves, and sync groups.

Launching the Application 

To use Xgig Performance Monitor:

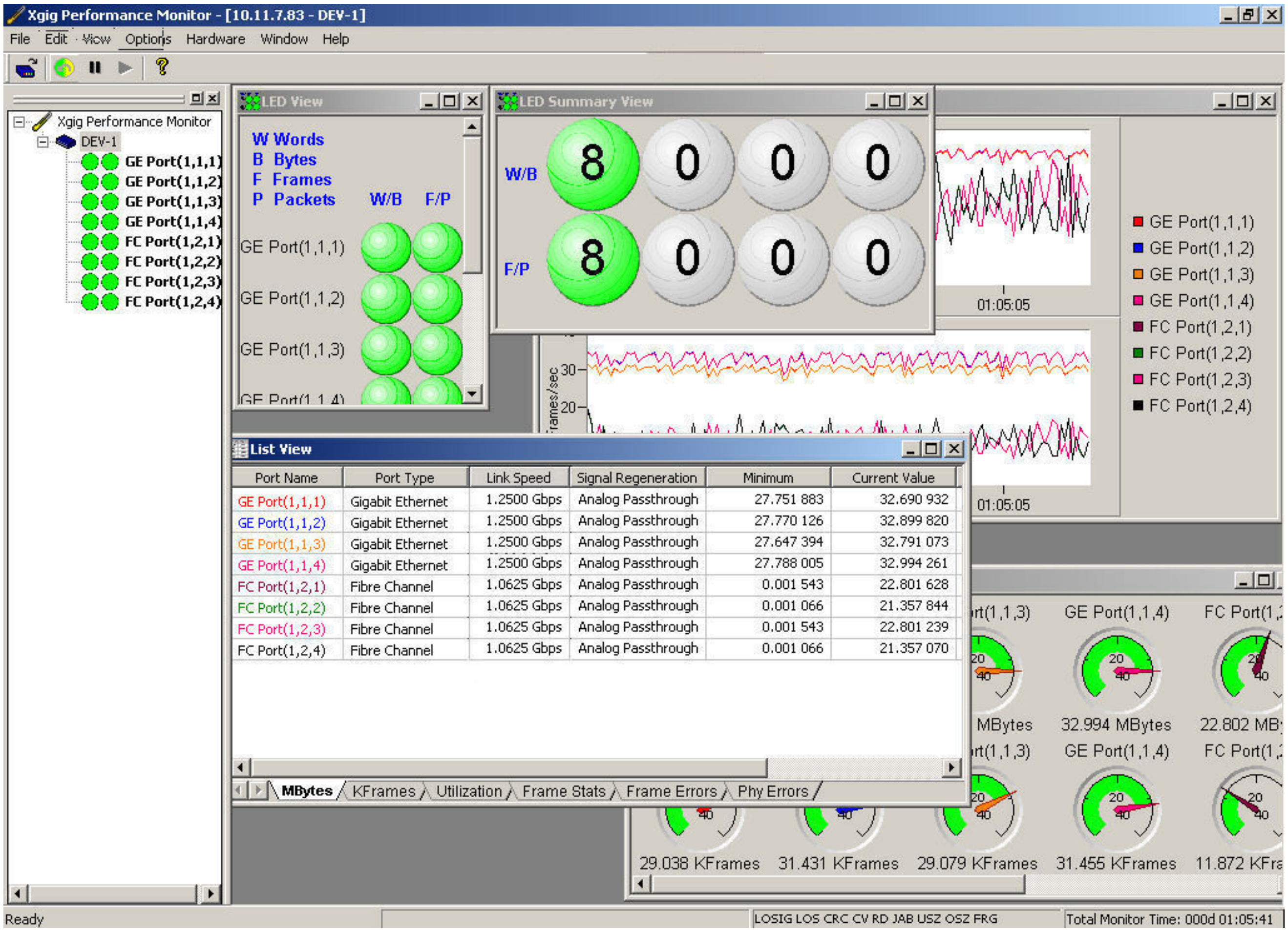
1. From the Desktop, double-click the Xgig Performance Monitor shortcut to launch the application.
2. When started for the first time, Performance Monitor does not begin monitoring. Xgig Performance Monitor automatically begins monitoring the last Sync Group that was monitored. You can also switch monitoring to another set of ports at any time.
3. Select ports to monitor by clicking on the Select Sync Group  button. See “Selecting the Sync Group” on page 170 for more information.

If you exit and restart Performance Monitor, changes to the position and placement of all view windows are preserved. It is recommended that you have no more than two instances of Performance Monitor running per domain.

For all views, Mbyte = 1,048,576 bytes, KFrame = 1,000 frames, and KPackets = 1,000 packets.

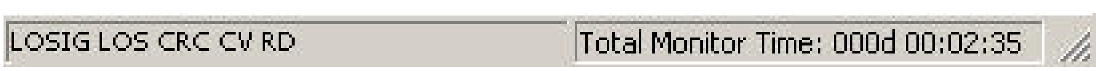
The figure that follows shows the main Performance Monitor window.

Figure 69: Xgig Performance Monitor



Status Bar Features

The status bar at the bottom of the window shows the errors currently seen on the network, SOF, if frame traffic is flowing, and the total monitor time.



List of Error Counters Displayed

All the errors currently seen on the network are listed in the status bar.

Total Monitor Time

The total running time of the current monitor session is displayed as the **Total Monitor Time**. If Performance Monitor is paused, the counter stops incrementing. When monitoring is restarted, the timer resumes.

Selecting the Sync Group

When you select a Sync Group to monitor in Performance Monitor, you monitor the statistics on the Sync Group's analyzer hardware. For Xgig Analyzers, the Sync Group is remote. The Sync Group can be either a single Xgig chassis or a set of cascaded Xgig chassis.

When accessing remote analyzer ports, Performance Monitor's ability to provide an accurate view of performance information will depend on the speed of your network connection.

To Select a Host:

1 Press the **Select Sync Group**  button or select **Select Sync Group…** from the **Hardware** menu. The **Select Ports To Monitor** dialog box appears. All Sync Groups within the local area subnet (including your local machine if applicable) are displayed in the window on the left.

2 Select the Sync Group containing the hardware ports you want to view. If the hardware you wish to access is on a different subnet, type in the IP Address or Machine Name and press **Discover**.

3 A graphical representation of hardware that can be monitored will appear in the right window when a Sync Group is selected in the left window.

To Change the Sync Group:

Follow the steps above. If you choose to monitor a new Sync Group, monitoring views of the old Sync Group are removed.

Chapter 9

Xgig Performance Monitor Port Configuration

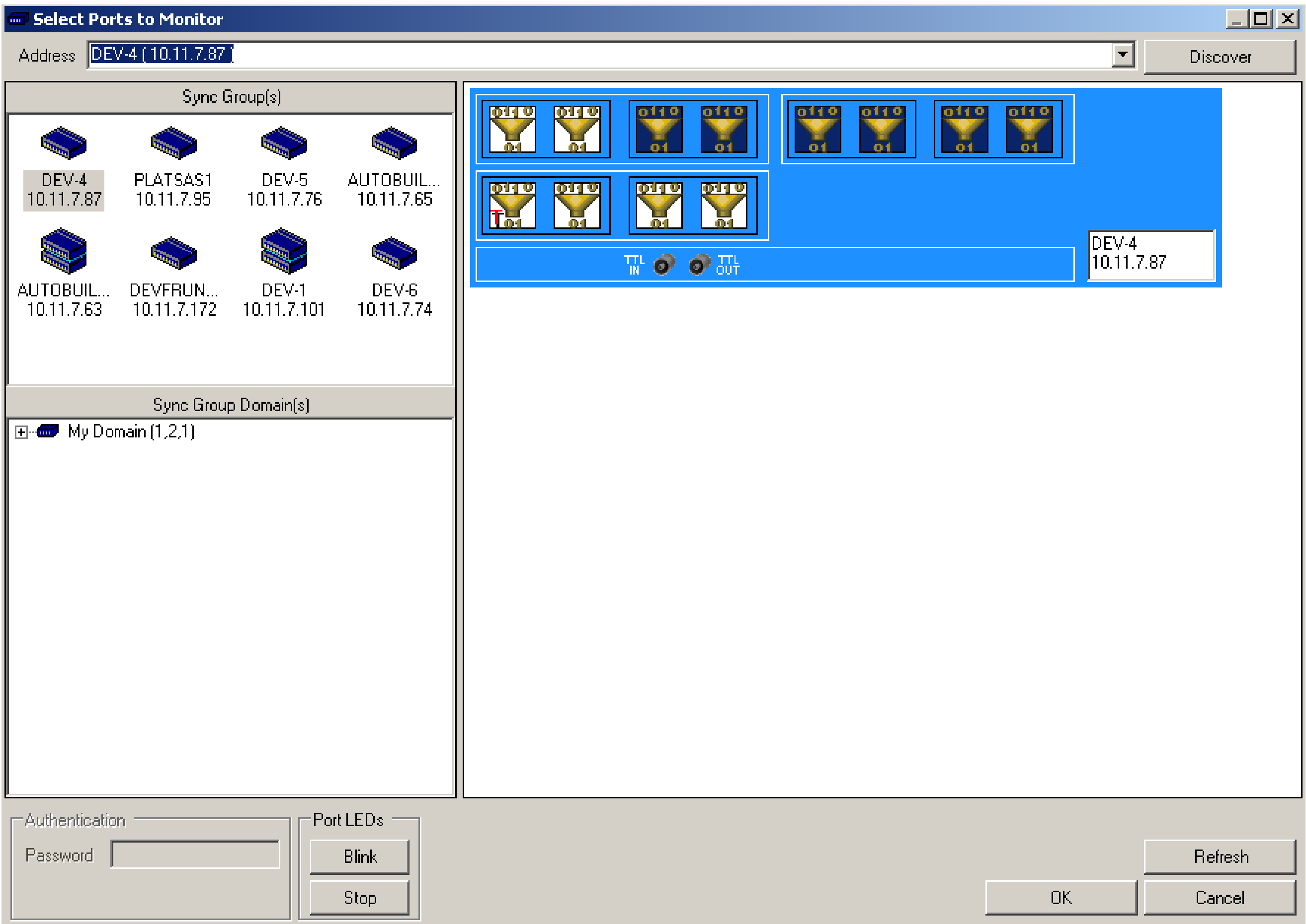
In this chapter:

- Select Ports to Monitor Dialog Box
- Chassis Upgrade and Maintenance Options
- Changing Port Functions

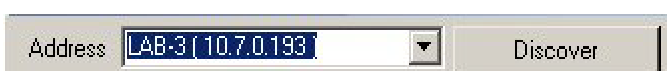
Select Ports to Monitor Dialog Box

Ports are selected for monitoring using the **Select Ports to Monitor** dialog box. Press the button on the toolbar to bring up the dialog. The dialog indicates the type, availability, and status of ports. It also allows you to discover Sync Groups on different subnets or flash the LEDs of ports on any Xgig chassis. Sync Groups can consist of multiple, cascaded Xgig chassis.

Figure 70: Select Ports to Monitor Dialog Box



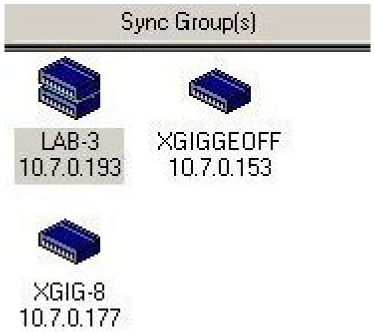
Discover Different Subnets



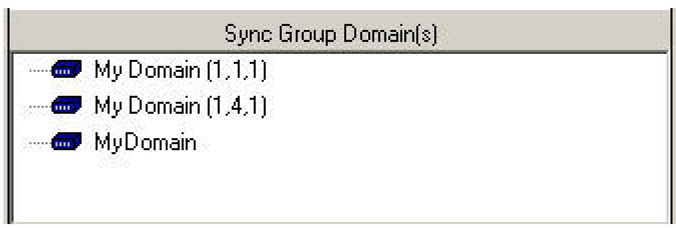
To select Sync Groups on a different subnet, enter the IP Address or DNS name in the Address field and press **Discover** (top of the dialog). The specific Sync Group you have requested and all other Sync Groups on the same remote subnet will be added to the left panel.

Sync Groups and Domains

All Sync Groups discovered on the local subnet are displayed in the upper left panel. When you select a Sync Group, its chassis, blades and ports display in the right panel showing all available ports. If multiple chassis are cascaded to form a Sync Group, the name and address of the master chassis within the Sync Group displays in the Sync Group(s) area. The IP address of slave chassis cascaded to the master will not be shown in the Sync Group(s) area. However, you can use the name or address of a slave chassis in the Address field described earlier to discover a Sync Group on a subnet.



The **Sync Group Domain(s)** area lists all the domains in the Sync Group selected above. Each domain within the Sync Group is shown as a hierarchical structure, showing all chassis, all links, and all ports that comprise the Domain.



Port Viewing and Selection

The dialog box displays an icon for each port, arranged as they physically exist within the analyzer hardware device(s). To select a port, click the port. Ports are always selected in pairs, so the port and remaining port of the port-pair are selected. Click ports again to remove them from the selections. Selected ports have a blue background; unselected ports have a white background.

The icons change as the selection, availability, and type of each port changes. See Selecting Chassis, Blades, and Ports for information on the display of port icons. See “Changing Port Functions” on page 176 for information on how to change the function of ports.

When selecting ports to monitor in Performance Monitor, you cannot explicitly create links. You can select either ports or a domain to monitor.

When Performance Monitor is launched from TraceControl, any defined links in TraceControl’s domain will be shown. Ports viewed in Performance Monitor that are chosen by selecting a domain from the domains tree will be shown with any defined links.

Dialog Buttons

If you are not logged into the Sync Group that contains the resources in the domain, use the **Password** field to login. Login is only required if the Sync Group is password protected.

The following buttons are available:

- **Blink**
  Causes the LEDs for the selected ports to blink. LEDs will blink for 40 seconds.
- **Stop**
  Causes the LEDs to stop blinking.
- **OK**
  Exit and use the selected ports for monitoring.
- **Refresh**
  Updates the status of blades and ports in the right panel and available hosts in the left panel.
- **Cancel**
  Exit without changes.

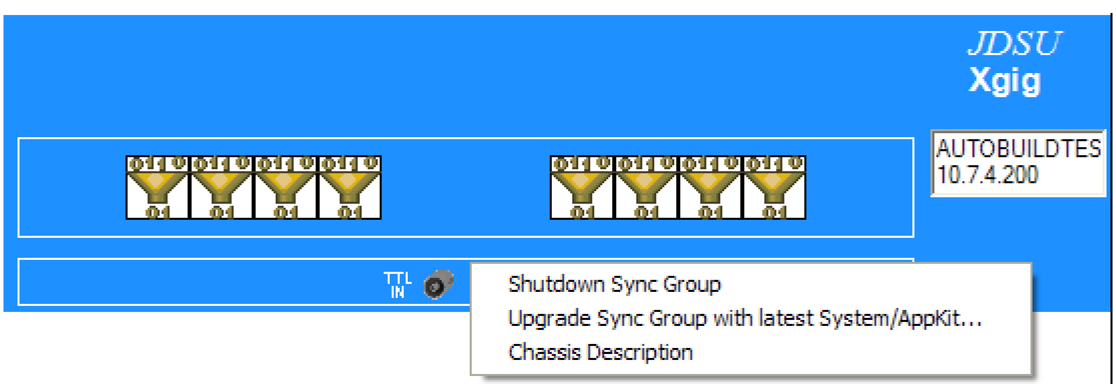
Setting Cable Lengths for Interconnected Chassis

You can specify the length of the sync cable(s) between chassis if you are required to use sync cables other than the ones provided with a chassis. Chassis can only sync using straight through RJ-45 cables and the Cascade In and Out ports on the chassis. The minimum value is 1 foot and the maximum value is 100 feet. The default is 3 feet, which is the length of the cable provided with the chassis. If authentication is enabled, you must provide the Xgig password prior to setting the cable length. Providing the proper sync cable length(s) is essential to ensure that the captures are properly time-aligned.

Chassis Upgrade and Maintenance Options

Chassis software upgrade and chassis shut down are available from the Select Ports to Monitor dialog box of Performance Monitor. Right-click a chassis, and select the option from the context menu. Refer to “Chassis Upgrade and Maintenance Options” on page 51 for complete information. Note that Performance Monitor has more tolerance than other Xgig applications for incompatibilities between client and server software version levels.

Figure 71: Chassis Context Menu, Performance Monitor Select Ports to Monitor Dialog



Changing Port Functions

For all Xgig Multi-Function Blades you can change the function of a port on the blade if you have a blade license for multiple functions.

- Fibre Channel Analyzer
- Gigabit Ethernet Analyzer
- SAS/SATA Analyzer
- PCIe Analyzer
- Fibre Channel Jammer
- Gigabit Ethernet Jammer
- SAS/SATA Jammer
- Fibre Channel BERT
- Gigabit Ethernet BERT
- SAS/SATA Generator
- SAS/SATA Target Emulator
- Fibre Channel or FCoE Load Tester
- Gigabit Ethernet Delay Emulator

In the Select Ports to Monitor dialog box, ports that have a BERT, Jammer, Generator, Target Emulator, Delay Emulator, or Load Tester function will display, but they must be changed to an Analyzer function before Performance Monitor can use them. Xgig ports with another function can be changed to an Analyzer function if the port is not locked by another user and the blade has the proper license.

To change a blade port function:

1. Select the port you want to change by clicking it, then right-click the port to view menu options.
2. From the **Use Port(s) as...** menu, select the function type you want. If only one function type is available for this blade, only one type will be shown. For example:

3. The list will contain only those functions that have been licensed for the blade.

Caution: The change in the function of the port(s) does not complete until you hit the **OK** button in the Select Ports to Monitor dialog box.

Licensing for Xgig Multi-Function Blades

The licensing for different functions is set up using the Xgig Web Utility. From Performance Monitor, you can only change the function of a port if the blade and port-pair has a license for multiple functions. If a blade or port-pair does not have the ability or the license to change functions, the options and menus in Performance Monitor described above will not be available.

For all Xgig blades, there is a blade license key and, if required, a license key for each port-pair. The port-pair license key allows specific functions for each port-pair. The port-pair license is only assigned if port-pairs within the blade are licensed for different functions. If all port-pairs on the blade have the same functions, only the blade license key is assigned and used.

The proper licenses are assigned and stored on the blade using the Xgig Web Utility. If the blade is moved to a different chassis, its blade and port-pair licenses, and therefore its ability to change functions, remains the same. In other words, the licenses “follow” the blade and are not associated with the chassis.

Chapter 10

Xgig Performance Monitor Configuration

In this chapter:

- Monitor Views
- Hardware options
- Performance Monitor Options
- Toolbar Functions

Monitor Views

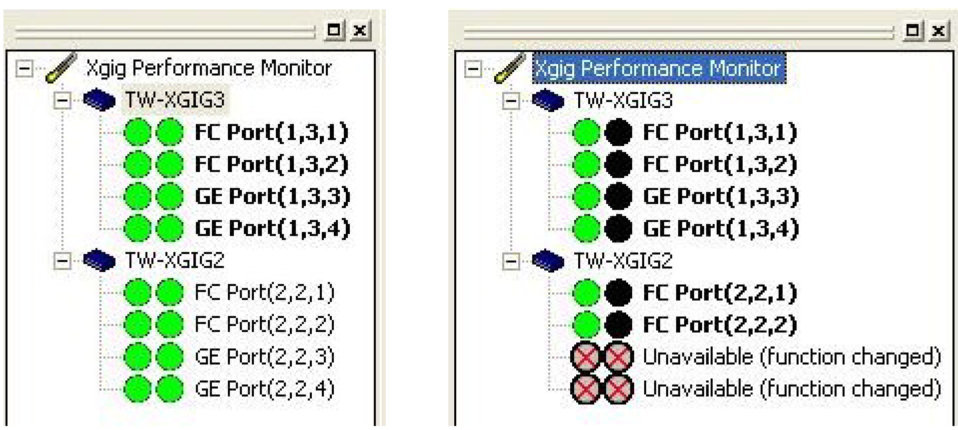
This section discusses the different views in Performance Monitor.

Resource Browser

The Resource Browser shows all ports that can be monitored from Performance Monitor. The **Words/Bytes** status LED and the **Frames/Packets** status LED are shown for each port. The **Words/Bytes** status LED is on the left and the **Frames/Packets** status LED is next to the port name. Select the ports you wish to display in the Performance Monitor views. See Table 9 on page 187 for a description of the LED colors and their meaning.

When you select a port or a chassis in the Resource Browser, the monitor views will automatically display monitoring information for the selected ports. For example, in Figure 72 if you select chassis TW-XGIG3, then all monitor windows will show information for the 4 ports under the TW-XGIG3 chassis.

Figure 72: Resource Browser Examples



When you choose ports from the **Select Ports to Monitor** dialog box and press **OK**, the Resource Browser lists the chassis and ports you have selected and Performance Monitor begins the monitoring process. If you have selected more than 32 ports, Performance Monitor begins monitoring only the first 32 ports; however, all selected ports will display in the Resource Browser.

When launching Performance Monitor from the TraceControl application, the Resource Browser lists the chassis and ports in the current domain. If there are more than 32 ports, Performance Monitor begins monitoring only the first 32 ports; however, all ports in the domain will display in the Resource Browser.

From the Resource Browser you can select a subset of ports to monitor. Use the **Shift** and **Ctrl** keys to select a group of ports, or select ports individually by clicking on the port. You can select ports from multiple chassis and all selected ports will be displayed in the Resource Browser.

You can also select all ports for a chassis by clicking on the chassis name. You can only select one chassis at a time, and cannot use either the **Shift** or **Ctrl** key to add ports or chassis to your selection.

All selected ports are displayed in bold characters. Unavailable ports are displayed with the text **Unavailable (function changed)** next to the port labels. This status will only be seen when the ports being monitored have changed function (via another client application). To begin monitoring these ports again, return to the **Select Ports to Monitor** dialog and re-select the ports.

Selections made in the Resource Browser have no effect on the LED Summary View. A count of all analyzer ports in the Resource Browser are shown within this view.

Chart View

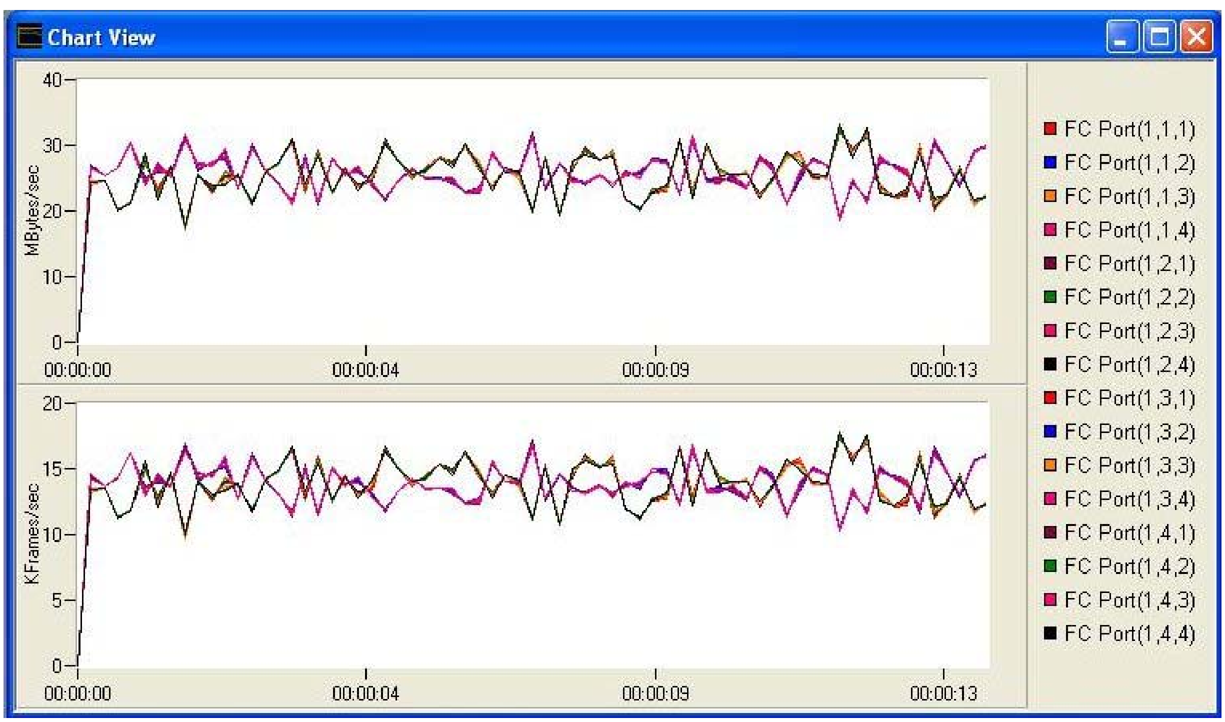
The **Chart View** presents a line graph of the transfer rate for all selected analyzer ports and links. Rates are expressed in Mbytes/sec and Kframes/sec. A **Total** line graph is displayed also depending on the selection from the Resource Browser.

When the **Frame Type** in the **Preferences** dialog is set to **SCSI Frames**, the **Chart View** displays transfer rates in SCSI Mbytes/sec (frames with RCtl=0x01 and Type=0x08) and SCSI Kilo Commands per second (frames with RCtl=0x06 and Type=0x08).

Right-click the pane to access the **Preferences** and **Metric Options** dialog boxes. From the menu that pops-up to select a configuration dialog, you are also provided a means to show or hide the legend. All scaling for the charts is done automatically and does not require configuration.

The MBytes/sec. axis can be changed to display as a utilization percentage. Right-click the graph and select the **Show Utilization** option. See "Utilization Display Option" on page 205.

Figure 73: Xgig Performance Monitor Chart View



Meter View

Meter View displays the progression of data collection as an analog meter with a needle indicating status. The **Meter View** presents the current transfer rate in Mbytes/sec and KFrames/sec for each port.

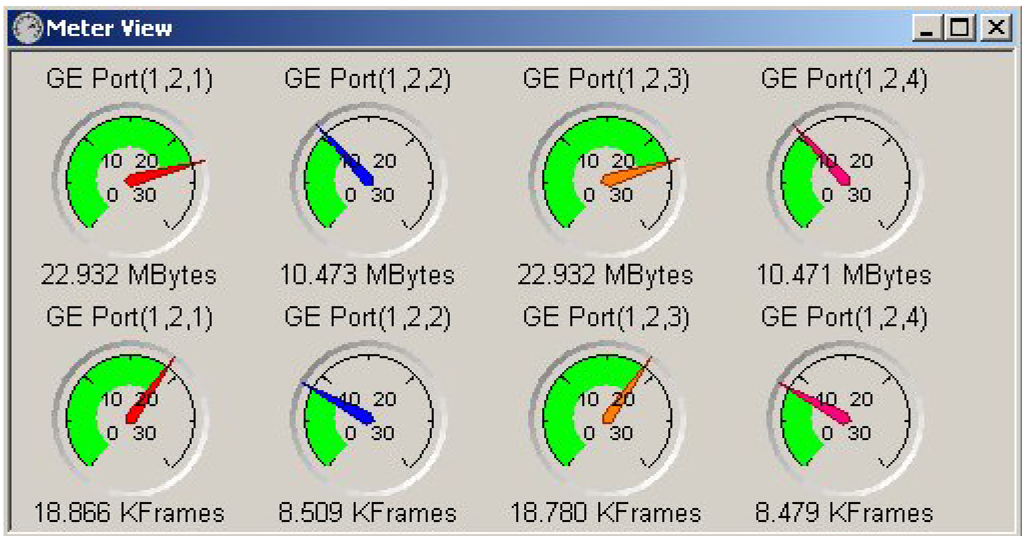
Right-click **Meter View** to access the **Preferences** and **Metric Options** dialog boxes. All scaling for the meters is done automatically and does not require configuration. All MByte meters will have the same scale and all KFrame meters will have the same scale. However, the MByte and KFrame meter scaling are independent of each other and solely based on the port that contains the highest data rate in the configured domain.

MByte meters can be changed to display as a utilization percentage. Right-click the graph and select the **Show Utilization** option. See “Utilization Display Option” on page 205. Snapshots of all data over time can be logged in .csv files; see “Statistics Logging Function” on page 207.

When the Frame Type tab of the Preferences dialog is set to SCSI Frames, the Meter View will display SCSI Megabytes per second and SCSI Kilo Commands per second. This option is available for 1/2/4/8G Fibre Channel ports only.

An example of Meter View is shown in Figure 74.

Figure 74: Xgig Performance Monitor Meter View



List View

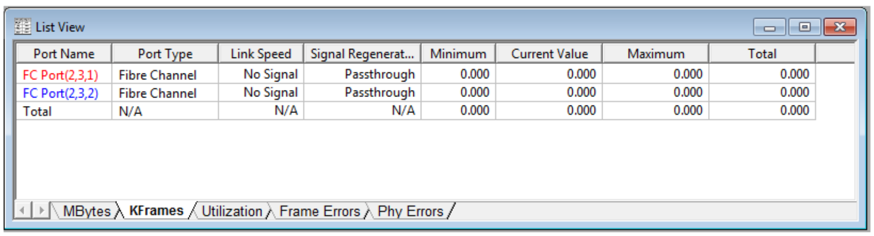
The **List View** presents vital statistics of each analyzer port or link such as utilization, data transfer rate in KFrames/sec, data transfer rate in MBytes/sec, frame errors, SAS/SATA error counters, PCIe errors, and phy errors. A **Total** row is also displayed depending on the selection from the Resource Browser. The statistical information is presented on several tabs within the view, so you can easily access the columns of information you want to view. The number of statistical tabs available is dependent on the types of analyzer ports configured in the domain.

All tabs within List View will show the port or link name, port or link type, link speed, and signal regeneration mode for each port or link. For PCIe, the link width is also shown. In the case of MBytes, KFrames and Utilization tabs, minimum, maximum and current rate values are available. The tabs within list view are described below.

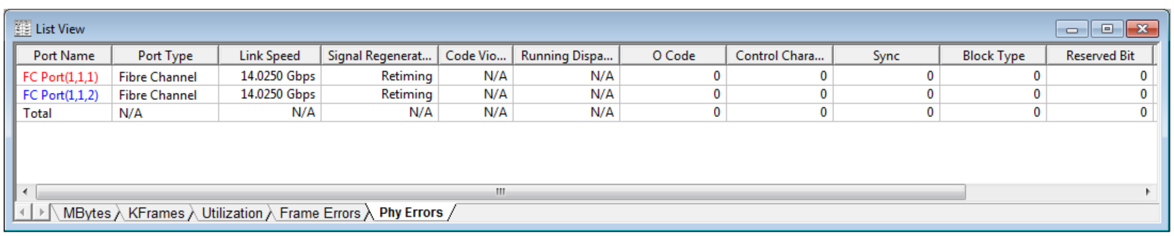
Right-click **List View** to bring up a menu of configuration options. See “Preferences” on page 193 for information on configuration options and a detailed description of the counters shown in **List View**. Snapshots of all data over time can be logged in .csv files; see “Statistics Logging Function” on page 207.

To reset all of the statistics in List View, select **Reset LEDs and Counters** from the **Edit** menu.

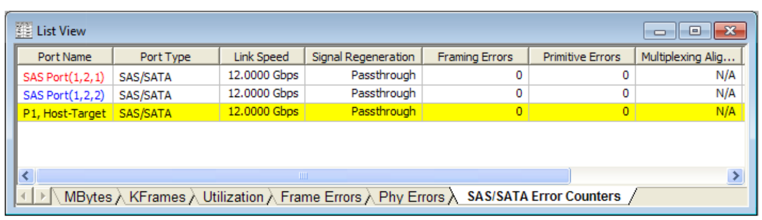
Figure 75: Xgig Performance Monitor List View Examples



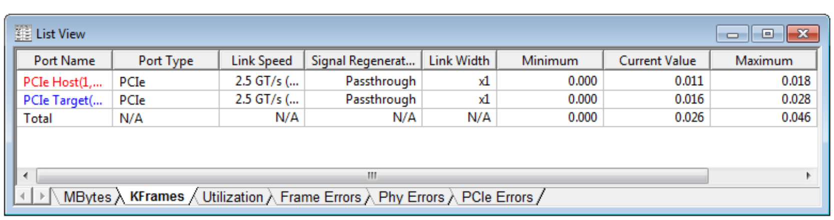
List View, Kframes Tab for GigE Ports



List View, Phy Errors Tab for FC Ports



List View, SAS/SATA Error Counters for SAS Ports



List View, KFrames Tab for PCIe Ports

MBytes Tab

The **MBytes** tab shows the minimum, maximum, and current rates for each port, expressed in Mbytes/sec.

When the **Frame Type** tab of the **Preferences** dialog is set to **SCSI Frames**, the **List View** displays SCSI Megabytes per second for all 1/2/4/8G FC analyzer ports.

KFrames Tab

The **KFrame** tab shows the minimum, maximum, and current rates for each port, expressed in Kframes/sec.

When the **Frame Type tab** of the **Preferences** dialog is set to **SCSI Frames**, the **List View** displays SCSI Kilo Commands per second for all 1/2/4/8G FC analyzer ports.

Utilization Tab

The **Utilization** tab shows the minimum, maximum, and current rates for each port, expressed as a percentage of total link bandwidth. The average utilization over the past 15 minutes is also shown.

Frame Stats Tab

The **Frame Stats** tab shows a running count (per port) for common Ethernet frame types. Counts are listed for Gigabit Ethernet ports only. This tab displays in List View only if the current domain contains any Gigabit Ethernet analyzer ports. Frame types counted are:

- Multicast Frames
- Broadcast Frames
- Unicast Frames
- Undersized Frames
- Oversized Frames
- VLAN Frames
- iSCSI Frames

Frame Errors Tab

The **Frame Errors** tab shows the error counts (per port) for common frame errors. A count is provided for the cumulative number of errors since monitoring was started.

CRC errors apply to all Fibre Channel frames, all Gigabit Ethernet frames with the exception of undersized and oversized GE frames, all SAS/SATA frames, and PCIe frames. Jabbers refer specifically to oversized GE frames with an incorrect CRC field while Fragments refer to undersized GE frames with an incorrect CRC field.

The Traffic Status field indicates CRC errors encountered in Fibre Channel, Gigabit Ethernet, SAS/SATA, and PCIe analyzer ports. It also indicates Loss of Signal and Loss of Sync errors.

Frame errors counted are:

- CRC
- Jabbers
- Fragments
- FCoE Embedded CRC

Phy Errors Tab

The **Phy Errors** tab shows the cumulative number of common physical errors (per port) since monitoring was started. No count is provided for ports for which the physical error makes no sense; for example, no count is made of 10Gbps O Code errors for SAS/SATA ports.

Physical errors counted are:

- Running Disparity
- Code Violation
- O Code Errors
- Control Character Errors
- Sync Error
- Block Type Errors
- Reserved Bit Errors
- FEC Parity Errors

For Xgig, Xgig5000, and Xgig1000 ports, columns for unselected physical error types (as configured within the **Phy Errors** tab of the **Preference** dialog) are not shown in the **Phy Errors** tab of List View. For example, if Code Violation errors are not selected, the Code Violation Errors column is not shown. For “state” errors, such as loss of signal or loss of sync, the current state will appear in the **Traffic Status** column.

SAS/SATA Error Counters Tab

The **SAS/SATA Error Counters** tab shows the cumulative number of common SAS/SATA errors (per port) since monitoring was started.

SAS/SATA errors counted are:

- Framing Errors
- Primitive Errors
- Primitive Sequence Errors
- Multiplexing Alignment Errors
- Any Errors

For the definitions of these errors, see Table 13. This tab will only be visible if SAS/SATA analyzer ports appear in the Resource Browser.

PCIe Errors Tab

The **PCIe Errors** tab shows the cumulative number of common PCIe errors (per port) since monitoring was started.

PCIe errors counted are:

- Logical Idle Errors
- Unknown OS Errors
- OS Errors
- Gen1-2 LOS Errors
- Gen 3 LOS Errors
- CRC16 Errors
- LCRC Errors
- ECRC Errors
- Poisoned TLP Errors
- Undef TLP Type Errors
- Invalid H0 TLP Length Errors
- Msg Violation Errors
- PAD Req Violation Errors
- Frame Length End Errors
- Misaligned SOP Errors
- Bad Sync Header Errors
- EDS then Data Block Errors
- EDS then Wrong OS Errors
- SDS then OS Errors
- No EDS before OS Errors
- Frame Block Errors
- Bad STP Errors
- Invalid STP TLP Length Errors
- EDB Errors

This tab will only be visible if PCIe analyzer ports appear in the Resource Browser.

Status LEDs (LED View)

The Status LEDs window (LED View) contains a Word/Byte LED and a Frame/Packet LED for each port. If not all port LEDs are visible, increase the size of the window or use the scroll bar.

Words are the typical size of a unit of traffic in Fibre Channel, which are 32 bits that are encoded to 40 bits on the wire. In SAS/SATA, the same quantity is referred to as a Dword. In Gigabit Ethernet, the unit of traffic is a byte. All Ordered Set, Frames, Primitives, and Packets are made up of words or bytes. Frames/Packets are structures that begin with SOF and end with a CRC and EOF. The meaning of the LEDs for words and frames are shown below. These definitions apply to the LED View, the LED Summary View, and the Resource Browser.

Table 9: Word and Frame Status LEDs

Word/Byte LED	**Reason**
Black	No signal or no light, often a result of a disconnected cable or unplugged SFP module
Red	Signal with errors, for example, illegal characters, running disparity violations, CRC mis-matches
Yellow	Had an error in the past, currently no errors
Green	Good signal, legal characters, proper disparity, good CRC if present
Frame/Packet LED	**Reason**
Black	No Frames detected
Red	CRC mismatch error detected
Yellow	Had a CRC error in the past, currently no errors
Green	Frames with good CRCs detected

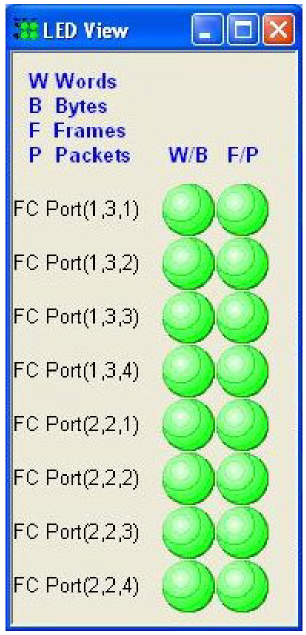
Right-click the view to access the **Preferences** dialog box.

Unselected error types (as configured within the **Frame Errors** tab, the **Phy Errors** tab, and the **SAS/SATA Errors** tab of the **Preferences** dialog box) are not used in determining the value of a status LED for a port. For example, if CRC errors are not selected, and the only errors discovered for a port are CRC errors, the status light for that port will remain green.

The LED will stay red if the error condition persists. If the error condition stops, the LED will turn to yellow instead of green. An example is shown in Figure 76.

To reset all LEDs from yellow back to all green, select **Reset LEDs and Counters** from the **Edit** menu.

Figure 76: Status LEDs



Summary of Status LEDs (LED Summary View)

The LED Summary View shows a summary of the status of all LEDs for all ports. The Summary of Status LEDs can be used to quickly discover if there are any general device or port problems. For example, if all 16 ports have black LEDs, the Xgig is probably disconnected from the network. Use the Resource Browser to see the status of individual ports. All ports in the Sync Group are summarized in the LED Summary View, regardless of what ports are actually selected in the Resource Browser for other monitoring views.

The number of ports that have the status indicated by the color of Status LED are shown inside each LED. There are two rows of LEDs, one for Words/Bytes and one for Frames/Packets. Numbers are large so the status can be seen at a distance.

See Table 9 for the meaning of the LED colors. An example is shown in Figure 77.

Figure 77: Summary Status LEDs

Hardware Options

Hardware options set the hardware link speed, hardware signal regeneration, Scrambling, FEC, CDR, Force Clock Re-Clock, and for PCIe, lane control.

Port Settings - General Settings Tab

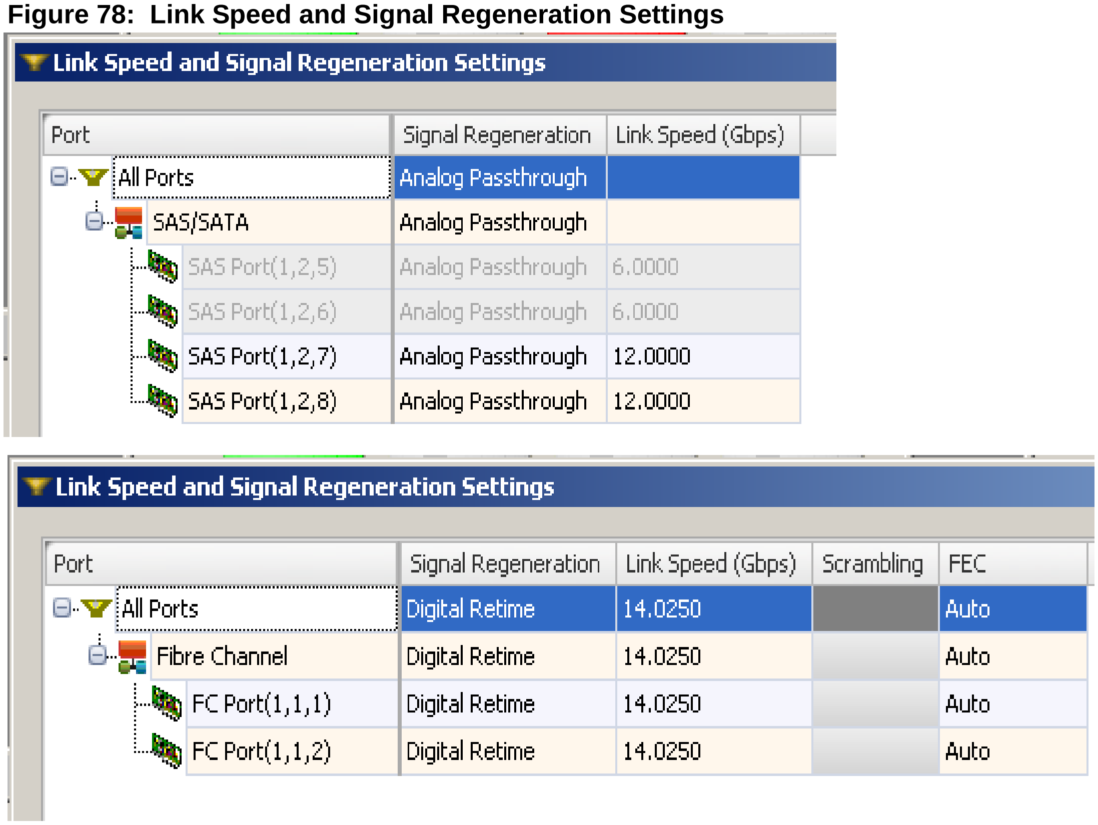
The **General Settings** tab in TraceControl's **Configuration Manager** is also shown in Performance Monitor. This section explains the settings available in this tab.

Each port-pair has a separate link speed setting. The signal can also be digitally retimed or set for analog passthrough. Select **Port Settings...** from the **Hardware** menu to set these options when the ports are not locked by the TraceControl application. The Link Speed and Signal Regeneration Settings dialog box appears showing all ports monitored. The settings that display initially are those currently set for each hardware port.

For FC ports set to 4.2500 or 8.5000 Gbps, Scrambling settings are shown. For FC ports set to 14.0250 Gbps and for 10GigE ports, FEC settings are shown.

If another user has locked the analyzer port, you cannot change the options.

Figure 78: Link Speed and Signal Regeneration Settings



Link Speed

See "Link Speed" on page 95 for more information about setting the link speed for various blade types.

For Fibre Channel, the link speed can be set to the highest speed supported by the blade containing the ports, or a supported lower speed. Available link speeds for Xgig Fibre Channel are 1.0625 Gbps, 2.1250 Gbps, 4.2500 Gbps, or 8.5000 Gbps. For example, the Xgig 2 Gigabit Multi-Function Blade ports can be set to **1.0625 Gbps** or **2.1250 Gbps**; however, higher rates are not supported. The link speed for Xgig5000 16G FC is 14.0250 Gbps and cannot be changed.

The link speed is fixed at **1.2500 Gbps** and cannot be changed for Gigabit Ethernet analyzer ports.

For 3G SAS/SATA blades, the link speed can be set to **1.5000 Gbps**, **3.0000 Gbps**, or **Auto**. For example, select the **3.0000 Gbps** option from the pull-down menu to set the link speed to 3.0000 Gbps.

For 6G SAS/SATA blades and systems, the link speed can be set to the highest rate supported by the blade containing the ports, a supported lower rate, or one of the **Auto** selections. The Xgig 6G SAS/SATA Wide-Port/4x Blade, the 6G SAS/SATA Narrow blade, and the LX and LXP fixed-port systems support 1.5000 Gbps, 3.0000 Gbps, and 6.0000 Gbps. For example, select the **3.0000 Gbps SAS** option from the **Link Speed** pull-down menu to set the link speed to 3.0000 Gbps. These blades and systems also have an auto-detect option, which will automatically detect the link speed between 1.5000 Gbps, 3.0000 Gbps, and 6.0000 Gbps.

The Auto options available for 6G SAS/SATA blades and systems are **SAS 6/3/1.5G & SATA 3/1.5G** and **SATA 6/3G.** For the **Auto** options, no actual negotiation or handshake takes place between the analyzer and any external device – the blade ports merely detect the data speed from the speed negotiation sequence happening on the link. The **Auto** options can automatically determine the link speed only if the Xgig ports see the link initialization activities that take place (for example, OOB and speed negotiation events). If link initialization sequence does not happen while an **Auto** option is set, the blade will retain its existing speed. For example, select the **1.5000 Gbps** option for the Link Speed in the TraceControl Configuration window to set the link speed to 1.5000 Gbps. Then select the **Auto (SAS 6/3/1.5G & SATA 3/1.5G)** option for the Link Speed. If no link initialization happens, the speed of the blade will still be 1.5000 Gbps.

For 12G SAS blades, the link speed can be set to the highest rate supported by the blade containing the ports, a supported lower rate, or one of the **Auto** selections. The Xgig5000 12G SAS Wide Port blade and the Xgig1000 12G SAS blade support a link speed 3.0000, 6.0000, or 12.0000 Gbps. These blades and systems also have an auto-detect option, which will automatically detect the link speed between 3.0000 Gbps, 6.0000 Gbps, and 12.0000 Gbps.

The Auto options available for 12G SAS blades are **Auto (SAS 12/6G)**, **Auto (SAS 12/6/3G)**, and **Auto (SAS 6/3G)**. For the **Auto** options, no actual negotiation or handshake takes place between the analyzer and any external device – the blade ports merely detect the data speed from the speed negotiation sequence happening on the link. The **Auto** options can automatically determine the link speed only if the Xgig ports see the link initialization activities that take place (for example, OOB and speed negotiation events). If link initialization sequence does not happen while an **Auto** option is set, the blade will retain its existing speed. For example, select the **3.0000 Gbps** option for the Link Speed in the TraceControl Configuration window to set the link speed to 3.0000 Gbps. Then, select the **Auto (SAS 6/3G)** option for the Link Speed. If no link initialization happens, the speed of the blade will still be 3.0000 Gbps.

For PCIe, the link speed can be set to the highest rate supported by the blade containing the ports, or a supported lower rate. Available rates for Xgig PCIe, in GT/s, are 2.5 (Gen1), 5.0 (Gen2), and 8.0 (Gen3). You can also select **Auto**, and the Xgig will select the correct speed based on the device under test, and if it cannot, it will default to 8.0 (Gen3).

For the Xgig5000 16G FC blade, the speed can be set to **4.2500**, **8.5000**, or **14.0250 Gbps**.

For the Xgig5000 10G Ethernet blade, if it is being used at 10G, the speed is set to **10.3125 Gbps** and cannot be changed. If the blade is being used as a 40G Analyzer, the speed is set to **41.2500 Gbps** and cannot be changed.

For the 10 Gigabit Multi-Function FC blade, the speed is fixed at **10.5187 Gbps** and cannot be changed. For the GE blade, the speed is fixed at **10.3125 Gbps** and cannot be changed.

Signal Regeneration

The signal can be digitally retimed. See “Signal Regeneration” on page 99 for more information about signal regeneration settings. Select the **Digital Retime** option in the **Signal Regeneration** column to retransmit the signal using the analyzer's clock. Jitter is eliminated and fill characters are added or deleted in compliance with the specification of the protocol for the network data. If the hardware setting is **Analog Passthrough**, the received signal is buffered and retransmitted without modification.

There are two Analog Passthrough options available, **Analog Passthrough** and **Analog Passthrough Multiplexed**. Note that **Analog Passthrough Multiplexed** is only available for 6G SAS/SATA blades.

Digital retiming is currently supported in FC, GE (except 40G Ethernet) and SAS/SATA Analyzer ports. For SAS/SATA Analyzer ports, **Digital Retime** is only available for the 6G Wide-Port blade.

Warning: Changing the signal regeneration between Analog Passthrough and Digital Retime may cause loss of data on the network. Changing the link speed when the signal is digitally retimed may also cause data loss.

Scrambling

This setting applies only to the 8G Fibre Channel ports and PCIe ports. However, the scrambling setting for PCIe ports is on the **Lane Control** tab in TraceControl, not on the **General Setting** tab. See “Lane Control” on page 136 for instructions on using the Scrambling setting on the Lane Control tab. This setting allows you to specify whether the capture will include scrambled data. Select Fibre Channel ports, and check the **Scrambling** box to enable scrambling.

When capturing data using analyzer ports on the new 8G Fibre Channel blade, you can set the link speed so that the capture will include or not include scrambled data. By default, scrambled data is turned on for 8.5000 Gbps captures and turned off for lower-speed captures. You must set the **Link Speed** to 8.5000 (Scrambling Off) to turn off the data scrambling feature for 8.5000 Gbps link speed. You must set the **Link Speed** to the 2.1250 (scrambling On) option to turn on the data scrambling feature for 2.1250 Gbps link speed.

When capturing data using analyzer ports on the Xgig1000 with 16G FC functionality, you can set the link speed so that the capture will include or not include scrambled data. By default, scrambled data is turned on for 8.2500 Gbps captures and turned off for 4.2500 Gbps captures.

If you toggle between the scrambling and the non-scrambling mode for the same link speed, you will not get a warning message since scrambling does not affect the data path but only how the data is written to the buffer.

CDR (Clock Data Recovery)

This setting only applies to the 10GigE ports on the 40G Xgig1000 chassis. The CDR cleans the signal output after passing through the analyzer. This is similar to a Digital Retime, but the signal is not completely re-created. It is just cleaned and re-clocked. The default setting is off.

Note: If you are using copper cables, turning the CDR setting on prevents the training signals from passing through the analyzer. If you want training signals to come through when using copper cables, turn this setting off.

FEC (Forward Error Correction)

This setting only applies to 16G Fibre Channel ports with the **Link Speed** set to 14.0250 Gbps, 10GigE ports on the 2 port 10G Multi-function Xgig blade, and 10GigE ports at all speeds on Xgig1000 systems. It allows you to specify whether FEC is enabled in the link or not. You can also set this option to **Auto**, and the Analyzer software will automatically determine whether or not the link contains FEC traffic and will capture the traffic either way. This is the default setting.

Force Clock Re-lock to Incoming Data

This option only appears when an 8G blade FC port or 6G blade SAS/SATA port is being monitored. When the Clock Detection Recovery (CDR) loses its lock on the incoming data signal, the link speed cell will turn red and display the message **CDR Loss of Lock**. This menu item forces the re-locking of the clock to incoming data on the corresponding port. If the ports are not locked or capturing, this menu will be grayed out.

For optical 8G blade FC ports, if this option fails to re-lock the signal, clean the fiber optic connections and check the signal.

Port Settings - Lane Control Tab

The **Lane Control** tab in TraceControl’s **Configuration Manager** is shown also in Performance Monitor. This tab is only available when a PCIe blade is being monitored. This tab has limited functionality in Performance Monitor. See “Lane Control” on page 136 for instructions on using all of the settings on this tab.

Performance Monitor Options

View options affect the monitoring display. Not all settings affect all views. Start by setting **Preferences**.

Preferences

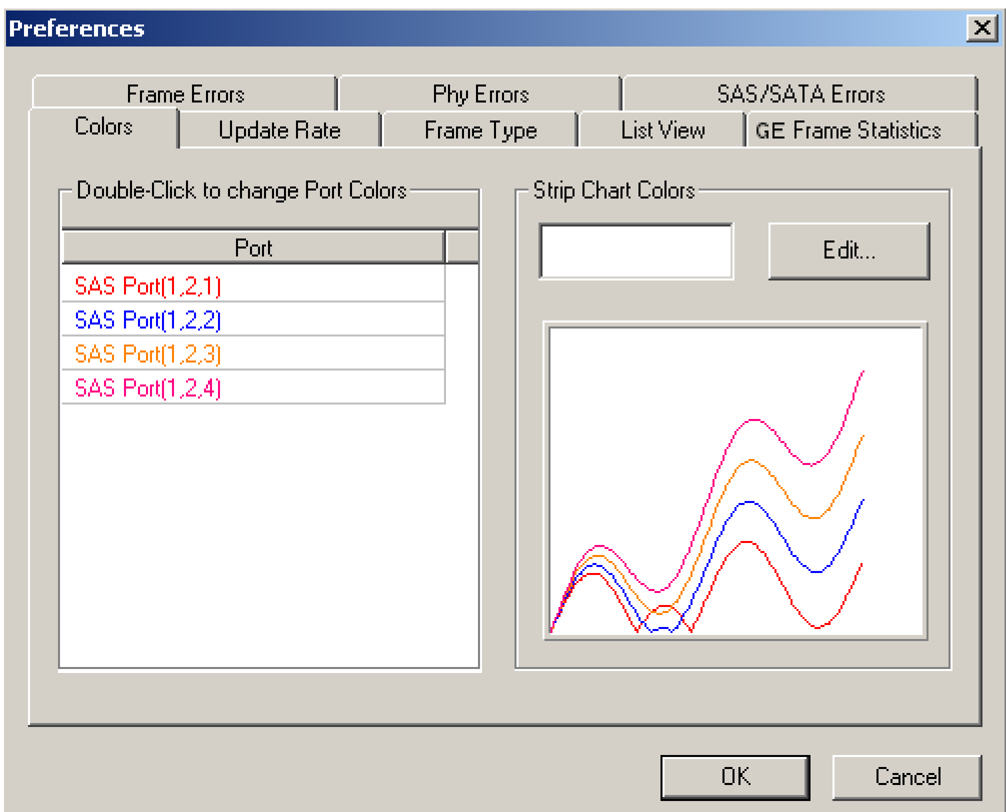
Set general display preferences by selecting **Preferences...** from the **Options** menu. You can also right-click in any view, and select **Preferences...** from the menu.

Color Preferences

Change the colors of the port names by double-clicking on the port name in the list on the left. A dialog box will display to select a new color for the port display.

The background of the strip chart can also be changed by pressing the **Edit** button. When you change the background color of strip chart, the strip chart color editor will be updated to preview the background color of the strip chart with the foreground colors of the ports.

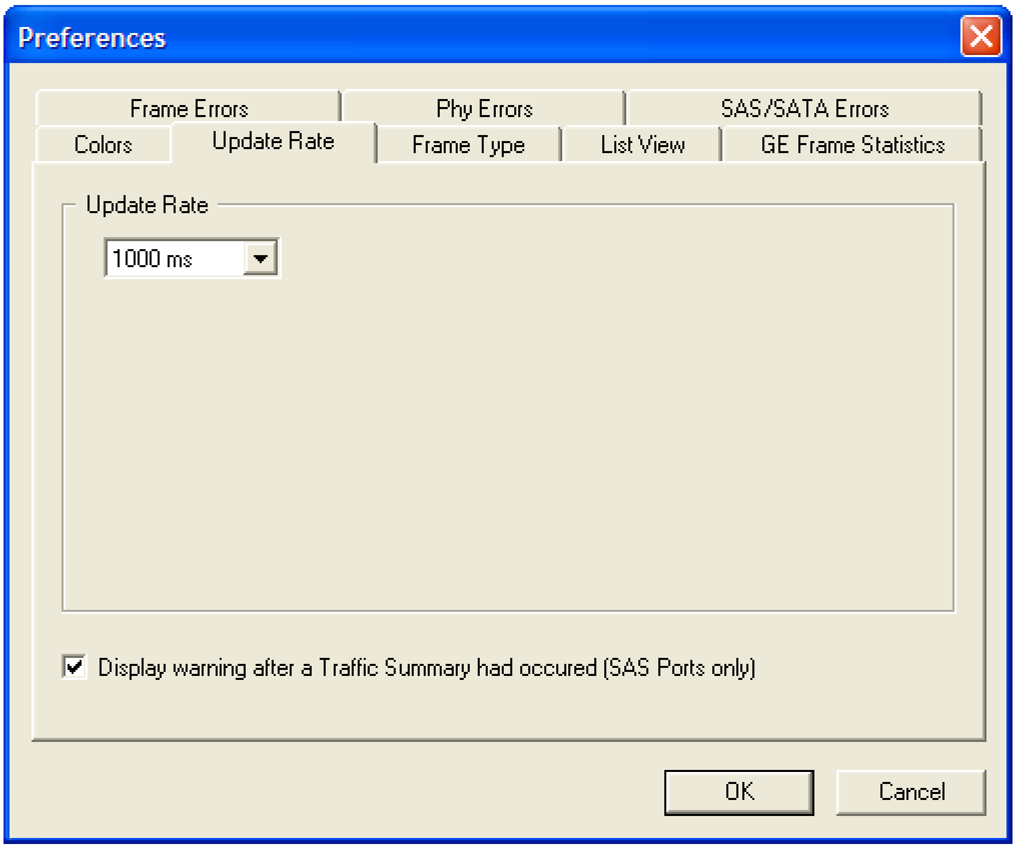
Figure 79: Color Preferences



Update Rate

Select the **Update Rate** tab to set the refresh rate for all monitor views. Choose the rate from the **Update Rate** pull-down menu. The default is to update all views every 1000ms. This tab also has a checkbox that, when checked, will display a warning after a Traffic Summary has occurred. This is for SAS ports only.

Figure 80: Update Rate Preference



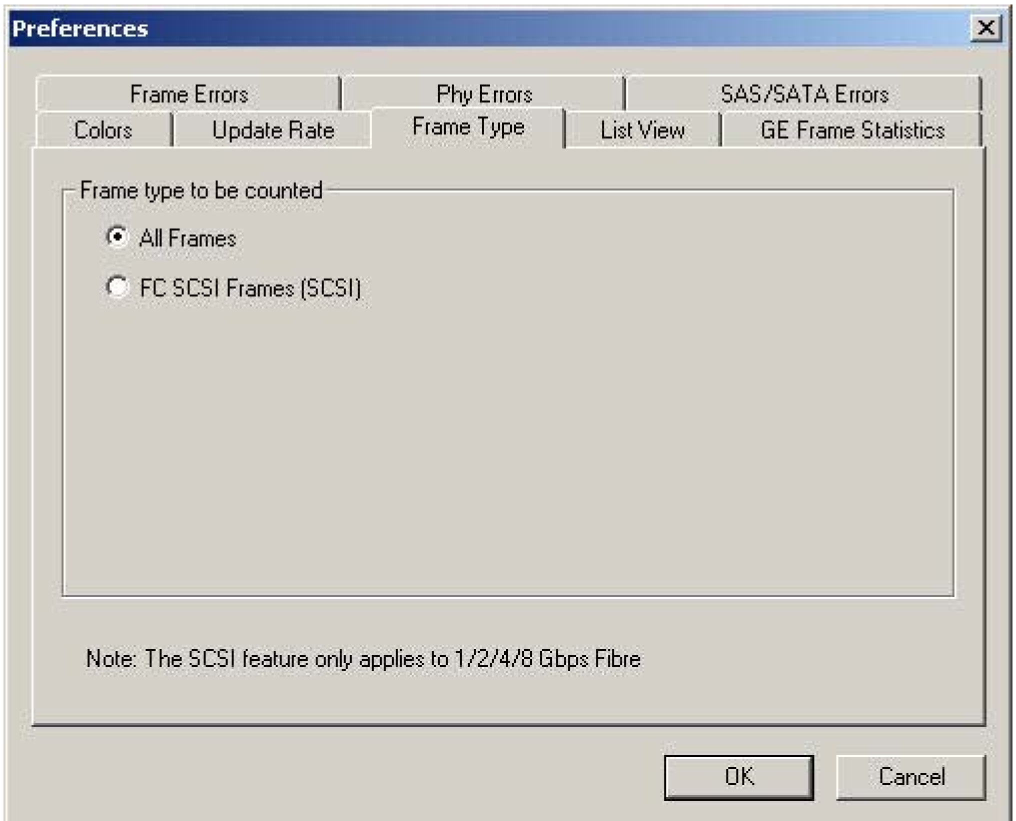
Frame Type

Select the **Frame Type** tab to choose the type of FC frames to display in all views. To view SCSI frames only, click the **FC SCSI Frames** radio button. To view all frames, click the **All Frames** radio button.

The **FC SCSI Frames** option applies to 1/2/4/8G Fibre Channel analyzer ports only. When this option is selected, the frame counter (in KFrames/sec) counts the SCSI Command frames only (frames with RCtl=0x06 and Type=0x08). The throughput (in MB/sec) is calculated based on SCSI Data frames (RCtl=0x01 and Type=0x08).

This option will be gray if there are no Fibre Channel ports being monitored.

Figure 81: Frame Type Preference

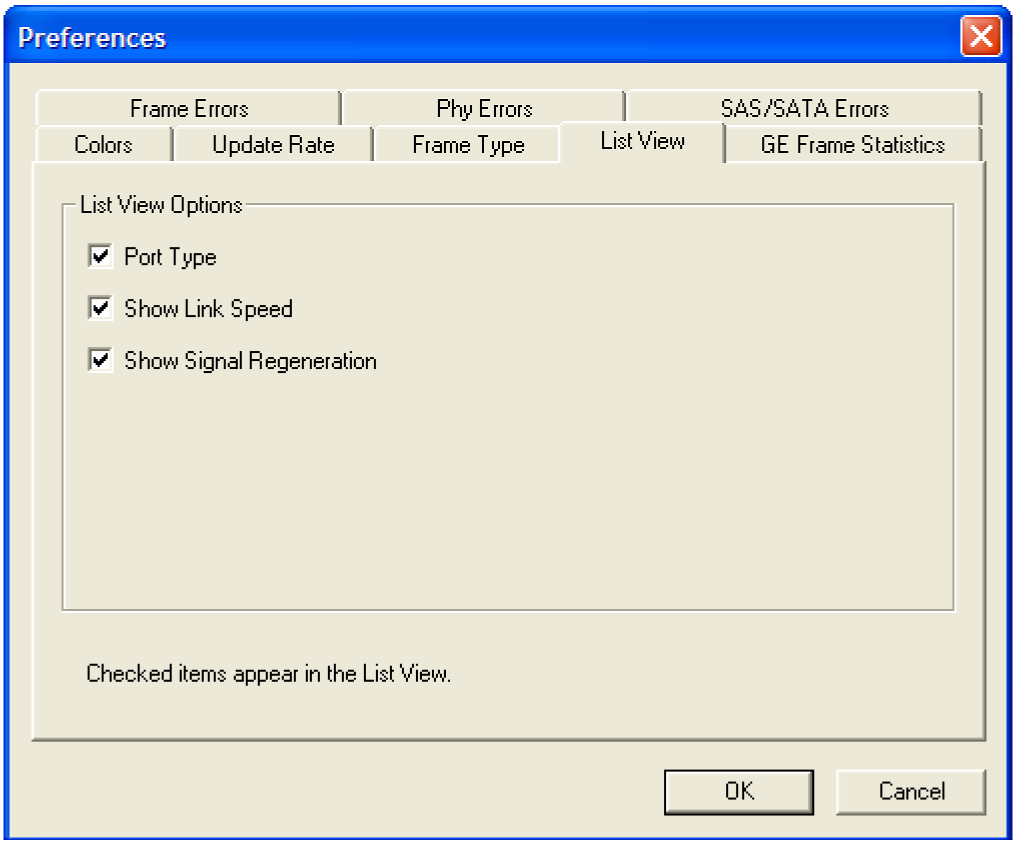


List View

Select the **List View** tab from the **Preferences** dialog box to hide or view certain columns in List View. Columns that can be displayed/hidden are:

- Port Type
- Link Speed
- Signal Regeneration

Figure 82: List View Preferences



GE Frame Statistics

Select the **GE Frame Statistics** tab from the **Preferences** dialog box to hide or view specific Gigabit Ethernet statistics in List View. All of the options will be gray if there are no Gigabit Ethernet ports being monitored.

Figure 83: Frame Statistic Preferences

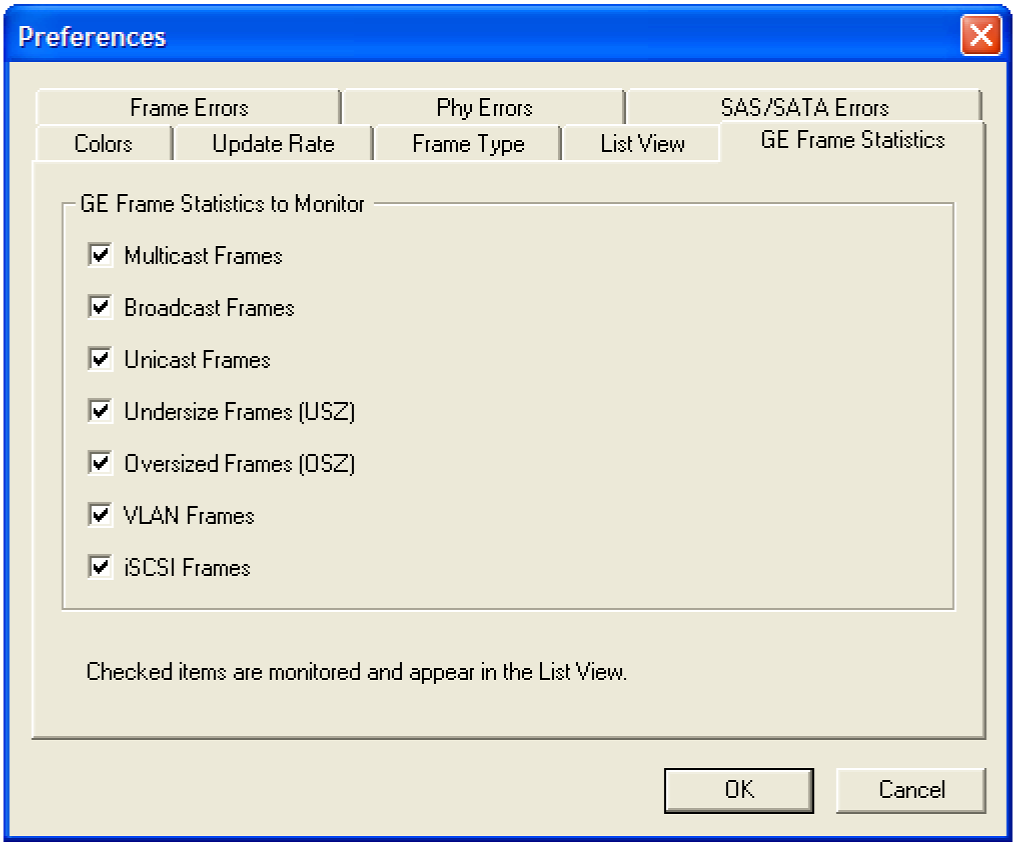


Table 10 shows the frame counters that are available when at least one GigE analyzer port is monitored and provides a brief definition of the frame counters.

Table 10: GE Frame Counters

Error Counter	1GigE Ports	10GigE Ports	Description
Mulitcast Frames	YES	YES	Count of all Ethernet multicast frames.
Broadcast Frames	YES	YES	Count of all Ethernet broadcast frames.
Unicast Frames	YES	YES	Count of all Ethernet unicast frames.
Undersized Frames	YES	YES	The total number of packets received that were shorter than 64 octets and were otherwise well formed (good FCS).
Oversized Frames	YES	YES	The total number of packets received that were longer than 1518 octets and were otherwise well formed (good FCS).
VLAN Frames	YES	YES	Count of all Ethernet frames containing VLAN IDs.
iSCSI Frames	YES	YES	Count of all SCSI frames encapsulated within Ethernet frames.

Frame Errors

Select the **Frame Errors** tab from the **Preferences** dialog box to hide or view specific frame errors in List View. Jabbers and Fragmented Frame error counters will be gray if no Gigabit Ethernet port is being monitored. The FCoE Embedded CRC error counter will be grayed out if no 10G port supporting FCoE is being monitored.

Figure 84: Frame Error Preferences

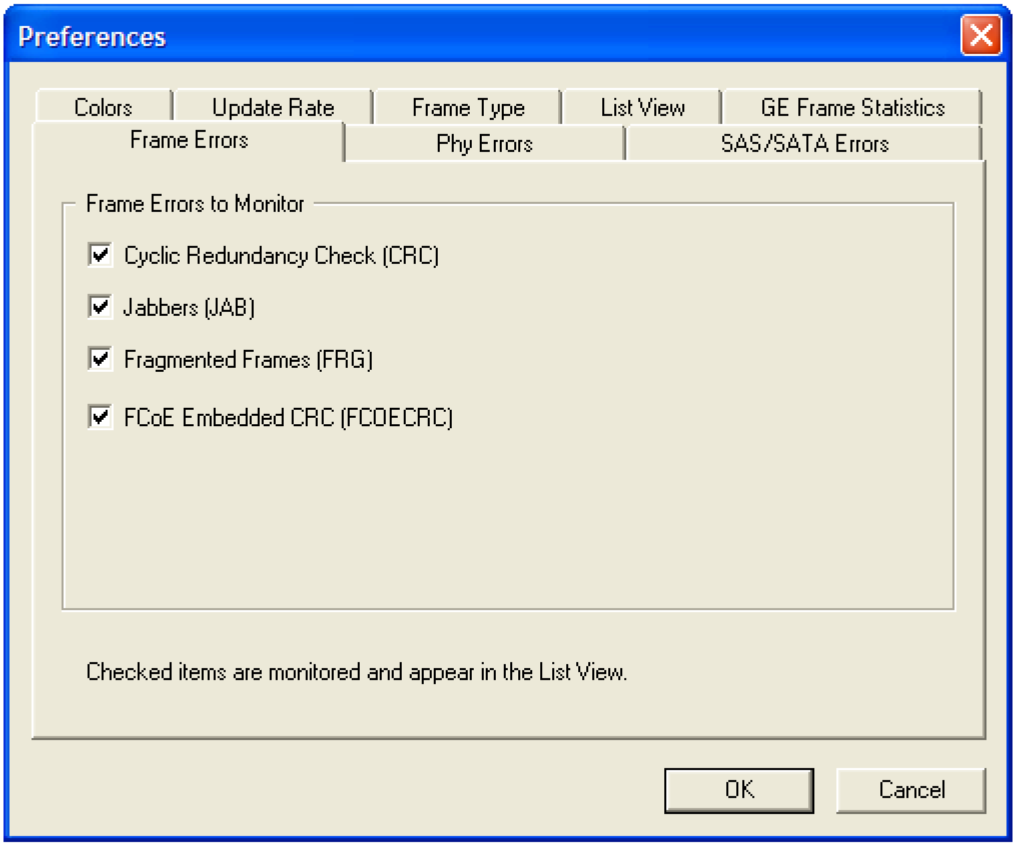


Table 11 shows the frame error counters that are available for each analyzer blade and provides a brief definition of the frame type.

Table 11: Frame Error Counters

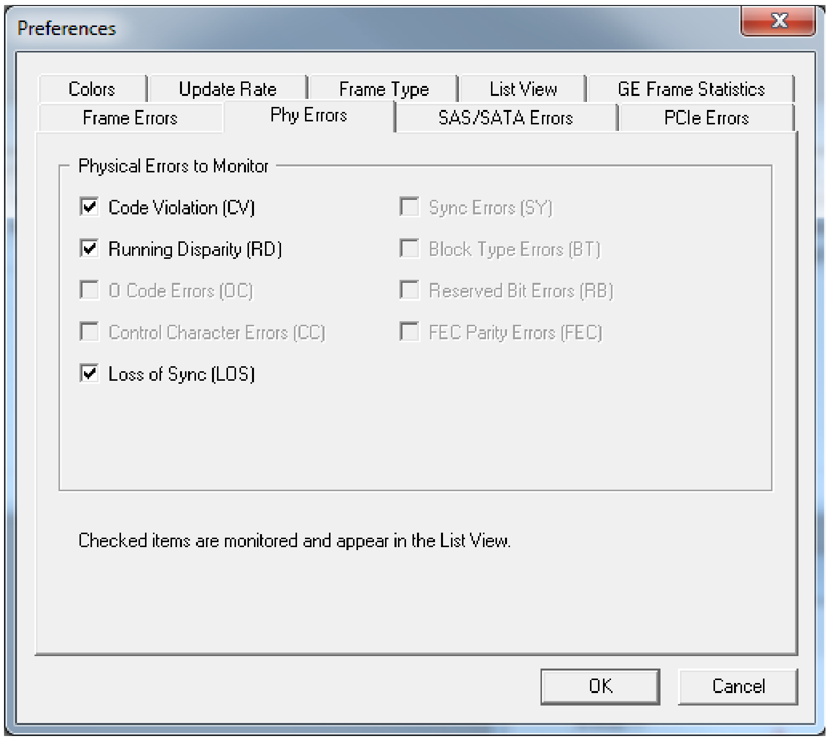
Frame Error Counter	1GigE Ports	10GigE Ports	FC Ports or SAS Ports	PCIe Ports	Description
Cyclical Redundancy Check	YES	YES	YES	YES	For GigE, the total number of packets received that had a length between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS/CRC Error) or a bad FCS with a non-integral number of octets (Alignment Error). For FC or SAS/SATA, checksum of encoded bits does not match the CRC value.
FCoE Embedded CRC	NO	YES	NO	NO	For FCoE, the total number of packets received where the checksum of encoded bits does not match the embedded CRC value.
Jabbers	YES	YES	NO	NO	The total number of packets that were received that were longer than 1518 octets and had either an FCS/CRC error or an Alignment Error.
Fragmented Frames	YES	YES	NO	NO	The total number of packets received that were less than 64 octets and had either an FCS/CRC error or an Alignment Error.

Phy Errors

Select the **Phy Errors** tab to choose which errors should be counted and displayed in the **List View.** Check the box for all error types to count and display. For example, if you want to count only CV errors, leave all boxes unchecked with the exception of CV errors.

Boxes for selecting an error counter are grayed out if they are not supported for the ports being monitored. This does not apply to Loss of Sync (LOS) errors.

Figure 85: Phy Error Display Preference



Unselected error types are not used in determining the value of a status LED for a port (see Status LEDs). For example, if CV errors are not selected, and the only errors detected for a port are CV errors, the status light for that port will remain green. Loss of Sync (LOS) errors are only available for PCIe ports.

For Xgig ports, columns for each selected error type that can be counted are displayed in List View. For Xgig ports, columns for unselected error types are not shown. For example, if CV errors are not selected, the CV Errors column will not display. For “state” errors, such as Loss of Signal or Loss of Sync, the current state will appear in the **Traffic Status** column.

Remote Xgig hosts may contain a mix of Xgig Analyzer ports that use different protocols and therefore have different error counters. If the Xgig host contains multiple port types that have different error counters, you will be able to select any counter that applies to least one of the ports in the host. In **List View**, the error counter will be marked with label N/A if the counter does not apply for a specific port on the host.

Table 12 lists the physical error counters that are available for each analyzer blade and provides a brief definition for each physical error.

Table 12: Phy Error Counters

Error Counter	1/2/4/8G Blades	3/6/12G (SAS/SATA)	10Gig Blade	Xgig5000 16G FC	PCIe	Description
Loss of Sync (LOS)	NO	NO	NO	NO	YES	Loss of Synchronization.
Running Disparity (RD)	YES	YES	NO	YES	YES	Incorrect Running Disparity value for an 8B/10B encoded block.
Code Violation (CV)	YES	YES	NO	YES	YES	Illegal 10-bit code in an 8B/10B encoded block.
O Code Errors (OC)	NO	NO	YES	YES	NO	The 4-bit O code in a 64B/66B encoded block contains an illegal value.
Control Character Errors (CC)	NO	NO	YES	YES	NO	Any control character in a 64B/66B encoded block contains an illegal value.
Sync Error (SY)	NO	NO	YES	YES	NO	The Sync Field in a 64B/66B encoded block has an illegal value (the first two bits of the block have a bit value of 00 or 11).
Block Type Errors (BT)	NO	NO	YES	YES	NO	The Block Type field in a 64B/66B encoded block contains a reserved value.
Reserved Bit Error (RB)	NO	NO	YES	YES	NO	A Reserved Bit field in 64/66b coding contains a 1. Reserved Bit fields in the block structure are expected to be sent as 0 (and ignored by the receiver).
FEC Parity Errors (FEC)	NO	NO	YES	YES	NO	Parity value of the FEC block is not correct.

SAS/SATA Errors

Select the **SAS/SATA Errors** tab from the **Preferences** dialog box to hide or view specific SAS/SATA errors in List View. These options will be gray if there are no SAS/SATA Analyzer ports currently being monitored.

Figure 86: SAS/SATA Error Preferences

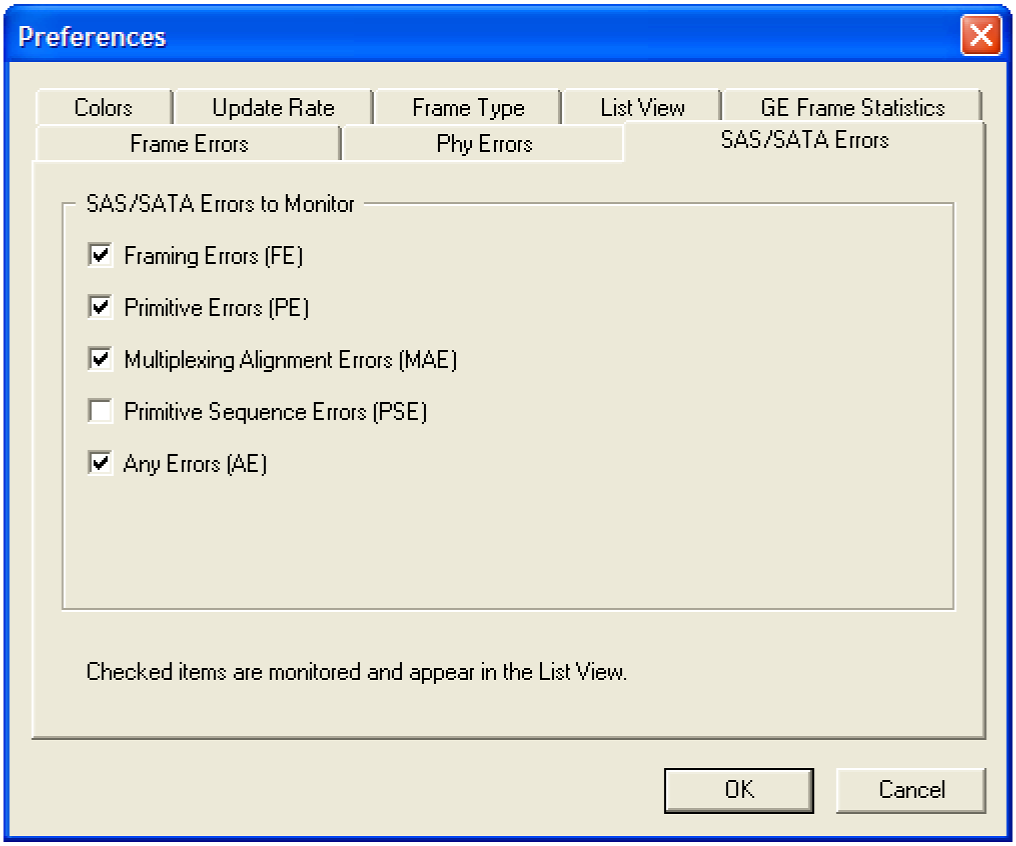


Table 13 shows the SAS/SATA error counters that are available for each SAS/SATA Analyzer port and provides a brief definition of the error type.

Note that Primitive Sequence Errors do not increment the Any Errors counter, regardless of which options are set.

Table 13: SAS/SATA Error Counters

SAS/SATA Error Counter	Description
Framing Errors (FE)	This counter increments when any of the following conditions are encountered: • An EOF that is floating and not completing a frame. • An SOF that comes after another SOF. • A Dword that abnormally terminates a frame (e.g., a Primitive during a frame that isn't allowed in frames).
Primitive Errors (PE)	This counter increments when any Dword that has a K-character does not translate into one of the standard SAS or SATA Primitives from the specification.

Table 13: SAS/SATA Error Counters (continued)

SAS/SATA Error Counter	Description
Primitive Sequence Errors (PSE)	This counter increments when any of the following conditions are encountered: • In SAS, when a Dword interrupts either a Triple or Redundant Primitive Sequence • In SAS, when a Triple or Redundant Primitive Sequence is started without having the required gap since the previous Primitive Sequence • In SAS, when more than 3 consecutive Identical Triple Primitives are detected as part of the Triple Primitive Sequence, or more than 6 consecutive identical Redundant Primitives are detected as part of a Redundant Primitive Sequence • In SATA, for any violation of the structure of a Continued Primitive Sequence. This is strictly 2 or more Primitives, followed by a CONT Primitive, followed by Scrambled Primitive Data or CONT Primitives. For example: One Primitive followed by a CONT, or a missing CONT Primitive, etc.
Multiplexing Alignment Errors (MAE)	This counter increments when a multiplexing alignment error occurs. These errors can occur only when the signal through the port contains two logical channels. Every other Dword on the physical port must belong to a single logical channel.
Any Errors (AE)	This counter increments when any of the following errors are encountered: • Bad OOB or Speed Negotiation error • Framing Error • CRC Error • Loss of Sync • CV • Disparity Error • Primitive Error

PCIe Errors

Select the **PCIe Errors** tab from the **Preferences** dialog box to hide or view specific PCIe errors in List View. These options will be gray if there are no PCIe Analyzer ports currently being monitored.

Figure 87: PCIe Error Preferences

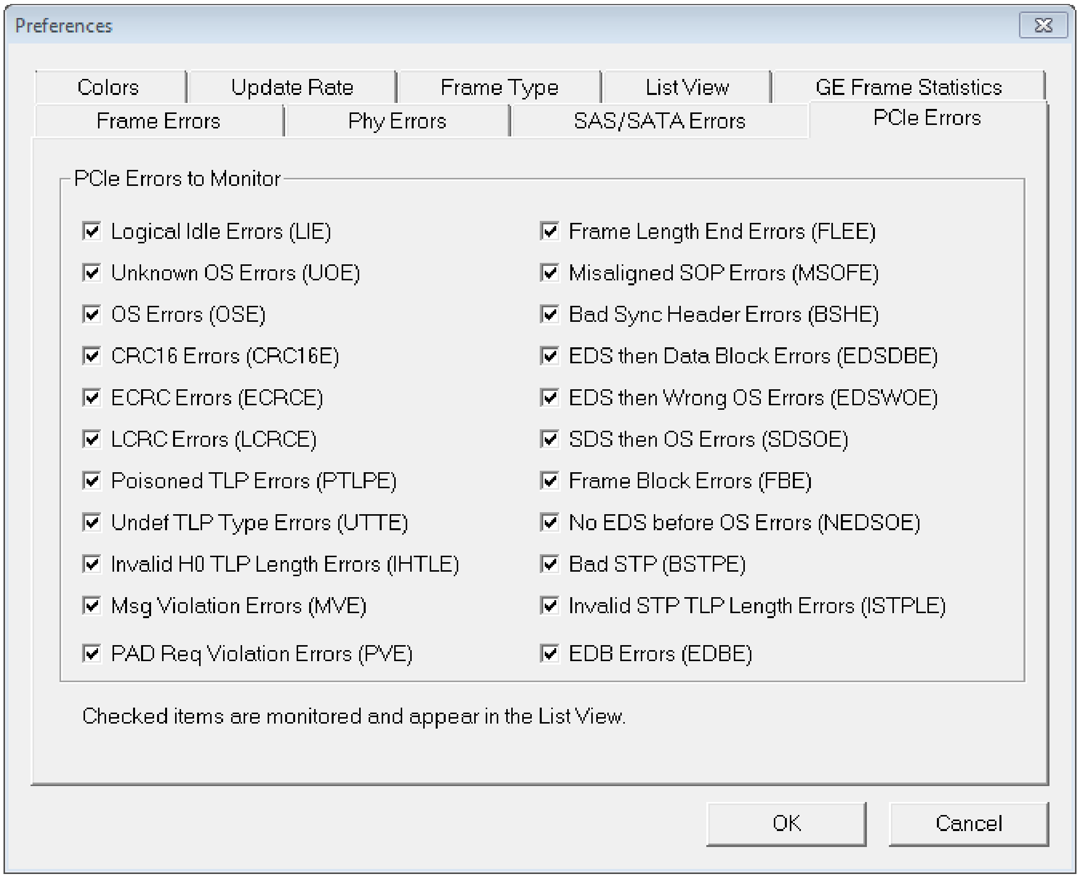


Table 13 shows the PCIe errors that are available for each PCIe Analyzer port and provides a brief definition of the error type.

Table 14: PCIe Errors

PCIE Errors	Description
Logical Idle Errors (LIE)	At Gen3, when the Logical Idles aren't 0x00 in a Data Block (with Sync Bits=10)
Unknown OS Errors (UOE)	At Gen1/2, when an Ordered Set is not one of the known Ordered Sets
OS Errors (OSE)	At Gen1/2, this indicates that this byte of an Ordered Set does not match the expected value for the current Ordered Set being decoded (or is an illegal value)
CRC16 Errors (CRC16E)	DLLP CRC error
LCRC Errors (ECRCE)	TLP LCRC error
ECRC Errors (LCRCE)	TLP optional Digest ECRC Error
Poisoned TLP Errors (PTLPE)	The TLP header bit "Error Forwarding" = 1
Undef TLP Type Errors (UTTE)	When the TLP "Fmt/Type" field has an invalid value

Table 14: PCIe Errors (continued)

PCIE Errors	Description
Invalid H0 TLP Length Errors (IHTLE)	At Gen3, when the STP TLP Length field is inconsistent with the TLP Header Length field (see also " Gen3 Invalid STP TLP Length")
Msg Violation Errors (MVE)	Within a TLP Message packet, one of the following: Any Assert_INTx/Deassert_INTx Message with Traffic Class other than TC0 Any Power Management Message with Traffic Class other than TC0 Any Error Signaling Message with Traffic Class other than TC0 Any Unlock Message with Traffic Class other than TC0 Any Unlock Message with Traffic Class other than TC0 Any Set_Slot_Power_Limit Message with Traffic Class other than TC0 Any LTR Message with Traffic Class other than TC0 Any OBFF Message with Traffic Class other than TC0 Any undefined value in the Message Code Field
PAD Req Violation Errors (PVE)	At Gen1/2, when a PAD Kchar is supposed to be present but isn't
Frame Length End Errors (FLEE)	At Gen1/2, when the TLP Length field is inconsistent with the End-of-Packet position, i.e. it is too small or too large compared to the End-of-Packet
Misaligned SOP Errors (MSOFE)	Gen1/2 Start-of-Packet isn't in lane 0 or lane 4
Bad Sync Header Errors (BSHE)	At Gen3, the 2 Sync Header bits are either 00 or 11, which is illegal
EDS then Data Block Errors (EDSDBE)	At Gen3, when a 130b Data Block (with Sync=10) is found after EDS, which is illegal
EDS then Wrong OS Errors (EDSWOE)	At Gen3, when the wrong 130b Ordered Set Block (with Sync=01) is found after EDS
SDS then OS Errors (SDSOE)	At Gen3, after a SDS, a Data Block is expected (Sync=10), but we got an Ordered Set Block (Sync=01)
No EDS before OS Errors (NEDSOE)	At Gen3, an EDS is expected at the end of a Data Block (Sync=10) before an Ordered Set Block (Sync=01), but it did not happen
Frame Block Errors (FBE)	At Gen3, this indicates when a frame is interrupted by a non-data Sync Header bits (i.e. Sync != 10)
Bad STP Errors (BSTPE)	Gen3 only, this indicates when there is an error detected in the FP or FCRC of the STP
Invalid STP TLP Length Errors (ISTPLE)	At Gen3, when the STP TLP Length field is smaller than 5 (see also "Invalid TLP Length")
Bad End of Packet (EDBE)	TLPs or DLLPs with EDB ending

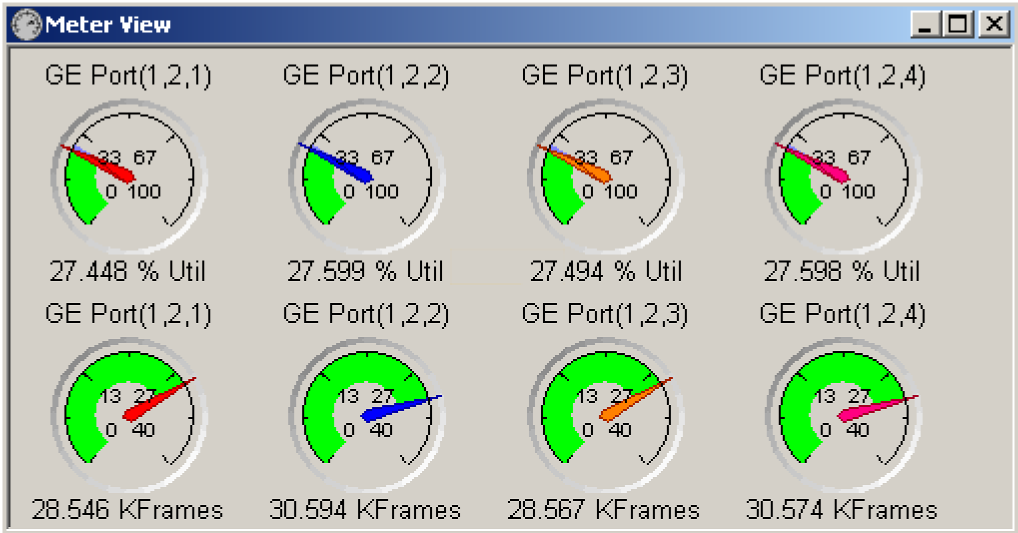
Utilization Display Option

Select **Show Utilization** from the **Options** menu or right-click in the Chart View or Meter View and select Show Utilization. This option allows you to change the display in Meter View or Chart View between a measurement expressed in MBytes/sec and a utilization percentage based on the total capacity of the link.

Note that the metric option to display Utilization or MBytes/sec must be selected in the Metric Options menu for the utilization percentages to display. The Metric Options menu is activated by selecting **Metric Options…** from the **Options** menu or by right-clicking on the Chart View or Meter View and selecting **Metric Options…**. The toggle between display of Utilization or MBytes/sec is a global setting and will affect both Chart View and Meter View.

The average utilization value is calculated by sampling and averaging the most recent 15 minutes of data. The utilization meters will display both running average and current utilization values on the same meter. The current value is displayed with green highlighting while the average is displayed with a purple highlight.

Figure 88: Utilization Percentage Display Example in Meter View



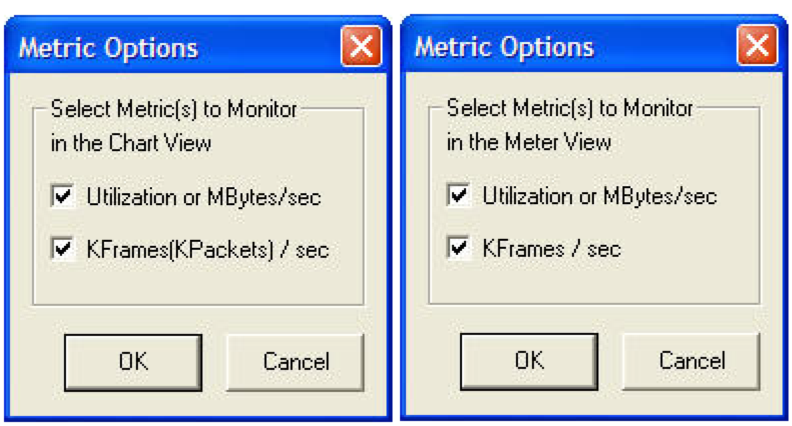
Metric Options

The Metric Options menu is activated by selecting **Metric Options…** from the **Options** menu or by right-clicking on the Chart View or Meter View and selecting **Metric Options…**.

The **Metric Options** dialog box allows you to change what is being monitored by the Chart View or Meter View, for example Utilization or MBytes/sec and KFrames/sec. **Either Utilization or MBytes/sec** can be selected from the **Show Utilization** option of the Options menu if this Metric Option is selected for the view**.**

Metric Options are applied to either **Chart View** or **Meter View**. The Metric Options for each view are independent of the other views.

Figure 89: Metric Options Dialog Boxes

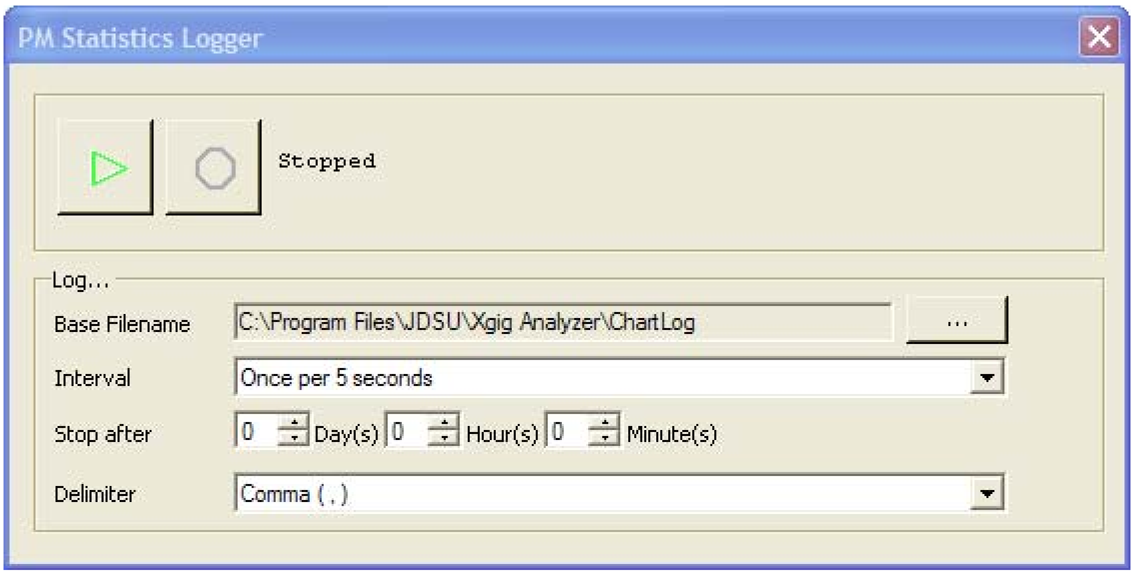


Statistics Logging Function

Performance Monitor data (the data in List View) can be saved to a .csv file. The .csv files can be directly imported into Microsoft Excel. In the PM Statistics Logger dialog box, you specify the interval at which data points are saved, how many hours Performance Monitor will continue to save log files, and the .csv file delimiter type. A separate log file is saved for each port and each link in the Resource Browser and List View. The values displayed on the various tabs in the List View are saved, regardless of which tab is currently active.

Select **Log Manager...** from the **Options** menu to bring up the PM Statistics Logger dialog box (see Figure 90). Use the start and stop buttons at the top of the dialog box to start and stop the logging process. Logging is turned off by default. You can also use the red record button in the toolbar to start and stop the logging process.

Figure 90: Performance Monitor Statistics Logger



Base Filename (and Location)
Data is saved as one file per port or link with the start date, start time, and port or link name appended to the base file name. The file name format is: <basefilename> _<day_month_year_hour.minute.second>_<Port_Name or Link_Name>; for example, **ChartLog_28_02_07_13.07.22_FC Port(1,1,1)**. All statistics in the List View will be saved to the file, one file for each port or link.

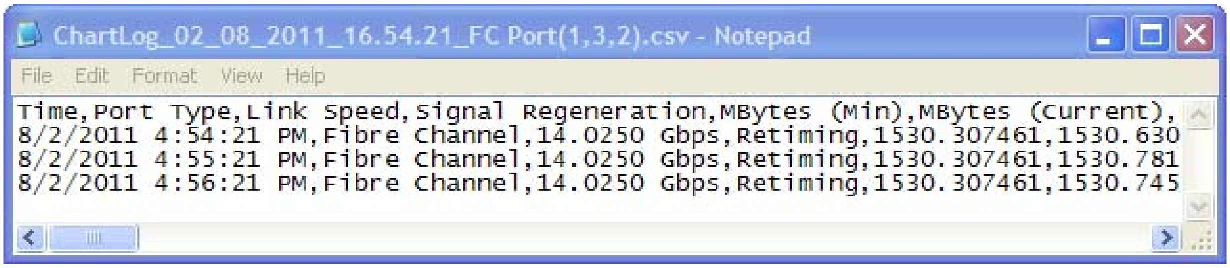
Stop after
Sets the overall time, in number of days, hours, and minutes, for which information will be written to log files. For example, if the **Interval** is set to 1 minute and **Stop after** is set to 2 hours (120 minutes), 120 log entries will be written to each single-port log file.

Interval
Sets the interval for gathering and writing data to the log file. Data for each interval shows in Microsoft Excel as another row. Options available are once per 1, 5, 20, or 30 seconds, 1 minute or 1 hour.

Delimiter
Delimiters provided are comma (,) , semicolon (;) , or tab (\t). The delimiter specifies the character(s) inserted in the .csv file to determine the end of a value and the beginning of a new value. Delimiters are interpreted by Microsoft Excel when the .csv file is imported. Comma is the default choice for the delimiter, which is also the default delimiter used by Microsoft Excel.

An example .csv file for a single port is shown in Figure 91 using a comma as the delimiter. Note that for display purposes not all entries are shown.

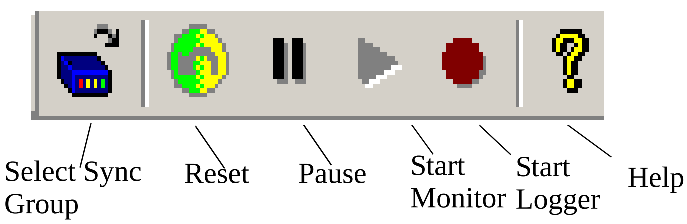
Figure 91: Example .CSV Log File


ChartLog_02_08_2011_16.54.21_FC Port(1,3,2).csv - Notepad
File Edit Format View Help
```
Time,Port Type,Link Speed,Signal Regeneration,MBytes (Min),MBytes (Current),
8/2/2011 4:54:21 PM,Fibre Channel,14.0250 Gbps,Retiming,1530.307461,1530.630
8/2/2011 4:55:21 PM,Fibre Channel,14.0250 Gbps,Retiming,1530.307461,1530.781
8/2/2011 4:56:21 PM,Fibre Channel,14.0250 Gbps,Retiming,1530.307461,1530.745
```

Toolbar Functions

You can start, pause, and reset Xgig Performance Monitor from the toolbar.

Figure 92: Toolbar Functions, Xgig Performance Monitor



PART FOUR: Using Xgig TraceView

Chapter 11
About Xgig TraceView

In this chapter:

- Introducing Xgig TraceView

Introducing Xgig TraceView

Xgig TraceView is one of the four programs that comprise the Xgig Analyzer software suite. Xgig TraceView views and analyzes a trace captured using Xgig TraceControl. TraceView allows you to:

- Display captured data from several perspectives: histogram, traffic flow, and frame content
- Search and filter data
- Export and import traces or sections of traces
- Add, move, and redefine display columns
- Navigate and view data density through a histogram display of the data
- Navigate via user-defined bookmarks
- Show embedded protocol values, including errors as 10-bit values

Xgig Analyzer software supports the Xgig family of test/analysis devices. The Xgig, Xgig1000, and Xgig5000 allow you to analyze networks with a variety of protocols, including Fibre Channel, SAS/SATA, Gigabit Ethernet, and PCIe. The function of ports on blades in a chassis is controlled through TraceControl software.

Chapter 12

Getting Started with Xgig TraceView

In this chapter:

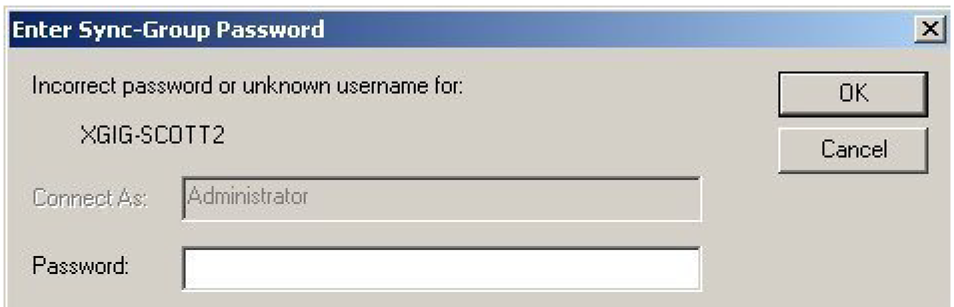
- Launching Xgig TraceView
- Working With Domains

Launching Xgig TraceView 

Secure Login for Xgig Chassis

Xgig chassis may be password protected to prevent access by unauthorized users. Password protection is set through the Xgig Web Utility for each Xgig chassis. If the Xgig chassis you are attempting to access is password protected, you are required to provide the password. The following login screen will appear. Enter the password to continue; the account name is always Administrator.

Figure 93: Xgig Analyzer Login



Login is only required once from any of the Xgig Analyzer applications or Xgig Maestro running on the same Xgig Analyzer PC client machine. For example, if you login through TraceControl, you will not be asked for the password again when you access the same Xgig chassis Sync Group through Xgig TraceView. To make sure you are completely logged off from all Xgig chassis, you must close all Xgig applications.

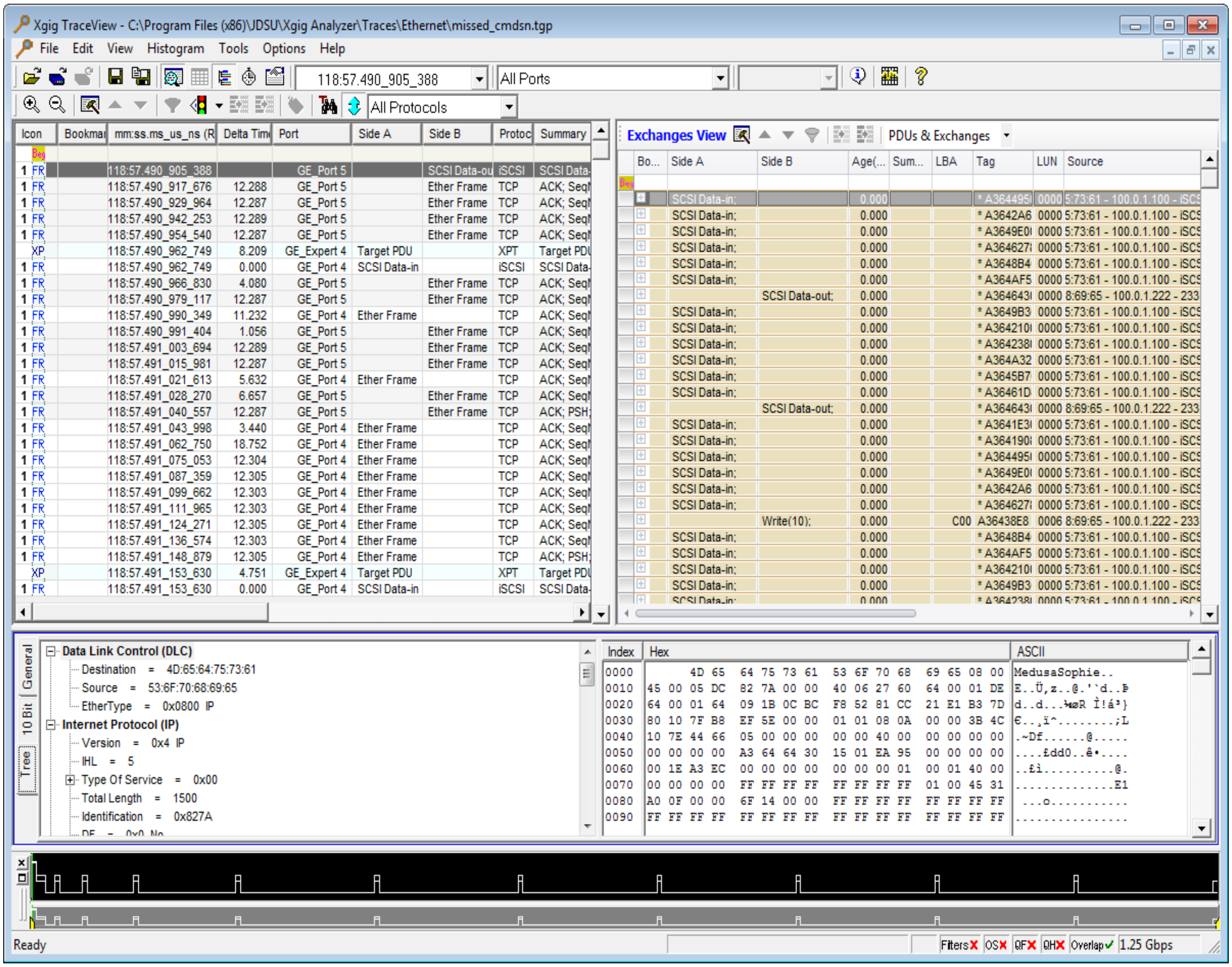
For login, the settings of a master chassis in a Sync Group prevail for all chassis in the Sync Group. If the master has authentication turned off and a slave(s) has authentication turned on, then the Sync Group as a whole has authentication turned off. The settings for the master chassis also prevail for the password; the password of the master chassis will be the password of any attached slave. See “Xgig Blade and Port Numbering” on page 45 and the *Xgig Family Hardware Guide*, the *Xgig5000 Family Hardware Guide*, or the *Xgig1000 Hardware Guide* for more information on master, slaves, and Sync Groups.

Launching the TraceView Application

Launch TraceView by pressing the **TraceView** icon on the desktop or by pressing the same icon in TraceControl. If you start TraceView from TraceControl and TraceControl has been used to capture traffic, the current contents of the analyzer devices will display in TraceView when you start the program. You can select **Open Domain...** from the **File** menu to select a domain of hardware ports and view the data in hardware buffers.

If you are using TraceView independently from TraceControl, select **Open File...** from the **File** menu to select the trace file you want to analyze.

Figure 94: TraceView Main Window



You can invoke the statistical analysis tool, Xgig Expert, from TraceView or have the Expert program launch at the same time as TraceView. Xgig Expert displays your trace in a chart form and a report form using an array of metrics. To invoke Xgig Expert from Xgig TraceView, select the **Xgig Expert**  icon from the toolbar.

A screen appears showing the progress of opening the trace in Expert. After the file has opened, the Expert Chart view screen appears.

By switching to Report View, you can view an abridged version of a report with compiled statistics taken over the entire trace. To return to TraceView, from the **Expert View** menu select Go to TraceView or click the **TraceView** icon on the toolbar.

Working With Traces

Traces are files that contain recorded information. Traces can be the information captured by a single pair or by multiple pairs of analyzer devices. If the trace contains recordings from multiple analyzers, the information is interleaved by timestamp when opened in Xgig TraceView.

If you choose to open a new trace, all your current views are closed. If you want to save your configuration and views, you should save the configuration before opening a new trace.

Working With Domains

Domains are a set of hardware analyzer ports. When you open a domain in Xgig TraceView you are viewing information that is currently stored in the capture buffers on analyzer hardware, but has not been saved to a trace file. A domain will only open if you have data in the buffers for ALL the ports belonging to the domain.

Domains are established and named in the Xgig TraceControl application. If you have multiple domains, you need to know what domains contain what hardware analyzers so you can pick the correct domain name.

If the domain contains multiple analyzers, the information is interleaved by timestamp when opened in Xgig TraceView.

If you choose to open a new domain, all your current views are removed. If you want to save your configuration and views, you should save the configuration before opening a new domain.

Open a Domain

To Open the Last Domain:

1 Press the **Open Last Domain** button. Or, from the **File** pull-down menu, select **Open Last Domain**.

2 If there is data in the analyzers for the last opened domain, the TraceView decode of the information will display. If there is no last domain, the **Select Ports/Domain to Analyze** dialog box appears. See the steps below for selecting a new domain. If no domains contain data or no domains have been established, TraceView returns an error message.

To Open a New Domain:

1 Press the **Open Domain** button. Or, from the **File** pull-down menu, select **Open Domain...**.

2 The **Select Ports/Domain to Analyze** dialog box appears. All Sync Groups within the local area subnet (including any Sync Group on your local machine) are displayed in the window on the top left. Select the Sync Group containing the hardware ports you want to view. If the hardware you wish to access is on a different subnet, type in the IP Address or Machine Name and press **Discover**.

3 If no domains contain data, no domains have been established for the Sync Group, or a data capture is in progress for the domain, TraceView returns a message informing you that no domain can be selected.

4 Select the domain name you want from the list.

5 If the domain you have selected contains multiple capture buffer segments, select the segment number from the **Segment(s)** drop-down box. No selection is required if there is only one segment.

6 Press the **OK** button.

Depending on the size of the trace buffer(s), it may take up to a minute for the information to load. It may take longer for trace buffers viewed over a LAN; the loading speed will depend on the speed of your network connection.

Opening a Trace

To Open a Trace:

1. Press the **Open File**  button. Or, from the **File** pull down menu, select **Open**. The **Open** dialog box appears.
2. Go to the directory where you have stored your trace. Select the file and select **Open**.

Depending on the size of the trace file, it may take up to a minute for the file to load.

When opening a trace, Xgig Expert is run automatically. If the trace has not been processed by Expert, a message appears asking if you would like to run Expert and process the trace. If you agree, Expert is run in the background. Once the trace has been processed, a message appears asking if you would like to reload the trace. You can also choose to view a partially processed trace; refer to “Viewing Partial Annotation in TraceView” on page 383. You can turn off automatic invocation of Expert by selecting *Options/Xgig TraceView Options* then choosing the **Expert / protocol decodes** tab and turning off the “Automatically launch Expert on new traces.” radio button in the **Annotations For New Traces** section.

Opening Files in Other Formats

TraceView and Expert support a wide variety of commonly used capture or trace file formats. Use the **Files of type:** option in the **Open** dialog to select the type of file to convert and open. Supported formats are listed below:

- Surveyor .hst and .cap files
- Bus Doctor (SAS, SATA)
- I-tech (SAS, SATA, Fibre Channel, GigE)
- Ethereal (including SUSE and RedHat special formats)
- libpcap / pcap
- tcpdump (Raw data format only, text or binary formats not supported)
- Sun Snoop (Raw data format only, text or binary formats not supported)
- Sniffer DOS format (not the newer Wildpackets or Sniffer Windows formats)
- Microsoft Network Monitor (NetMon) v2.0. (NetMon 1.x files are not supported.)
- NetScout v1.0 and v2.0 - both Ethernet and Fibre Channel formats

See “Converting Bus Doctor Files” on page 394 for complete information on converting Bus Doctor traces. See “Converting I-Tech Files” on page 396 for complete information on converting I-tech traces.

Cisco VT captures through Ethereal are detected and the embedded Fibre Channel inside of the Ethernet (Cisco's proprietary format) is converted to a Fibre Channel trace automatically.

TraceView and Expert launch a converter tool to convert the foreign file into a .tgp file in the same folder, and then they open the .tgp file. A progress bar with a cancel button is displayed during the conversion. If a .tgp file is found with the same name in the folder, a dialog will present conversion options. Options are to proceed with the conversion and overwrite the existing file, to reopen the open file dialog, or to cancel the current operation and return to the main application.

Data from foreign file formats are saved in a non-channelized format. That is, Tx and Rx captures are put into a single file, thus losing the original information about direction. The converter automatically re-channelizes the information so that Expert can display it correctly.

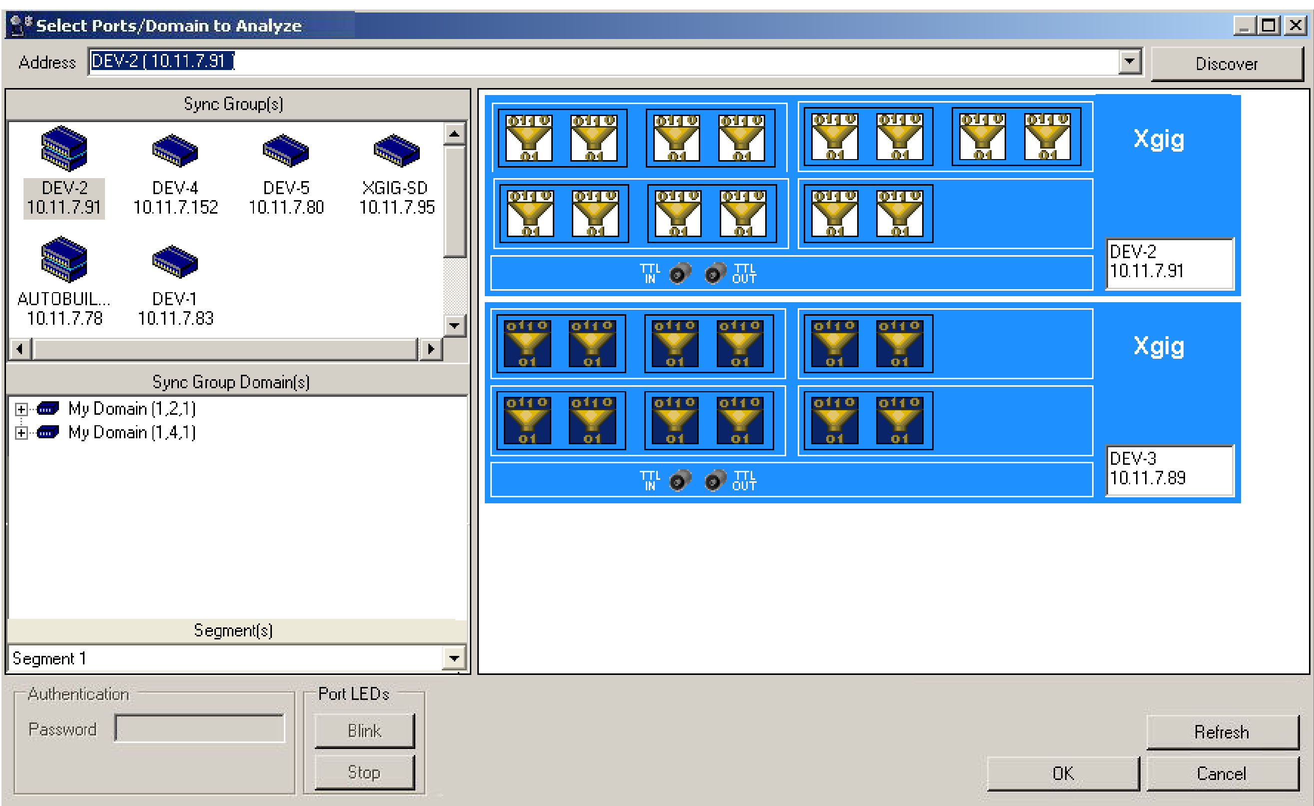
The converter also supports data rates and physical layers that are not handled/decoded by TraceView and/or Expert - i.e., ATM, SNAP, Token Ring, HLDC, IRDA, etc. Conversion is possible, but no useful decode information will be available.

During conversion to a .tgp file format, if a CRC value is not present for a frame, a placeholder value is inserted into the converted trace.

Select Ports/Domain to Analyze Dialog Box

Hosts are selected for viewing using the **Select Ports/Domain to Analyze** dialog box. Press the  button on the toolbar to bring up the dialog. The dialog indicates the type, availability, and status of ports. It also allows you to flash the LEDs of ports on an Xgig chassis.

Figure 95: Select Ports/Domain to Analyze Dialog Box



Discover Different Subnets

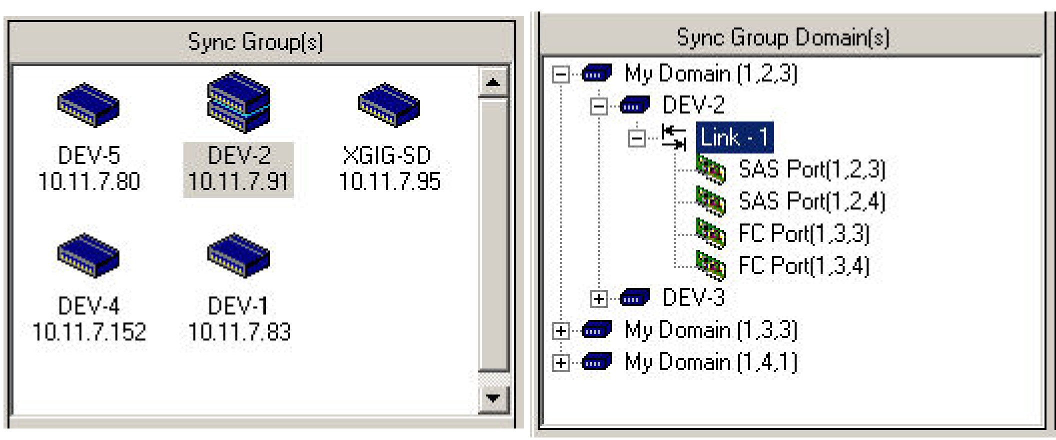
To select Sync Groups on a different subnet, enter the IP Address or DNS name in the **Address** field and press **Discover** (top of the dialog). The specific Sync Group you requested and all other Sync Groups on the same remote subnet will be added to the left panel.

Sync Groups and Domains

All Sync Groups discovered on the local subnet are displayed in the upper left panel. When you select a Sync Group, its chassis, blades and ports display in the right panel showing all available ports. If multiple chassis are cascaded to form a single Sync Group, the name and address of the master chassis within the Sync Group displays in the **Sync Group(s)** area. The addresses of slave chassis cascaded to the master do not display. However, you can use the name or address of a slave chassis in the **Address** area to discover a Sync Group on the subnet.

The **Sync Group Domain(s)** area lists all the domains of the selected Sync Group. Only one domain can be selected and used. When you select a domain where the ports in the domain contain no valid data, the **OK** button is grayed out. If none of the ports within the Sync Group contain valid capture data, a message appears in the Port Viewing and Selection area informing you that there is no domain for TraceView to interpret for the selected Sync Group.

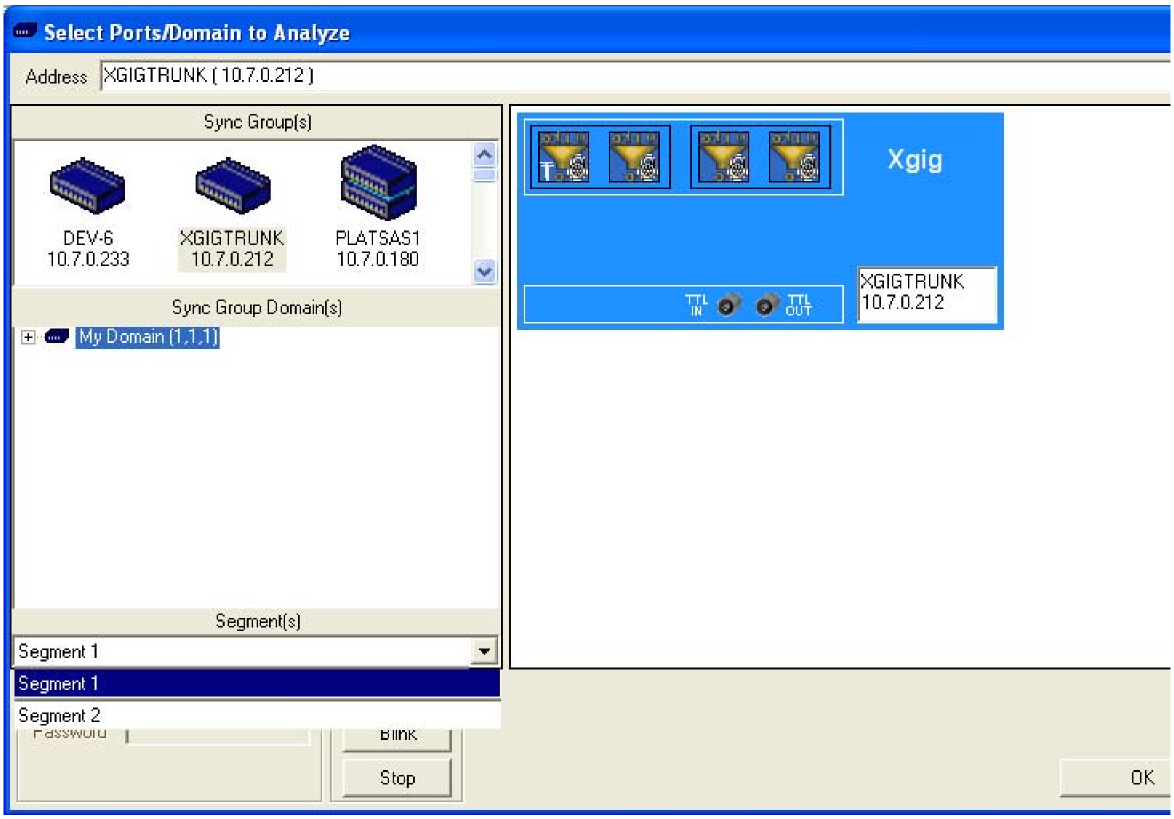
The **Sync Group Domain(s)** area shows the domain as a tree structure. The Sync Group and all links and ports within the Sync Group that comprise the domain are listed within the tree, providing a visual description of the domain contents. Ports may be listed directly under the Sync Group or listed under links if a link has been created for the domain. Links only apply to a single protocol where several port-pairs can be aggregated into a single physical link (for example, wide-port SAS). Links, like domains, are created in TraceControl. See “Sync Groups, Domains, Links, and Ports” on page 33 for more information on creating links.



Important: A valid capture is a capture that was previously made on the port. The domain that includes the port must still be intact for the capture to be valid; that is, the domain cannot be deleted or the ports assigned to a different domain. There must be no reboot or Sync Reset operation on the hardware since the last capture was made for the capture to remain valid.

Segment Selection

If the domain you have selected contains capture buffers that have been segmented, choose the segment to view from the **Segment(s)** drop-down box. If the capture buffer is not segmented, no selection is required. The segment you are viewing can also be changed later from the toolbar in the TraceView decode display.



Port Viewing and Selection

The right panel displays an icon for each port, arranged as they physically exist within the Xgig chassis. To select a port, click the port. Single ports can be selected within TraceView. Click the background area of a port-pair to select both ports in the pair. Click ports again to remove them from the selection. Selected ports have a blue background, unselected ports have a white background.

TraceView allows the selection of ports that contain valid capture data only. If no ports contain valid capture data, no port can be selected. The icons change as the selection, availability, and type of each port changes. See “Selecting Chassis, Blades, Ports, and Segments” on page 221 for information on the display of port icons.

Dialog Buttons

If you are not logged into the Sync Group that contains the resources in the domain, use the **Password** field to login. Login is only required if the Sync Group is password protected.

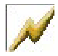
The following buttons are available:

- **Blink**
  Causes the LEDs for the selected ports to blink. LEDs will blink for 40 seconds.
- **Stop**
  Causes the LEDs to stop blinking.
- **OK**
  Exit and use the selected chassis and ports in TraceView.
- **Cancel**
  Close the window; no domains or ports will be used.
- **Refresh**
  Updates the status of blades and ports in the right panel and available Sync Groups in the left panel.

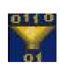
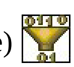
Selecting Chassis, Blades, Ports, and Segments

The dialog box displays an icon for each port, arranged as they physically exist within the analyzer hardware device(s). The icons change as the selection, availability, and type of each port changes. Ports show individually but have the same status for each port in a port-pair. In TraceView, you can select individual ports for display. You can view the trace of up to 64 ports at the same time from TraceView. Note that a “tool tip” displays showing information about the port when you pass the cursor over any port.

Port Types

- **Analyzer Port** 
  Indicates the port-pair is configured to operate as a Fibre Channel, SAS, PCIe, or a Gigabit Ethernet Analyzer port. Right-click, or pass the mouse over the port to see which protocols are used by this port.
- **Jammer Port** 
  Indicates that the port is configured to operate as a Jammer port. Jammer ports cannot be selected within TraceView.
- **BERT Port** 
  Indicates that the port is configured to operate as a BERT port. BERT ports cannot be selected within TraceView.
- **Generator Port** 
  Indicates that the port is configured to operate as a Generator port. Generator ports cannot be selected within TraceView.
- **Target Emulator Port** 
  Indicates that the port is configured to operate as a Target Emulator port. Target Emulator ports cannot be selected within TraceView.
- **Load Tester Port** 
  Indicates that the port is configured to operate as a Load Tester port. Load Tester ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a SAS/SATA Analyzer port.
- **Delay Emulator Port** 
  Indicates that the port is configured to operate as a Delay Emulator port. Delay Emulator ports cannot be selected within TraceControl. If you have the proper license, you can change the port function to be a GE Analyzer port.
- **Unknown Port**
  Indicates that the floating Jammer license dongle has been removed, and the Jammers have been terminated. In this case, the port icons turn white to indicate that the ports have changed to an unknown state. From this state, the ports can be configured to operate as any other licensed function.

Port Selection and Other Indicators

- **Selected** (port icon background is Blue) 
  Indicates the port is selected. You can select a port that is locked or has triggered and view its captured data in TraceView.
- **Unselected and Unlocked** (port icon background is White) 
  Indicates the port is not selected and is not locked.
- **Locked** (lock appears in the port icon) 
  Another user or an instance of TraceControl owns the port-pair.
- **Port Triggered** 
  Indicates that data received on this port has triggered the analyzer.
- **Port Locked and Triggered** 
  Indicates that data received on this locked port has triggered the analyzer.

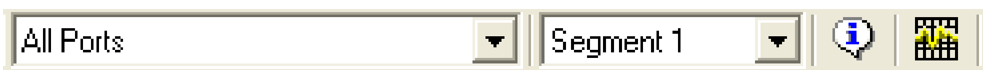
Xgig Port Selection by Chassis or Blade

Ports are shown within blades, and blades are shown within chassis within the **Select Ports/ Domain to Analyze** dialog box. As a shortcut, you can select a chassis and add all its ports to the selection by clicking on the **Viavi Xgig** logo above the chassis name. You can also click the blade area surrounding ports to add all the ports in the blade to the selection.

Segment Selection

When viewing a trace from the hardware buffer, the buffer may be segmented. The initial segment to view is selected in the **Select Ports/Domain to Analyze** dialog box. However, you can change the segment you are viewing without returning to this dialog box.

If the domain you have selected contains capture buffers that have been segmented, choose the segment to view from the **Segment:** drop-down box in the TraceView toolbar. The drop-down box only contains segments that contain valid capture data for viewing. Each segment is completely independent when viewed in TraceView; each segment has its own bookmarks and triggers.



Note that viewing a segment in TraceView when a capture is in progress for another segment within the domain is not allowed. You also cannot view multiple segments within the same domain from the same instance of TraceView.

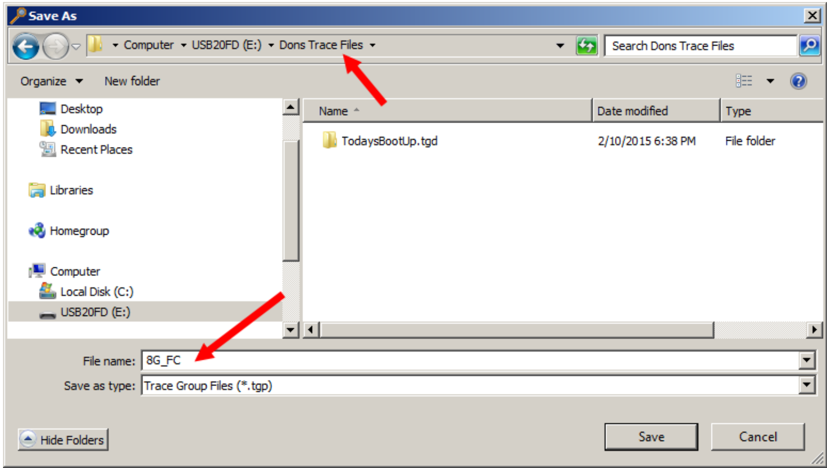
Saving a Trace

You can save your trace or a portion of the trace to a file for detailed analysis.

Select the **Save As**  button or select **Save Trace…** from the **File** menu.

When the **Save As** dialog box opens, navigate to the location that you would like to save the files. Then enter the file name in the **File name:** text box.

Figure 96: Save As Dialog Box with the Directory Path and a File Name Entered



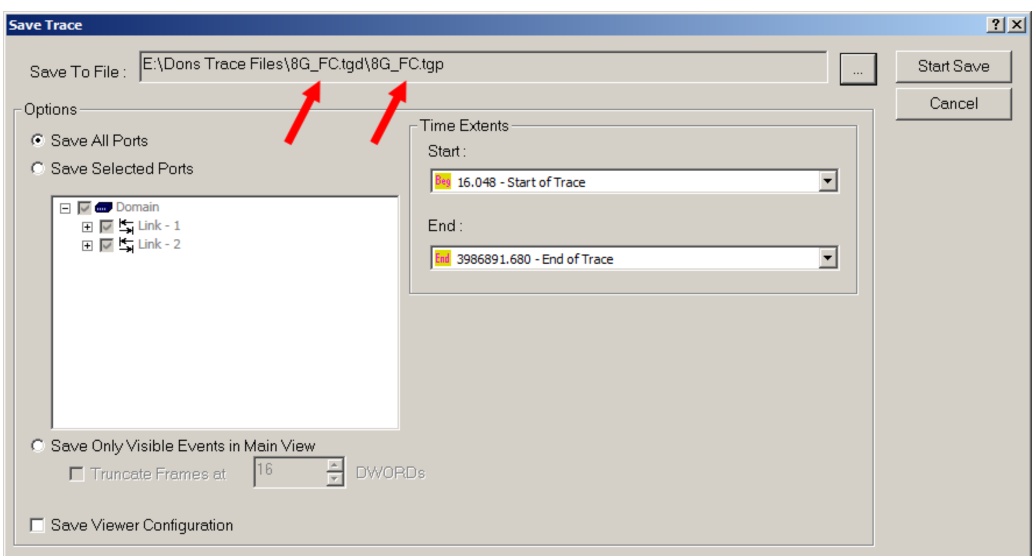
In this case, I have navigated to "Don's Trace Files" sub-directory on the E: drive and entered a file name of "8G_FC".

The **Save as type** will be Trace Group Files (*.tgp) for traces.

Note: The **Save as type** can be also be changed to PCapNg Files (*.pcapng) or Surveyor Capture Files (*.cap). Refer to "PCapNg Files Format Option for Save" and "Surveyor Format Options for Save" on page 226 for additional information on these file types.

Select the **Save** button to open the **Save Trace** dialog box.

Figure 97: Save Trace Dialog Box



Notice the information that has been entered in the Save to File entry shown in Figure 97. To the path that was specified in Figure 96, the file name "8G_FC"has been entered as:

8G_FC.tgd/8G_FC.tgp

The file name that is appended with .tgd is the Trace Group Directory which means a sub-directory named **8G_FC.tgd** has been added to the E:/Dons Trace Files directory. All of the trace files (including **8G_FC.tgp**) will be added to this new sub-directory. The following restrictions are imposed when saving a trace file:

- No other directory with a ".tgd" extension is allowed in the selected path.
- Once a trace file has been saved in a directory, no other trace file with the same name can be saved into that directory. If a the same name exists, an error message is displayed asking you to select a different path or a different name.

The **Save Trace** dialog box also has several options.

You may choose to save ports/data in one of three ways.

- **Save All Ports** – When you select this option, you save all port data.
- **Save Selected Ports** – Select ports or links from the tree shown in the dialog.
- **Save Only Visible Events in Main View** – When this option is applied, it will save the filtered events visible on main view. Using the **Truncate Frames** check box, you can also specify to truncate the frames while saving.

If the **Save Viewer Configuration** check box is selected, the current configuration information (column displayed, colors, applied filters, etc.) is saved with the new trace data file. If you do not select this check box, the last used configuration information is applied to the trace file when it is opened in Xgig TraceView.

The **Time Extent** selections set the limits of the trace data to save using the **Start:** and **End:** fields. The timestamp values to use as the beginning and end points of the save operation are available from each pull-down menu. Two defaults are provided: **Start of Trace** and **End of Trace**.

You can set the limits of the trace data to save by clicking on events in the spreadsheet. Click an event and its timestamp is entered in the **Start:** field. Click the **End:** field and then on another event in the trace. Its timestamp is entered in the **End:** field.

Other timestamps are made available in the pull-down menu by adding bookmarks. Select a timestamp in the trace, right-click the bookmarks column, and select **Bookmark Editor…** to create a bookmark. Once the bookmark is created, the bookmark name appears in the pull-down menus for the **Start:** and **End:** fields.

Select the **Start Save** button to start saving the trace files to the new Trace files sub-directory. When you start the save, the screen portion shown in Figure 98 is appended to the bottom of the Save Trace dialog box. This allows you to monitor the progress of the save to completion.

Figure 98: Save Trace Progress Screen Portion (Appended to Save Trace Dialog Box)

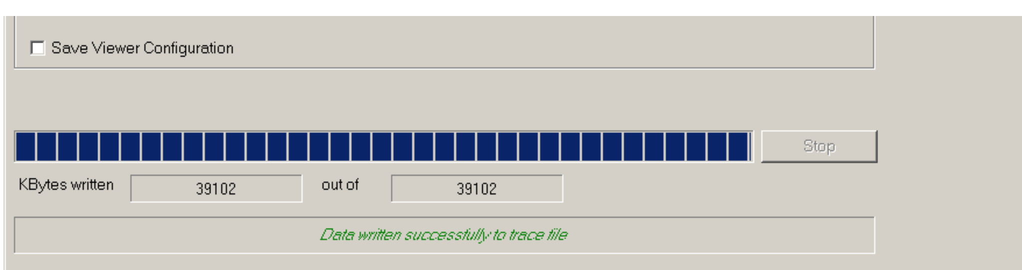
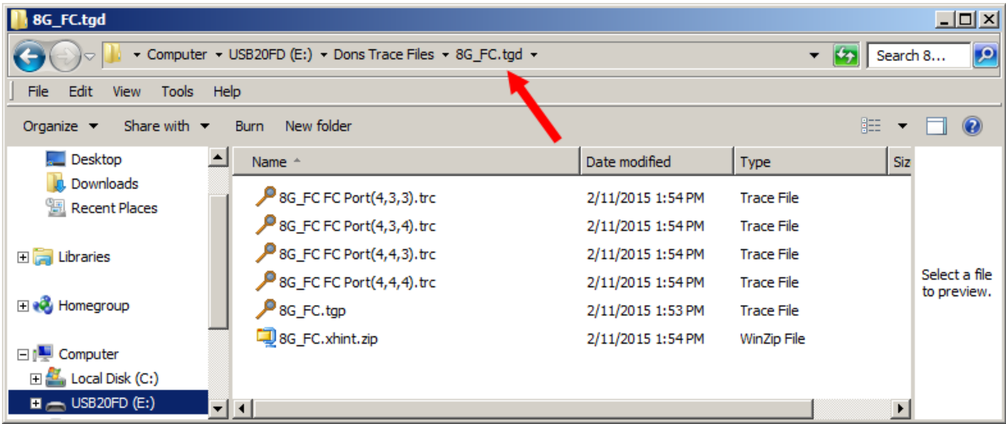


Figure 99 shows that all of the trace files are saved in the new “8G_FC.tgd” sub-directory.

Figure 99: Completed Save Trace Sub-directory



This sub-directory can now be copied or zipped to share complete traces with your associates.

PCapNg Files Format Option for Save

TraceView supports traces being saved as PCapNg (PCAP Next Generation) files so that they can be used by applications other than Xgig Analyzer. These files are saved with the .pcapng file extension.

Surveyor Format Options for Save

Gigabit Ethernet captures can be saved as Surveyor format files. The Surveyor application can be used to open and view the decodes. To save the trace in Surveyor format use the **Save As Type:** box in the **Save As** dialog box and select **Surveyor Histogram Files (.hst) or Surveyor Capture Files (.cap)** as the file type.

When saving as a .cap file, TraceView may save the trace as multiple files. More than one .cap file is created when the total number of bytes converted exceeds 512MB. Subsequent files will have a similar file name as the first converted file with a number in the file name. For example, if you save a trace as temp_GE.cap where the trace contains 1250MB, the save results in three files named in the following format:

temp_GE.cap
temp_GE_0536870928.cap
temp_GE_1073741864.cap

Chapter 13

Configuring Xgig TraceView

In this chapter:

- TraceView Configuration
- Navigating a Trace
- Filter and Hide
- Working with Columns
- Detailed Find/Filter/Color Window

TraceView Configuration

TraceView comes with a variety of pre-defined configurations that can be selected from the **File** menu. These standard configurations are:

- Fibre Channel
- FICON
- Gigabit Ethernet
- iSCSI
- Ports Side-by-Side
- SAS
- SATA
- PCIe

For Xgig TraceView 3.1 and later versions, TraceView automatically detects the physical layer protocol in an opened capture and it loads the default configuration matching that protocol if the last configuration doesn't match that protocol.

If any of the default configurations does not fit your specific needs, you can modify them and overwrite the files in the *.../Viavi/Xgig Analyzer/TraceView Configs/Default* directory.

There are other pre-defined configurations supplied in the Xgig Analyzer installation folder that may better suit your configuration needs. Select **Load Configuration...** from the **File** menu and navigate to the *.../Viavi/Xgig Analyzer/TraceView Configs/Default* directory to load any of these configurations. Configurations in this directory that begin with the prefix **Default** are those already available from TraceView menus. Check with customer support if you need a complete description of these configurations or you would like to suggest a standard configuration that should be added to the product.

Saving a Configuration

An Xgig TraceView configuration file controls the display of data. All columns, colors, searches, finds, groups, and views are saved with the configuration. You can restore the display by loading the configuration file at a later time.

Configuration files for Xgig TraceView must have an extension of `.cfg`.

1. Select **Save Configuration…** from the **File** menu. The **Save As** dialog box appears.
2. If needed, use the dialog box to navigate to the folder where you want to store the configuration file. Configuration can be stored in any location, but are typically stored in the same directory as the trace.
3. Name the Xgig TraceView configuration file and press **OK**.

Loading a Configuration

Configuration files for Xgig TraceView must have an extension of `.cfg`.

All columns, colors, searches, finds, and groups are loaded with the configuration. When a configuration is loaded, the current port selection is not affected.

Loading a Configuration

1 Select **Load Configuration** from the **File** menu. Select a default configuration or select **Custom Configuration..**. For the default configurations, a single column is used to designate the ports except in **Default Ports Side-by-Side**. For information on Ports Side-by-Side, see "Ports Side-by-Side Configuration" on page 229.

2 If you select a default configuration, the selected configuration is applied. If you select **Custom Configuration..**., the **Open** dialog box appears.

3 Use the dialog box to navigate to the folder containing the configuration file. Configuration can be stored in any location, but are typically stored in the same directory as the trace.

4 Select the Xgig TraceView configuration file and press **OK**. TraceView will display only one view loaded with the selected configuration.

Initial Configuration Applied When Opening a Trace

If no last-used configuration is saved, then a default configuration corresponding to the physical protocol is loaded. If the last-used configuration is for the same protocol as that of the trace being opened, this configuration is used. Otherwise, the default configuration corresponding to the protocol of the trace is loaded.

Ports Side-by-Side Configuration

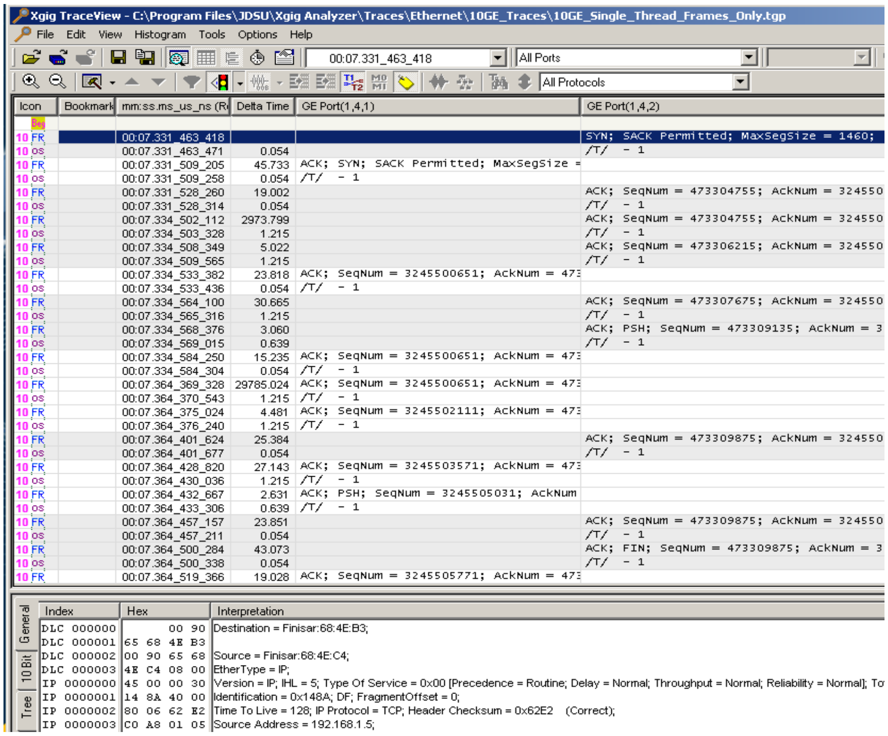
TraceView can display a multiple-port trace with a separate column in the display for each individual port. This allows easy identification of which port is associated with each decoded event. The column with the summary information for each port is titled by the name given to the port. Select this option from the **File > Load Configuration > Default Ports Side-by-Side**.

For the **Ports Side-by-Side** configuration, an EOF in a trace is shown as a unique event in the spreadsheet. The spreadsheet view must have ordered sets shown for EOFs to display as separate events.

For the **Ports Side-by-Side** configuration, you can quickly display all port columns in equal-width columns. Select **Autofit All Port Columns in View** from the **View** menu. Information will wrap in the column if it will not fit in the column width for the port.

An example of using side-by-side port view is shown below. Summary information for Channel 1-A is shown in column Channel 1-A and summary information for Channel 1-B is shown in column Channel 1-B.

Figure 100: Ports Side-by-Side View



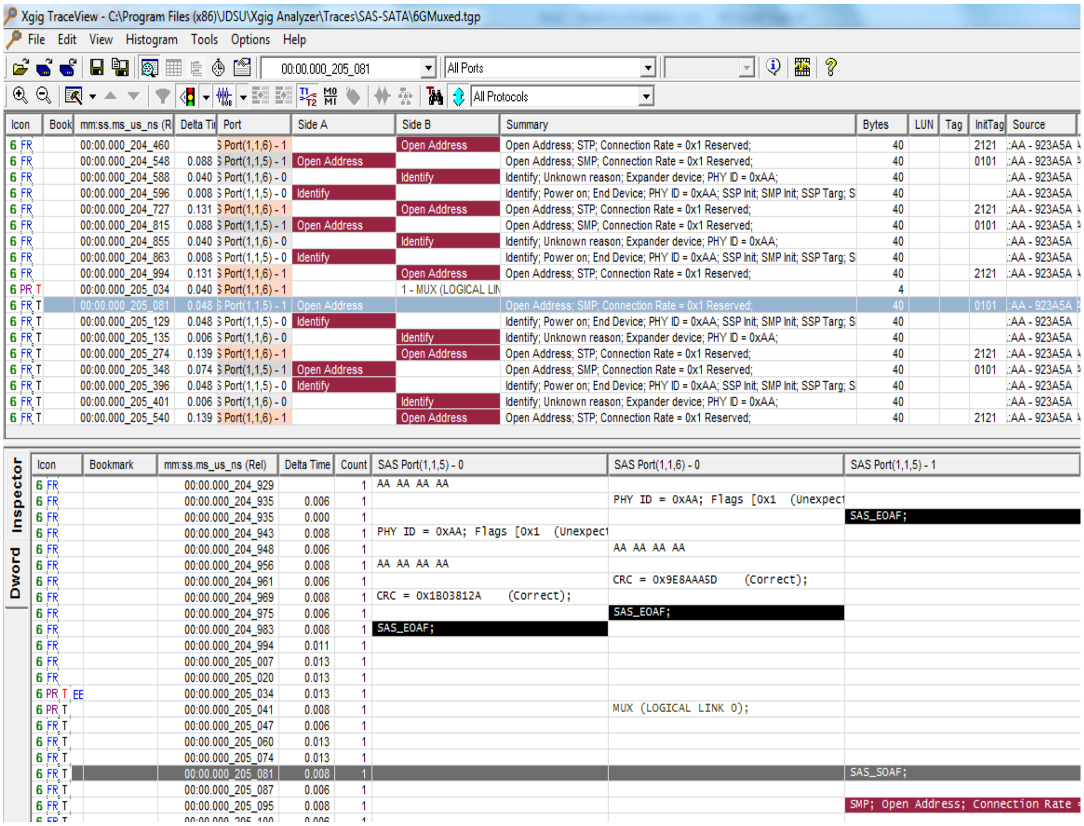
Multiplexed Ports in Port Side-by-Side View

In a Port Side-By-Side configuration, logical links within a multiplexed SAS/SATA port are displayed separately as a unique column. A multiplexed port displays as two columns, one for each logical link in the traffic. Multiplexed links display with a "**- 0**" and a "**- 1**" after the Xgig port name to identify the two logical links within the single port. For example, **SAS Port (1,2,1) - 0** and **SAS Port (1,2,1) - 1** indicate the two logical links passing through a single physical port (port 1 on blade 2).

See Figure 101 for an example of Port Side-By-Side configuration of multiplexed ports. In the example, assume the multiplexed traffic is on the first and second port on the second blade. The columns **SAS Port (1,2,1) - 0** and **SAS Port (1,2,2) - 0** show traffic for one of the logical links and **SAS Port (1,2,1) - 1** and **SAS Port (1,2,2) - 1** for the other logical link.

Use the MUX button to toggle Port Side-by-Side view between viewing logical link ports together and physical ports together. The columns **SAS Port (1,2,1) - 0** and **SAS Port (1,2,1) - 1**, which comprise the physical signal for SAS Port (1,2,1), would display next to each other if the button is used to set the view to physical ports side-by-side. Note that the MUX button has no effect on configurations other than port side-by-side.

Figure 101: Ports Side-by-Side View, MUXed Ports, Logical Links Together



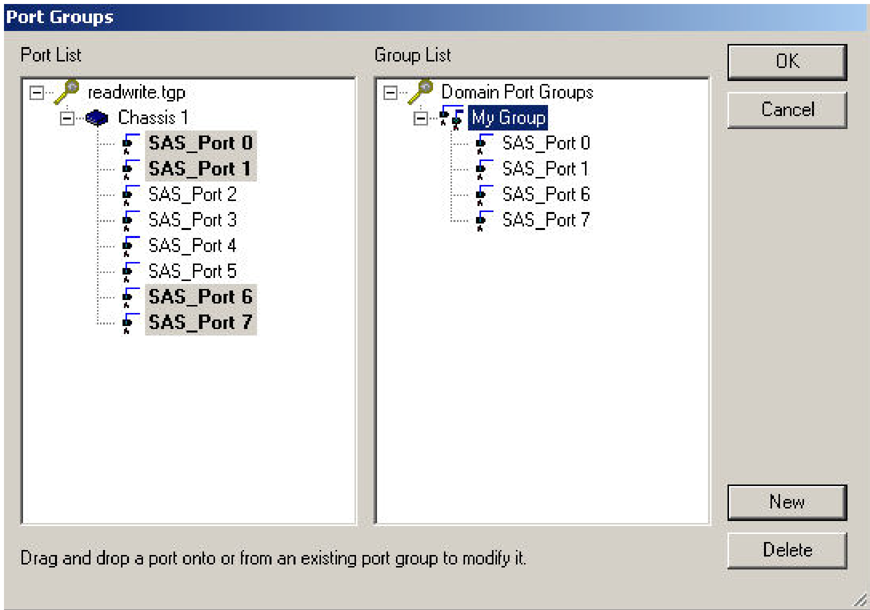
Setup Port Groupings

Traces often consist of data from many ports across many devices. TraceView allows you to divide ports into Port Groups and display only the data for that group of ports. Different filters and color displays can be applied to each group created for the trace. The Port Group pull-down on the toolbar allows you to select a Port Group for viewing within the trace or return to viewing all trace data.

Creating Port Groups

1 Select **Define Port Groups...** from the **Tools** menu. The **Port Groups** dialog box appears.

Figure 102: Port Groups Dialog Box



2 Press the **New** button to create a new Port Group. A default name is supplied.

3 It is suggested that you rename the group within the **Group List** box. Select the Port Group in the **Group List** box, press `F2`, or click the Port Group name. Type in the new name. Port group names must be unique.

4 Drag-and-drop ports from the **Port List** box to the new group list. If you attempt to insert a port that already exists in the group, the port will blink several times.

5 Press **OK** to exit the dialog.

You can modify or delete a Port Group by bringing up the **Port Groups** dialog box. Drag-and-drop additional ports to the group. To delete a port or Port Group, select it and press the **Delete** button.

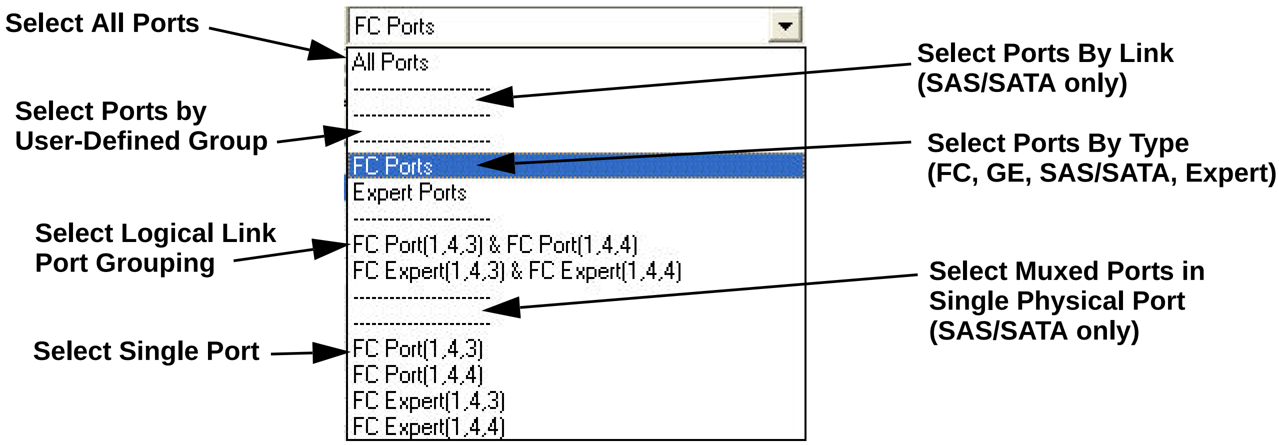
For multiplexed data, each link within the single physical port is selected and added separately to the port group. For example, **SAS Port (1,2,1) - 0** and **SAS Port (1,2,1) - 1** will appear as separate ports with the port group display and each can be added to the port group.

Selecting Port Groups

Use the **Port Groups** pull-down menu on the toolbar to select the group to apply to the entire display. The pull-down shows options for selecting all ports, links, user-defined port groupings, port-pairs, single ports, ports annotated by Expert, or single links within multiplexed ports. Different selections types are divided by a dashed line, as shown in Figure 103.

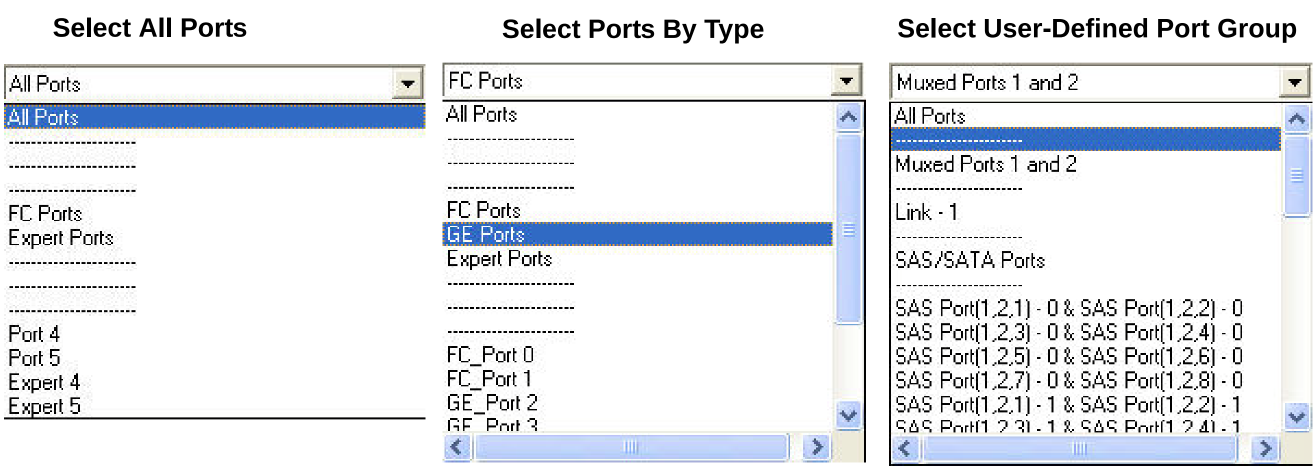
Refer to “Working with Traces Annotated by Expert” on page 382 for more information on creating Expert traces.

Figure 103: Port Selection Menu



Some examples of port selection are shown in Figure 104.

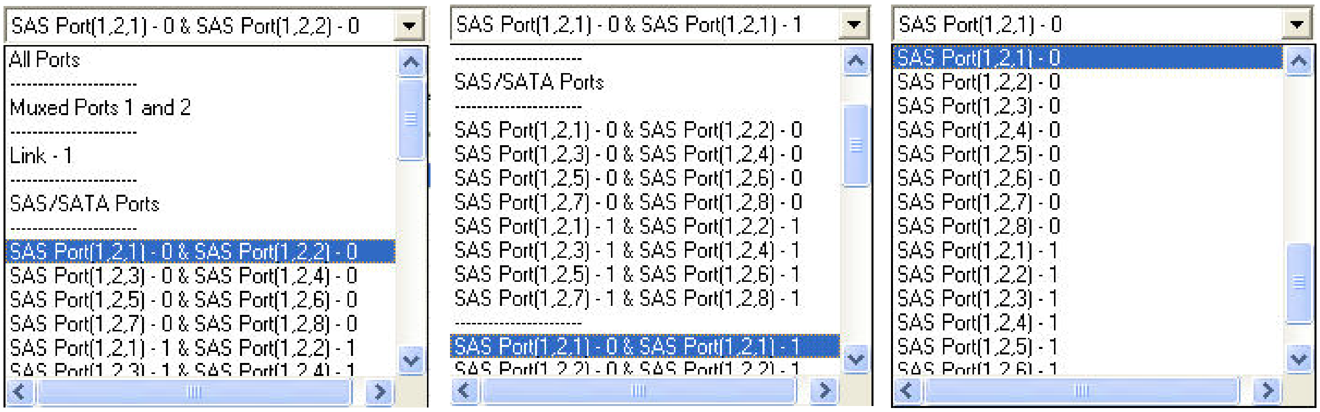
Figure 104: Port Selection Menu Examples



For multiplexed ports, ports can be selected by single physical port, single logical link, or single side of a logical link. Remember that if a single physical port is selected (for example, **SAS Port (1,2,1) - 0** and **SAS Port (1,2,1) - 1**) you will see the trace information for one-half the traffic of two different logical links. Some examples of port selection for multiplexed ports are shown in Figure 105.

Figure 105: Port Selection Menu Examples for Multiplexed Ports

Select Single Logical Link with Multiplexed Traffic | **Select Single Physical Port with Multiplexed Traffic** | **Select One Logical Link within One Physical Port**



Navigating a Trace

Xgig TraceView supplies a variety of ways to locate information within a trace. All incorporate basic Windows user interface navigation tools, including mouse actions (for left and right mouse buttons), window controls (resizing and scrolling), cursor controls (arrow keys), and keyboard shortcuts.

The methods used to locate specific trace information include marking locations within a trace, controlling the histogram of the trace, and using Xgig search tools such as Traffic Summary View if applicable.

Search Tools

Xgig TraceView provides tools that enable you to quickly search for specific trace data.

Marked Locations

You can find marked locations within a trace using bookmarks, timestamps, and trigger positions. These marks enable you to move to locations or change the current display for a trace.

Histogram Controls

Histograms can graphically represent an entire trace from start to end. They also allow you to expand and collapse the view of the trace to look at a graphic display of a detailed portion of the trace. You can use histogram controls to locate specific trace information.

Traffic Summary View

When enabled for 6G and 12G SAS/SATA traces and Fibre Channel traces on 8G Xgig blades, 16G Xgig5000 blades, and 16G ports on Xgig1000 systems, this tool displays counters for all events in the trace and allows you to navigate to each occurrence of an event.

Exchanges View

When enabled, this tool displays the following:

- Completed SCSI exchanges from FCP-SCSI, iSCSI, and SAS physical layers
- Completed SATA exchanges from SAS/SATA physical layers
- Reassembled iSCSI, FCIP/iFCP, SMB/CIFS, and NFS/RPC PDUs from Ethernet physical layers
- Completed Memory and IO Read/Write PCIe exchanges from PCIe physical layers
- Completed NVMe Admin, Read, and Write exchanges from PCIe physical layers

Using the Find Tab to Set Up Complex Searches

Use the **Find** tab of the Detailed Find/Filter/Color window to set up a complex search operation.

1. Select **Detailed Find/Filter/Color...** from the **Edit** menu to bring up the Detailed Find/Filter/Color window.
2. Select a template from the **User Library** or the **Viavi Library**.

   You can either navigate through the library tree or type the path of a template into the search field with each level separated by a period, for example:
   `SAS.SCSI.CMD.ADC.Inquiry - 0x12`
   The matching templates will be displayed in a drop-down window.
3. Drag templates to the **Find** tab's **Find all Events like this** pane.
4. If needed, drag templates to the **Find** tab's **Except all Events like this** pane.
5. Continue to select, drag, and drop templates until you are satisfied with the conditions.
6. Press **OK** when you are done.

Once the find operation is started, use the **Find Previous Event** and **Find Next Event** buttons (black Up and Down arrows in the toolbar) to find the other events of this type. All events that meet the search criteria are shown in blue in the spreadsheet display. You can also use the menus or control keys, **Edit > Detailed Find Previous (Shift+F3)** and **Edit > Detailed Find Next (F3),** to find events.

The **Except all events like this** pane can be used to further refine the search. It sets events to ignore that would be found based on the search criteria established in the **Show all Events like this** pane.

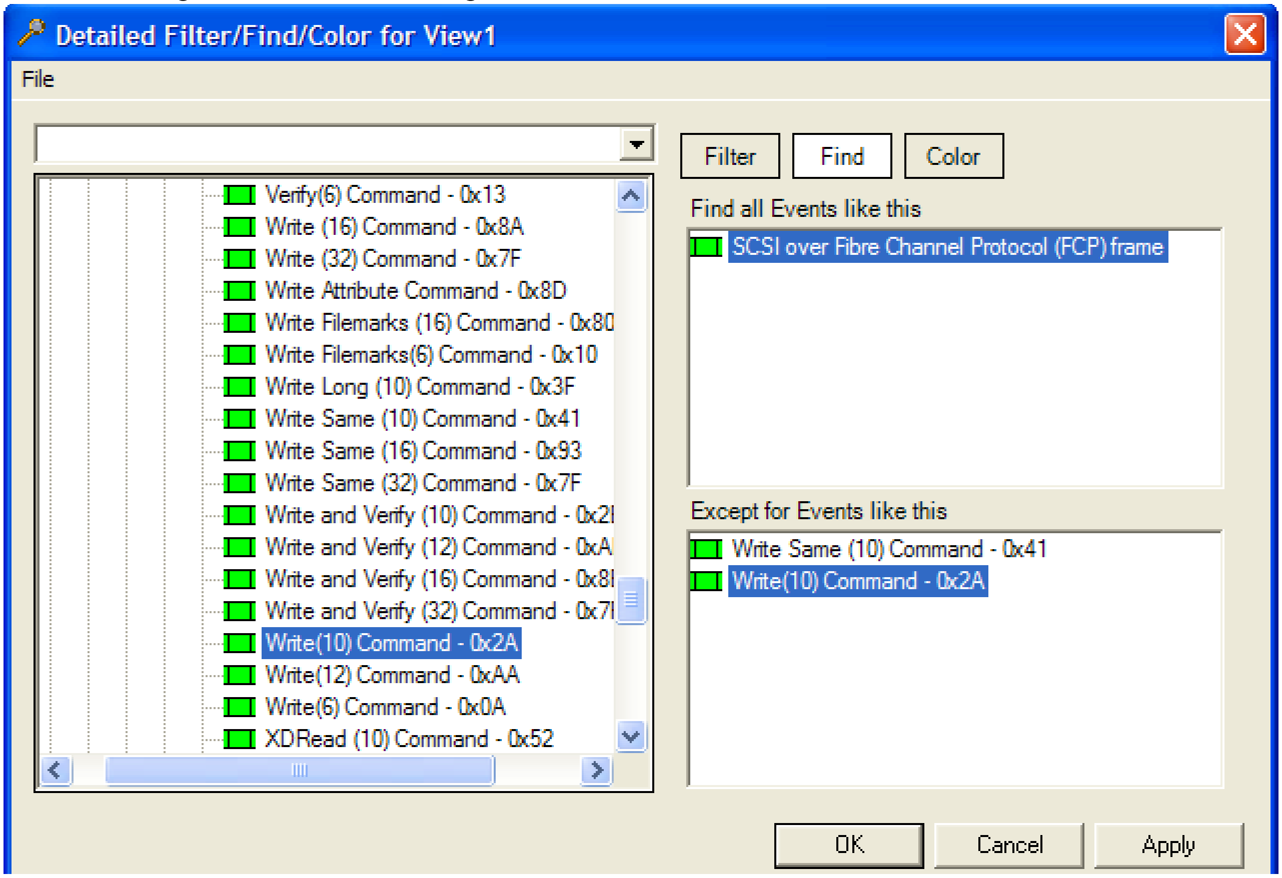
The **Find** tab of the Detailed Find/Filter/Color window is available for the main spreadsheet view and for Exchanges View. This function is not available for the Dword View.

Find Tab Example

Figure 106 shows an example of a find operation. All templates for this example were dragged and dropped from the Viavi Library section of the Available Templates Browser. Double-click a template to modify its contents. Right-click a template to perform copy, cut, paste, rename, or delete operations.

In the example, when the search is applied the next SCSI frame that is not a write operation is found. All SCSI frames will be found except SCSI Write (10) and SCSI Write Same (10) operations.

Figure 106: Search Using the Find Tab

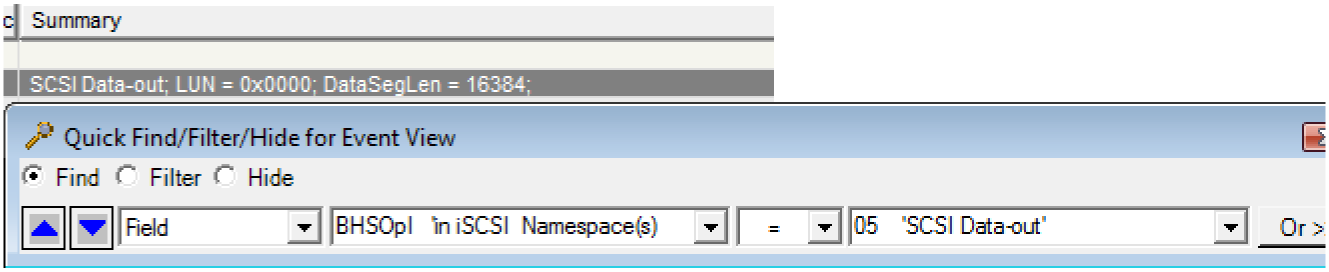


Quick Find

The easiest and fastest way to find, filter, or hide any event in a trace is to use Quick Find. Just double-click any TraceView cell or any Inspector field, and the Quick Find dialog will popup, ready to find the currently visible field. For compound columns like the Summary, the Quick Find dialog comes up with the first visible field in the column if the column is left-aligned, or the last visible field if the column is right-aligned. The other visible fields in the column are quickly accessible in a drop-down.

For example, if you double-click the Summary column on an iSCSI Data-out frame, the Quick Find dialog pops-up as follows:

Figure 107: Quick Find Dialog Box



Not only does Quick Find allow you to quickly find the fields visible in any TraceView cell, it allows you to find any field values or events in the trace with the help of drop-downs and auto-completion text boxes.

Note: An alternative way of performing search operations is to use the Detailed Find/Filter/Hide dialog. That dialog allows to define search operation on templates in a similar fashion as Xgig-TraceControl. The Detailed Find/Filter/Hide dialog offers a complementary option for searching. It is especially useful if you want to define two sets of filters or find criteria and quickly toggle between the two. Refer to section "Using the Find Tab to Set Up Complex Searches" on page 235 for more details.

To perform Quick Find:

1 Right-click the column value in an event row that you wish to search on.

2 Select **Quick Find/Filter/Hide**. The **Quick Find/Filter/Hide** dialog box appears.

3 The dialog box displays the information field you have selected, a logical operator, and the value of the field in the display. The default logical operator is equal to (=). You can modify the information in the dialog box to use any field or any of the Quick Find options.

4 Press the **Previous** or **Next** buttons in the display to search backward (up) or forward (down) from the current location in the trace file.

You can also use the menus or control keys, **Edit > Quick Find/Filter/Hide (Ctrl+F3)**, to bring up the dialog box. You can also double-click a row to invoke a Quick Find.

Quick Find Options

The Quick Find dialog offers different search options when accessing a trace file versus an Xgig chassis with an older or newer AppKit software installed. It also offers different options when the decode library in the CurrentProtocols.pmd file has been modified by the user.

The Quick Find options are best when accessing a trace file. They are as follows:

Field: Decode each event and search for a field
Template: Use a template from the Template Library to perform the search
Fixed hex: Specify a fixed offset hexadecimal value to search on
Sliding hex: Search a hexadecimal pattern at any offset inside each event
ASCII string: Search an ASCII string at any offset inside the event
EBCDIC string: Search an EBCDIC string at any offset inside the event

Unicode string: Search a Unicode string (UCS-2LE) at any offset inside the event
Decoded string: Search for a string in the inspector window and all TraceView columns (slow)

Note: If the CurrentProtocols.pmd file has been customized by the user, then the user is notified, the **Field** option becomes **Factory search** and two more options become available:

Factory search: use factory compiled decodes to decode and search for a field (fast, but does not work for custom decodes)
Simplified search: Use simplified criteria to search quickly for a field in custom decodes
Custom search: Use the modified CurrentProtocols.pmd to decode and search for a field (slow)

When accessing Xgig buffers, the search and filter operations are performed on the chassis, and the client only gets notification of the results. The **Field** (or **Factory search**) option requires the chassis to decode each event while searching. The factory-compiled decoder on the chassis has to be in sync with the CurrentProtocols.pmd file on the client side in order to return results matching what is visible on the TraceView client slide. For this reason, TraceView notifies the user if the AppKit on the chassis does not match the client version, and the **Field** option is replaced by **Factory search** and **Simplified search** options. The **Simplified search** option becomes the default option in that case, but the user can easily change it to **Factory search** if desired. Note that Xgig chassis AppKits prior to Xgig-A 5.3 do not have the ability to decode each event before searching, therefore these options are not available for those AppKits.

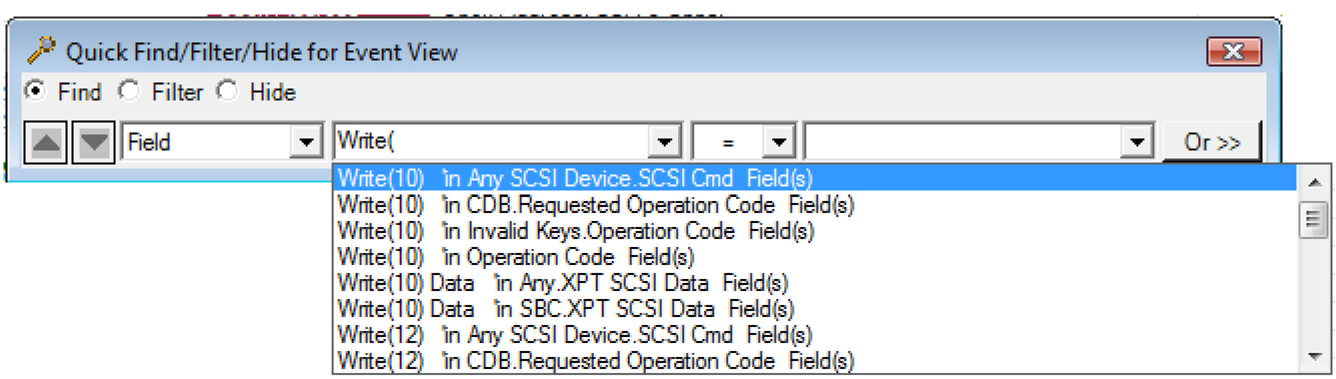
The Quick Find dialog only searches for DWORD-size events in the DWORD view and therefore it has a very limited set of search options in that case: **Field** or **Fixed Hex**.

A filter or hide operation from the main spreadsheet does not affect the Dword display or Exchanges View. Conversely, a filter or hide operation from the Dword spreadsheet or Exchanges View does not affect the main spreadsheet display. See “Find/Filter/Hide in Dword View” on page 333 for more information on Quick Find/Filter/Hide in Dword view.

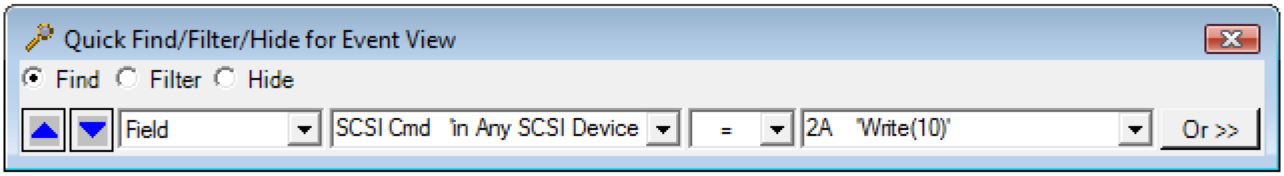
When selecting different Quick Find options, the fields for specifying values will change. Each Quick Find option is described below.

Field (or Factory search)

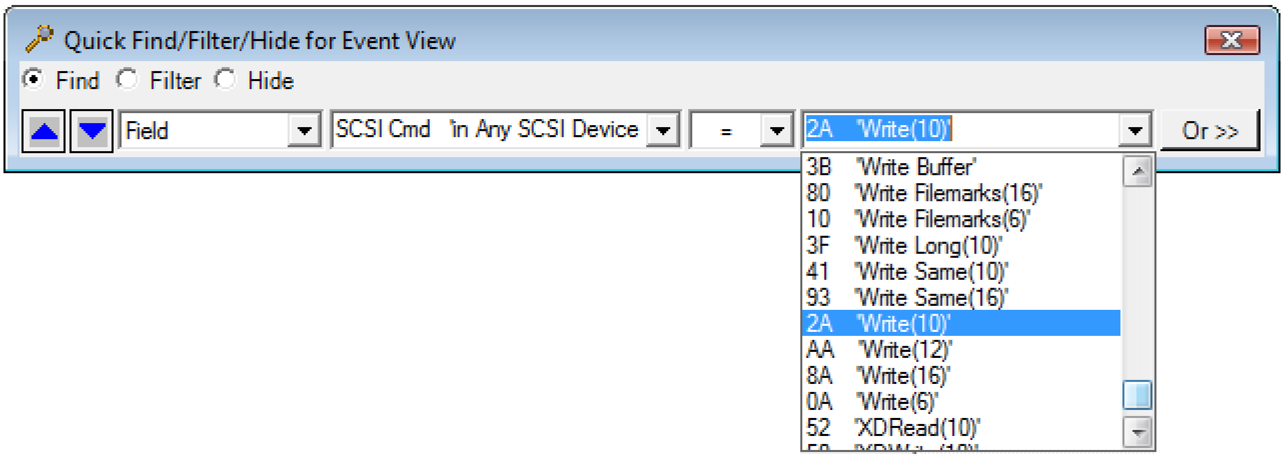
This option allows to search for any field value defined in the decode library. The second drop down in the dialog supports auto-completion. You can type any event field name or interpretation and the drop-down will provide you with valid options as you type. For example, if you want to search for the next Write(10) command in the trace, you can start typing *Write(* and the drop-down will give the choices of all the fields and interpretations matching *Write(*:



You can then click the item desired, in this case it is the first choice provided: *Write(10) ' in Any SCSI Device.SCSI Cmd Field(s)*. The Quick Find dialog then sets the field name in the 2nd drop down to *SCSI Cmd ' in Any SCSI Device* and the value of *2A 'Write(10)'* in the value drop-down:



Once a valid field is chosen in the 2nd drop down, then the 4th drop down gives the choice of all the interpretations or user defined aliases for this field:



The 3rd drop down is the operator and it gives a choice of 5 operators on the field value:

=	Equal
!=	Not equal
>	Greater than
<	Smaller than
&	Bitwise And
in	Match if the value is anyone in the comma-separated list
! in	Do not match if the value is anyone in the comma-separated list
range	Match if the value is within the dash-separated range X-Y specified (where X and Y are included in the comparison)
!range	Do not match if the value is within the dash-separated range X-Y specified

The **Field** (or **Factory search**) option decodes and searches each event using an optimized factory-compiled-decode engine. It is better than **Simplified search** option to search for deeply buried fields in the protocol stack, like iSCSI fields or any other TCP payload field. However, it requires the chassis AppKit to be in sync with the client software CurrentProtocols.pmd file.The **Factory search** option becomes available when the chassis AppKit does not match the client software or when the client CurrentProtocols.pmd file has been customized by the user. This option also becomes available when the user chooses the **Force decoding of every frame while searching** or the **Force using simplified criteria while searching** options in the **Search** tab of the TraceView Options dialog.

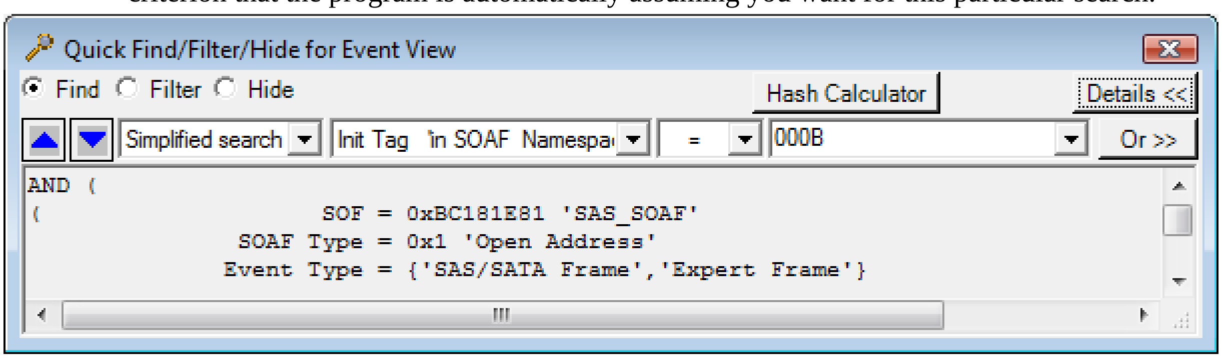
Also, the **Field** option in the DWORD View does not support auto-completion because the limited number of fields to search on are available in the drop-down.

Simplified search
This option becomes available when the chassis AppKit does not match the client software or when the client CurrentProtocols.pmd file has been customized by the user. This option also becomes available when the user chooses the **Force decoding of every frame while searching** or the **Force using simplified criteria while searching** options in the **Search** tab of the TraceView Options dialog. The Quick Find dialog fields for this option are very similar to the **Field** option except:

- The second drop-down does not support auto-completion. It only gives a choice of all the fields in the current event (or the fields in the **Summary**, **Source** or **Destination** columns if you double clicked in those columns).
- A **Details** >> button becomes visible to display the additional criteria used for searching

Compared to the **Field** (or **Factory search**) option, this one does not decode every event while searching. Instead, it searches for the field at the same byte offset as in the current event, and it searches for some additional criteria to match similar events. The additional criteria are computed based on the CurrentProtocols.pmd file on the client side. This way, this method produces accurate search results even when the CurrentProtocols.pmd file has been customized or when the Xgig chassis AppKit does not match the client software version. However, this method can give misleading results when a field would be found at different byte offsets in different events of the trace. Although this is an uncommon scenario, it could happen in Ethernet traces containing mixtures of VLAN/non-VLAN frames, mixtures of TRILL, CN-Tag, VnTag frames or mixtures of TCP option sizes.

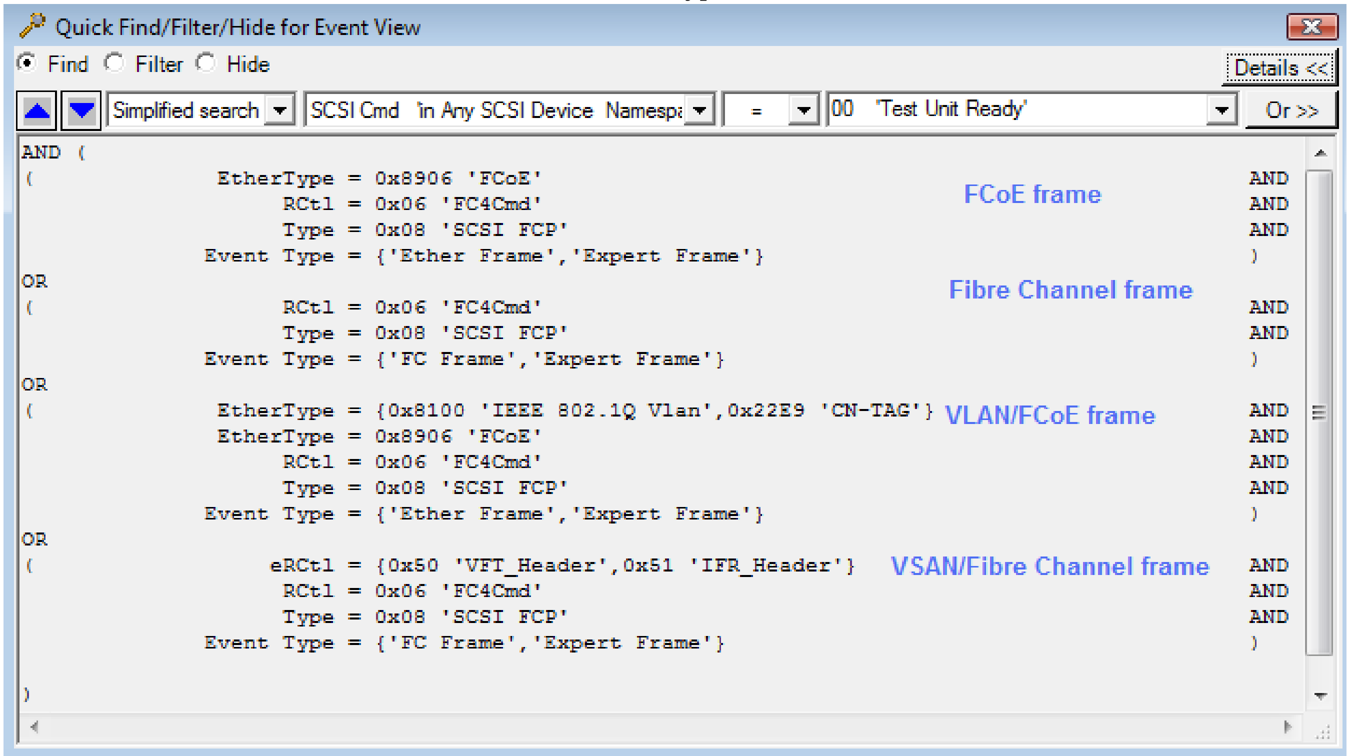
If you click the **Details** >> button, the **Quick Find/Filter/Hide** dialog shows the additional criterion that the program is automatically assuming you want for this particular search.



Note that for Fibre Channel and SCSI traffic, the **Simplified search** method searches for the selected field in the following frame types:

- FCoE
- VLAN/FCoE
- Fibre Channel
- VSAN/Fibre Channel

The Details window shows all the frame types that will be searched.



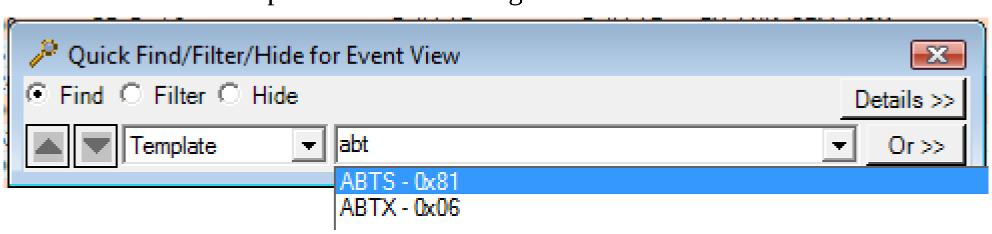
Custom search

This option becomes available when the client CurrentProtocols.pmd file has been customized by the user. The option is only available for trace files, not Xgig buffers. The Quick Find dialog fields for this option are identical to the **Field** (or **Factory search**) option.

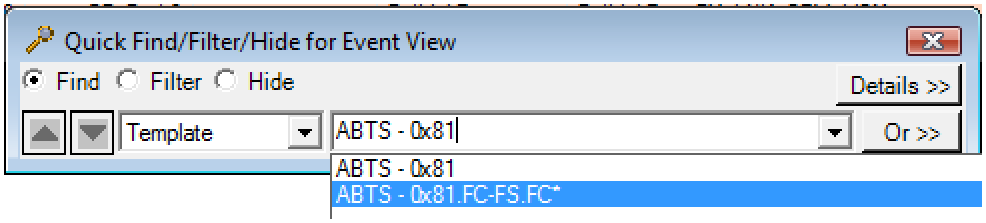
This option decodes every event while searching using the protocol definitions inside the CurrentProtocols.pmd file. So, even if that file is customized by the user, this option still produces accurate results. However, compared to the **Field** (or **Factory search**) option, this search option is extremely slow and it works best on small trace files.

Template

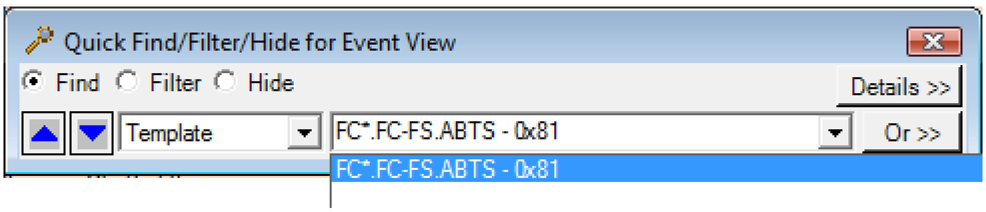
This option allows you to search using any template in the Viavi library as available in TraceControl or TraceView's Detailed Find dialog. The second drop-down in the dialog supports auto-completion. You can type any template name or path and the drop-down will provide you with valid options as you type. For example, if you want to search for the next Fibre Channel Abort Sequence frame (ABTS), then you can start typing *ABT* and the drop-down will give the choices of all the template names matching *ABT*:



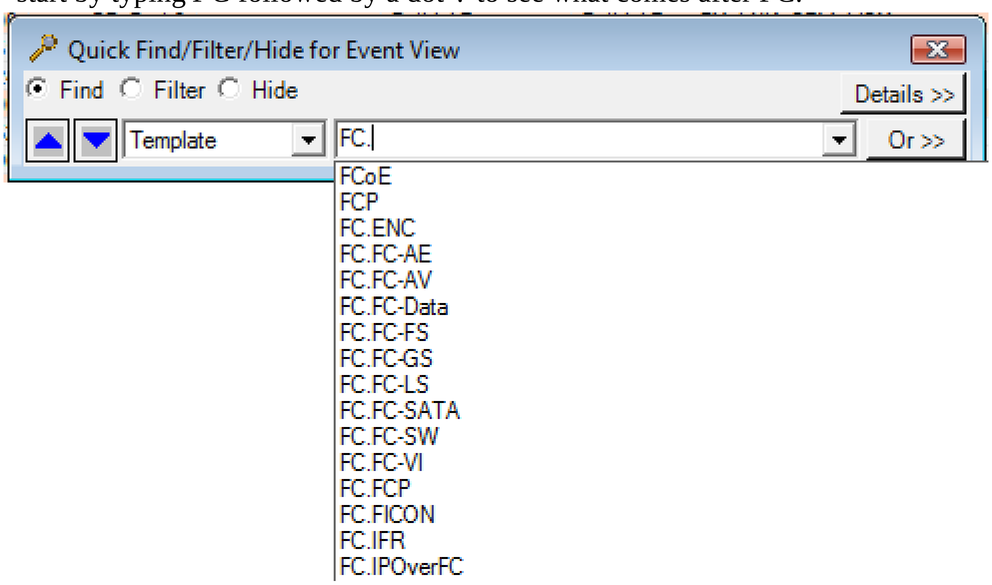
Then, click *ABTS - 0x81*, and the drop-down will show you all possible frames containing the *ABTS - 0x81* field. In that case, there is only one choice, so you click it:



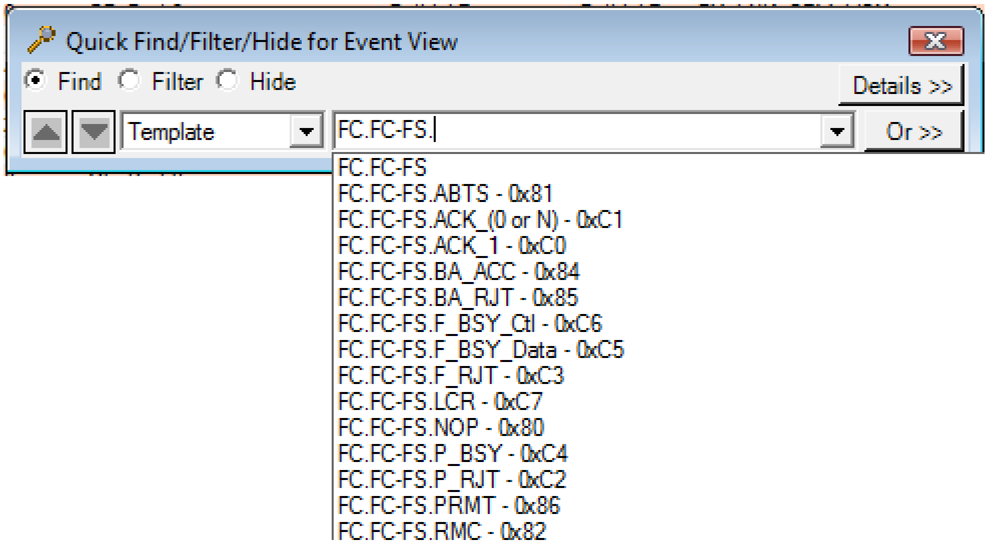
Finally, the dialog will reverse the path from tip to root to a path from root to tip so that this template can be found again in the future, and you can click it to select that choice:



Another way to get to the ABTS template is to start typing the path from root to tip. So, you can start by typing *FC* followed by a dot '.' to see what comes after FC:

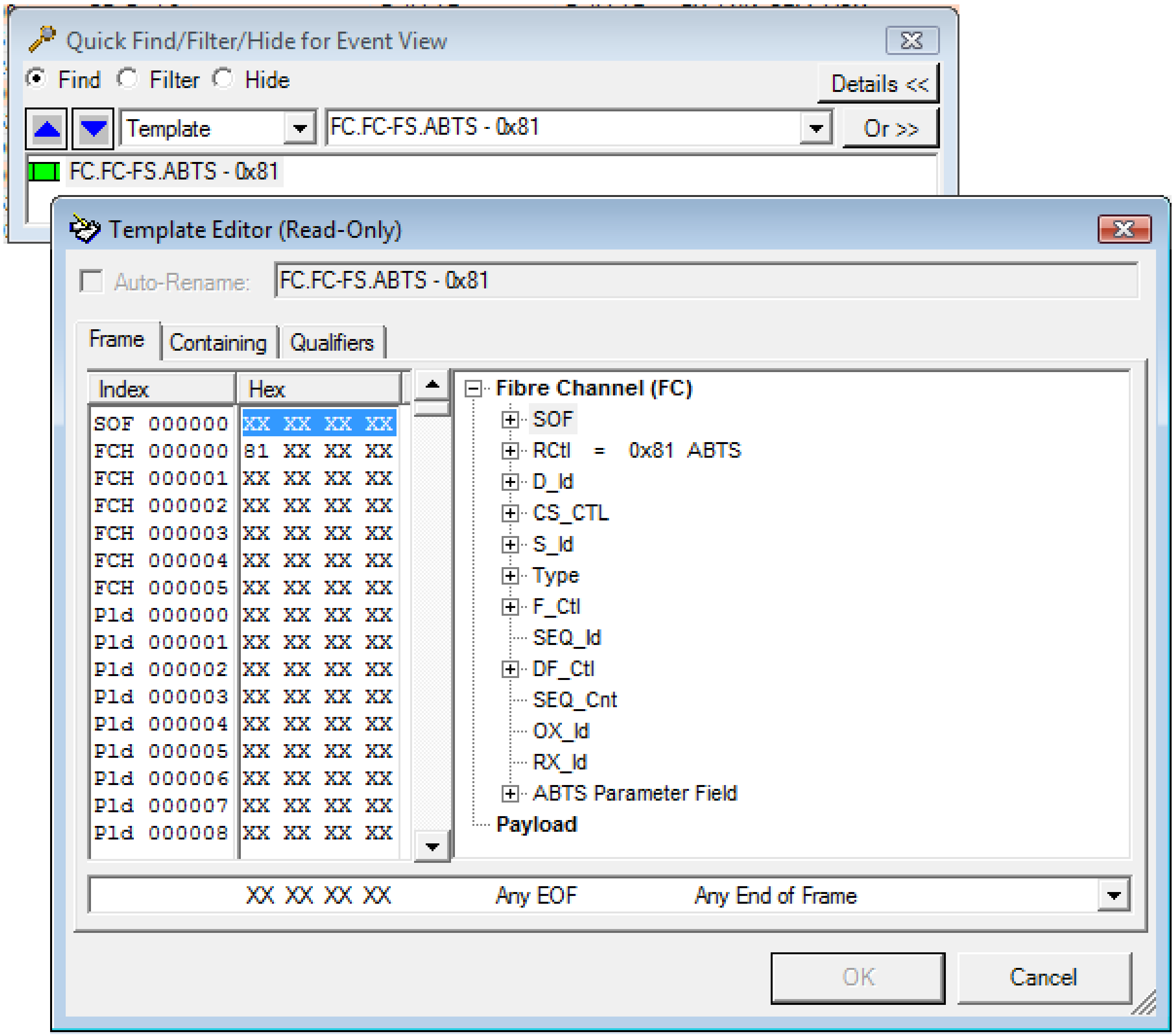


Then, select *FC.FC-FS* and add another dot '.' to see what comes after the FC-FS layer:



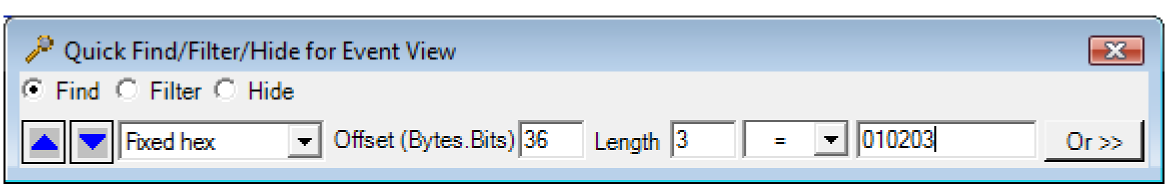
Then, you can click the *FC.FC-FS.ABTS* - *0x81* item, and you are ready to search.

If you want to see the template associated with *FC.FC-FS.ABTS - 0x81*, then you can click the Details >> button and double-click the template name to bring up the template editor and view the content of that template.



Fixed Hex

This option allows searching for a specific value at a specific offset and length. For example, if you are searching for a frame with an undecoded raw value of 0x010203 at byte offset 36, you can use this search method as shown in the picture below.

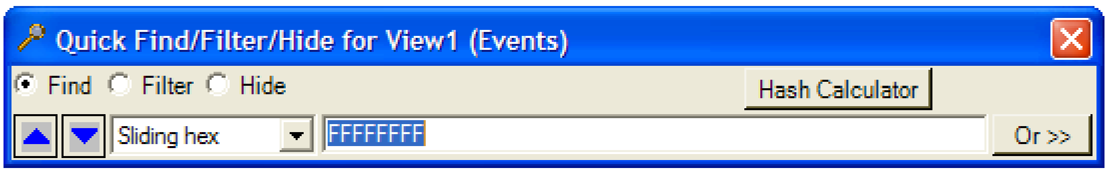


If you want to search for the value 0x010203 in all frames, but you don't know the offset for it (which is typically the case), then you should use the search method **Sliding Hex** instead.

The hex specification can be useful when looking at portions of events that are not completely decoded by TraceView. TraceView also supports bit-level searches. See "Bit Level Find/Filter/Hide" on page 258.

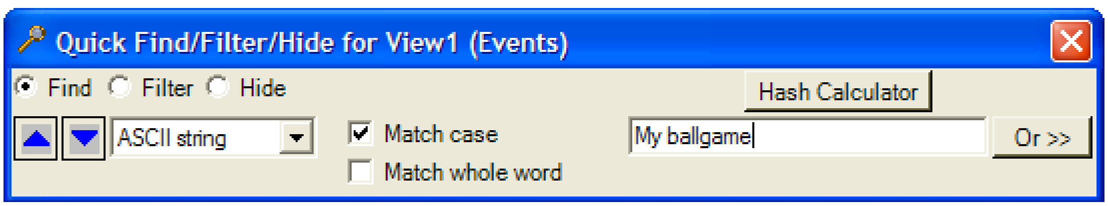
Fixed hex does not search in the End fields, including CRC.

Sliding Hex
This option allows searching for a specific value at any offset inside the frames (or any other events). For example, if you want to search for a marker value of 0xFFFFFFFF inside all frames, you can use this method as shown in the picture below.



Sliding hex does not search in the End fields, including CRC

ASCII String
This option allows searching for an ASCII string anywhere in the frame payload. The search is non-case sensitive, and you can choose to match partial words by default. You can choose to match the case and to match whole words.



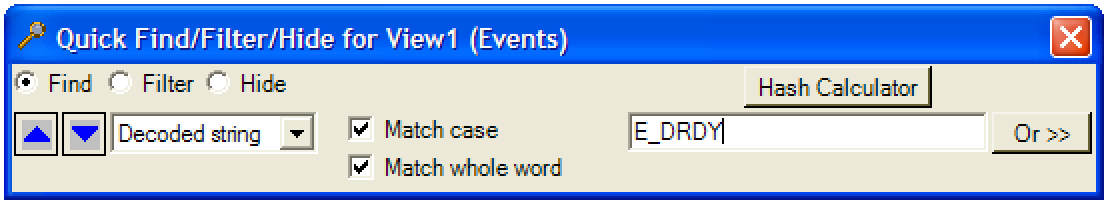
Unicode String
This option allows searching for a UNICODE string anywhere in the frame payload. The search is non-case sensitive and it matches partial words by default. You can choose to match the case and to match whole words.

EBCDIC String
This option allows searching for an EBCDIC string anywhere in the frame payload. The search is non-case sensitive and it matches partial words by default. You can choose to match the case and to match whole words.

Note that TraceView's inspector window displays EBCDIC characters when the menu **View > Data Inspector > Show EBCDIC character set** is selected.

Decoded String
The **Decoded string** method decodes every frame before trying to match the string in the field names or interpretations for each frame. This method also searches in TraceView's **Summary** column, **Errors/Warnings** column, etc. The search is non-case sensitive and it matches partial words by default. You can choose to match the case and to match whole words.

Note that this method does not search the inspector text as a whole. For example, if you search for “SCSI Cmd = Read(10)”, it won't find this value; use the **Decoded field** method for this type of search. However, the **Decoded string** method will work if you search for “Read(10)” or “SCSI Cmd”.



It is not possible to use the **Decoded string** method when viewing a trace on a remote Xgig chassis. For traces within buffers, the **Decoded string** option will not be visible.

Advanced Quick Find

You can use advanced Quick Find to set up more elaborate search operations. You can change the type of field, the logical operator, or the value of the field.

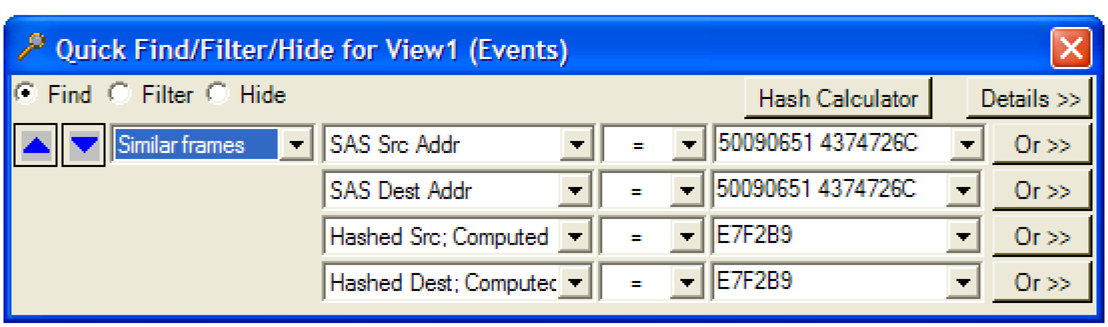
For columns containing numerical data, the **Quick Find** feature can also be used with the logical operators *equal to* (=), *not equal to* (!=), *(&) and*, *less than* (<), *greater than* (>), *Match if the value is anyone in the comma-separated list (in), Do not match if the value is anyone in the comma-separated list (! in), Match if the value is within the dash-separated range X-Y specified (where X and Y are included in the comparison) (range)*, and *Do not match if the value is within the dash-separated range X-Y specified (!range).* For non-numeric data, only the equal to and not equal to operators are available.

You can also use the **Or>>** button to add an additional condition to your Quick Find. Using the **Or>>** button to add another condition means that EITHER condition will be searched for. To add another condition using **And**, click the **>>** button, then click the **Or** button, and it changes to **And.** Use the pull-down menus to set up the second Quick Find. Quick find supports up to eight And/Or conditions.

Search for SAS 8-Byte World Wide Names

If you double-click in the **Source** or **Destination** column on an SOAF Open Address or Identify frame, the **Quick Find/Filter/Hide** dialog comes up with the 8-byte World Wide Name select, plus the equivalent 3-byte hashed address. For example, if an SOAF Open Address frame has a SAS Src Addr of 0x5000536572766572, then the **Quick Find/Filter/Hide** dialog comes up as follows:

Figure 108: SAS Address Search



The search assumes you want to find all events with the address, both 8-byte World Wide Names and 3-byte hashed values for the address. You can reduce the number of conditions searched for by using the **Or <<** button. However, you cannot find/filter/hide if any of the 4 field values is deleted.

If you search for an event that has a 3-byte hashed address, you will only find those events with the same 3-byte address. TraceView will not find events with the 8-byte value, as there is no way to determine the full 8-byte address from the 3-byte hashed address.

A conversion tool is included to translate 8-byte World Wide Names to their 3-byte hashed value. The **Hash Calculator** button will automatically appear in **Quick Find/Filter/Hide** dialog when you double-click an SOAF event to launch the dialog. It will also appear after filtering for fields **SAS_SOAF**, **SAS Src Addr**, and **SAS Dest Addr**. See "SAS Hashed Address Calculator" on page 402 for more information.

Search for Marked Locations

Bookmarks

Bookmarks are powerful tools for locating information in a trace. Use them to mark event times you want to track or compare to other events, or events you want to return to over and over again.

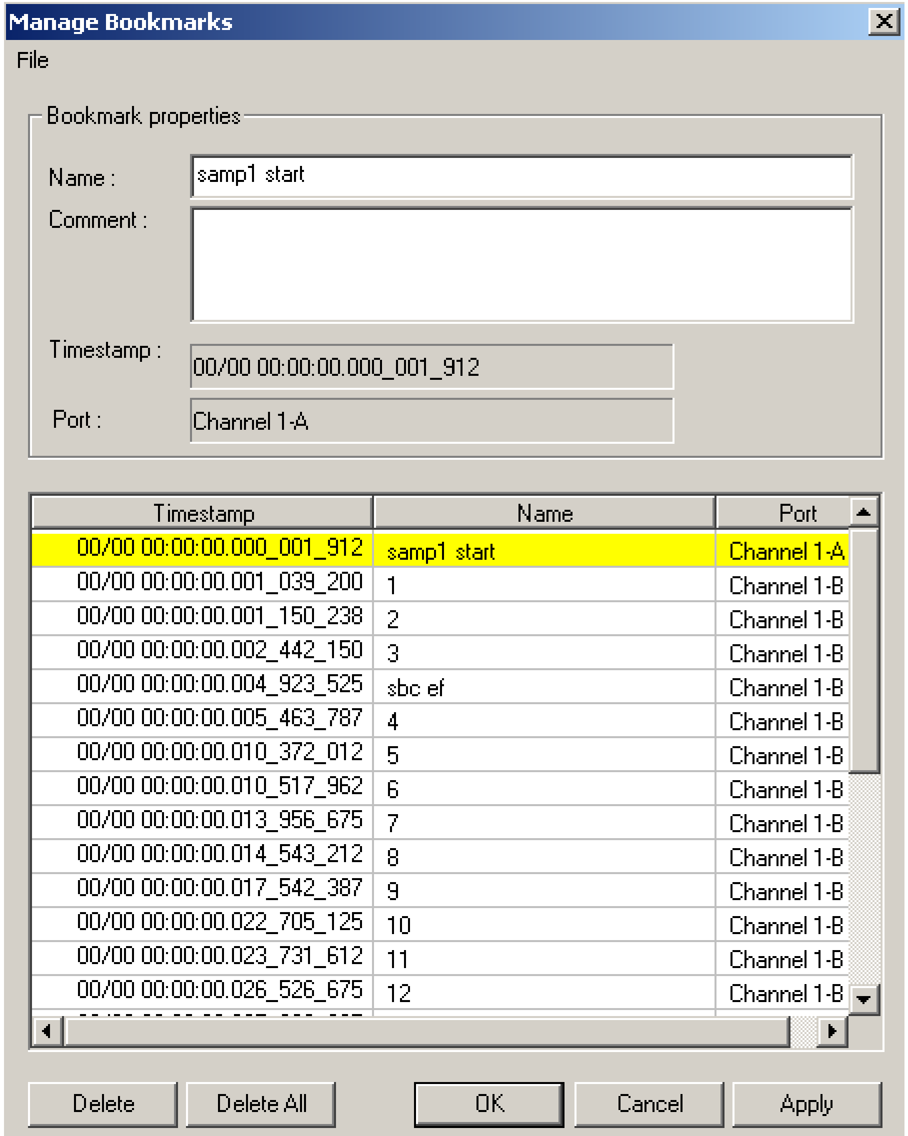
Bookmarking adds a tag to the event structures at that specific point in time. Bookmarks are referenced in many other operations, such as finds, searches, and navigation to a specific timestamp. Bookmark information is embedded within the trace file. Therefore, you will see bookmarks even if you look at the data using a different Xgig TraceView configuration.

The Bookmark Event pull-down menu in the Xgig TraceView toolbar contains all bookmarks. Selecting a bookmark from the menu takes you to that line in the trace.

Managing and Editing Bookmarks

A tool is available for viewing and managing all bookmarks from a list. Bookmarks may be modified or deleted. You can also add a descriptive comment about the bookmark. Select **Tools > Manage Bookmarks...**. All bookmarks for the trace are shown in this dialog. However, if you click a bookmark that is outside the histogram's current time extent, a message may appear saying, "This bookmark is filtered by the current time extents."

Figure 109: Manage Bookmarks Dialog



You can also export bookmarks to a .csv file and then import this bookmark file to the same trace. This allows two users to work with the same trace and exchange information about key points in the trace. Select **Export Bookmarks** or **Import Bookmarks** from the **File** menu. If you have deleted or added bookmarks, press the **Apply** button to accept your changes before starting the Export operation.

The export/import of bookmarks is designed to work for a single trace. Since bookmarks are related to a specific timestamp, it makes no sense to import them into a different trace. You can import bookmarks and export bookmarks between a partial trace file and its original trace file. If you import bookmarks and the specific event for an imported bookmark already is marked, TraceView will ask if you want to overwrite the original bookmark.

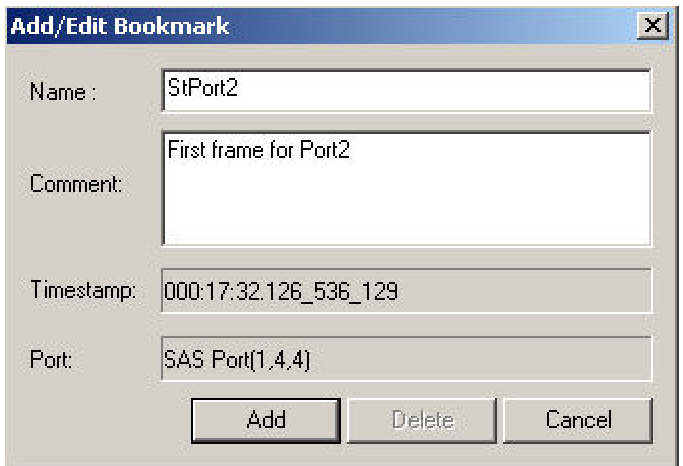
Adding, Deleting, and Modifying Bookmarks in the Spreadsheet

To add a bookmark with comment:

1 Right-click in the **Bookmark** column in the event you wish to bookmark, and select **Bookmark Editor...** from the menu. The **Add/Edit Bookmark** dialog box appears.

2 Type the name of the bookmark, enter a descriptive comment in the **Comment** field, and press **Add**. The bookmark is added. The bookmark name will have a star at the end of its name in the spreadsheet display if the bookmark has a comment.

Figure 110: Bookmark Editor Dialog



To add a bookmark (with no comment):

1 Select the event to bookmark and double-click in the **Bookmark** column. Or, select the bookmark column with the right mouse button and select **Set Bookmark**. The cursor displays in the **Bookmark** column.

2 Type the name of the bookmark. The bookmark is added.

To modify/delete a bookmark:

1 Right-click in the **Bookmark** column in the bookmarked event, and select **Bookmark Editor...** from the menu.

2 Retype the name of the bookmark, enter a descriptive comment in the **Comment** field, and press **Change**. The bookmark is modified. To delete the bookmark, press **Delete**.

>> OR:

1 Double-click with the mouse on the bookmark name in the **Bookmark** column. Or, select the bookmark column with the right mouse button and select **Set Bookmark**. The current contents of the **Bookmark** column are highlighted.

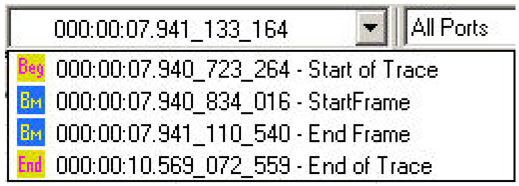
2 Retype the name of the bookmark. To delete the bookmark, press the **Delete** key.

Go To Bookmark

This feature allows you to quickly go to a previously bookmarked timestamp in the trace by selecting it from a Bookmark Event pull-down menu.

To go to a selected timestamp:

1 Find the Bookmark Event pull-down box on the Xgig TraceView toolbar.



2 From the Bookmark Event pull-down menu, select the bookmark that you want to view.

Timestamps are made available in the Bookmark Event pull-down menu by adding bookmarks. Select a timestamp in the trace, right-click the bookmarks column, and select **Set Bookmark** to create a bookmark. Once the bookmark is created, the bookmark name appears in the pull-down menu, with the **Bm** icon next to it.

To go to a timestamp not marked by a bookmark, you can enter the timestamp in the bookmark combo box.

Go to Trigger

The trigger button jumps to the trigger in the trace.

Select the **Go to Trigger**  button. All the events after the trigger in the trace are displayed with Ts in the **Icon** column. You can also use the **Tools > Go To Trigger** menu item.

Display Protocol Layers

Use the **Protocol Layer** drop-down menu in the toolbar to limit the data to a specific protocol layer. This also allows you to isolate protocol layer-specific decodes. If you have defined filters for the trace, these filters are ANDed with the protocol layer filter. If you change the port selection and the current protocol layer no longer applies, it will be changed to **All Protocols**. Based on the selected protocol layer, some of the metrics in **Traffic Summary** view may not be visible. The protocol layer filter is not applied to **DWORD** view.

Display Lane for PCIe

Use the **Lane** drop-down list menu in the toolbar to display the ordered set decodes for a specific lane. When you select a lane number, all the ordered set decodes change to reflect the contents in the selected lane. This selection affects both the event grid and **LaneView** tab in the Details pane. Lane selection does not affect frame decodes as frames are always striped across lanes.

Filter And Hide

Filtering data eliminates events from the spreadsheet display to speed up your analysis. There are three primary ways of filtering data in the spreadsheet display:

- Use the **Quick Filter** feature to select certain types of events based on information in the spreadsheet display.

- Use the **Quick Hide** feature to hide certain types of events based on information in the spreadsheet display.
- Set up complex filters using the **Filter** tab of the Detailed Find/Filter/Color window.

Traces annotated by Expert contain additional information that can be used to filter/hide information in the trace. See “Working with Traces Annotated by Expert” on page 382 for information on annotated traces.

There are also some common filtering operations that are available from the toolbar, such as hiding ordered sets or displaying only overlapping data. A filter status area provides you a quick synopsis of all the filtering you have applied to the trace.

Filter Status Area

In lower right corner of the TraceView window is an area that shows the status of the filters that can be applied to the trace. The following status fields are shown:

- **Filters** -- indicates if filters set up in the Filter tab are applied.
- **OS** -- indicates if ordered sets are displayed.
- **QF** -- indicates if Quick Filters are applied to the data.
- **QH** -- indicates if Quick Hides are applied to the data.
- **Overlap** -- indicates if only overlapping data is displayed.

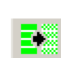
The speed of the link is also displayed in the status area.

An example is shown below.

In the example, the first red X indicates that no filters set up through the Filters tab are applied to the display. The red X next to OS indicates that ordered sets are not displayed. The green check marks indicate that the Quick Filters (QF) and Quick Hides (QH) that have been set up are applied to the data, and that only overlapping data is displayed. The last indicator lets you know the network speed of the trace.

Quick Filter

Use Quick Filter to select frames or other event information that you want to see exclusively in the display. Quick Filter is primarily for filtering events based on the value of fields as you find them in the display. For example, show only all data for Port 3. For more complex filtering operations, see the Detailed Find/Filter/Color window.

Once you have set up a Quick Filter, use the **Apply Quick Filter**  button to enable or disable the Quick Filter condition. Multiple Quick Filters can be created and they can be completely removed rather than disabled. Use the **Quick Filter list...** button to bring up the dialog to view/ remove conditions in the Quick Filter list. See “Multiple Quick Filters” on page 254.

The **Quick Find/Filter/Hide** dialog field combo box contains only the fields for the current event. For the **Summary**, **Source**, and **Destination** columns, the combo only gives a choice of the subset of visible fields in the column.

The **Quick Find/Filter/Hide** dialog also lists the last ten finds, filters, and hides that you have performed and lists them in the drop-down menu.

If you double-click in the **Summary** column (or any other compound column), the **Quick Find/Filter/Hide** dialog comes up with the first visible field in the column if the column is left-aligned, or the last visible field if the column is right-aligned.

To filter data:

1 Right-click the column value in an event row that you wish to select.

2 Select **Quick Find/Filter/Hide…**. The **Quick Find/Filter/Hide** dialog box appears.

3 The dialog box displays the information field you have selected, a logical operator, and the value of the field in the display.

4 Select the **Filter** radio button.

5 Click the **Filter** button. This action removes all events except those that meet the condition. If you have set multiple conditions, events are selected if they meet any one of the multiple conditions.

You can use the menus or control keys, **Edit > Quick Find/Filter/Hide (Ctrl+F3)**, to bring up the dialog box. Once Quick Filters have been established, you can clear the list by selecting the **Clear** button from the **Quick Find/Filter/Hide** dialog box.

Quick Filter Options

When you select a field, the option in the pull-down box of **Quick Find/Filter/Hide** dialog is set to the value of **Field**. Quick Filter options are identical to the options for Quick Find. See "Quick Find Options" on page 237 for a more detailed description of the options and examples. The options are:

- **Field**
- **Simplified search** (available under certain conditions) See "Quick Find Options" on page 237 for details.
- **Factory search** (available under certain conditions) See "Quick Find Options" on page 237 for details.
- **Template**
- **Fixed hex**
- **Sliding hex**
- **ASCII string**
- **Unicode string**
- **EBCDIC string**

- **Decoded string**

Important: The **EBCDIC string** method is only available if you have upgraded your Xgig Chassis server software to version 3.2.

Advanced Quick Filter

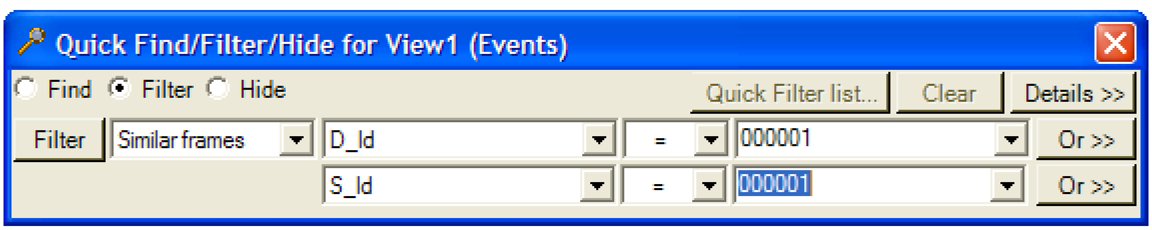
You can use Quick Filter to set up more elaborate filtering operations. You can change the type of field, the logical operator, or the value of the field.

For columns containing numerical data, the **Quick Filter** feature can also be used with the logical operators *equal to* (=), *not equal to* (!=), *(&) and*, *less than* (<), *greater than* (>), *Match if the value is anyone in the comma-separated list (in), Do not match if the value is anyone in the comma-separated list (! in), Match if the value is within the dash-separated range X-Y specified (where X and Y are included in the comparison) (range)*, and *Do not match if the value is within the dash-separated range X-Y specified (!range).*

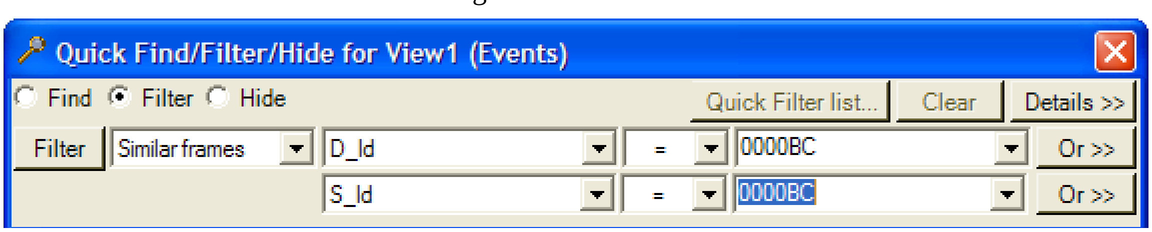
You can also use the **Or>>** button to add an additional condition to your Quick Filter. Using the **Or>>** button to add another condition means that Events containing either condition will be displayed. Use the pull-down menus to select the field and the value of the field for the second Quick Filter. You can also use the **Quick Filter list...** button to select another Quick Filter to OR conditions together.

Filter Source/Destination Addresses

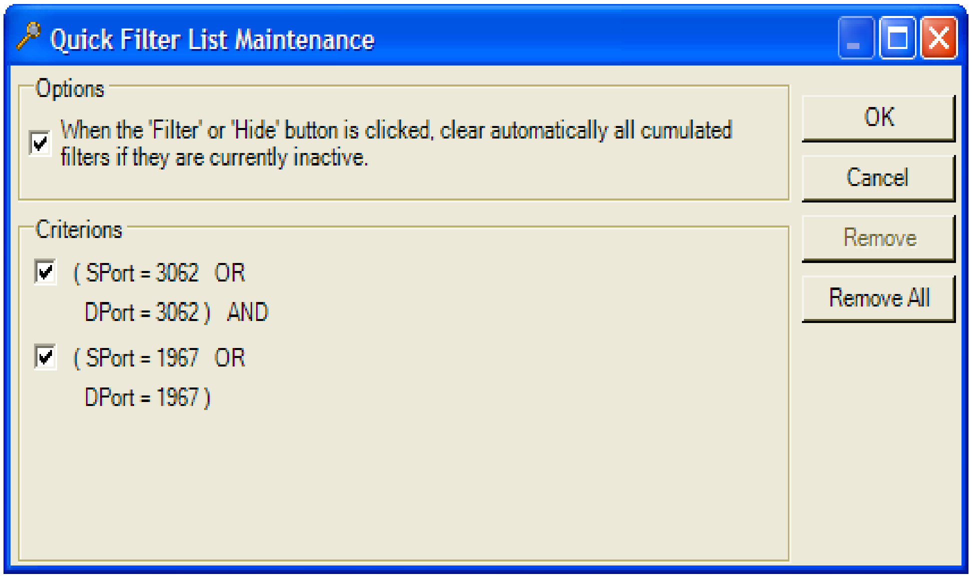
When you double-click in a cell under the **Source** or **Destination** column, the **Quick Find/Filter/ Hide** dialog comes up with a combination of the **Source** OR **Destination** column automatically. For example, if you double-click in the **Destination** column on a Fibre Channel frame, the **Quick Find/Filter/Hide** dialog comes up as follows:



Filtering using such criterion allows you to quickly isolate all conversations to and from one host with ID 000001. Repeating this step with another host will result in filtering on all conversations between 2 hosts. In the example below, the result has been filtered a 2nd time with the ID = 0000BC. This results in filtering on all conversations between 000001 and 0000BC:



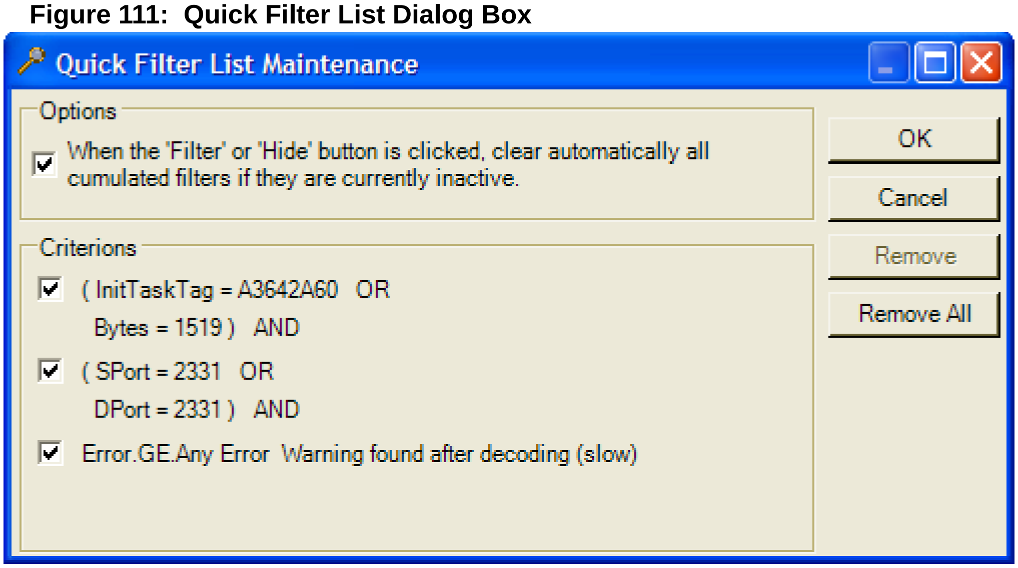
With both quick filters applied, the Quick Filter List dialog will display as in the example below. See the section below for more information on multiple quick filters.



Multiple Quick Filters

You can set up multiple Quick Filters. All Quick Filters are stored in a list. Use the **Quick Filter List > Edit…** options from the **Tools** menu to bring up the list of Quick Filter items. Or, click the **Quick Filter list...** button from the **Quick Find/Filter/Hide** dialog box when the **Filter** radio button is selected.

Figure 111: Quick Filter List Dialog Box



From the list, you can remove or disable any Quick Filter. To disable a Quick Filter, uncheck the box next to the item. To remove the item from the list, select the item and click **Remove**. To delete all Quick Filters, select **Quick Filter List > Clear** from the **Tools** menu or press **Remove All** in the dialog box.

If you set up a Quick Filter using two filtering operations, each filter operation is listed separately in the Quick Filter list. The last column in the table shows that all rows are ANDed for the filter operation; in other words, adding rows narrows the data in the decode display.

A Quick Filter list also exists for Dword view and Exchanges View. The Quick Filter list for Dword and Exchanges View are completely separate from the list for the main spreadsheet display. Make sure you have selected the correct display (main spreadsheet, Dword, or Exchanges View) before you select **Quick Filter List** from the **Tools** menu. The Quick Filter List for Dword view and Exchanges View will have the view's name in the window title bar.

Filter SAS 8-Byte World Wide Names

See "Search for SAS 8-Byte World Wide Names" on page 246 for a detailed description of the feature. The feature works the same for Quick Filter as for Quick Find.

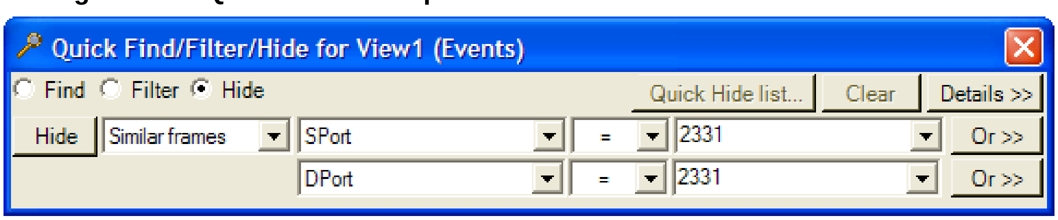
Quick Hide

Use Quick Hide to filter out frames or other event information that you want to remove from the spreadsheet view. Quick hide is primarily for hiding events based on the value of fields as you find them in the display. For example, hide all data from Port 3. For more complex filtering operations, see the Detailed Find/Filter/Color window.

Once you have set up a Quick Hide, use the **ApplyQuick Hide** button to enable or disable the Quick Hide condition. Multiple Quick Hides can be created and Quick Hides can be completely removed rather than disabled. Use the **Quick Hide list...** button to bring up the dialog to view/remove conditions in the Quick Hide list. See "Multiple Quick Hides" on page 257 for more information on removing Quick Hides.

An example Quick Hide window is shown below. The Quick Hide window was created after double-clicking an event in the **DTPort** column and then selecting the **Hide** radio button.

Figure 112: Quick Hide Example



The **Quick Find/Filter/Hide** dialog field combo box contains only the fields for the current event. For the **Summary**, **Source**, and **Destination** columns, the combo only gives a choice of the subset of visible fields in the column.

If you double-click in the **Summary** column (or any other compound column), the **Quick Find/Filter/Hide** dialog comes up with the first visible field in the column if the column is left-aligned, or the last visible field if the column is right-aligned.

To hide data:

1. Right-click the column value in an event row that you wish to hide.
2. Select **Quick Find/Filter/Hide…**. The **Quick Find/Filter/Hide** dialog box appears.

3 The dialog box displays the information field you have selected, a logical operator, and the value of the field in the display.

4 Select the **Hide** radio button.

5 Click the **Hide** button. This action removes all events that meet the condition.

You can also use the menus or control keys, **Edit > Quick Find/Filter/Hide (Ctrl+F3)**, to bring up the dialog box. Once Quick Hides have been established, you can clear the list by selecting the **Clear** button from the **Quick Find/Filter/Hide** dialog box.

Quick Hide Options

When you select a field, the option in the pull-down box of **Quick Find/Filter/Hide** dialog is set to the value of the field. Quick Hide options are identical to the options for Quick Find. See "Quick Find Options" on page 237 for a more detailed description of the options and examples. The options are:

- **Field**
- **Template**
- **Fixed hex**
- **Sliding hex**
- **ASCII string**
- **Unicode string**
- **EBCDIC string**
- **Decoded string**

Important: The **EBCDIC string** method is only available if you have upgraded your Xgig Chassis server software to version 3.2.

Advanced Quick Hide

You can use Quick Hide to set up more elaborate filtering operations. You can change the type of field, the logical operator, or the value of the field.

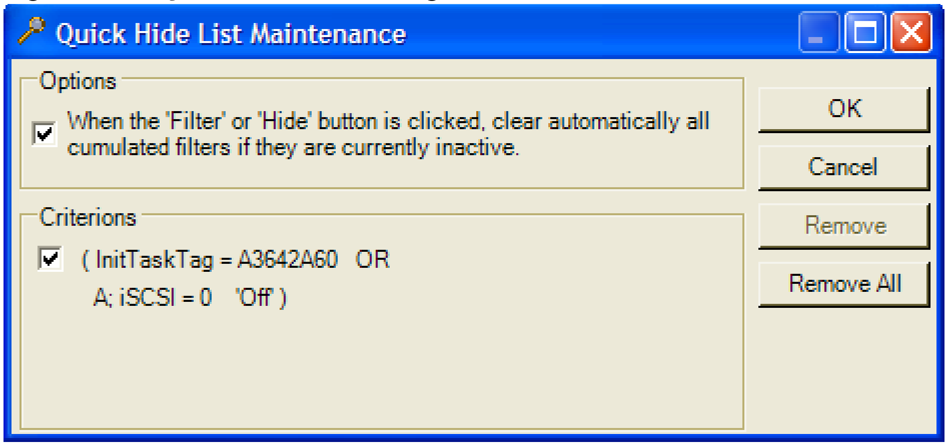
For columns containing numerical data, the **Quick Hide** feature can also be used with the logical operators *equal to* (=), *not equal to* (!=), *(&) and, less than* (<), *greater than* (>), *Match if the value is anyone in the comma-separated list (in), Do not match if the value is anyone in the comma-separated list (! in), Match if the value is within the dash-separated range X-Y specified (where X and Y are included in the comparison) (range),* and *Do not match if the value is within the dash-separated range X-Y specified (!range)*.For non-numerical data, only the equal to and not equal to operators are available. For OOB fields, only the equal to operator is available.

You can also use the **OR>>** button to add an additional condition to your Quick Hide. Using the **OR>>** button means that BOTH conditions will be hidden. Use the pull-down menus to select the field for the second Quick Hide and the value of the field to hide.

Multiple Quick Hides

You can set up multiple Quick Hides. All Quick Hides are stored in a list. Use the **Quick Hide List > Edit…** options from the **Tools** menu to bring up the list of Quick Hide items. You can also manage the list from the **Quick Find/Filter/Hide** dialog box by pressing **Quick Hide list...** button when the **Hide** radio button is selected.

Figure 113: Quick Hide List Dialog Box



From the list, you can remove or disable any Quick Hide. To disable a Quick Hide, uncheck the box next to the item. To remove the item from the list, select the item and click **Remove.** To delete all Quick Hides, select **Quick Hide List > Clear** from the **Tools** menu or press the **Remove All** button.

If you set up a Quick Hide using two filtering operations, each filter operation is listed separately in the Quick Hide list.

A Quick Hide list also exists for Dword view and Exchanges View. The Quick Hide list for Dword view and Exchanges View are completely separate from the list for the main spreadsheet display. Make sure you have selected the correct display (main spreadsheet, Dword, or Exchanges View) before you select **Quick Filter List** from the **Tools** menu. The Quick Hide List for Dword view will have the name of the view in the window title bar.

Hide SAS 8-Byte World Wide Names

See “Search for SAS 8-Byte World Wide Names” on page 246 for a detailed description of the feature. The feature works the same for Quick Hide as for Quick Find.

Hide Source/Destination Addresses

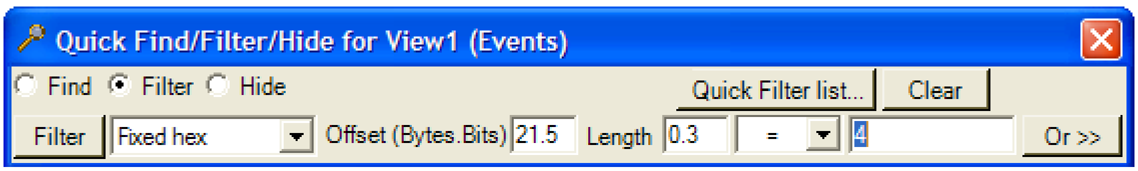
See “Filter Source/Destination Addresses” on page 253 for a detailed description of the feature. The feature works the same for Quick Hide as for Quick Filter.

Bit Level Find/Filter/Hide

With the hex option, it is also possible to Find/filter/hide based on bit strings as well as byte strings. Bit level offsets are specified by a “dot” notation, where the first value expresses the bytes and the second value expresses bits. For example, 4.3 means bit 3 within byte number 4. Bit-level lengths are also specified in “dot” notation. For example, 2.1 equals a length of 17 bits (2*8 + 1 = 17). For bit-level matches, the string to match is expressed in hexadecimal.

For example, assume you want to match a string of three bits, the first bit set to “on” (value of 1) and the last two bits set to “off” (value of 0). The bits you are matching are bits 5, 6, and 7 with the byte at offset 21. Set up the conditions so you will match the bit string by making the following entries in the **Quick Find/Filter/Hide** dialog box.

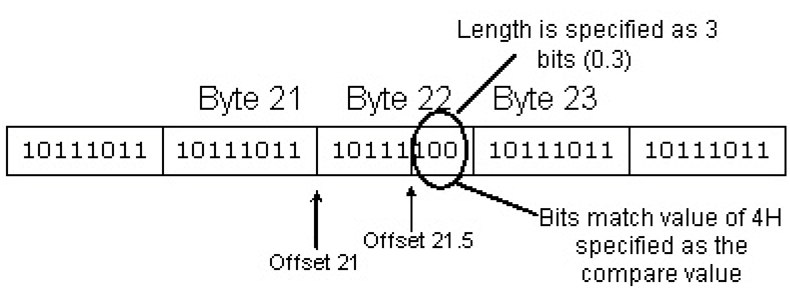
Figure 114: Quick Filter, Bit Level



The offset field value of 21.5 indicates start the bit string match at bit 5 of byte 22 (byte 22 is offset by 21 bytes). The length field is set to 0.3 to indicate you are looking for a string that is three bits long. The bits are compared with the bits indicated by the hexadecimal number specified as the value (4H). The value 4H is interpreted as a bit string for the compare process, so 4H becomes “0100” as a bit string.

The compare starts for the number of bits counting from the right of the bit string (the last three bits are used for the compare). The compare starts bit by bit from the first bit on the left. In the example, if bit 21.5 has a value of 1 it matches the compare bit (X1XX). If bit 21.6 has a value of 1 it would not match the compare bit (XX0X). See the picture below for a look at the compare process for the example.

Figure 115: Bit Level Filter Example



You must specify the bit compare carefully to get the results you want. Note that any “extra” bits in the compare value are not used. In the example, only the lowest three bits of the value 4H are used for the compare; the other bits are ignored. In the example, the value CH (fourth bit set on) would produce the same result as 4H (fourth bit set off). If you specify a hexadecimal value that does not represent enough bits for the length of the bit compare, the hexadecimal value is automatically filled with zeros so enough bits are represented for the compare.

The actual action taken as a result of the compare depends on which radio button is selected in the dialog: find, filter, or hide. If searching, the first event that matches the bit string compare is selected. If filtering, all events that match the bit string compare are included in the display and all others are removed. If hiding, all events that match the bit string compare are removed from the display.

Using the Filter Tab to Perform Filter Operations

Use the **Filter** tab of the Detailed Find/Filter/Color window to perform filter operations.

1 Select **Detailed Find/Filter/Color...** from the **View** menu to bring up the Detailed Find/Filter/Color window.

2 Select a template from the **User Library** or the **Viavi Library**.

3 Select the **Filter** tab.

4 Drag templates to the **Filter** tab's **Show all Events like this** pane.

5 If needed, drag templates to the **Filter** tab's **Except all Events like this** pane.

6 Continue to select, drag, and drop templates until you are satisfied with the conditions.

7 Press **OK** to apply the filter.

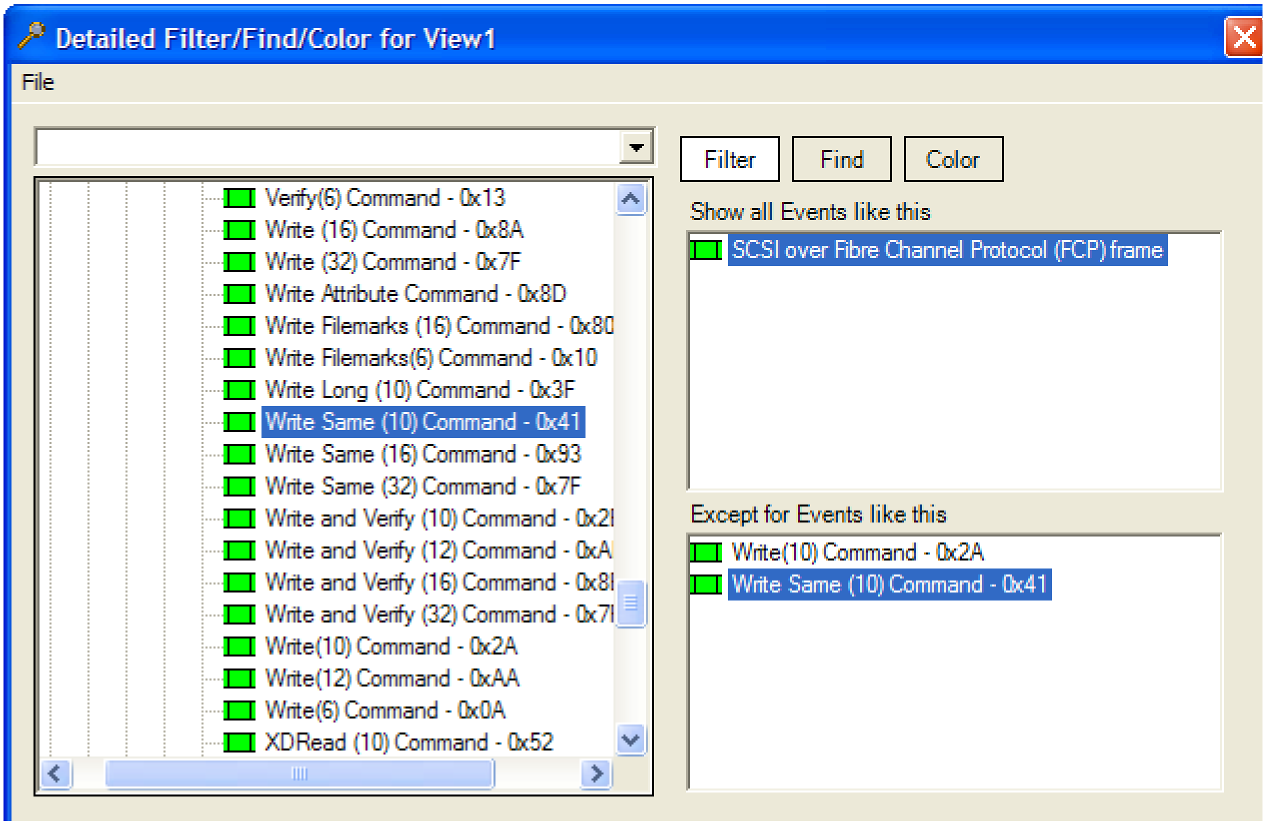
Once the filter is applied, use the **Apply Filters**  button to toggle between applying and removing the filter.

The **Except all events like this** pane can be used to further refine the filter. It filters out events that are passed by the filters in the **Show all Events like this** pane that you do not want to display.

Filter Tab Example

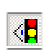
An example of a filter created using the **Filter** tab is shown below. When the filter is applied all events other than SCSI frames are not shown. SCSI frames that have write commands are also not displayed. All templates for this example were dragged and dropped from the Viavi Library in the Available Templates Browser. Double-click a template to modify its contents. Right-click a template to perform copy, cut, paste, rename, or delete operations.

Figure 116: Filter Using the Filters Tab



Ordered Sets

Ordered sets, called primitives in SAS/SATA, are units of traffic that are used to manage or control a particular protocol and encapsulate data into frames.

Press the **Show Ordered Sets**  button to toggle between showing and hiding ordered sets. Hiding ordered sets can narrow your data display when you only need to look at frames or packets. For example, when you hide this information in Fibre Channel, all you see are frames.

TraceView handles the display of ordered sets in different ways depending on the settings described in this section. For example, certain types of ordered sets may be hidden. This can make it easier to view important trace events. Another feature that helps focus the display is that consecutive, equal ordered sets are represented in one row with a repeat count.

You can refine the display to show all ordered sets, show only ordered sets that are communication oriented, or show only acknowledgment and error ordered sets, or hide all ordered sets. Select the type of ordered sets you want to view from the drop-down menu next to the **Show Ordered Sets** button, or deselect the button to hide all ordered sets.

If you set the option to **Show All Ordered Sets** (default value for all except PCIe traces), all the ordered set primitives are displayed. The display/hide of primitives works by toggling the button. When you select the button, all primitives will display. When you de-select the button, only frames will display. Note that certain primitives never display in the TraceView main grid. See the information below for the primitives that do not display for each protocol.

If you set the option to **Show Connection Only Ordered Sets**, only the ordered set primitives that are connection-oriented (for example, Open and Close) are displayed. Non-connection primitives such as R_RDY will not display. When you set the options to show connection only ordered sets, the button in the toolbar will change to a traffic light with a C next to it . The display/hide of primitives works by toggling the button. When you select the button, the communication-oriented primitives will display. When you deselect the button, only frames will display.

If you set the option to **Show Acknowledgment and Error Only Ordered Sets**, only the ordered set primitives for errors or acknowledgments (for example, R_RDY) are displayed. Non-acknowledgment primitives such as DONE will not display. When you set the options to show acknowledgment and error ordered sets, the button in the toolbar will change to a traffic light with an A next to it . The display/hide of primitives works by toggling the button. When you select the button, these primitives will display. When you deselect the button, only frames will display.

If you set the option to **Show ACK DLLPs and Errors only**, which is the default value for PCIe traces, only TLP packets, Ack, Nak, InitFC1/2-x DLLP Packet, TS1, TS2, and Any other ordered set with a physical error on it are displayed. When you set the options to show ACK DLLPs and errors only, the button in the toolbar will change to a traffic light with a A next to it . The display/hide of primitives works by toggling the button. When you select the button, the ACK DLLPs, and error ordered sets display. When you deselect the button, only frames will display. To display all ordered sets for PCIe traces, select **Show All Ordered Sets** from the drop-down menu.

Connection-oriented and acknowledgment and error primitives are a subset of all ordered sets – when you display all ordered sets you will also display these primitive types.

Elements for ordered sets within the Detailed Find/Filter/Color window are indicated by the icon. Ordered sets in the spreadsheet show in the **Icons** column as “**OS**”.

Primitives Displayed with Ordered Set Options, SAS/SATA

All primitives other than those on the list below display in the main spreadsheet when you select the **Show All Ordered Sets** option. For SAS/SATA, these primitives only display in the main spreadsheet if an error occurred in the primitive. All primitives in the list below will display in the Dword View:

- SATA_R_IP
- SATA_HOLD
- SATA_HOLDA
- ALIGN(s)
- NOTIFY(s)
- SATA_SYNC
- SATA_CONT
- SAS Scrambled Idle Dwords

The following primitives are displayed when you select **Show Connection Only Ordered Sets** and then display ordered sets for SAS/SATA:

- AIP(s)
- OPEN_ACCEPT
- OPEN_REJECT(s)
- DONE(s)
- CLOSE(s)
- BREAK

The following primitives are displayed when you select **Show Acknowledgment and Error Only Ordered Sets** and then display ordered sets for SAS/SATA:

- RRDY
- ACK
- NAK(s)
- SATA_R_OK
- SATA_R_ERR
- SAS_ERROR
- SATA_ERROR
- HARD_RESET
- OPEN_ACCEPT
- OPEN_REJECT(s)
- CLOSE(s)

Primitives Displayed with Ordered Set Options, Fibre Channel

All Fibre Channel ordered sets display when you select the **Show All Ordered Sets** option.

The **Show Connection Only Ordered Sets** and **Show Acknowledgment and Error Only Ordered Sets** options are not available for Fibre Channel.

Out-of-Band Data (SAS/SATA Only)

Press the **Show OOB Data**  button to toggle between showing and hiding OOB data in the trace. Hiding OOB data can decrease the amount of data in the main spreadsheet when it is not necessary to see these commands. OOB commands only apply to SAS/SATA. For other protocols, this button is disabled.

You can refine the display to show advanced OOB Events. Use the drop-down menu next to the **OOB Data** button to select either **Show Only Basic OOB Events** or **Show Advanced OOB Events,** or deselect the button to hide all OOB information.

If you set the option to **Show Only Basic OOB Events** (default value), only essential OOB events display. The display/hide of OOB events works by toggling the button. When you select the button, basic OOB events will display. When you de-select the button, no OOB events will display.

If you set the option to **Show Advanced OOB Events**, additional OOB events such as speed negotiation events are displayed. The display/hide of events works by toggling the button. Only when you select the button will the OOB events display. When you deselect the button, no OOB events will display. For OOB Begin/End markers to display, you also need to set TraceView to display these events in the **Expert/Protocol Decodes** tab of TraceView options. Select the **Show OOB Begin/End Markers** check box in the dialog box to show these events.

OOB Signal Detection and Interpretation

TraceView uses timing measurements to determine whether the OOB signal detected is good or bad. Figure 117 shows a diagram of OOB bursts and D.C. Idles between OOB bursts. Based on the time lengths (see Table 15) of the first through fourth D.C. Idle, TraceView will categorize the event as good or bad. This evaluation is different for each type of event – COMINIT, COMRESET, COMSAS, or COMWAKE.

Figure 117: OOB Event Detection Diagram

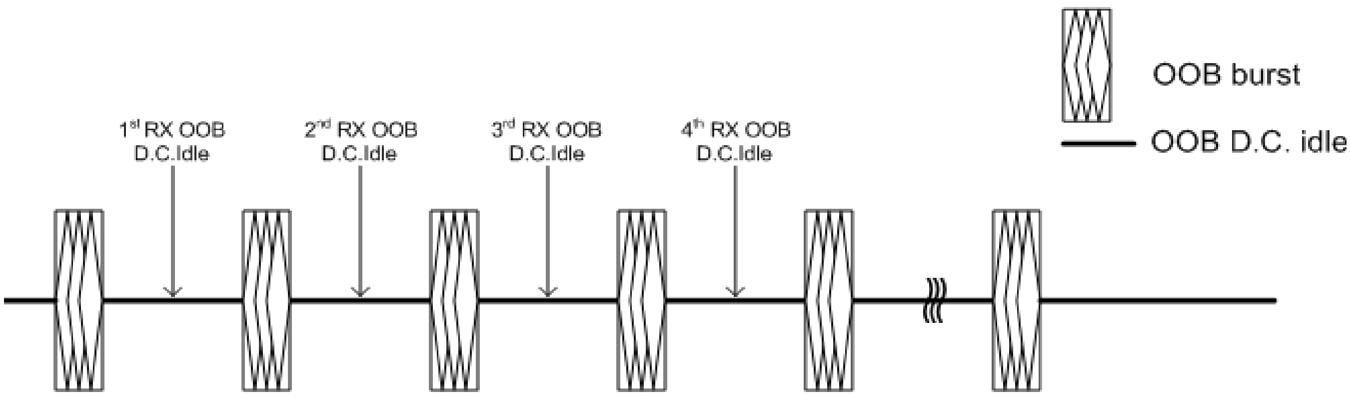


Table 15: Minimum and Maximum Values for Good OOB Signals

OOB Signal	Rx D.C. Idle Time Minimum	Rx D.C. Idle Time Maximum
COMINIT	255 ns	465 ns
COMSAS	700 ns	1525 ns
COMWAKE/COMRESET	70 ns	160 ns

Table 16: SATA Port Selection Timing

SATA Port Selection Timing	Minimum	Maximum
SATA Port Selection T1 Time	1.6 ms	2.4 ms
SATA Port Selection T2 Time	7.6 ms	8.4 ms

OOB Event Detection and Speed Negotiation is unique to each version of the SAS protocol, SAS-1 or SAS-2. The tables below describe the OOB events for each version.

SAS-1, Good/Bad OOB Event Detection

The following table describes how TraceView uses the timing measurements of idles to determine if the signal is good for each type of event for SAS-1.

Table 17: Good/Bad OOB Event Detection

Good/Bad OOB Event Detected	Event Description
Good COMINIT/COMRESET	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMINIT OOB signal is within the range specified in Table 15.
Bad COMINIT/COMRESET	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMINIT OOB signal is not within the range specified in Table 15.
Good COMSAS	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMSAS OOB signal is within the range specified in Table 15.
Bad COMSAS	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMSAS OOB signal is not within the range specified in Table 15.
Good COMWAKE	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMWAKE OOB signal is within the range specified in Table 15.
Bad COMWAKE	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMWAKE OOB signal is not within the range specified in Table 15.

SAS -1, Speed Negotiation Decodes

TraceView uses timing values and other criterion to determine events reported for speed negotiation using OOB signals. The description of how TraceView determines these events are shown in Table 18.

Table 18: Speed Negotiation Decodes

Speed Negotiation Decodes	Event Description
Successful G1 speed Neg	This event is set when a SAS device sends and receives ALIGN(1) primitives during G1 window of the SAS speed negotiation sequence.
Unsuccessful G1 speed Neg	This event is set when a SAS device does not send or receive ALIGN(1) primitives during G1 window of the speed negotiation sequence.
Successful G2 speed Neg	This event is set when a SAS device sends and receives ALIGN(1) primitives during G2 window of the speed negotiation sequence.
Unsuccessful G2 speed Neg	This event is set when a SAS device does not send or receive ALIGN(1) primitives during G2 window of the speed negotiation sequence.
Successful G3 speed Neg	This event is set when a SAS device sends and receives ALIGN(1) primitives during G3 window of the speed negotiation sequence.
Unsuccessful G3 speed Neg	This event is set when a SAS device does not send or receive ALIGN(1) primitives during G3 window of the speed negotiation sequence.
Good RCDT detected	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a SAS speed negotiation window time. This event is set when the measured RCDT value lies within this range: 492.5 us < RCDT < 507.5 us.
Bad RCDT detected	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a speed negotiation window time. This event is set when the measured RCDT time <= 492.5 us or RCDT time >= 507.5 us.
Good SNTT detected	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time lies within this range: 102.5 us < SNTT < 117.5 us
Bad SNTT detected	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time <= 102.5 us or SNTT time >= 117.5 us.
1.5 Gbps speed detected	This event is set during SATA speed negotiation sequence, if a SATA device sends and receives ALIGN(0) primitives at 1.5 Gbps rate.
3.0 Gbps speed detected	This event is set during SATA speed negotiation sequence, if a SATA device sends and receives ALIGN(0) primitives at 3.0 Gbps rate.
6.0 Gbps speed detected	This event is set during SATA speed negotiation sequence, if a SATA device sends and receives ALIGN(0) primitives at 6.0 Gbps rate. This event applies only to the 6G SAS/SATA blade.
Speed Neg. Failed	This event is set when the SAS speed negotiation sequence or the SATA speed negotiation sequence fails between two devices trying to communicate using the SAS/SATA protocol.

SAS-2 and SAS-3, OOB Decodes

The following table describes how TraceView uses the timing measurements of idles to determine if the signal is good for each type of event for SAS-2.

Table 19: SAS-2 and SAS-3, OOB Decodes

OOB Decode	Event Description
COMINIT/ COMRESET detected	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMINIT/ COMRESET OOB signal is within the range specified in Table 15.
COMINIT/ COMRESET (incorrect timing) detected	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMINIT/ COMRESET OOB signal is not within the range specified in Table 15.
COMINIT/ COMRESET Begin	This event marks the beginning of the COMRESET /COMINIT OOB signal.
COMINIT/ COMRESET End	This event marks the end of the COMRESET/COMINIT OOB signal.
COMSAS detected	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMSAS OOB signal is within the range specified in Table 15.
COMSAS (incorrect timing) detected	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMSAS OOB signal is not within the range specified in Table 15.
COMSAS Begin	This event marks the beginning of the COMSAS OOB signal.
COMSAS End	This event marks the end of the COMSAS OOB signal.
COMWAKE detected	This event is set when the timing of the first, second, third, and fourth D.C. idle time of a received COMWAKE OOB signal is within the range specified inTable 15.
COMWAKE (incorrect timing) detected	This event is set when the timing of the second or third or fourth D.C. idle time of a received COMWAKE OOB signal is not within the range specified in Table 15.
COMWAKE Begin	This event marks the beginning of the COMWAKE OOB signal.
COMWAKE End	This event marks the end of the COMWAKE OOB signal.
SATA Port Selection OOB detected	This event is set when a SATA Port Selection OOB signal is detected.
OOB Begin	This event marks the beginning of the OOB sequence.
OOB End	This event marks the end of the OOB sequence.

SAS -2, Speed Negotiation Decodes

TraceView uses timing values and other criterion to determine events reported for speed negotiation using OOB signals. The description of how TraceView determines these events are shown in the table below for SAS-2.

Table 20: SAS -2, Speed Negotiation Decodes

Speed Negotiation Decode	Event Description
SNW-1 Begin	This event marks the beginning of the SNW-1 window of the SAS speed negotiation sequence.
SNW-1 End	This event marks the end of the SNW-1 window of the SAS speed negotiation sequence.
Valid SNW-1 detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 1.5 Gbps during SNW-1 window of the SAS speed negotiation sequence.
Invalid SNW-1 detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 1.5 Gbps during SNW-1 window of the SAS speed negotiation sequence.
SNW-2 Begin	This event marks the beginning of the SNW-2 window of the SAS speed negotiation sequence.
SNW-2 End	This event marks the end of the SNW-2 window of the SAS speed negotiation sequence.
Valid SNW-2 detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
Invalid SNW-2 detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
SNW-3 Begin	This event marks the beginning of the SNW-3 window of the SAS speed negotiation sequence.
SNW-3 End	This event marks the end of the SNW-3 window of the SAS speed negotiation sequence.
Valid SNW-3 detected	This event is set when the analyzer receives one or more SAS-2 SNW-3 phy capabilities bits transmitted as COMWAKE OOB signals during SNW-3 window of the SAS speed negotiation sequence.
Invalid SNW-3 detected	This event is set when the analyzer receives no SAS-2 SNW-3 phy capabilities bits during SNW-3 window of the SAS speed negotiation sequence.
SNW-3 phy capabilities bits Begin	This event is set to indicate the beginning of SNW-3 phy capabilities bits transmission window during SNW-3.
SNW-3 phy capabilities bits End	This event is set to indicate the end of SNW-3 phy capabilities bits transmission window during SNW-3.
SNW-3 phy capabilities bit	This event is set when a COMWAKE OOB signal is received during the SNW-3 window to indicate the specific SNW-3 phy capabilities bit received.
SNW-3 phy capabilities value	This event is set to indicate the 32-bit SNW-3 phy capabilities value received during SNW-3 window. The 32-bit value has bit 0 (START bit) as the MSB and bit 31 (PARITY bit) as the LSB.

Table 20: SAS -2, Speed Negotiation Decodes (continued)

Speed Negotiation Decode	Event Description
Final-SNW (1.5 Gbps) Begin	This event marks the beginning of the Final-SNW speed negotiation window at 1.5 Gbps rate.
Final-SNW (1.5 Gbps) End	This event marks the end of the Final-SNW speed negotiation window at 1.5 Gbps rate.
Valid Final-SNW (1.5 Gbps) detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 1.5 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Invalid Final-SNW (1.5 Gbps) detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 1.5 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Final-SNW (3.0 Gbps) Begin	This event marks the beginning of the Final-SNW speed negotiation window at 3.0 Gbps rate.
Final-SNW (3.0 Gbps) End	This event marks the end of the Final-SNW speed negotiation window at 3.0 Gbps rate.
Valid Final-SNW (3.0 Gbps) detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Invalid Final-SNW (3.0 Gbps) detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Train-SNW (1.5 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 1.5 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (1.5 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 1.5 Gbps rate with SSC enabled.
Valid Train-SNW (1.5 Gbps w SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 1.5 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (1.5 Gbps w SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 1.5 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC enabled.
Train-SNW (1.5 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 1.5 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (1.5 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 1.5 Gbps rate with SSC disabled.
Valid Train-SNW (1.5 Gbps w/o SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 1.5 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (1.5 Gbps w/o SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 1.5 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC disabled.

Table 20: SAS -2, Speed Negotiation Decodes (continued)

Speed Negotiation Decode	Event Description
Train-SNW (3.0 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (3.0 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC enabled.
Valid Train-SNW (3.0 Gbps w SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (3.0 Gbps w SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC enabled.
Train-SNW (3.0 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (3.0 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC disabled.
Valid Train-SNW (3.0 Gbps w/o SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (3.0 Gbps w/o SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC disabled.
Train-SNW (6.0 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (6.0 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC enabled.
Valid Train-SNW (6.0 Gbps w SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (6.0 Gbps w SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC enabled.
Train-SNW (6.0 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (6.0 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC disabled.

Table 20: SAS -2, Speed Negotiation Decodes (continued)

Speed Negotiation Decode	Event Description
Valid Train-SNW (6.0 Gbps w/o SSC) detected	This event is set if a SAS-2 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (6.0 Gbps w/o SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC disabled.
RCDT (Rate Change Delay Time) within spec	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a SAS speed negotiation window time. This event is set when the measured RCDT value lies within this range: 492.5 us < RCDT < 507.5 us.
RCDT (Rate Change Delay Time) outside spec	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a speed negotiation window time. This event is set when the measured RCDT time falls within this range RCDT time <= 492.5 us or RCDT time >= 507.5 us.
SNTT (Speed Negotiation Transmit time) within spec	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time lies within this range: 102.5 us < SNTT < 117.5 us
SNTT (Speed Negotiation Transmit time) outside spec	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time <= 102.5 us or SNTT time >= 117.5 us.
ATT (Actual Training time) within spec	This event is set when the measured value of ATT is within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
ATT (Actual Training time) outside spec	This event is set when the measured value of ATT is not within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
SAS Phy reset problem	This event is set when SAS-2 phy reset problem condition is detected on a SAS link.
Speed Negotiation Begin	This event marks the beginning of the Speed Negotiation window.
Speed Negotiation End	This event marks the end of the Speed Negotiation window.
SATA speed negotiation failed	This event is set when speed negotiation is not successful on a SATA link.
SATA 1.5 Gbps speed detected	This event is set when ALIGN(0) primitives are detected from host and drive at 1.5 Gbps on a SATA link.
SATA 3.0 Gbps speed detected	This event is set when ALIGN(0) primitives are detected from host and drive at 3.0 Gbps on a SATA link.

SAS -3, Speed Negotiation Decodes

TraceView uses timing values and other criterion to determine events reported for speed negotiation using OOB signals. The description of how TraceView determines these events are shown in the table below for SAS-3.

Table 21: SAS -3, Speed Negotiation Decodes

Speed Negotiation Decode	Event Description
SNW-2 Begin	This event marks the beginning of the SNW-2 window of the SAS speed negotiation sequence.
SNW-2 End	This event marks the end of the SNW-2 window of the SAS speed negotiation sequence.
Valid SNW-2 detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
Invalid SNW-2 detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
SNW-3 Begin	This event marks the beginning of the SNW-3 window of the SAS speed negotiation sequence.
SNW-3 End	This event marks the end of the SNW-3 window of the SAS speed negotiation sequence.
Valid SNW-3 detected	This event is set when the analyzer receives one or more SAS-2 SNW-3 phy capabilities bits transmitted as COMWAKE OOB signals during SNW-3 window of the SAS speed negotiation sequence.
Invalid SNW-3 detected	This event is set when the analyzer receives no SAS-2 SNW-3 phy capabilities bits during SNW-3 window of the SAS speed negotiation sequence.
SNW-3 phy capabilities bits Begin	This event is set to indicate the beginning of SNW-3 phy capabilities bits transmission window during SNW-3.
SNW-3 phy capabilities bits End	This event is set to indicate the end of SNW-3 phy capabilities bits transmission window during SNW-3.
SNW-3 phy capabilities bit	This event is set when a COMWAKE OOB signal is received during the SNW-3 window to indicate the specific SNW-3 phy capabilities bit received.
SNW-3 phy capabilities value	This event is set to indicate the 32-bit SNW-3 phy capabilities value received during SNW-3 window. The 32-bit value has bit 0 (START bit) as the MSB and bit 31 (PARITY bit) as the LSB.
Final-SNW (3.0 Gbps) Begin	This event marks the beginning of the Final-SNW speed negotiation window at 3.0 Gbps rate.
Final-SNW (3.0 Gbps) End	This event marks the end of the Final-SNW speed negotiation window at 3.0 Gbps rate.
Valid Final-SNW (3.0 Gbps) detected	This event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.

Table 21: SAS -3, Speed Negotiation Decodes (continued)

Speed Negotiation Decode	Event Description
Invalid Final-SNW (3.0 Gbps) detected	This event is set when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Train-SNW (3.0 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (3.0 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC enabled.
Valid Train-SNW (3.0 Gbps w SSC) detected	This event is set if a SAS-3 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (3.0 Gbps w SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC enabled.
Train-SNW (3.0 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (3.0 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 3.0 Gbps rate with SSC disabled.
Valid Train-SNW (3.0 Gbps w/o SSC) detected	This event is set if a SAS-3 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (3.0 Gbps w/o SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 3.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC disabled.
Train-SNW (6.0 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (6.0 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC enabled.
Valid Train-SNW (6.0 Gbps w SSC) detected	This event is set if a SAS-3 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (6.0 Gbps w SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC enabled.

Table 21: SAS -3, Speed Negotiation Decodes (continued)

Speed Negotiation Decode	Event Description
Train-SNW (6.0 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (6.0 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 6.0 Gbps rate with SSC disabled.
Valid Train-SNW (6.0 Gbps w/o SSC) detected	This event is set if a SAS-3 phy has transmitted at least 4 TRAIN_DONE patterns and received at least 1 TRAIN_DONE primitive at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (6.0 Gbps w/o SSC) detected	This event is set if a phy has not transmitted at least 4 TRAIN_DONE patterns or not received 1 TRAIN_DONE at 6.0 Gbps rate within MTT (Maximum Training time ~ 20 ms), during Train-SNW speed negotiation window with SSC disabled.
Train-SNW (12.0 Gbps w SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 12.0 Gbps rate with SSC (Spread Spectrum clocking) enabled.
Train-SNW (12.0 Gbps w SSC) End	This event marks the end of the Train-SNW speed negotiation window at 12.0 Gbps rate with SSC enabled.
Valid Train-SNW (12.0 Gbps w SSC) detected	This event is set if a SAS-3 phy has successfully completed both transmitter and receiver training at 12.0 Gbps, during a Train-SNW speed negotiation window with SSC enabled.
Invalid Train-SNW (12.0 Gbps w SSC) detected	This event is set if either transmitter training or receiver training fails at 12Gbps, during Train-SNW speed negotiation window with SSC enabled.
Train-SNW (12.0 Gbps w/o SSC) Begin	This event marks the beginning of the Train-SNW speed negotiation window at 12.0 Gbps rate with SSC (Spread Spectrum clocking) disabled.
Train-SNW (12.0 Gbps w/o SSC) End	This event marks the end of the Train-SNW speed negotiation window at 12.0 Gbps rate with SSC disabled.
Valid Train-SNW (12.0 Gbps w/o SSC) detected	This event is set if a SAS-3 phy has successfully completed both transmitter and receiver training at 12.0 Gbps, during a Train-SNW speed negotiation window with SSC disabled.
Invalid Train-SNW (12.0 Gbps w/o SSC) detected	This event is set if either transmitter training or receiver training fails at 12Gbps, during Train-SNW speed negotiation window with SSC disabled.
Train_Tx-SNW Begin	This event marks the beginning of the Transmitter training-SNW speed negotiation window at 12.0Gbps rate

Table 21: SAS -3, Speed Negotiation Decodes (continued)

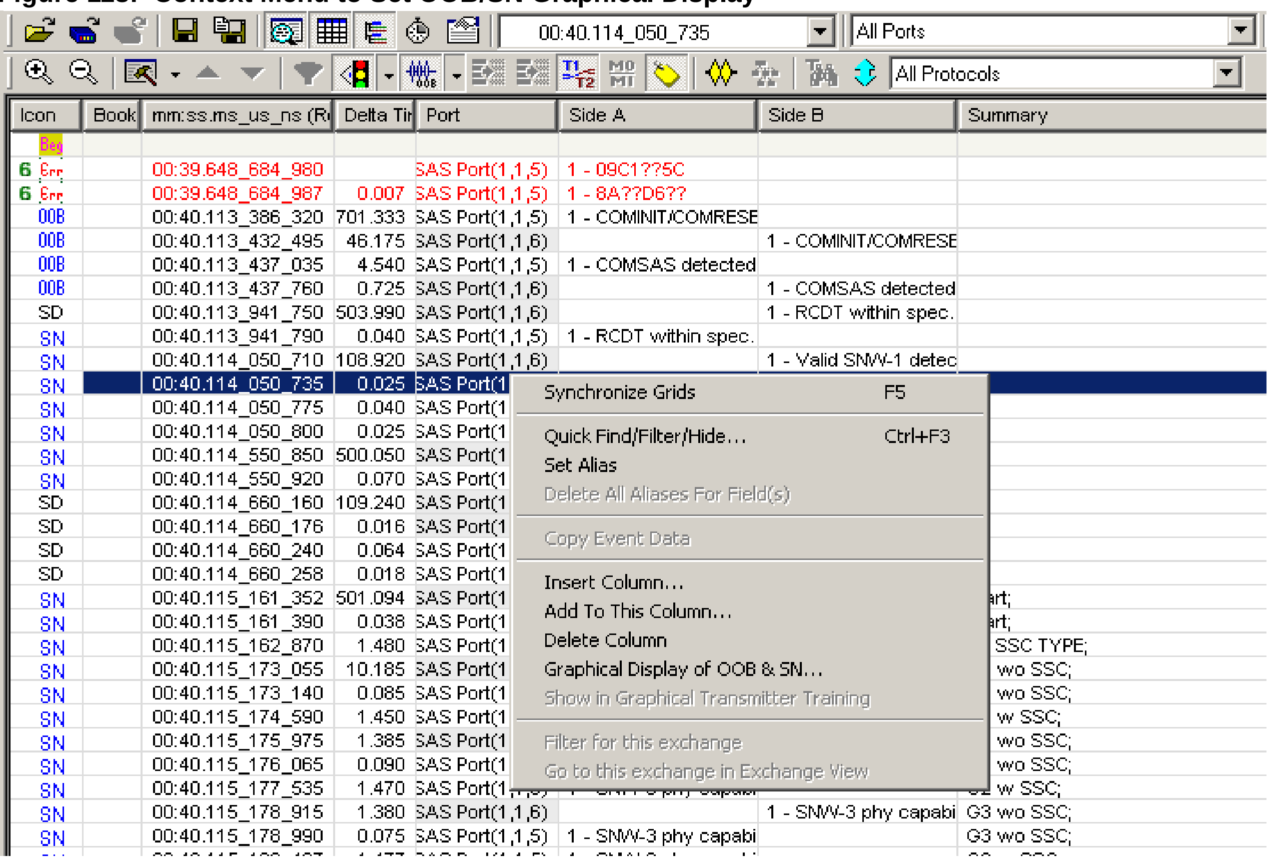
Speed Negotiation Decode	Event Description
Train_Tx SNW End	This event marks the end of the Transmitter training-SNW speed negotiation window at 12.0Gbps rate
RCDT (Rate Change Delay Time) within spec	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a SAS speed negotiation window time. This event is set when the measured RCDT value lies within this range: 492.5 us < RCDT < 507.5 us.
RCDT (Rate Change Delay Time) outside spec	A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a speed negotiation window time. This event is set when the measured RCDT time falls within this range RCDT time <= 492.5 us or RCDT time >= 507.5 us.
SNTT (Speed Negotiation Transmit time) within spec	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time lies within this range: 102.5 us < SNTT < 117.5 us
SNTT (Speed Negotiation Transmit time) outside spec	A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. This event is set when the measured SNTT time <= 102.5 us or SNTT time >= 117.5 us.
ATT (Actual Training time) within spec	This event is set when the measured value of ATT is within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
ATT (Actual Training time) outside spec	This event is set when the measured value of ATT is not within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
SAS Phy reset problem	This event is set when SAS-2 phy reset problem condition is detected on a SAS link.
Speed Negotiation Begin	This event marks the beginning of the Speed Negotiation window.
Speed Negotiation End	This event marks the end of the Speed Negotiation window.

Graphical Display of OOB and Speed Negotiation Events

OOB and Speed Negotiation data can be viewed graphically in TraceView. You can graphically view, scroll, and view greater/lesser detail (zoom) for OOB/SN events. Select **Graphical Display of OOB & SN...** from the event grid context menu or the OOB Display button to bring up the graphical display. See Figure 118.

When viewing a trace file, the OOB Display  button and the **Graphical Display of OOB & SN...** menu item and will only be available when you have selected an OOB/SN event on a trace captured with the 6G SAS/SATA blade. If you have selected a non-OOB/SN event or the OOB events are captured with 3G SAS/SATA blades, the button/menu item will be grayed out. Out-of-band data only applies to SAS/SATA traces, so this button/menu item will also be grayed out for Fibre Channel and Gigabit Ethernet traces. If the trace was not captured with Xgig Analyzer 4.0 or later, a dialog will appear with following message: **This trace is not captured with Xgig Analyzer 4.0 or later. Graphical display of OOB & Speed Negotiation is not supported for this trace**.

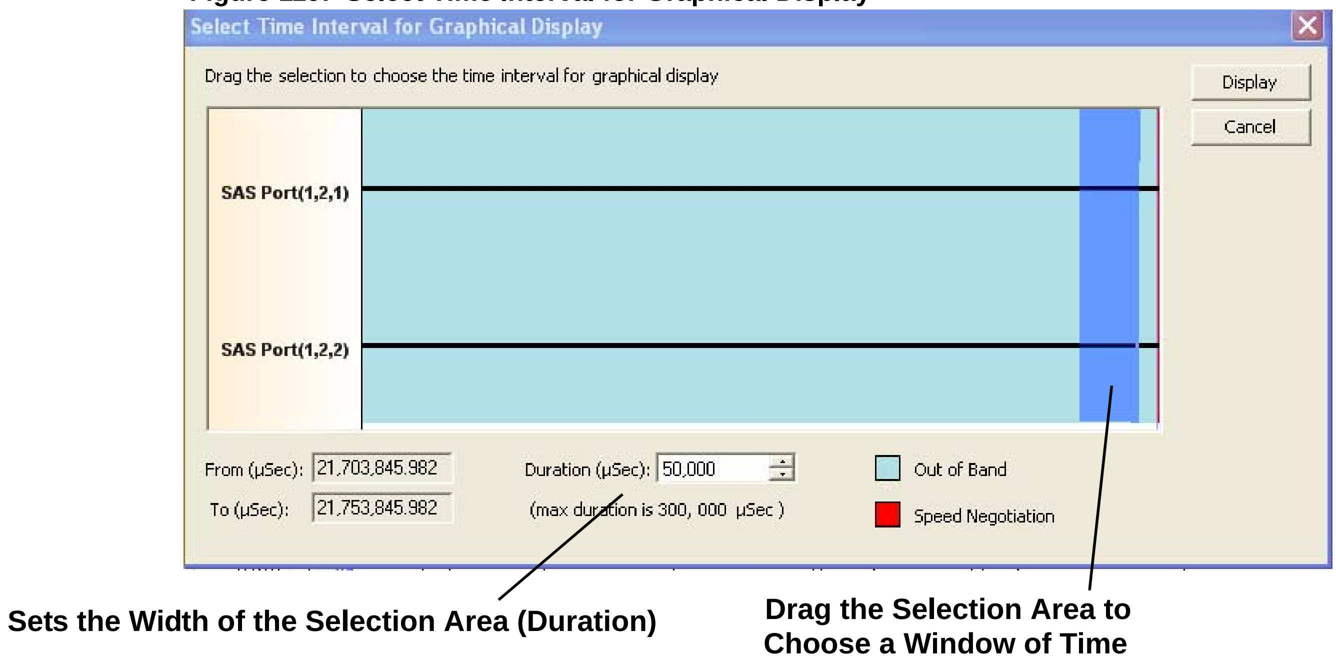
Figure 118: Context Menu to Set OOB/SN Graphical Display



If the duration of OOB is more than 300 msec, the **Select Time Interval for Graphical Display** dialog box is presented to select time range, as shown in Figure 119. If the duration of OOB session is less than 300 msec, time range selection dialog is not presented and the main display for the viewing OOB/SN events is displayed.

The **Select Time Interval for Graphical Display** dialog displays the time extents of the OOB session. Duration for each of the ports in the port pair is shown as a horizontal line, and OOB and SN periods within the time line are color-coded. Select the total time range to view in the **Duration (uSec)** field (the maximum duration is 300 msec). Drag the selection area (lavender color) to choose the time period for graphic display. Click the **Display** button to complete time interval selection and view the OOB/SN graphical display.

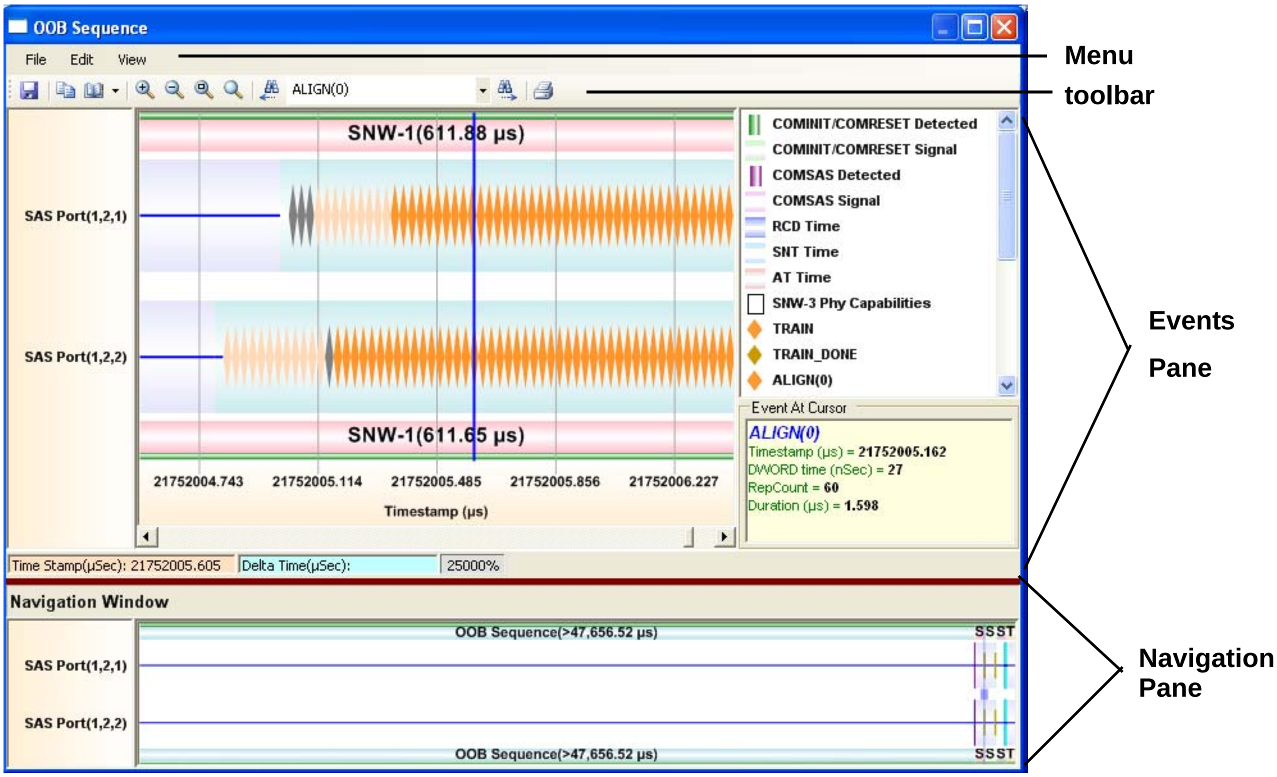
Figure 119: Select Time Interval for Graphical Display



OOB/SN Graphical Display/Dialog Box

The OOB/SN graphical display and dialog box is shown in Figure 120. The OOB/SN graphical display has two panes. The lower pane is the navigation pane and the upper pane is the events pane. All the events in the OOB session (or events within the selected time range) are displayed in the navigation window. A subset of OOB events are magnified and are shown in the events pane. A toolbar and menu provide the controls to navigate, zoom, and print events.

Figure 120: OOB and Speed Negotiation Sequence Graphical Display



Events Pane

The events pane shows events in a scrollable window. You can use the scroll bar to navigate to different parts of the trace. Change the zoom to view the events at a different granularity. On the left side of the events pane, port names are displayed. On the right side of the events pane, legends are shown to describe different events. At the bottom of the events pane, the timestamp at the cursor location is displayed.

When the mouse is moved over the events pane, the timestamp displayed is synchronized with the mouse cursor. There is no need to click the events pane to see the timestamp at the current cursor location. You can select events by pressing the left-mouse button and dragging the mouse over the events pane before releasing the mouse button. The selection is highlighted as shown in Figure 121.

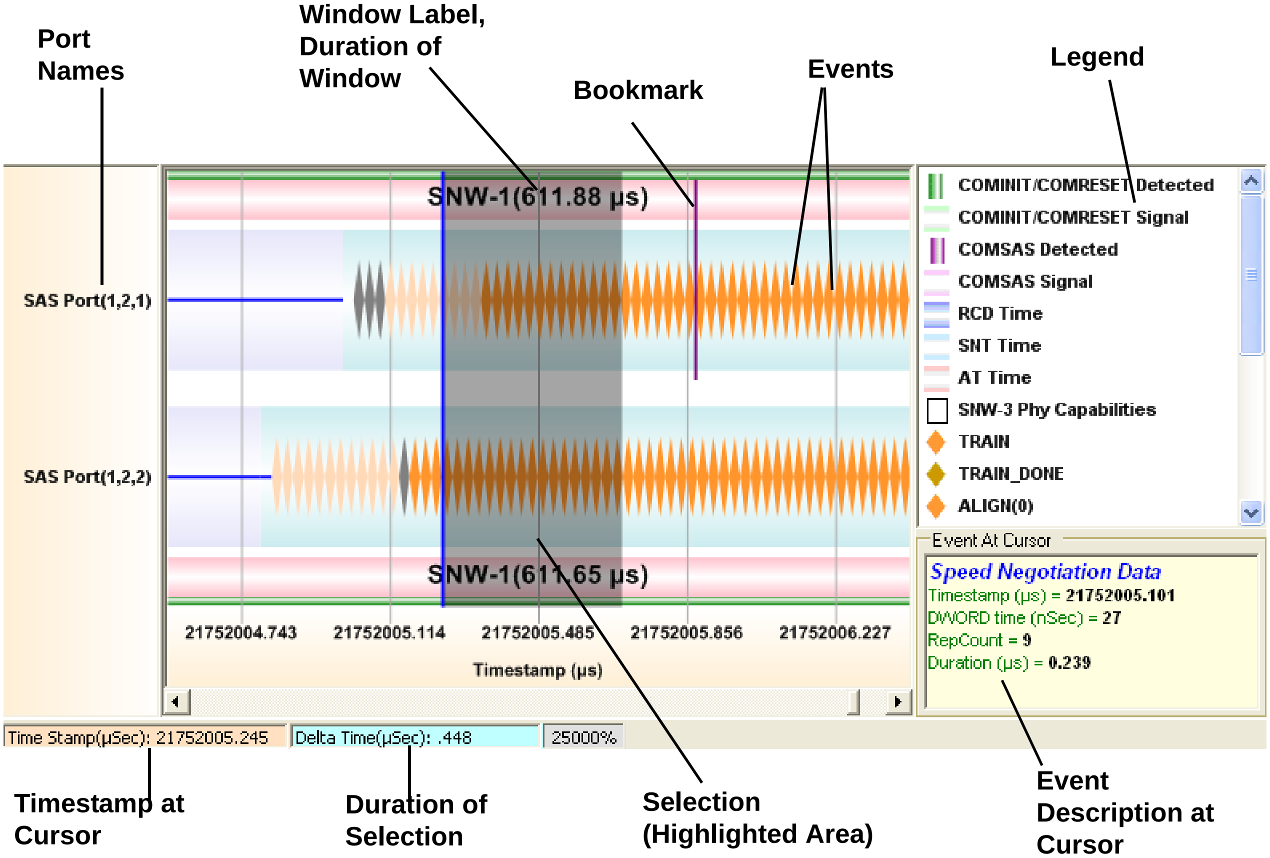
Duration of the current selection is displayed at the bottom of the events pane if there is a selection. When the mouse is hovered on an event, details of the event are displayed in a tool tip. Click outside the selection to cancel the selection. Click the right-mouse button on any event in the events pane to invoke context menus.

The various windows for speed negotiation are labeled within the graphic display; for example, **SNW-2 (611.88 *us*)**. The duration of the window is shown in parenthesis. The speed negotiation windows can be different durations for each port, so the windows are labeled separately for each port. There are nine possible windows for speed negotiation. Not all devices go through all nine negotiations; device capabilities dictate which windows they go through.

Most of the events have repeat count of greater than one. The timestamp at the bottom shows the time corresponding to mouse cursor. Timestamp in right bottom window shows the start timestamp for the event. If cursor is not at the beginning of the event, these two timestamps will be different.

When 12G SAS devices are connected with optical cables, optical OOB events, such as OOB_IDLE instead of DC_IDLE, are displayed in the legend and the event description at cursor sections of the OOB/SN Graphical Displays, Events pane. These sections are labeled in the figure below.

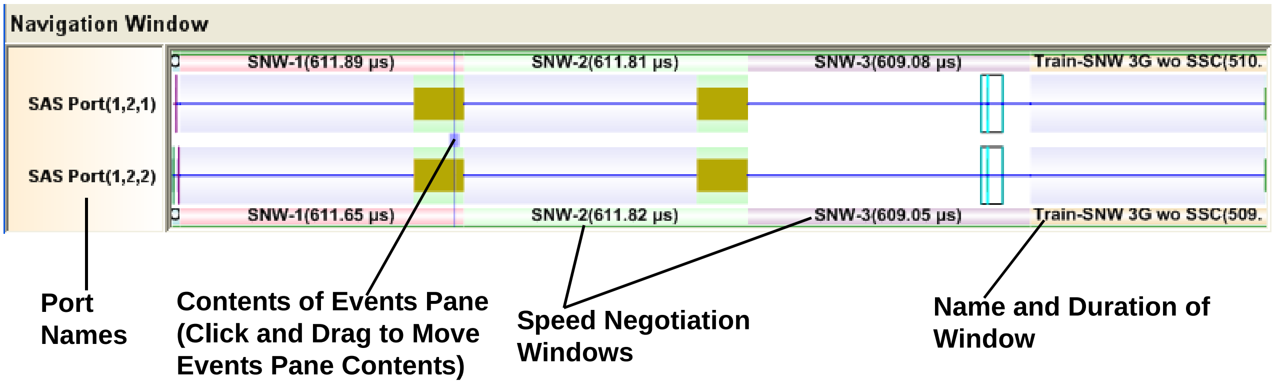
Figure 121: OOB/SN Graphical Display, Events Pane



Navigation Pane

The navigation pane displays all the events present. The time period corresponding to the contents of the events pane is highlighted. Drag the highlighted time window or double-click the navigation pane to view different regions of the OOB section of the trace. The events pane will update to contain the events corresponding to the new time interval. The navigation pane provides a fast way of locating any part of the OOB section of the trace.

Figure 122: OOB/SN Graphical Display, Navigation Pane



OOB/SN Graphical Display Toolbar, Buttons, and Menus

Figure 123 shows the menus available for the **OOB and Speed Negotiation Sequence Graphical Display** and Figure 124 shows the toolbar. See Table 22 for a description of all controls.

Figure 123: OOB/SN Graphical Display Menus

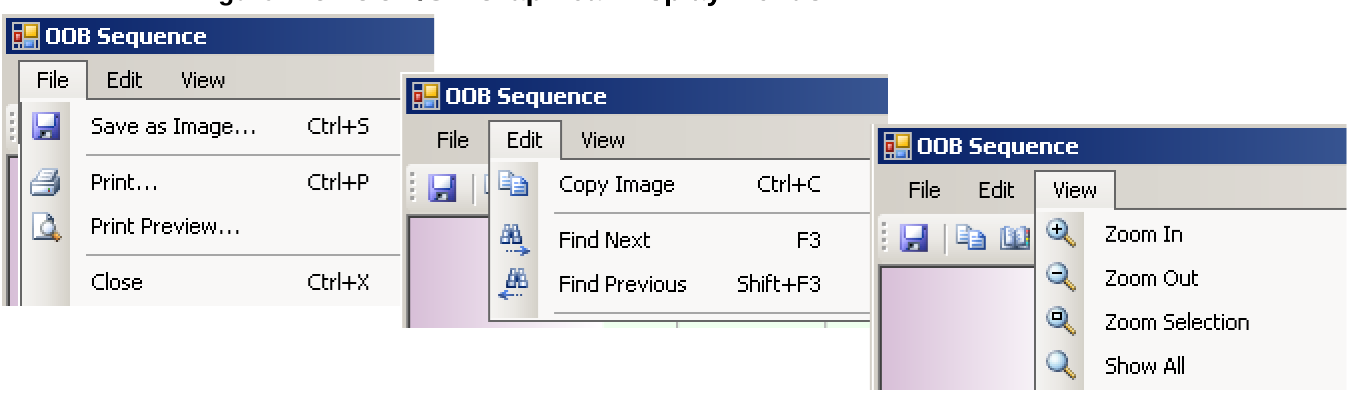


Figure 124: OOB/SN Graphical Display Toolbar

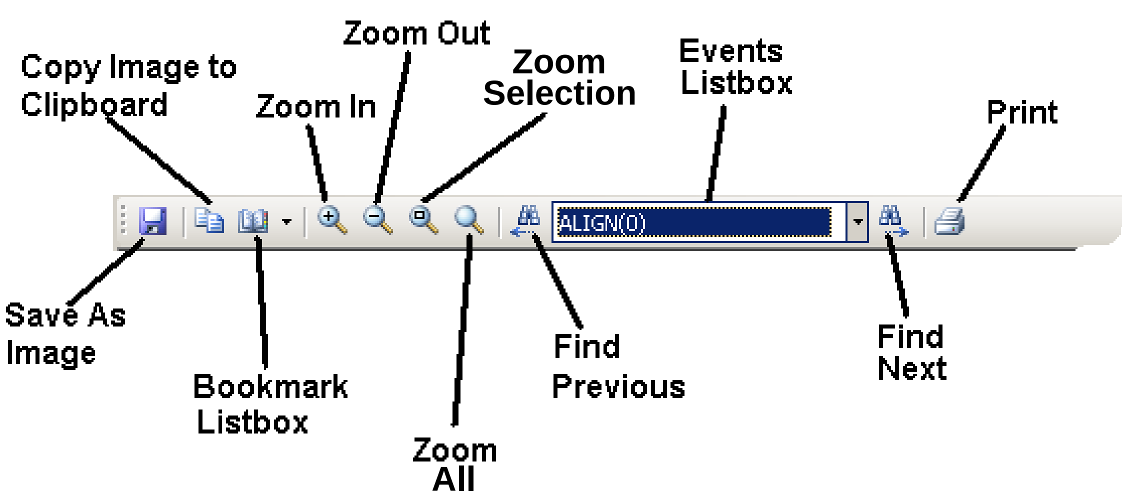


Table 22: Buttons and Controls for OOB/SN Graphical Display

Button / Menu Item	Description
Save As Image	Brings up a standard file save dialog box to save the events pane as an image. The image can be saved in bmp, jpeg, or tiff format.
Copy Image To Clipboard	Copies the events pane to the clipboard as an image. This image can be pasted into a document using any word processor application.
Bookmark Listbox	Lists all bookmarks in a drop-down list. Select a bookmark to quickly jump to that location.
Zoom In	Click this button to show fewer events (more detail). The maximum allowed zoom is determined by the data being viewed.
Zoom Out	Click this button to show more events. Zoom can be decreased until all the events are displayed in the events pane.
Zoom Selection	Select a portion of events displayed in the event grid and click **Zoom Selection** to adjust the zoom so that the selection fits into the whole width of the events pane.
Zoom All	Sets the zoom to minimum level so all events fit into the events pane.
Find Previous	Finds the previous occurrence of a selected event type. By repeatedly clicking this button, navigate quickly within the trace based on an event type.
Events Listbox	Lists all the event types in a drop-down list. Select an event and use **Find Next** / **Find Previous** buttons to navigate in the events pane.
Find Next	Same as **Find Previous** except in forward direction.
Print	Prints the events pane.
Print Preview	Shows the print preview of the events pane.

Context Menus

When you click the right-mouse button when the mouse is on events pane, a context menu is displayed as shown in Figure 125. See Table 23 for a description on each menu selection.

Figure 125: OOB/SN Graphical Display Context Menus

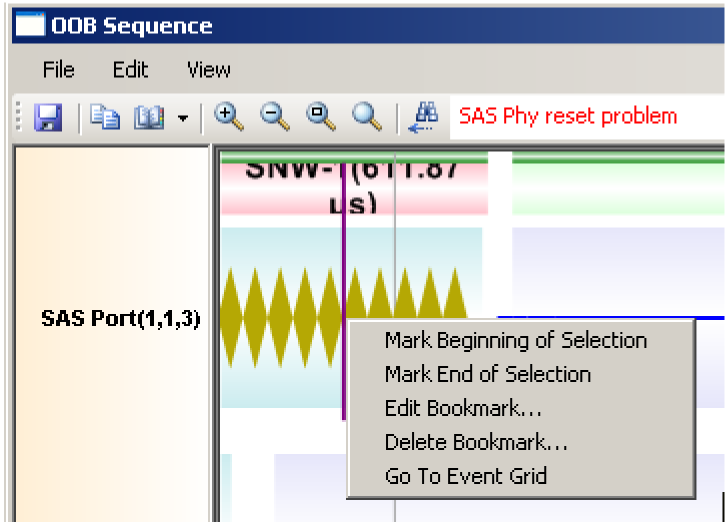


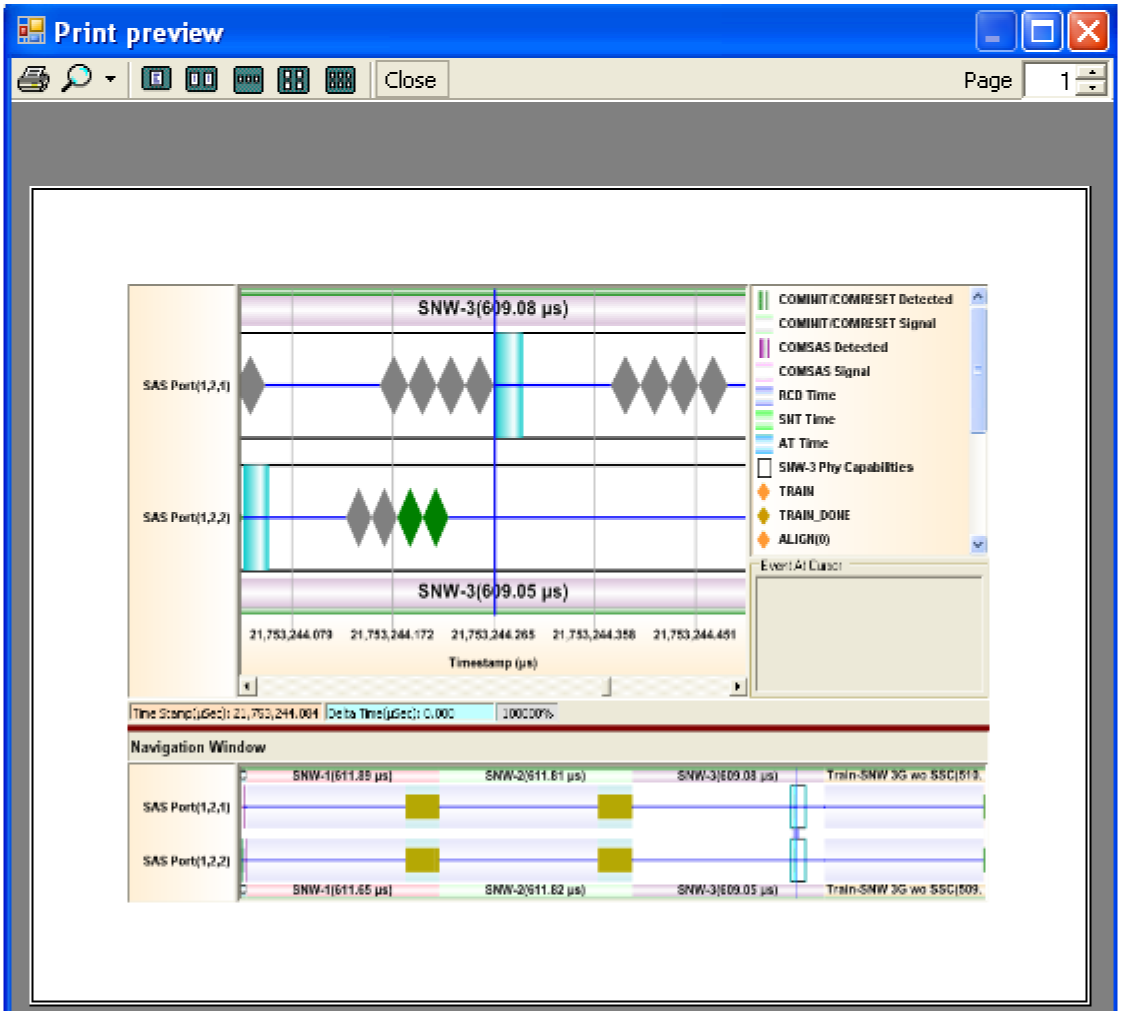
Table 23: Context Menu Options for the OOB/SN Graphical Display

Menu Selection	Description
Mark Beginning of Selection	Sets the beginning of the selection to the current time stamp.
Mark End of Selection	Sets the end of the selection to the current time stamp.
Add Bookmark…	Brings up a dialog to add a bookmark at the current event. This menu is displayed only if the current event does not have a bookmark associated with it. If already a bookmark is present, the **Edit Bookmark…** menu item is displayed.
Edit Bookmark…	Brings up a dialog to edit an existing bookmark.
Delete Bookmark...	Deletes the current bookmark after showing a confirmation message box.
Go To Event Grid	Closes the graphical display of OOB & SN, and takes you to main event grid in TraceView. The highlighted event's timestamp in the grid is the same as the timestamp corresponding to the cursor location when this menu item was invoked.

Print Preview Dialog

The print preview dialog shows the contents of the events pane as it will print. You can choose the printer and start the print of the events pane from this dialog.

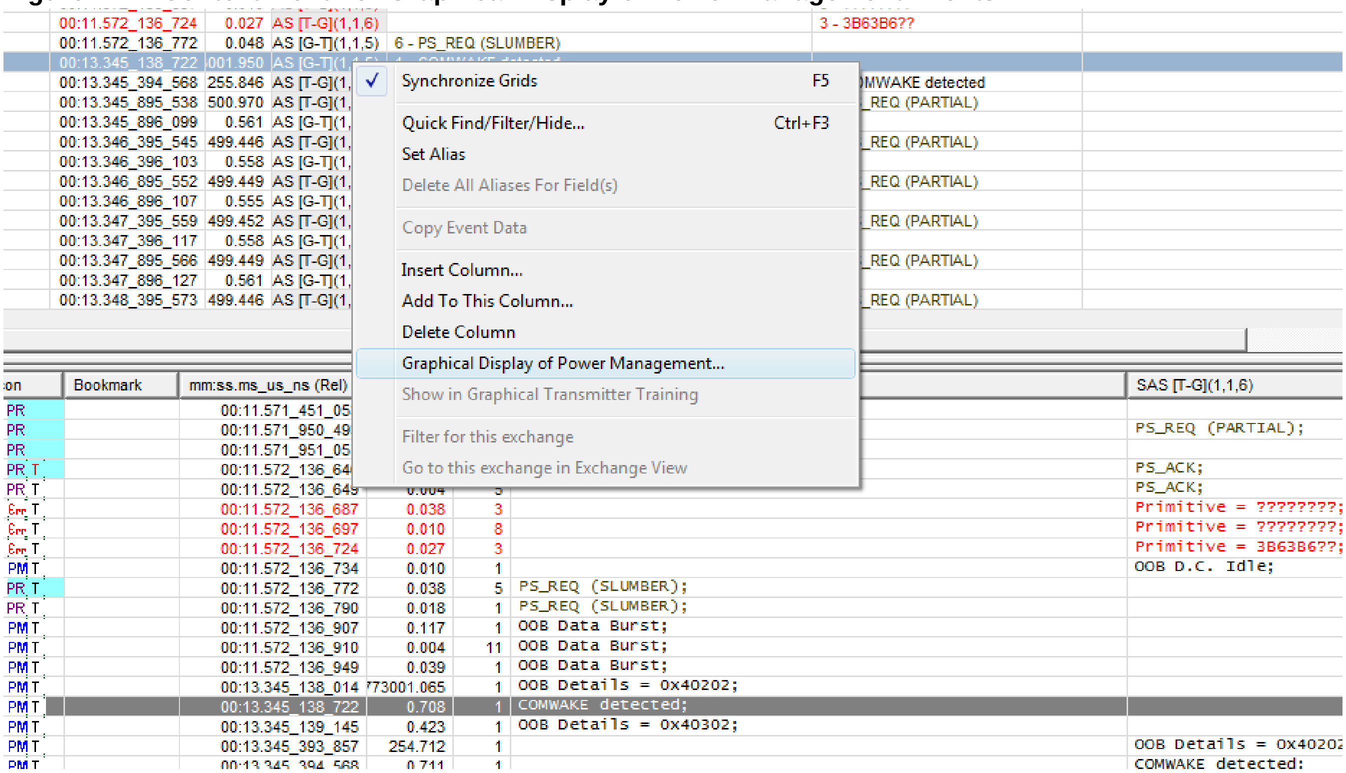
Figure 126: Print Preview Dialog Box



Graphical Display of Power Management Events

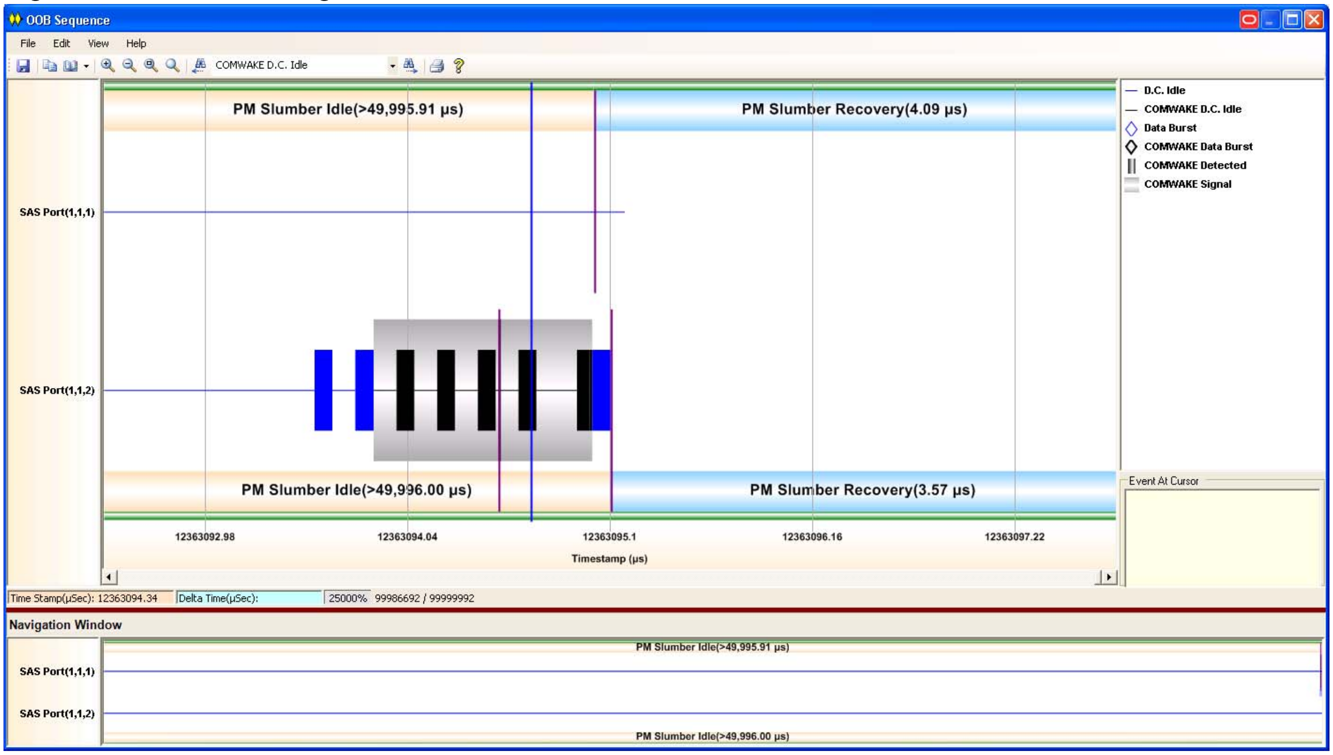
Power Management data can be viewed graphically in TraceView. You can graphically view, scroll, and view greater/lesser detail (zoom) for Power Management events represented by a PM in the icon column. Right-click a Power Management event in the main grid or DWord view, and select **Graphical Display of Power Management...** from the event grid context menu to bring up the graphical display.

Figure 127: Context Menu for Graphical Display of Power Management Events



The buttons, controls, and functions in the graphical display are the same as those shown in the Graphical Display of OOB and Speed Negotiation Events section above.

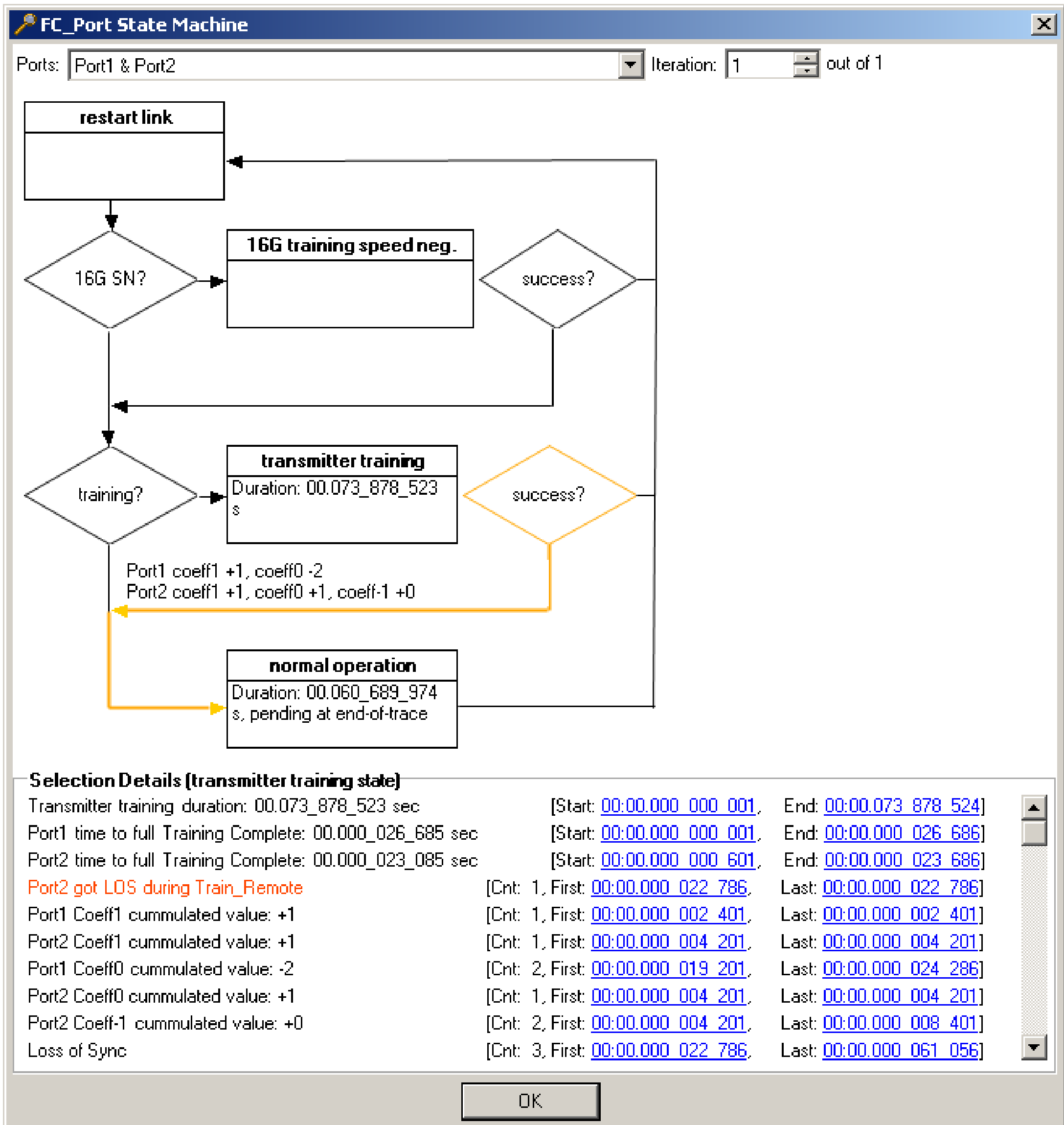
Figure 128: Power Management Events Window



Graphical Transmitter Training States

You can view transmitter training states for 16G FC traces by clicking the **Graphical Transmitter Training States** button in the TraceView toolbar or by selecting **View/Graphical Transmitter Training States**. TraceView parses the entire trace file on the ports selected in the TraceView toolbar then displays the FC_Port State Machine dialog containing all training frames found. While the file is being parsed, a dialog with a progress bar appears. You can choose to cancel the process by clicking the **Cancel** button.

Figure 129: Graphical Transmitter Training States Dialog



The **Port** drop-down menu contains every 16GFC port pair where at least one training frame was seen. Changing the port pair in the combo box refreshes the entire dialog content with the states for that port pair.

The **Iteration** field displays how many full training sequences were detected for that port pair, and it allows you to choose which training sequence you want to view.

The graphical state machine has four states, and it corresponds to the state machine displayed in the FC_Port state machine section of the FC-FS-3 specification. However, the speed negotiation state has been renamed to 16G training speed neg. because the Xgig analyzer does not detect the speed negotiation phase, but it captures the training frames in that phase, and that is what is shown in the state machine.

The graphical state machine highlights the path taken in the training sequence with a mixture of green, yellow and red lines. The green line shows a successful path. The red line shows an error path. The yellow line shows a successful path with some warnings.

To view the details of any state or any state transition, click inside the state box or the state transition text, and the **Selection Details** section is automatically populated with the details.

All the counters, symptoms, warnings, and errors are displayed in the **Selection Details** section. The errors causing the state transition are displayed in red. Warnings are displayed in orange, but they do not cause a state transition.

The details for the transmitter training state also contain the Training_Sequencer sub-states for both ports in the port pair ordered by timestamp.

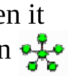
Following are the context menus available in the **Selection Details** section:

- **Copy All**: Copy the entire **Selection Details** section to the clipboard so it is possible to paste the content to a text editor.
- **Go to occurence...**: This context menu is available on lines where a count (Cnt) is shown for a counter. It opens a dialog where you can select a number in the range (1-Count). Then, the main TraceView grid highlights that occurrence of the event, and you can navigate in the main grid in parallel to this dialog.
- **Description**: Opens a tooltip with a full description of that event.

When you click a hyperlink in the **Selection Details** section, the main TraceView grid highlights the event corresponding to that timestamp. You can navigate in the main grid in parallel to this dialog. You can also right-click any event in the main grid and select the context menu **Show in Graphical Transmitter Training**, and the dialog will highlight the state containing that event.

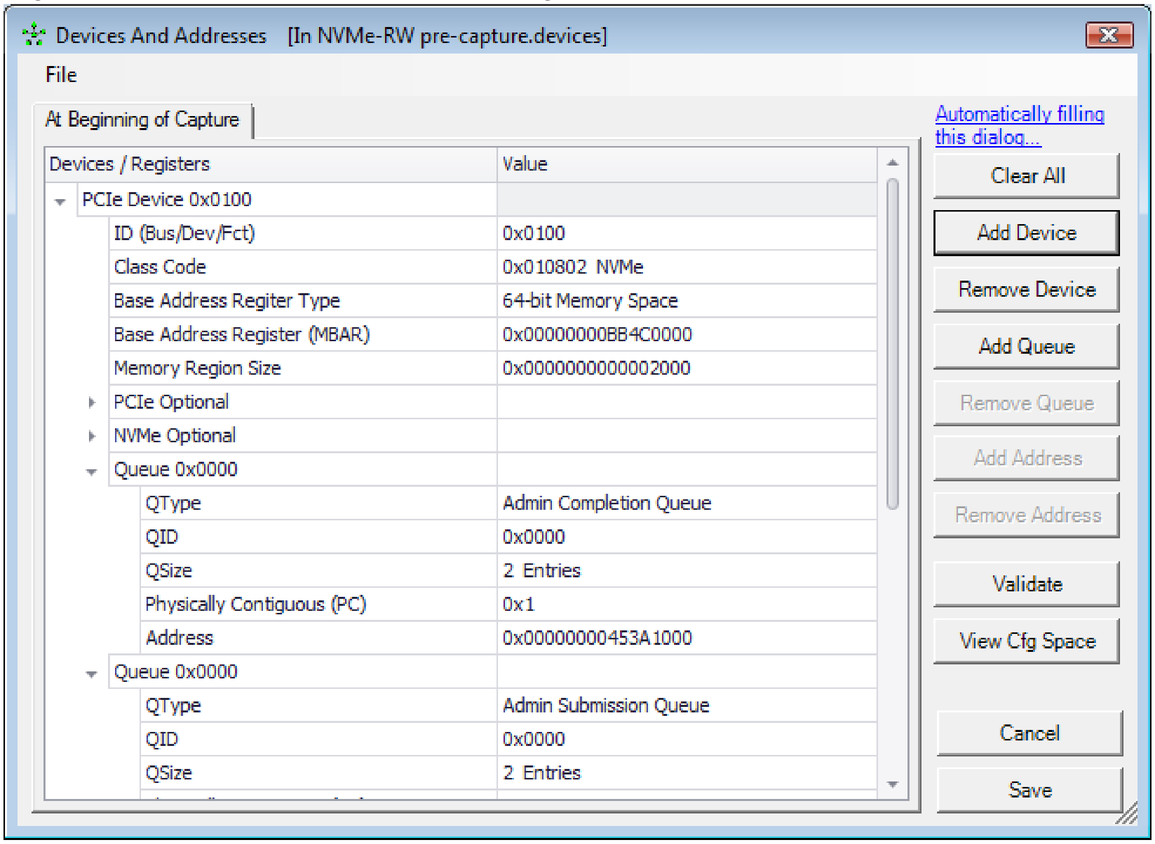
When you right-click any error transition text in the graphical state machine, and select **Show in main grid**, that menu will highlight the event that caused the error transition in the main grid.

PCIe Device and Address Mappings

The PCIe Analyzer remembers the devices and address mappings from a prior boot-up sequence in order to analyze and decode future traces. You can manually enter the all devices and addresses in the **Devices And Addresses** dialog. Expert automatically generates those mappings when it processes a boot-up sequence. To open the dialog, click the Devices And Addresses button  in TraceView's toolbar, or select **Devices and Addresses...** from the **Edit** menu. This button is enabled when you open a trace file or capture buffer.

The **Devices And Addresses** dialog has either one or two tabs. The first tab shows the mapping stored in the pre-capture.devices file. If present, the second tab shows the mapping in the post-capture.devices file.

Figure 130: Devices And Addresses Dialog



Expert generates the end-of-capture mapping in the post-capture.devices file. When present, that mapping is displayed in read-only so you can see the devices, addresses and configuration spaces at the end of a boot-up sequence. The mapping at the beginning of the capture is always editable and when you change it, TraceView prompts you to re-run Expert to regenerate the expert annotations.

When a capture stops, TraceControl copies the device mapping from the first domain port into the pre-capture.devices file for the domain so that every capture's pre-capture.device file is initialized from TraceControl's domain device mapping.

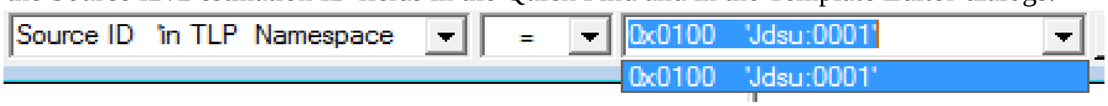
The devices and addresses mapping is mandatory for TraceView and Expert to decode any protocols over PCIe, such as NVMe. The information is exchanged during the boot sequence between the host and the devices. It may change from one reboot to the next.

You can fill the device mapping in two ways. First, you can click the “Automatically filling this dialog” hyperlink at the top of the dialog. When you do, a popup appears instructing you how to fill the dialog automatically. Second, you can enter the information manually. The buttons on the dialog's right-hand side allow you to add or remove devices, queues, and addresses.

If you are adding information manually, you should add every PCIe device found in the capture and provide the Device ID, Class Code, and the Base Address Register (BAR) information for the address ranges used in the capture. When the device is of Class Code 0x010802 (NVMe), then you should also create the NVMe queues that are used in the trace and verify that the Memory Page Size (MPS) and Sector Size are set correctly. The NVMe queues have an ID, type, and size. The regular Submission and Completion queues can be Physically Contiguous or not, while the Admin queues are always physically contiguous. When physically contiguous, a queue has only one starting address. When non-contiguous, then the queue uses a PRP List, and you need to enter the starting address of every memory page covering the queue (not the address of the PRP List itself, but all the addresses inside the PRP List).

There are several optional settings in the dialog that improve Expert's analysis, annotations and decodes for the capture.

- **PCIe Device/Vendor ID**: This combination uniquely identifies a PCIe device worldwide. When provided, TraceView displays “VendorName:DeviceID” in the Source/Destination fields to identify that device. Also, it provides the list of VendorName:DeviceID as choices for the Source ID/Destination ID fields in the Quick Find and in the Template Editor dialogs.

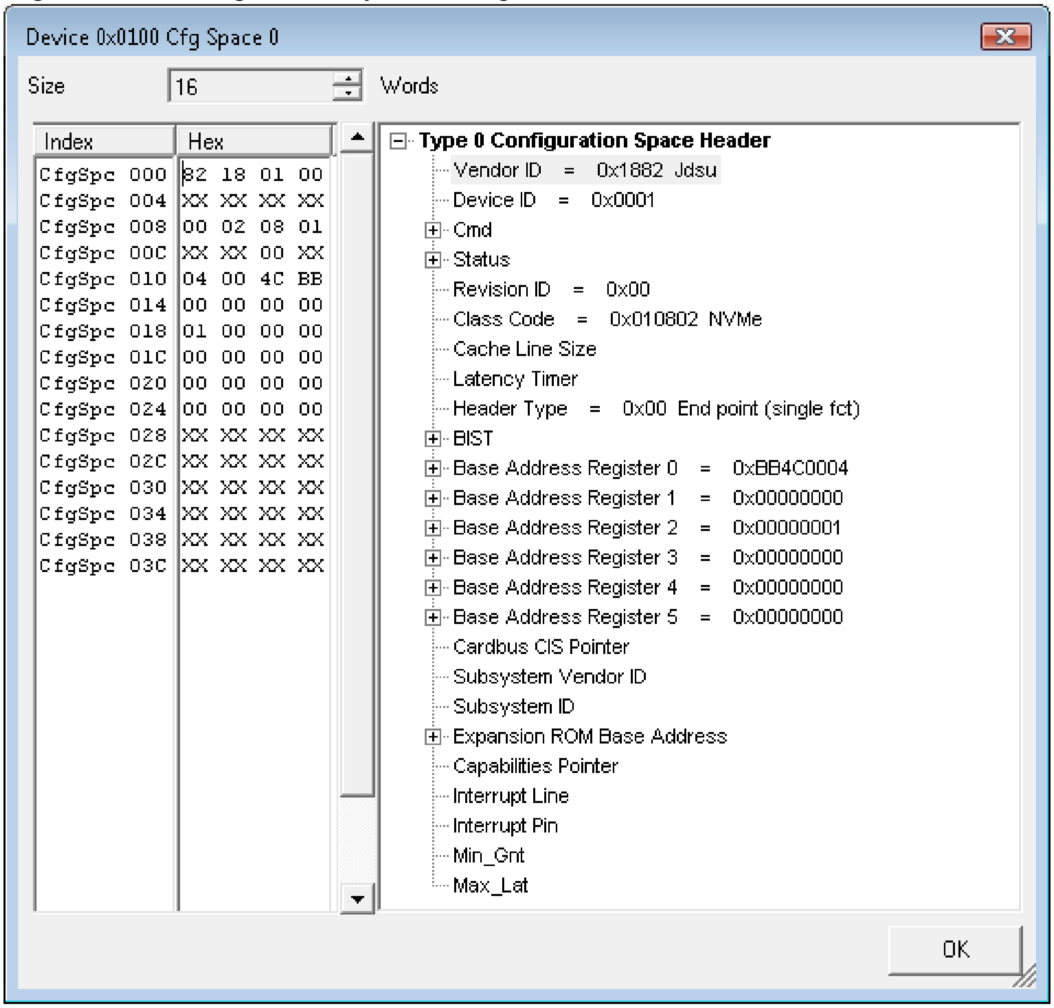


- **Revision ID, Header Type**: Informational only for this release
- **Expansion ROM Base/Size and Additional BARs**: Used by Expert to identify the target device of a packet routed by address
- **MSI Interrupts**: Addresses for each MSI interrupt sent by the device
- **MSI-X Interrupts**: Addresses for each MSI-X interrupt sent by the device
- **TC to VC Mapping**: Traffic Class to Virtual Channel mapping as found in the Virtual Channel Capability of the device
- **NVMe Version**: Informational only for this release

Once you have finished editing the device mapping, you can click the **Validate** button to check the consistency and reports issues. This process ensures that all the memory regions do not overlap, the device IDs are unique, and the queue IDs and types are appropriate. TraceView performs the validation when you click the **Save** button.

To view the Configuration Space for each device, click the **View Cfg Space** button.

Figure 131: Configuration Space Dialog

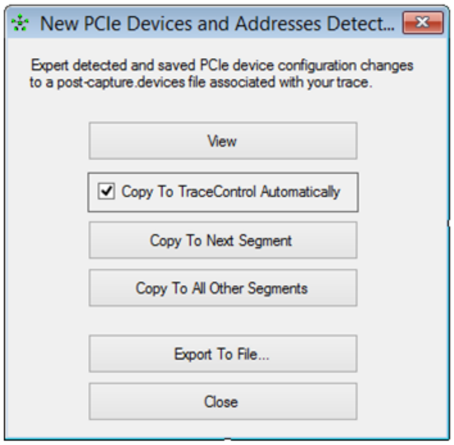


This can be useful when the device mapping was automatically populated by Expert. Expert stores the data for every successful CfgRd/CfgWr transaction for the entire configuration space accessed during a boot-up sequence (up to 4KB). When a DWORD contains XX XX XX XX, it means that it was not accessed during that capture.

When you click the **Save** button in the **Devices And Addresses** dialog, TraceControl prompts for re-processing the trace in Expert. When Expert finishes processing the trace, TraceView prompts you to reload the trace with the new annotations.

When Expert processes a PCIe boot-up sequence or an AHCI driver load, it extracts the PCIe/AHCI devices and addresses and automatically saves them to a post-capture.devices file associated with the capture, and it prompts to save them when it finishes.

Figure 132: New PCIe Devices and Addresses Detected Dialog



Click the **View** button to open the **Devices and Addresses** dialog with a single tab for the post-capture.devices file only. You can modify the content and click **Save** to your changes. After you save the changes, the Devices And Addresses dialog will have two tabs. The first tab will contain the pre-capture.devices file, and the second tab will be for the post-capture.devices file in read-only mode.

Ensure the **Copy To TraceControl** checkbox is checked to automatically save the new devices and addresses to TraceControl. When the save has completed, a popup notifies you that this information was saved successfully and that it will be used for all future captures. If Expert reads the PCIe boot-up sequence from a trace file instead of a capture buffer, then the **Copy to TraceControl** button is grayed out.

The **Copy To Next Segment** button is displayed when more than one segment has a capture in it. When Expert pops-up the New Devices and Addresses Detected dialog, click this button to carry over the boot-up info and changes from one segment to the next. Also when Expert does not pop-up this dialog, you can carry over the information to the next segment by opening the Devices and Addresses dialog and select "Copy To Next Segment".

The **Copy To All Other Segments** button is displayed when more than one segment has a capture in it.

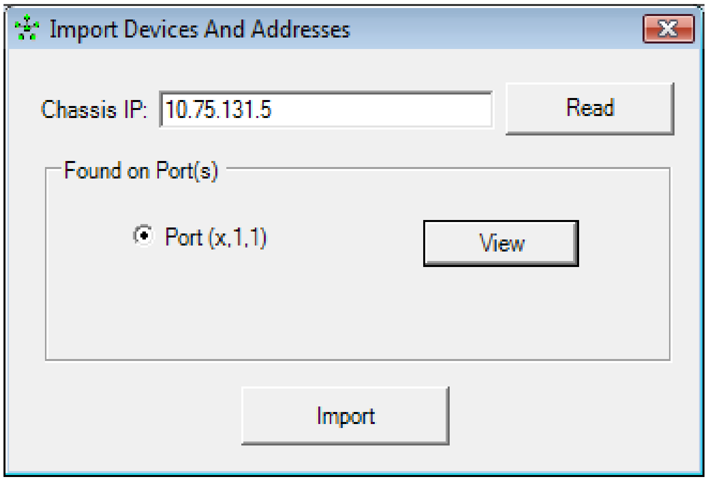
Click the **Export To File...** button to save the mappings to a *.devices* file on the local hard drive for future use. Once you export the devices and addresses to a file, you can import that file into the **Devices and Addresses** dialog in the future.

Exporting/Importing Device Mappings

To export or import device mappings, use the selections in the File menu in the **Devices And Addresses** dialog.

The options in the File menu are based on the tab you are currently viewing. When you are viewing the read-only post-capture file, only “Export To File...” is visible. When you click “Import From File...”, the **File Open** dialog appears. When you click “Export To File”, the **File Save** dialog appears. When you click “Import From Chassis Ports” the following dialog appears.

Figure 133: Import From Chassis Ports Dialog



Type the IP address of a chassis in the “Chassis IP” field, and click the **Read** button to read all the mappings for all the port pairs on that chassis.

Click the **View** button to open the **Devices And Addresses** dialog in read-only mode, to view the port's mappings.

When you click the **Import** button, the **Import** dialog closes, and the original dialog is filled with the new devices and addresses, copied from the port selected.

Overlapping Data

Overlapping data is data within the trace from different sources within the same link that have overlapping timestamps. Each link (either a wide link or a port-pair) has its own set of start and stop timestamps with the trace. The **Show Overlapping Data** button is always active. When it is selected TraceView shows only the overlapped data. When it is unselected, TraceView shows the whole trace. When showing all trace data by toggling the **Show Overlapping Data** button, you may display data that does not contain the corresponding response data from the other side of the link. For most types of analysis, this data from only one side of the link will not be very useful.

When the **Show Overlapping Data** button is selected, TSV data, along with grid & exchange data, is updated to correspond to current time extents. Overlapped time is calculated per link. If a partial link is available (because a subset of ports are opened from chassis, or a single `.trc` file is opened) only available ports are used to determine overlapped time extents.

By showing overlapping data, you are reducing the amount of data displayed for the trace. Showing overlapping data only can narrow your view to critical sections when viewing large traces. If you select to show overlapping data only, the yellow extent bars in the histogram will move if this operation eliminates some of the data in the trace from the display. If you select to show overlapping data, the yellow tickers are shown at lowest of the start times for all links and highest of the end times for all the links. If you select to show the entire trace, the yellow tickers are shown at the beginning and end of the trace. Ticker marker positions are not altered based on port selection. You can select custom time extents by sliding yellow ticker markers. When **Show Overlapping Data** button is toggled, previous custom time extents will be lost.

For example, assume port 1 captures data from second 1 through second 4 and port 2 captures data from second 2 through second 4. When showing only overlapping data, the overlapping data will be the data from second 2 through second 4. When showing all trace data, the data from second 1 through second 4 is displayed, but the first part of the data contains data only from port 1.

Working With Columns

The basic display in TraceView is a spreadsheet with each trace event shown as a row and the interpretation of the data for each event displayed in columns. You can add, delete, or move columns. Some columns are pre-defined summary fields that contain extensive decode information. You can set up the columns in any way you wish, including adding the exact information you want to any column. TraceView includes a large library of pre-defined columns that you can add to the spreadsheet display.

In the main spreadsheet view, traffic is summed up into one row events. Frames are shown in one row with a summary. In SAS/SATA, only OOB events (as determined by the state machines in the hardware) are shown. Also, SAS/SATA Primitive Sequences are shown as single row events, unless they are interrupted by errors. Error are always shown in the main spreadsheet view. If you wish to see the word-by-word details of this events, use the Details Pane.

You can enlarge or reduce the size of the font in the spreadsheet view by using the  and  zoom buttons.

An example of the spreadsheet display of events is shown below.

Figure 134: Example Spreadsheet Display

Bookmark	:mm.ss.ms_us	DT/Port	Port	Primitive	Protocol	Summary	Bytes
	000:00:02.1...	1.237	Port 2	Ordered Set			4
	000:00:02.1...	0.075	Port 3	Frame	SCSIc	SCSI Cmd = '...	68
	000:00:02.1...	0.038	Port 2	Ordered Set			4
	000:00:02.1...	0.640	Port 3	Ordered Set			4
	000:00:02.1...	0.105	Port 3	Ordered Set			4
	000:00:02.1...	0.038	Port 3	Ordered Set			4
	000:00:02.1...	0.786	Port 2	Ordered Set			4
	000:00:02.1...	0.075	Port 3	Ordered Set			4
	000:00:02.1...	0.038	Port 3	Ordered Set			4
	000:00:02.1...	0.862	Port 2	Ordered Set			4
	000:00:02.1...	0.038	Port 2	Ordered Set			4
	000:00:02.1...	0.412	Port 2	Ordered Set			4
	000:00:02.1...	0.038	Port 2	Ordered Set			4
	000:00:02.1...	167.774	Port 3	Ordered Set			4
	000:00:02.1...	167.437	Port 2	Ordered Set			4
	000:00:02.1...	1.162	Port 3	Ordered Set			4
	000:00:02.1...	0.038	Port 3	Ordered Set			4
	000:00:02.1...	0.112	Port 3	Ordered Set			4
	000:00:02.1...	0.038	Port 3	Ordered Set			4
	000:00:02.1...	0.075	Port 3	Ordered Set			4
	000:00:02.1...	0.038	Port 3	Ordered Set			4
	000:00:02.1...	0.075	Port 3	Ordered Set			4

Icon Column

The first column of the spreadsheet is the **Icon** column. The icons in this column provide a quick reference to the type of event that this row contains and information about its relationship to other events in the trace.

The **Icon** column displays up to three different icons that provide a quick synopsis of the event. The **Icon** column for most events will contain less than the maximum of three different icons. Indicators within the **Icon** column are separated by a colon (for example, FR:EE:T).

The table below provides a list of the icons and their meaning.

Table 24: Icon Meanings in the Icon Column

Icon	Description
Beg	Indicates the beginning of the trace data. No event information is associated with this icon.
End	Indicates the end of the trace data. No event information is associated with this icon.
OS	Indicates that this is an Ordered Set. This icon will display only in protocols that use Ordered Sets such as Fibre Channel and PCIe.
FR	Indicates that the event is a frame containing data. The FR icon for a start of sequence event has a light cyan background color; otherwise, the background color is white.
PA	Indicates that the event is a preamble frame for Gigabit Ethernet data.
OOB	Indicates that the event is an out-of-band event within the SAS or SATA protocol. This icon will display only for traces using the SAS or SATA protocols.
PR	Indicates that this is a primitive within the SAS protocol. This icon will display only for traces using the SAS protocol. If the PR icon has a cyan background, it indicates the start of a primitive sequence.
PM	Indicates that the event is a power management event within the SAS protocol. This icon will only display for traces created using the 12G SAS blade at 12, 6, or 3 Gbps.
T	Indicates that the event occurred after the Trigger event in the trace. A red T indicates trigger events, a black T indicates post-trigger events. It is possible for multiple ports to trigger simultaneously, so more than one event may have a red T. The red T icon is only applicable to SAS/SATA traces.
XP	Indicates that the event is has been post-processed using the Xgig Expert application.
SD	Indicates that the Xgig ports are syncing to data. Events are shown as SD when the Xgig ports cannot lock onto the exact data. This can happen for a brief period after the conclusion of a speed negotiation or if the Xgig ports lose sync with the data. This icon will display only for traces using the SAS or SATA.
W	Indicates that the event is a warning. Warnings are not actual errors, but are conditions that could indicate problems. For example, a response of No to speed negotiation asking if 6G is supported would generate a warning. For a 3G device this would be an expected response, but could indicate a problem for a 6G device.
SN	Indicates that the event is a speed-negotiation event. SN events are only applicable to SAS/SATA traces. The SN icon for a start of sequence event has a light cyan background color; otherwise, the background color is white.
Err	Indicates that the event is associated with an error condition detected in the trace.
EE	Indicates that this is an embedded event. An embedded event is embedded in other event, or an event with embedded primitives. Since successful extended events always occur inside of frames, the FR icon will always appear with the blue EE icon. A red EE indicates an embedded event with errors.

Table 24: Icon Meanings in the Icon Column (continued)

<number>	A numeric value in the Icon column indicates the speed of the link associated with the event. For example, 3 indicates 3Gbps.
Bm	Indicates that a bookmark has been set for this event. The name of the bookmark will appear in the **Bookmark** column. If the background color is blue, the bookmark was created in the main spreadsheet. If the background color of the bookmark is magenta, the bookmark was created in the **Dword** view.
Red Diamond	Indicates that the event has been marked as bookmark named **Global Cursor 1** or **Global Cursor 2**. See “Bookmarks” on page 247 for more information on using the preset bookmark names.
Tf	Indicates a training frame
Tp	Indicates a training pattern for 16G Fibre Channel
Dp	Indicates the DLLP protocol layer in PCIe.
Tp	Indicates the TLP protocol layer in PCIe.
Idl	Indicates a logical idle for PCIe.
Ei	Indicates an electrical idle for PCIe.
Ed	Indicates an EDS token for PCIe.

Spreadsheet Options

The spreadsheet options dialog allows you to customize the spreadsheet display of trace data. You can set up ports with different colors, select a protocol-based color scheme, or choose not to use any color coding. You can also change the font and grid lines of the spreadsheet.

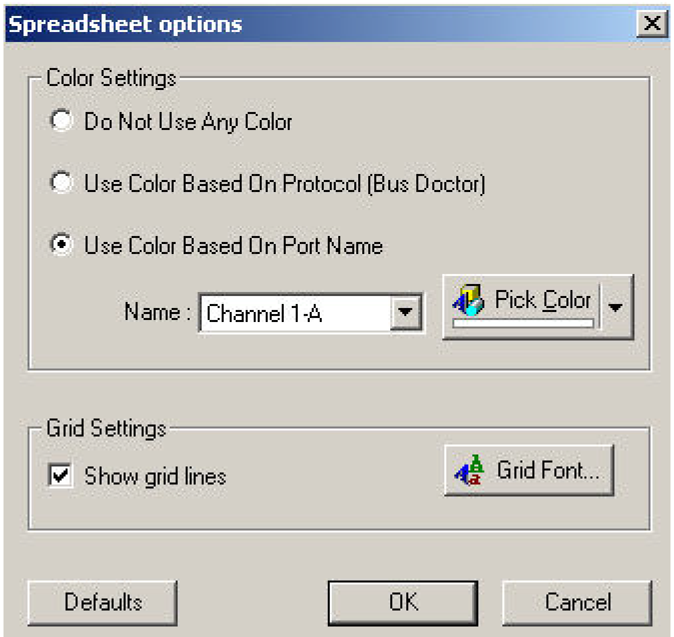
Click the **Spreadsheet Options**  button to customize the appearance of the spreadsheet. This action opens the **Spreadsheet Options** dialog box. You can also use the **View > Spreadsheet Options...** menu item.

Set the **Do Not Use Any Color** to completely remove any color coding from the display.

Select **Use Color Based on Protocol (Bus Doctor)** to use a protocol-based color scheme for display. The protocol-based color scheme is the same color scheme used by Viavi’s Bus Doctor Plus bus analyzer product. See “Protocol Display Color Coding” on page 437 for information on the meaning of this color scheme.

Colors in the Dword View will be applied to the summary cell of the Dword matching the field code or event type.

Figure 135: Spreadsheet Options Dialog Box



To select a background color for a port:

1 Select the **Use Color Based On Port Name** radio button.

2 Select the port you want to set from the **Name:** box.

3 Press the **Pick Color** button. The **Color** dialog box appears.

4 Select the background color you want to display for all events related to a single port. Select the desired color from the standard palette or select **Custom Colors** to create your own colors. Press **Default** to return the background color for this port to the default color.

5 Press **OK**.

To return to the standard background color for all ports:

1 Select **Defaults** from the **Spreadsheet Options** dialog box.

2 Press **OK**

To change the spreadsheet font and select a foreground color for the spreadsheet font:

1 Press the **Grid Font…** button. The **Font** dialog box displays.

2 Select the font, font style, size, and script for the spreadsheet font.

3 Select the desired color from the **Color:** pull-down box.

4 Select the font effects such as Strikeout or Underline, if desired.

5 Press **OK**.

To show/hide grid lines:

>> Select the **Show grid lines** box to display grid lines. Remove the check from the **Show grid lines** box to hide grid lines.

Context Menu Options for Columns

The primary display for trace data is a column and row spreadsheet. Rows contain events discovered in the trace. Columns provide the interpretation of the data.

A variety of controls are provided in menus when you click the right mouse button over a column value or column heading. The right mouse button is context sensitive in Xgig TraceView. You will see a list of options that make sense for the column value or column header you have selected.

The following table describes the menu items that may appear when you right mouse click a column header.

Table 25: Right Mouse Options for Column Headers

Column Header Right Mouse Options	Description
Display Interpretation	Displays the interpretation of the data for each field in the column. For example, the interpretation for a TCP **SPort** field value 3260 is **iSCSI**. If no interpretation is found, the raw data is displayed in the default field format (for example, ASCII, IP dotted notation, decimal etc.). This option is the default for all columns.
Display Value&Interpretation	Same as Display Interpretation, except that the raw data is always displayed when a field has an interpretation. For example, a column would display *3260 iSCSI* for a TCP SPort field value of 3260.
Display Shorter Interpretation	Same as Display Interpretation, except that a shorter interpretation is displayed if one is available. Among others, when a field value is displayed in hexadecimal as the default format, then this option strips the leading zeros for the field. For example, the Fibre Channel Header field S_Id is a 24 bit hexadecimal field; when a hexadecimal S_Id field value of *000012* is displayed for the Display Interpretation option, the shorter value *12* is displayed with this option.
Display Hexadecimal	Displays the raw value of the data for each field in hexadecimal format. For example, if you select **Display Hexadecimal** for the **Summary** column, it will display the raw bytes of each event (a maximum of 32 bytes is displayed). For Fibre Channel frames, the **Summary** column displays the raw bytes of the payload, skipping the Fibre Channel header.
Display Uninterpreted	Displays the port designation only, chassis number, blade number, port number within the blade, for example, 1,1,5.
Display Decimal	Displays the raw value of the data for each field in decimal format. For example, if you select **Display Decimal** for the **CRC** column, it will display the 32- bit CRC values in decimal format.
Display Default Format	Displays the raw value of the data in the default format for each field. For example, if you select **Display Default Format** for a TCP **SPort** field interpreted as iSCSI, it will show the raw value 3260 in the default decimal format for the **SPort** field.
Show Frame Word Offset	When this context menu option is selected, a three-digit decimal word offset is shown at the beginning of each Dword view or LaneView line belonging to a frame.

Table 25: Right Mouse Options for Column Headers (continued)

Show ports…	Brings up the **Show/Hide Ports** dialog box to show or hide information in the selected column for specific ports. In the dialog box, use the arrows to set which ports to show and which ports to hide in the column. For example, hiding port 1-A for the Count-OS-RCtl column means that no data will display in that column for events associated with port 1-A.
Insert Column…	Brings up the **Insert Column** dialog box for inserting a new column to the right of the current column.
Add To This Column…	Brings up the **Add To Column** dialog box for adding new information to this column.
Delete Column	Immediately deletes the column from the display.
Bookmark Editor…	Brings up the **Bookmark Editor** dialog box for creating bookmarks. This is only available from the **Bookmarks** column header.
Timestamp Formats...	For the timestamp, the time can be displayed in a variety of formats. See “Timestamp Options” on page 406 for information on available formats.
ss.ms_us_ns mm:ss.ms_us_ns (other timestamp formats)	For other columns that contain timestamps, select the specific timestamp format from the menu.
Display UTC Time	Available for columns that contain a timestamp that shows a calendar time. When selected, the time is displayed as UTC Time.
Display Local Time	Available for columns that contain a timestamp that shows a calendar time. When selected, the time is displayed in Local Time. For example, in Pacific Standard Time, eight hours are subtracted from UTC to display Local Time.
Display Calendar Time	Available for columns that contain a timestamp. Sets the timestamp in the column as a calendar time based on the system clock at the time of capture.
Display Time Relative to Event	Available for columns that contain a timestamp. Sets the timestamp in the column as a time relative to the currently selected event (current event equals time zero).
Display Time Relative to Capture	Available for columns that contain a timestamp. Sets the timestamp in the column as a time relative to the start time of the capture.
Display Hex Data	For Dword view data columns only, display the data for Dwords in Hexadecimal format.
Display 10 Bit Data	For Dword view data columns only, display the Dword data in Binary (10 bit) format.
Display K/D Char	For Dword view data columns only, display the Dword data in K/D Character format.
Display Scrambled Data	For Dword view data columns only, display the Dword data as Scrambled data.
Display ASCII Data	For Dword view data columns only, display the Dword data in ASCII format.
Synchronize Grids (F5)	Synchronizes the timestamps between the main spreadsheet view, Dword view, and Exchanges View as closely as possible.
Manage Aliases	Brings up the **Manage Aliases** dialog.

The following table describes the menu items that may appear when you right mouse click a column value.

Table 26: Right Mouse Options for Column Values

Column Value Right Mouse Options	Description
Quick Find/Filter/Hide	Brings up the **Quick Find/Filter/Hide** dialog box. The dialog box is automatically filled with the type of data and its value to allow for a Quick Find or Quick Hide operation.
Set Alias	Places the cursor in the current field to enter an alias for the current value. Press a cursor key or the **Tab** key to exit the field without setting an alias. Alias values apply only to the column they are created in. Use the **Alias Editor** to maintain a complete list of aliases for a column.
Delete All Aliases for field(s)	Deletes all aliases set for that field(s).
Copy Event Data	Copies all the data associated with this event to a buffer. This option is disabled for OOB events.
Delta Calculator...	Brings up the **Delta Calculator** dialog box to calculate the time difference between two timestamps. The selected timestamp is entered as the first timestamp used to calculate a difference.
Display Calendar Time	Available for columns that contain a timestamp. Sets the timestamp in the column as the calendar time based on the system clock at the time of capture.
Display Time Relative to Event	Available for columns that contain a timestamp. Sets the timestamp in the column as a time relative to the currently selected event (current event equals time zero).
Display Time Relative to Capture	Available for columns that contain a timestamp. Sets the timestamp in the column as a time relative to the start time of the capture.
Insert Column…	Brings up the **Insert Column** dialog box for adding a new column to the right of the current column.
Add To This Column…	Brings up the **Add To This Column** dialog box for adding new information to this column.
Delete Column	Immediately deletes the column from the display.
Set Bookmark	Places the cursor in the bookmark field for entering the name of a bookmark.
Set Global Cursor 1	Creates an instant bookmark named Global Cursor 1. A red diamond appears in the **Icons** column to indicate that this event has been marked. This option is only available for the **Bookmark** and **Timestamp** column values.
Set Global Cursor 2	Creates an instant bookmark named Global Cursor 2. A red diamond appears in the **Icons** column to indicate that this event has been marked. This option is only available for the **Bookmark** and **Timestamp** column values.
Synchronize Grids (F5)	Synchronizes the timestamps between the main spreadsheet view, Dword view or LaneView, and Exchanges View as closely as possible.
Filter for this exchange	Creates a Quick Filter and applies it to the event grid on the left so that all the frames for the current exchange are shown in that grid. To disable the filter on the event grid, click inside the grid so that it gets focus and depress the toolbar button "Apply Quick Filter". To delete that filter, select the menu Tools / Quick Filter List / Clear.

Table 26: Right Mouse Options for Column Values (continued)

Go to This Exchange in Exchanges View	This context menu is enabled for SAS/SATA, FC, PCIe, and NVMe frames in the event grid that are part of an exchange. When clicking this menu, the corresponding exchange is selected in the Exchanges View. If the capture contains multiple links and an exchange can be found over multiple links, this menu will highlight the exchange on the first link, not necessarily the link correspond to this specific frame.
Go to This PDU in Exchanges View	This context menu is enabled for iSCSI PDUs events. When clicking this menu, the corresponding PDU is selected in the Exchanges View.
Show Frames For This Exchange	This context menu displays all frames for the exchange.
Graphical Display of OOB & SN	This context menu brings up the graphical OOB display for 6G SAS/SATA events.
Show in Graphical Transmitter Training	This context menu brings up the Graphical Transmitter Training display for 16G FC events.
Synchronize Grids	This context menu synchronizes the event grid and Dword view or LaneView with Exchanges View.
Show Frame Word Offset	When this context menu option is selected, a three-digit decimal word offset is shown at the beginning of each Dword view or LaneView line belonging to a frame.

Summary Fields and Field Groups

Xgig TraceView has a set of pre-defined summary fields called Field Groups that are very useful in viewing the decode information. The Field Groups contain a set of decode information that would commonly be useful to look at when analyzing packets or frames. Different sets have been created so you can easily select a pre-defined set of summary decode information.

Field Groups are added just like any other column to the display. Right-click a column header then select **Insert Column** or **Add To This Column...** option. From the associated window, expand the **Field Groups** item to see all pre-defined Field Groups.

You can create your own set of decode information by adding information to one of the Field Groups or one of the other columns in the display.

Summary Field Group

The **Summary** column is a special Field Group that changes based on the protocol you are viewing. It shows the pertinent decode information for the highest-level protocol seen within the packet or frame. The **Summary** column is a 'default' set of decode information that appears as one of the columns for any protocol. The **Summary** column can be added to, moved, expanded, or deleted just like any other column.

Example displays of the **Summary** field in the decode for various protocols are shown below:

iSCSI Trace

Protoc	Summary
iSCSI	Data-out; InitTaskTag = 0xA3646430; DataSegLen = 16384;
TCP	SeqNum = 4166158196; AckNum = 568439677; Wnd = 32696; Len = 1448;
TCP	SeqNum = 4166159644; AckNum = 568439677; Wnd = 32696; Len = 1448;
TCP	SeqNum = 4166161092; AckNum = 568439677; Wnd = 32696; Len = 1448;
TCP	SeqNum = 4166162540; AckNum = 568439677; Wnd = 32696; Len = 1448;
TCP	SeqNum = 568439677; AckNum = 4166158196; Wnd = 32132; Len = 1448;
TCP	SeqNum = 4166163988; AckNum = 568439677; Wnd = 32696; Len = 1448;

FC Trace

Count - Type	Count - Type	Summary
	1 - FC4Status	Good;
1 - FC4Cmd		Read(10); LBA = 0x00002A00; FCP_DL = 0x00010000;
	1 - FC4SData	SCSI Data; Offset = 0x0000D800; Len = 0x800
	1 - FC4SData	SCSI Data; Offset = 0x0000E000; Len = 0x800
	1 - FC4SData	SCSI Data; Offset = 0x0000E800; Len = 0x800
	1 - FC4SData	SCSI Data; Offset = 0x0000F000; Len = 0x800
	1 - FC4SData	SCSI Data; Offset = 0x0000F800; Len = 0x800
	1 - FC4Status	Good;
	1 - FC4SData	SCSI Data; Offset = 0x00000000; Len = 0x800
	1 - FC4SData	SCSI Data; Offset = 0x00000800; Len = 0x800

SCSI Inquiry Data

Count - Type	Count - Type	Summary
1 - FC4Cmd		Inquiry; FCP_DL = 0x00000024;
1 - FC4Cmd		Inquiry; FCP_DL = 0x00000024;
	1 - FC4SData	SCSI Inquiry Data
	1 - FC4SData	SCSI Inquiry Data

SATA Identify Device Data

SATA	32	Reg: Host -> Dev; Identify Device; FIS Features [7:0] = 0x00; LBA = 0x0; Sect Cnt = 0;
SATA	32	PIO setup; LBA = 0x0; DRDY; DRQ; Sect Cnt = 256; Transf Cnt = 0x0200; E_DRDY;
SATA	528	ATA Identify Device

Other Field Group Column Displays

TraceView has several other Field Groups that appear by default in the decode spreadsheet. All default configurations except **Default Ports Side-by-Side** and **Default iSCSI Configuration** display the following Field Group columns in TraceView:

- **Side A/ Side B**
- **Destination**
- **Source**
- **LUN** and/or **InitTag**
- **Tag**
- **Errors**

Side A/Side B Columns

Port	Side A	Side B
SAS Port(1,2,7)	49 - SATA_X_RDY	
SAS Port(1,2,7)	254 - SATA_X_RDY	
SAS Port(1,2,7)	109 - SATA_X_RDY	
SAS Port(1,2,8)		202 - SATA_R_RDY
SAS Port(1,2,7)	Reg: Host -> Dev	
SAS Port(1,2,7)	137 - SATA_WTRM	
SAS Port(1,2,7)	254 - SATA_WTRM	

The **Side A/Side B** Field Group columns display the basic type for the current set, ordered set raw unframed data, K character, etc. Example Side A/ Side B columns for SAS are shown above. For frames, it displays the following fields:

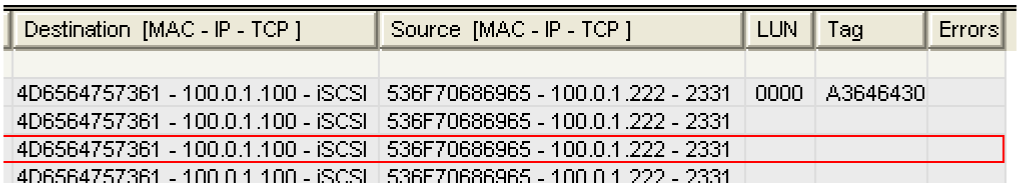
- RCtl for Fibre Channel frames
- IU Type for SAS frames
- FIS for SATA frames
- BHSOp for iSCSI frames

Event Types for PCIe (Side A=targets / SideB=hosts)

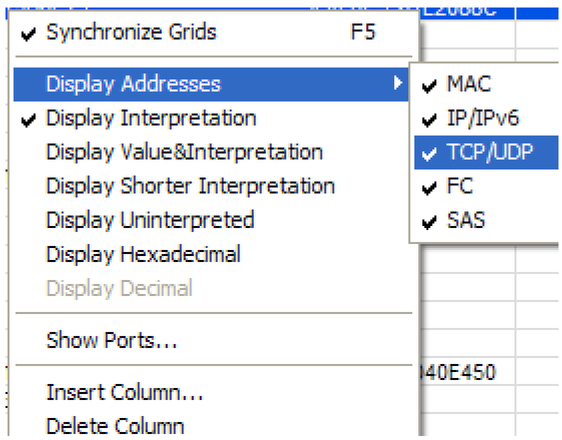
- PCIe Non-OS
    - **EDS**: Gen3 End of Data Stream as described in the PCIe spec
    - **EI**: Electrical Idle as defined in the PCIe spec
    - **Loss of Sync**: Happens at Gen 1/2 when there are too many code violations. At Gen3, it happens when there are too many consecutive 130b blocks with Sync bits 00 or 11 (invalid). In both cases, the XGIG HW stops capturing the garbage and captures and counts the number of DWORDs during the Loss-of-sync, until proper synchronization happens again. From there, the HW resumes capturing the proper events instead of a loss-of-sync.
- PCIe DLLP Packet
- PCIe TLP Packet
- PCIe Ordered Set
    - EIEOS
    - EIOS
    - FTS
    - SDS
    - SKP
    - TS1
    - TS2
    - Unbonded: Used at Gen1/2 when the lanes are misaligned. Also, it is used at Gen1/2/3 when an ordered set is not one of the defined ordered sets.

Source and Destination Columns

The **Destination; Group** Field Group column contains all the destination fields for all protocols and it only displays the ones that are available in the current frame. Following is an example of the **Destination** column for iSCSI:



The address fields display the MAC address followed by the IP address followed by the TCP port number. It is possible to view and control which addresses are displayed in the **Destination** or **Source** columns. Select the addresses to display by clicking the right mouse in column header and selecting **Display Addresses**.



For the PCIe protocol, the **Source/Destination** columns contain the TLP Source ID and Destination ID fields. These fields are interpreted with the Vendor ID/Device ID information provided in the **Devices And Addresses** dialog (under the PCIe Optional node). Otherwise, they are displayed as the raw 16-bit hexadecimal value.

The **Source** column works in the same way as the **Destination** column. If change the addresses displayed for the **Destination** column, the **Source** column automatically syncs up, and vice-versa. Note that the settings on which address is displayed is persistent across configuration files.

The **Source** and **Destination** columns are right-aligned. When you double-click them, they bring up the **Quick Find/Filter/Hide** dialog on the first field visible on the right side of the column.

LUN Column

The **LUN** column displays one of the following fields (by order of importance):

- XPT LUN (SAS and FC): Generated by Expert, LUN in the first frame of the conversation propagated to all the frames of the conversation.
- LUN: Logical Unit Number found in the first frame of the conversation only.
- Targ Lun: Generated by Expert, target's real LUN derived from the iSCSI Exchange.

InitTag Column

The **InitTag** column displays one of the following fields:

- XPT Init Tag (SAS/SATA): Generated by Expert, SAS Init Tag containing target information from the first frame propagated to all the frames of the conversation.
- Init Tag: SAS Init Tag in the Open Address Frame (the first frame of the conversation).

Tag Column

The **Tag** column displays one of the following fields (by order of importance):

- OX_Id (FC)
- InitTaskTag (iSCSI)
- Task Tag (SSP)
- XPT QueueTag (SATA): Generated by Expert, Queue Tag of the first frame of a particular command added to all events that are associated with that command.
- Queue Tag (SATA): Queue Tag of the first frame of a particular command.
- 8-bit TLP Tag (PCIe)
- 32-bit NVMe exchange ID for packets with an NVMe payload. That exchange ID is composed of the 16-bit SQID (Submission Queue ID) followed by the 16-bit CID (Command ID). You can filter on that tag to isolate all the packets of one NVMe exchange.

Errors/Warnings Column

The **Errors/Warnings** column displays a summary of all the errors detected in the current frame or primitive. The details of all the errors can be viewed in the inspector dialog. TraceView detects frame embedded CRC and checksum errors. The **Errors/Warnings column** reports all the errors detected by TraceView, as well as the hardware detected errors.

Stateful Errors

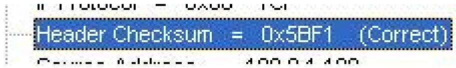
TraceView can store between 0 and 3 stateful errors per event. If Expert is unable to report all stateful errors, the text “More information in Expert” will appear in the Errors/Warnings column of TraceView’s main window.

Multiplexing Alignment Errors

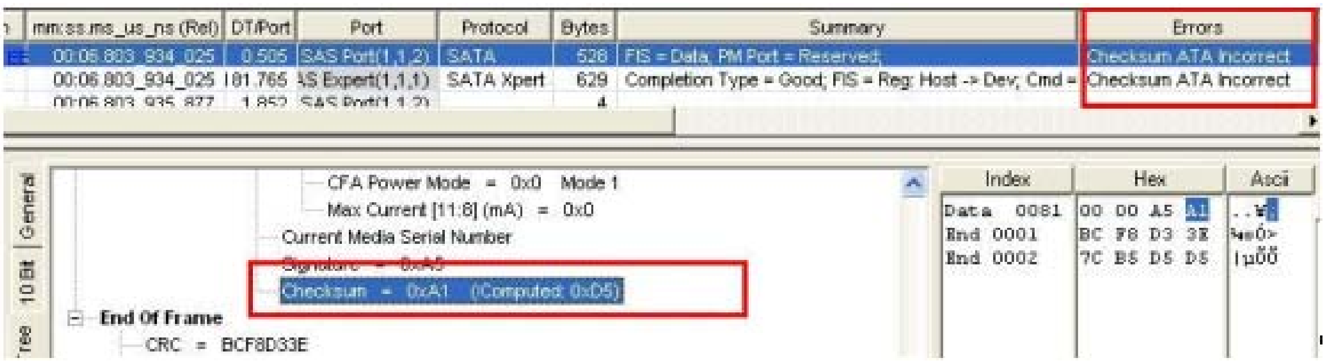
For multiplexing alignment errors, the MUX-1 and MUX-0 primitives will be marked with an alignment error if the hardware had to re-sync the multiplexing and redirect a MUX primitive to the correct logical link. The hardware will always direct MUX primitives to the correct lane, thus re-syncing the multiplexing. You should never see a MUX-1primitive on logical link 0, and never see a MUX-0 primitive on logical link 1.

CRC and Checksum Errors

TraceView computes and validates the embedded CRCs and Checksums for each frame. TraceView reports correct checksums and CRCs in the inspector window by indicating **(Correct)** next to the value.



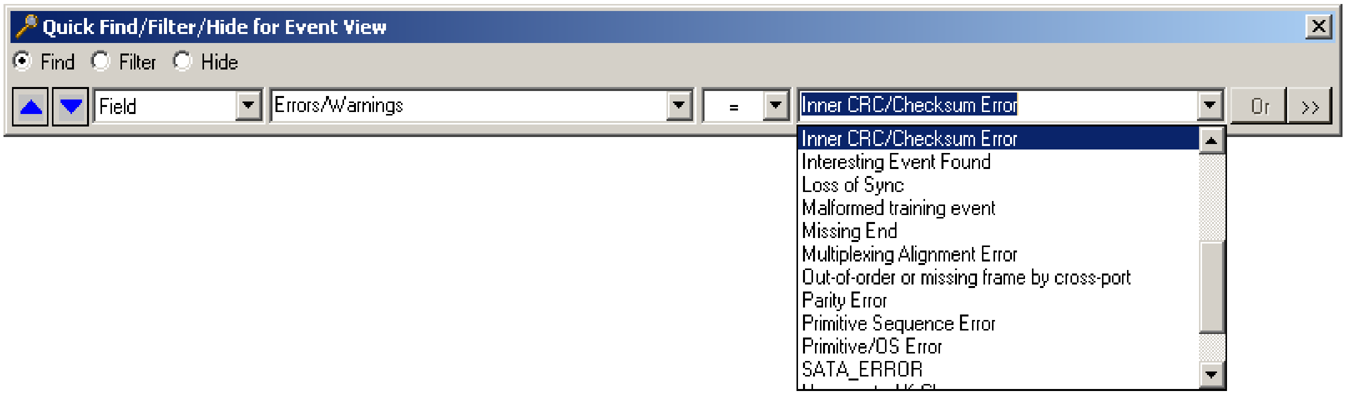
TraceView reports incorrect CRCs and checksums inside the Inspector window, as well as inside the **Errors/Warnings column**. TraceView does not recompute the end-of-frame CRC for every frame. However, if the hardware reported a CRC Error on a frame, TraceView will display the correct computed value for this frame within parenthesis, for example, **(Computed: 0xD5)**, next to the incorrect value.



The following is a list of all CRC/Checksums computed by TraceView:

- Fibre Channel, GigE, SAS/SATA, or FCoE embedded frame CRC (when the HW marks a CRC Error)
- IP Checksum
- TCP Checksum over IP and IPv6
- UDP Checksum over IP and IPv6
- ICMP over IP and IPv6
- IGMP Checksum
- OSPF Checksum
- LSA Checksum
- SATA Identify Device Checksum
- SB-2 LRC
- FCIP CRC
- FCP CRC (both CRCs are calculated)
- iSCSI Header and Data Digest CRCs
- MPA ULPDU CRC

Note that it is possible to Quick Find on CRC/Checksum errors in the **Errors/Warnings column**.



Errors Found Only in Saved Traces

Listed below are two types of errors that can only be found in saved traces. These errors are not available when searching a buffer trace. Performance will be slower when searching for these error types in a saved trace.

- Embedded CRC&Checksum Errors
- All Error reported by HW & SW

Column and Decode Display for Partial Frames

It may be possible to start or stop the analyzer during the middle of a frame transmission. So, at the start of the capture the analyzer will automatically remove these partial frames that are missing their SOFs from the main view. However, the words on the wire are still available in the Dword view for protocols that support Dword view. Similarly, for the partial frames at the end of the capture – those missing their CRC/EOF – the analyzer will not display those partial frames at the end of the capture in the main TraceView grid. However, if the partial frame has a physical error (RD, CV or CRC error), then the partial frame will be shown in the main view with limited decodes.

Column Operations

Insert New Column

Inserting a new column allows you to display whatever trace information you find useful.

You can insert a column in the main spreadsheet view, in Dword view, or LaneView; however, the dialog box and steps for adding a column are different.

To insert a new column in the main spreadsheet view:

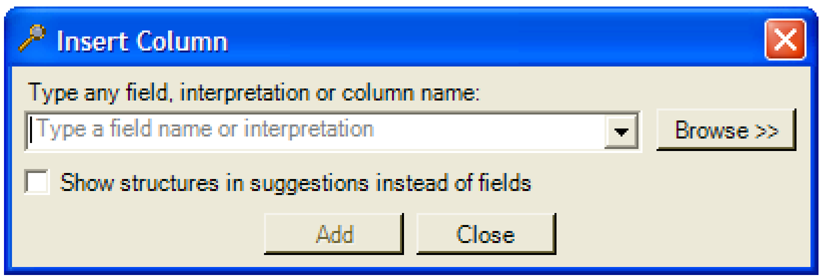
1. Right-click the column heading to the left of where you want to insert a column.
2. Select **Insert Column…** from the menu. The **Insert Column** dialog box appears.
3. Begin typing the name of the column you want to insert. The autocomplete feature will suggest options based on what you have typed. Field names are case-sensitive.
4. Press the **Add** button. The new column appears immediately in the column display.

5 You can repeat and insert as many columns as you want. When finished inserting columns, press the **Close** button.

You can also insert a column by right-clicking on a cell, and selecting the menu **Insert Column…**. This will bring up a dialog with a drop down box of all the fields in the current frame, in alphabetical order. The **Browse** button brings up the tree view, so you can browse through the tree instead of using the auto-completion feature.

By default, the auto-completion dialog only show fields and interpretations. However, if you check the Show structures in suggestions instead of fields check box, the dialog will show structures allowing you to choose a structure as a column.

Figure 136: Insert Column



To insert a new column in Dword view or LaneView:

1 Right-click the column heading to the left of where you want to insert a column.

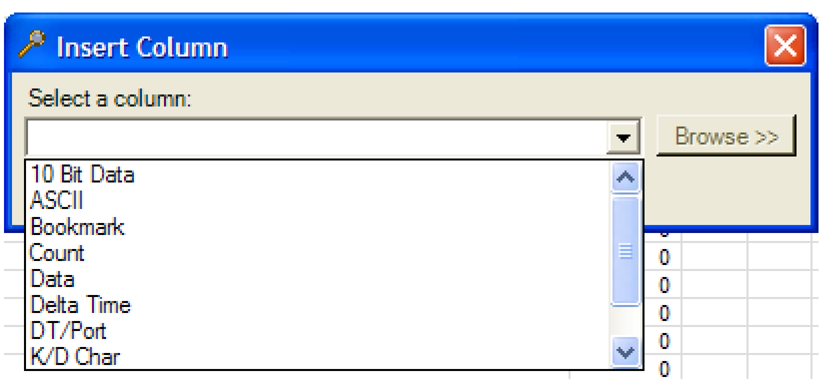
2 Select **Insert Column…** from the menu. The **Insert Column** dialog box appears.

3 Select a column from the pull-down box in the dialog. The pull-down box has a list of all information fields in alphabetical order that can be added to the view.

4 Press the **Add** button. The new column appears immediately in the column display.

5 When finished inserting columns, press the **Close** button.

Figure 137: Insert Column for Dword View



Add to this Column

Adding to a column allows you to display whatever trace information you find useful in a single column. It performs a similar function to inserting a new column, except this function inserts the new information into the selected column rather than creating a new column. Add to this column functions are only applicable to the TraceView main spreadsheet view.

To add information to an existing column:

1. Right-click the column heading where you want to add information.
2. Select **Add to This Column…** from the menu. The **Add To This Column** dialog box appears. See Figure 136.
3. Expand or collapse the hierarchy of information in the dialog box until you see the item containing the information you want to add. You can also type in the name of information field in the **Select Field** drop-down box at the bottom of the dialog. The drop down box has a list of all information fields in alphabetical order. If you do not know the complete field name, type the first few letters and use the pull-down menu to select the correct field name. Field names are case-sensitive.
4. Press the **Add** button. The new information appears immediately in the column display for the currently selected column.
5. You can repeat and add as much information as you want to a column. When finished adding information to the current column press the **Close** button.

You can also add to a column by selecting a column value in the column where you want to add information. However, this will bring up a dialog which does not give a hierarchy of the information you can add to the column. This method is only recommended if you know the name of the column you are adding and can type the column name into the field. The drop down box has a list of all information fields in alphabetical order. If you do not know the complete field name, type the first few letters and use the pull-down menu to select the correct field name. Field names are case-sensitive.

Expanding a Column

You can expand a column by clicking it.

To expand a column:

1. Place the cursor on the right edge of the heading of the column you wish to expand or contract.
2. A double-headed arrow appears. Drag the arrow to the right or to the left to expand or contract the column.

You may also just double-click a column heading and it will auto-size to display all values in the column.

Delete Column

This feature allows you to delete an entire column on your spreadsheet.

To delete a column:

1. Right-click the column heading you wish to delete.
2. Select **Delete Column** from the menu. The column is deleted.

Moving a Column

Moving a column is helpful for viewing types of data that you are interested in side-by-side with other columns of similar information.

To move a column:

1. Select the column you want to move by clicking on the column heading and holding the button down. Drag the column and a green line appears to help you position the column between two existing columns.
2. Click and drag the column to the new location on the spreadsheet, then release the mouse. The column is now in a new position.

Detailed Find/Filter/Color Window

Detailed Find/Filter/Color Overview

Select the **Detailed Find/Filter/Color**  button to bring up the Detailed Find/Filter/Color window. The Detailed Find/Filter/Color window allows you to set up complex searches, filters, and color modifications.

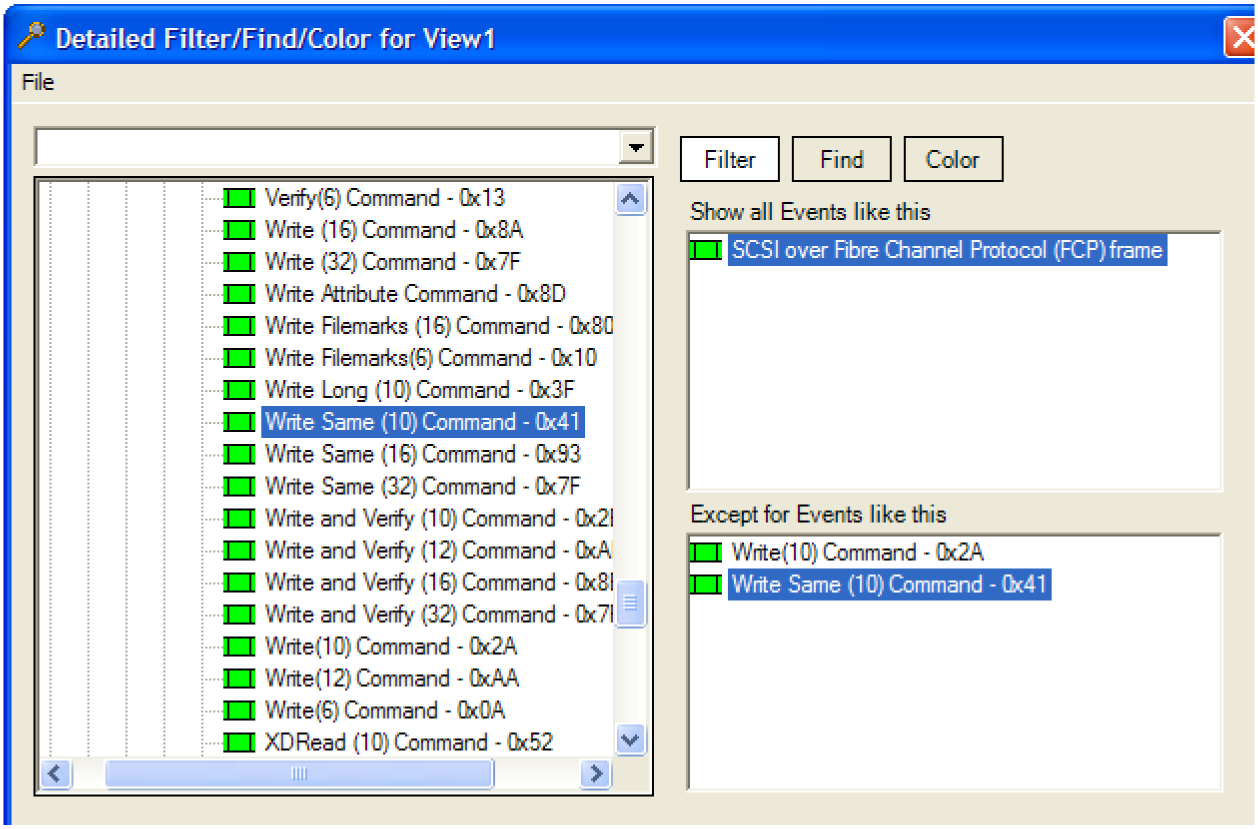
The left of this window is the Available Templates Browser, which provides a library of templates to use for searches and filters. On the right of this window are the **Find**, **Filter**, and **Color** tabs. You click and drag templates from the browser to one of the tabs to set up the conditions for your search or filter. Your last ten filter, find, and colors will be listed in the drop-down menu for the Available Templates Browser.

Right-click a template to perform Open, Cut, Copy, Paste, Delete and Rename operations. An Open operation shows the contents of the template and opens it for editing. You can also double-click templates already in one of the tabs or in the **User Library** section to edit the template using the Template Editor.

The conditions for **Find**, **Filter**, and **Color** are set up on different tabs, but are applied to the data at the same time by selecting the **OK** button.

Note that filter operations can override other operations or make them meaningless. For example, if you have set the **Filter** tab to display only SCSI writes, and you set up the **Find** tab to search for SCSI reads, your search operation will not find any read events.

Figure 138: Detailed Find/Filter/Color Window



Available Templates Browser

The **Available Templates Browser** is a hierarchical display of templates in the Detailed Find/ Filter/Color window. It functions like Windows Explorer, allowing you to view and create a hierarchical structure for templates. The names of the folders in the Available Templates Library in TraceControl and TraceView are shortened by default. There is a context menu that allows you to display the longer versions of the folder names.

Finding a Template

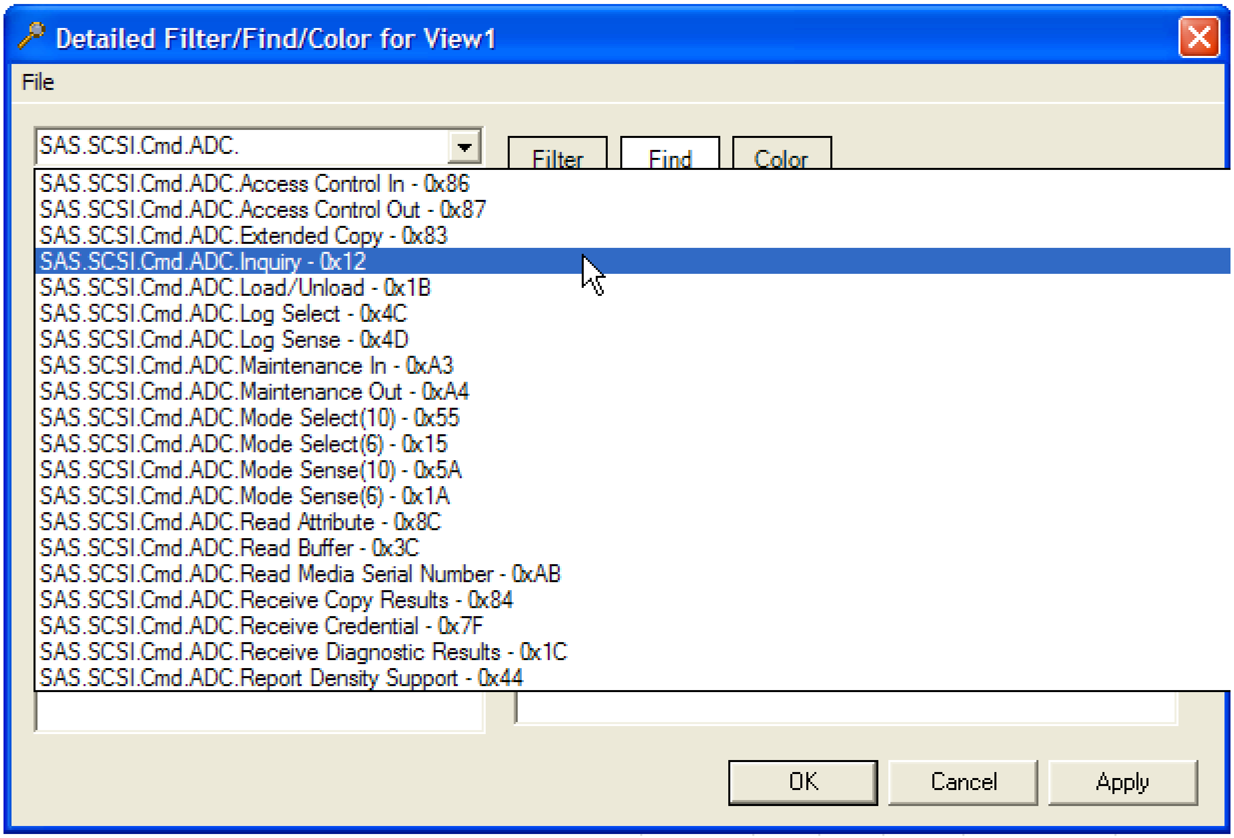
In addition to navigating through the library tree, you have the option of using the search field. This field allows you to search the Viavi library. To use the search field, type the name of a template into the field with each level separated by a period, for example:
`SAS.SCSI.CMD.ADC.Inquiry - 0x12`
The matching templates will be displayed in a drop-down window as shown in the figure below.

For some protocols like Fibre Channel and Ethernet, the template search field supports some wildcarded folder names. These wildcarded folder names map to multiple paths at the same time. They are useful to provide templates that can match frames with a variety of optional headers:

- DLC*: Maps to the Ethernet basic frame and all frames containing the following optional Ethernet tags: VLAN, TRILL, CN-TAG, VnTag
- FC*: Maps to the Fibre Channel basic frame, the VSAN-tagged frames and FCoE frames with all optional and common Ethernet tags.

- TCP*: Maps to the basic 5-word TCP Header and the common 8-word TCP Header.
- iSCSIcmd*: Maps to all iSCSI commands
- MPAcmd*: Maps to all MPA/DDP/RDMA commands

Figure 139: Template Search Field

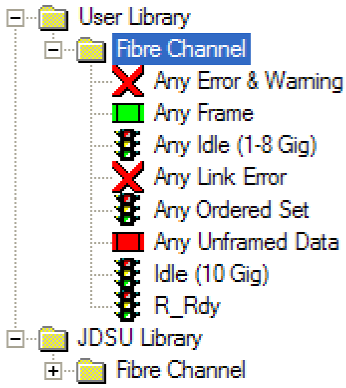


You can name, rename, open, or move templates/folders within the **User Library** section. Double-click a template to change its contents with the Template Editor.

The Available Templates Browser is context-sensitive in TraceView. For example, if you are looking at a SAS/SATA trace, the browser will only show templates that apply to SAS/SATA traces.

An example of the Available Templates Browser is in Figure 140.

Figure 140: Example Available Templates Browser.



There are three types of templates, and one template for unrecognized data:

Frames or packets
Frames or packets as defined by the protocol being used.

Primitives or Ordered Sets
Specific words defined by a particular protocol's specification.

Errors
Recognized error conditions within the data stream reported by the protocol. The error template name indicates if the template includes hardware errors only or both hardware and software errors.

Unframed data
Data that cannot be interpreted as any of the three other types.

The **Viavi Library** section is read-only. You cannot move templates into this section, rename templates, change templates, or change the structure. You can copy templates to the Find, Filter, or Color tabs from the **Viavi Library**.

Creating a New Folder in Your User Library:

1 Click one of the protocol folders inside the **User Library**, or any subfolders.

2 Right-click to view a pull-down menu. Select **New Folder**.

3 Type a name for the new folder.

Dragging a Template From the Viavi Library to Your User Library:

1 In the **Viavi Library**, select a template. For example, **SCSI Frames**.

2 Drag selected template to the folder you created in **User Library** and drop it.

Applying a Template for Find, Filter, or Color:

1 Click the **Find**, **Filter**, or **Color** tab.

2 Select a template.

3 Drag the template to one of the tab's display boxes and drop it.

Filter Groups

You can save the set of information you have applied to the **Find**, **Filter**, and **Color** tabs as a Filter Group file. The Filter Group saves all information about which template is applied to each tab, including any modifications to templates using the **Frame**, **Qualifiers**, or **Containing** tabs. The Filter Group file can be recalled by opening it from the Detailed Find/Filter/Color window.

To Save a Filter Group:

1 Drag all templates you want to the **Find**, **Filter**, or **Color** tabs.

2 Make any modifications or name changes to the templates by opening the template and using the Template Editor.

3 Select **Save...** or **Save As...** from the **File** menu in the Detailed Find/Filter/Color window. Filter groups must have an extension of `.ffg`.

4 Name the new Filter Group file and press **Save**.

Open a Filter Group:

1 Select **Open...** from the **File** menu in the Detailed Find/Filter/Color window.

2 Find the Filter Group you want to display. Filter Groups must have an extension of `.ffg`.

3 Press **Open**.

Aliases (Name Replacement)

Sometimes it is useful to assign symbolic names to values you are analyzing that are customized to your application or are different from the default settings. This is accomplished by assigning names to values in the spreadsheet, creating an alias for this data type.

Aliasing only applies to the column type you set it in. It substitutes the aliased text in the display for items that perfectly match (arithmetically) to values you are aliasing. Any value in a column can be assigned a name. This feature is most appropriate for naming source and destination fields like S_ID and D_ID. When an alias is saved for S_ID, it is also applied to D_ID. Aliases propagate across all views, the events grid, **Exchanges View**, and **DWORD** view.

Depending on if you have trace buffers or a file opened in TraceView, aliases are saved in three different ways:

1 For trace files, aliases are loaded and saved in a file named TRACE_FILE_NAME.aliases in the same folder as the trace itself.

2 For trace buffers, aliases are loaded and saved in the same global file for all trace buffers: %APPDATA%\Viavi\Xgig Analyzer\last aliases.txt. This way, aliases for trace buffers are remembered from one buffer to the next.

3 The Manage Aliases dialog has a checkbox.**Use local aliases instead of the ones in trace files** that is only visible for trace files. When this option is checked, trace file aliases are loaded/saved in the same global file as for trace buffers. This way, the aliases are remembered

from one trace file to the next. When the option is unchecked, then the trace file aliases are stored as explained in Step1 above.

You can modify the .aliases file for a trace in a text editor. You can also copy the .aliases file from a trace to another trace. Use the Enable Aliases button in TraceView's main window menu bar to enable or disable all aliases within a trace.

Use the Enable Aliases  button in TraceControl's main window menu bar to enable or disable all aliases within a trace.

To Quickly Assign an Alias:

1. Right-click the column value you want to alias.
2. Select **Set Alias**.
3. Type the alias text in the field.
4. When you exit the field, all other values in the column that match the original text will be changed to the alias.

If a column has multiple fields, only the first field (or the last if the column is right-aligned) will be aliased.

Using the Manage Aliases Editor to Assign or Modify an Alias:

1. Right-click the column heading, and select **Manage Aliases...**, or select **Manage Aliases** from the **Tools** menu. The **Manage Aliases Editor** for the column you selected appears.
2. Select the field you want to alias.
3. Select the value to alias.
4. In the **Alias** field, type the name you want to add. Press the **Add\Replace** button.
5. Click the **Save** button to save all the changes you made in the **Manage Aliases Editor.**

The **Aliases Enabled** check box affects all aliases in the trace just as the **Enable Aliases** button in the menu bar.

As stated above, the **Use local aliases instead of the ones in trace files** check box is available for trace files, not for trace buffers. When the check box is checked, the Manage Aliases dialog content is refilled from the global alias file %APPDATA%\Viavi\Xgig Analyzer\last aliases.txt and aliases will be loaded/saved to that file from now on. When the checkbox is unchecked, then the aliases are loaded/saved to a TRACE_FILE_NAME.aliases file next to the trace file itself.

The following options are available from the **File** menu:

- **Import Aliases...**: to import aliases from an .aliases file in text format.
- **Export Aliases...**: to export all the current aliases to an .aliases file in text format.

  Additional menus are available for trace files when the option **Use local aliases instead of the ones in trace files** is unchecked:

- **Import Local Aliases**: To import the aliases from the global alias file %APPDATA%\Viavi\Xgig Analyzer\last aliases.txt.

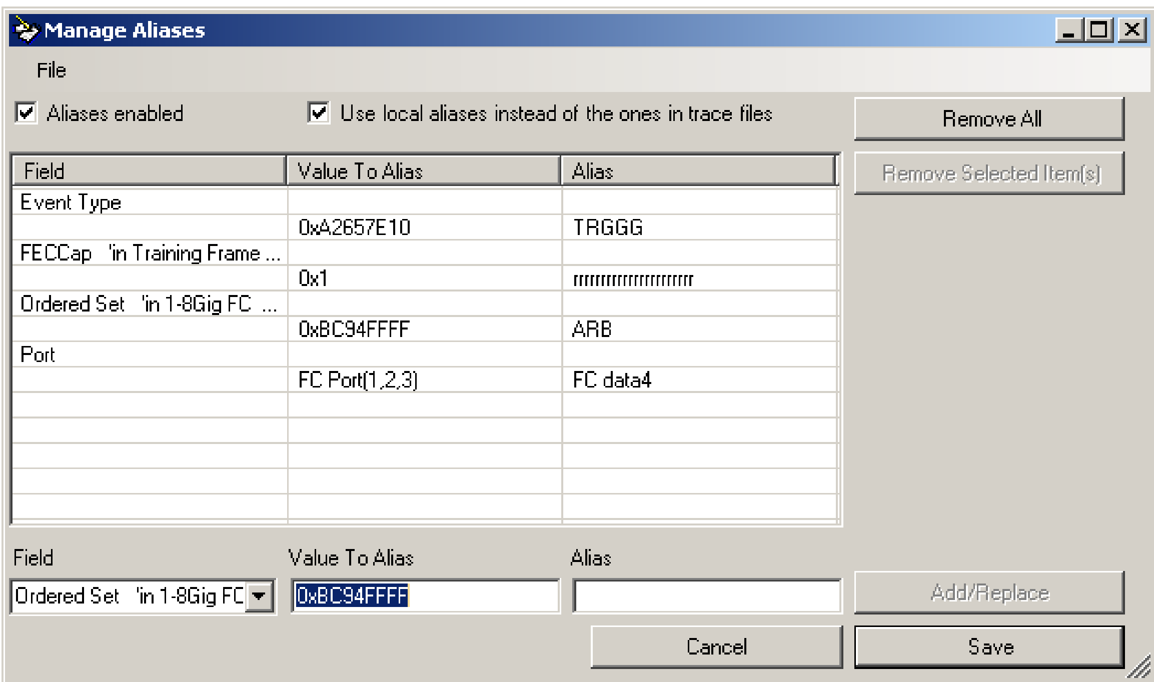
- **Save To Local Aliases**: To export the aliases to the global alias file %APPDATA%\Viavi\Xgig Analyzer\last aliases.txt.

  An additional menu is available for trace files when the option **Use local aliases instead of the ones in trace files** is checked:

- **Save Aliases To Trace**: To save the aliases to a TRACE_FILE_NAME.aliases file next to the trace file itself.

To delete an alias, right-click an alias, and select **Delete All Aliases For Field(s)**. The alias is deleted.

Figure 141: Manage Alias Editor



The **Add Alias**, **Delete Alias**, **Delete All Aliases For This Field**, and **Manage Alias** options are also available in Template Editor by right -clicking a field, and selecting the **Alias** menu item.

Merging Aliases from Other Files

To import aliases from another file and merge them to the current `.alias` file, select **Import Aliases** from the File menu in the **Manage Aliases Editor** . If there are conflicts, a dialog will appear prompting you to cancel all, overwrite all, or ignore conflicting items from the file.

Assigning Colors

Use the **Color** tab of the Detailed Find/Filter/Color window to perform color operations.

1. Select **Detailed Find/Filter/Color...** from the **Edit** menu to bring up the Detailed Find/Filter/ Color window.
2. Select the **Color** tab.
3. Select a template from the **User Library** or the **Viavi Library**.

4 Drag templates to the **Color** tab’s **Show all Events like this in color** pane.

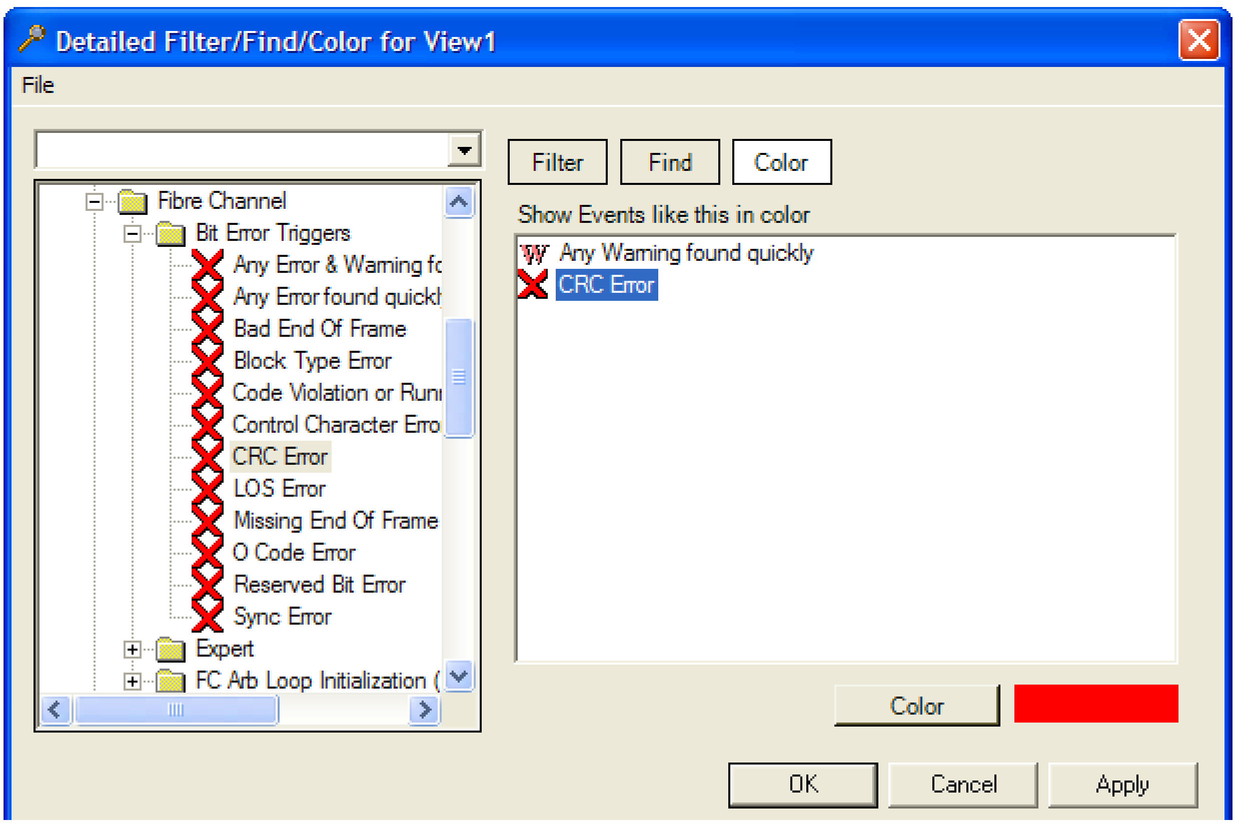
5 Continue to select, drag, and drop templates until you are satisfied with the conditions.

6 If needed, press the **Color** button to change the color. A dialog box will display to select the color. The default color is red.

7 Press **OK** to apply the color. Once the color is applied, all events that match the condition will appear in the specified color.

An example is shown below. When the color filter is applied, any CRC errors are shown in red. Double-click a template to modify its contents. Right-click a template to perform copy, cut, paste, rename, or delete operations.

Figure 142: Set Colors for Display Using the Colors Tab



Chapter 14

Using the Secondary Panes in Xgig TraceView

In this chapter:

- Using the Exchanges View Pane
- Using the Details Pane
- Using the Traffic Summary Pane
- Using the LTSSM Panes for PCIe

Using the Exchanges View Pane

The **Exchanges View** pane displays the following information:

- Completed SCSI exchanges from FCP-SCSI, iSCSI, and SAS physical layers
- Completed SATA exchanges from SAS/SATA physical layers
- Completed Memory and IO Read/Write PCIe exchanges from PCIe physical layers
- Completed NVMe Admin, Read, and Write exchanges from PCIe physical layers

Note: Exchanges View hides PCIe exchanges for NVMe devices once the NVMe exchanges have started.

- Reassembled iSCSI, FCIP/iFCP, SMB/CIFS, and NFS/RPC PDUs from Ethernet physical layers
- 12G SAS Transmitter training summary events (only when the selected ports contain transmitter training summary events). See “Tx Training Summary Pane” on page 320.

By default, the exchanges or PDUs for the currently selected ports are displayed as first level nodes in a tree. For exchanges, the wire events corresponding to each exchange are displayed as second level nodes in the hierarchy. For PDUs (also referred to as reassembled events) the wire events or frames that comprise the PDU are displayed as second level nodes in the hierarchy. This view is available for buffers as well as for saved traces only after post-processing by Xgig Expert. Exchanges, wire events, and PDUs are listed by timestamp just as in TraceView’s main event grid. Wire events include only frames, no primitives.

You can change which information is displayed in the hierarchy by selecting an entry from the **Exchanges View** drop-down menu, for example PDUs and Exchanges, PDUs, or Exchanges by making a selection from the **Exchanges View** drop-down menu.

Select **Exchange View** from the **View** menu to show or hide Exchanges View. You can also click the **Show/Hide Exchange View** button in the main window’s toolbar. When opening a trace, Expert is run automatically. If the trace has not been processed by Expert, a message appears asking if you would like to run Expert and process the trace. If you agree, Expert is run in the background. Once the trace has been processed, a message appears asking if you would like to reload the trace. You can turn off automatic invocation of Expert by selecting *Options/Xgig TraceView Options* then choosing the **Expert / protocol decodes** tab and turning off the “Launch Expert automatically every time a trace is opened.” radio button.

Exchanges View information accessed on one domain will not be available on another domain if you access the trace using the buffers. The temporary Expert information generated by processing the trace is stored locally. Therefore, when accessing the trace on another domain, you will be prompted again to process the trace using Expert. You can set the location where temporary Expert files are stored using Expert.

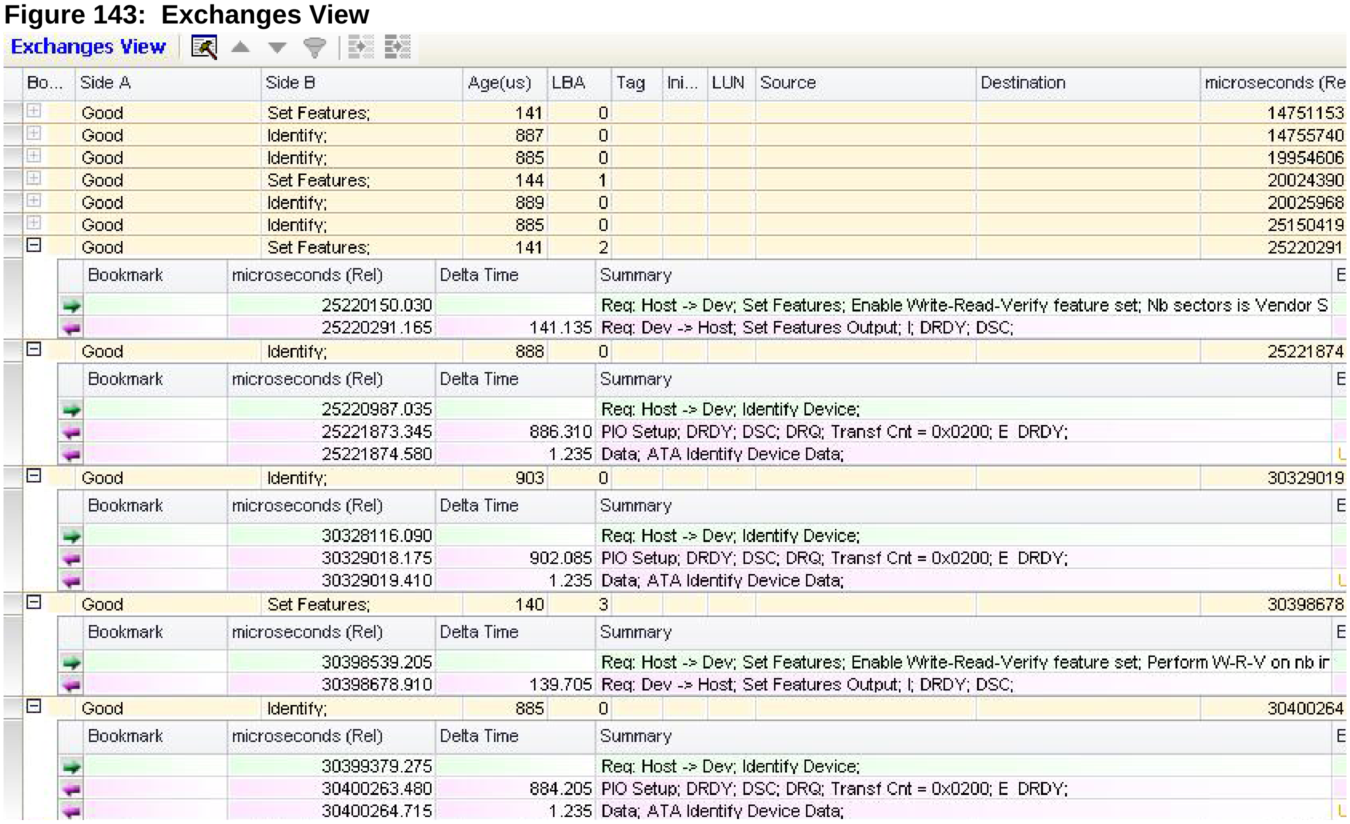
Contents of Exchanges View

Exchanges View contents are limited to the ports in the current port selection. When port selection changes in the event grid, **Exchanges View** contents are refreshed to reflect new port selection. When a single port is selected in the port selection, exchanges corresponding to that port are displayed. Exchanges displayed can originate or end on that port based on the configuration used in Expert while processing the trace. The text for a wire event or PDU with an error is shown in red. Similarly, the text for an wire event or PDU with a warning is shown in orange, and a warning icon is shown next to the exchange.

When an exchange is expanded, wire events and PDUs in both directions may be displayed if both ports are loaded. If some of the ports are not loaded, the error message, “No port is loaded” is displayed in summary column for the wire events not loaded. The direction of a wire event or PDU is indicated by an arrow next to the wire event. A right arrow indicates traffic from host to drive, and a left arrow indicates traffic from drive to host.

Exchanges View contains a toolbar with some of the same functionality as the main bar for the main event grid. The toolbar allows you to open the **Detail Filter/Find/Color** window, find previous/next event, apply detailed filter, apply quick filter, or apply quick hide.

Figure 143: Exchanges View



Expert does not generate an exchange if the beginning of the exchange is not part of the capture. However, Expert will generate a pending exchange when the beginning of the exchange is part of the capture but the end of the exchange is not.

When creating extractions from a trace, if only the exchange ending timestamp is within the extraction time slot and beginning timestamp is not, wire events or PDUs at the beginning of the exchange are not extracted. In such cases, the error message, “Not saved” is shown as decode in the summary column for the missing wire events.

When an exchange contains more than 100 frames or PDUs, first 99 frames are displayed under an exchange and there is a placeholder which shows how many more frames are there in that exchange.

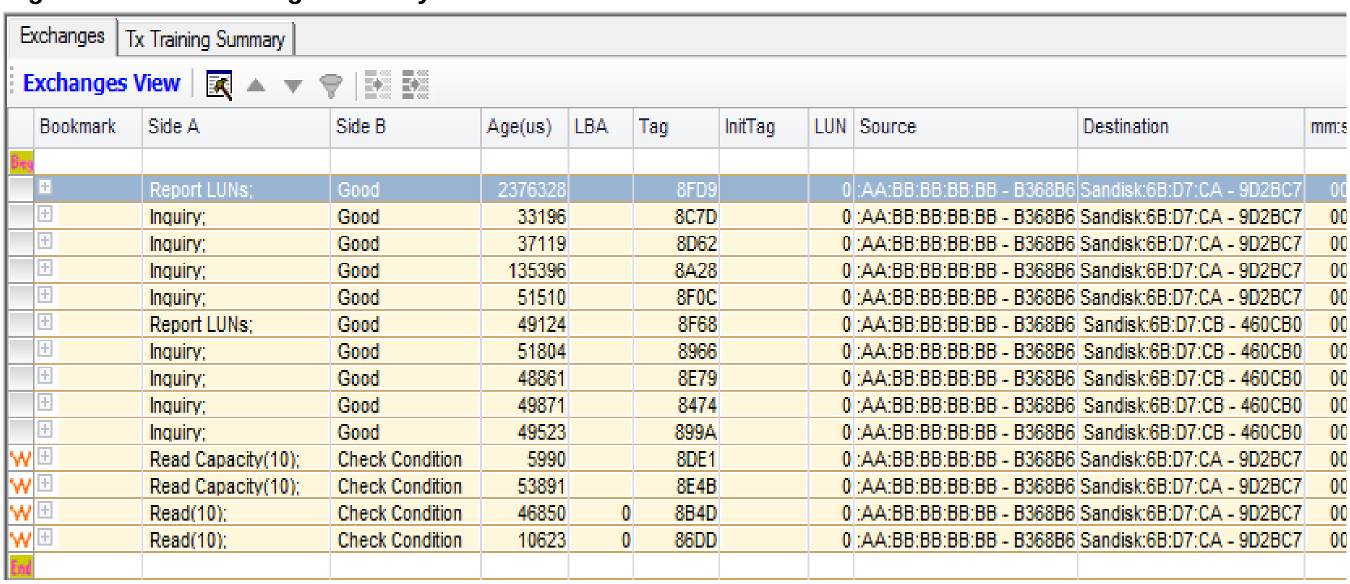
If only one port is explicitly opened from the buffer, the corresponding .xpt file will be automatically opened if it is available. If a .trc file is opened, the corresponding .xpt file is not automatically opened even if it is available.

There are no changes to the display or decodes in the other grids due to the presence or absence of **Exchanges View**.

Tx Training Summary Pane

Exchanges View has a Tx Training Summary pane. This pane is present only when the selected ports contain transmitter training summary events. If selected ports contain both regular exchanges and transmitter training summary events, two tabs are displayed, one for exchanges and one for transmitter training summary events.

Figure 144: Tx Training Summary Pane



Bookmark	Side A	Side B	Age(us)	LBA	Tag	InitTag	LUN	Source	Destination	mm:s
	Report LUNs;	Good	2376328		8FD9		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
	Inquiry;	Good	33196		8C7D		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
	Inquiry;	Good	37119		8D62		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
	Inquiry;	Good	135396		8A28		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
	Inquiry;	Good	51510		8F0C		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
	Report LUNs;	Good	49124		8F68		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CB - 460CB0	00
	Inquiry;	Good	51804		8966		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CB - 460CB0	00
	Inquiry;	Good	48861		8E79		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CB - 460CB0	00
	Inquiry;	Good	49871		8474		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CB - 460CB0	00
	Inquiry;	Good	49523		899A		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CB - 460CB0	00
W	Read Capacity(10);	Check Condition	5990		8DE1		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
W	Read Capacity(10);	Check Condition	53891		8E4B		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
W	Read(10);	Check Condition	46850	0	8B4D		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00
W	Read(10);	Check Condition	10623	0	86DD		0	:AA:BB:BB:BB:BB - B368B6	Sandisk:6B:D7:CA - 9D2BC7	00

Navigating in Exchanges View

Click an exchange, wire event, or PDU to select it. Use the +/– icon for an exchange to collapse/ expand it.

Whenever an exchange, wire event, or PDU is clicked in **Exchanges View**, the **Inspector** tab of the **Details** pane shows the details just as it does whenever an event is selected in the event grid.

When you select the right-click option Synchronize Grids, both the event grid and Dword or LaneView tab of the **Details** pane navigate to the timestamp corresponding to selected event when an exchange or wire event is selected. If the selected event is filtered out, both panes navigate to the event with the nearest timestamp.

If you want to navigate to a timestamp from within **Exchanges View**, you can right-click the icon next to the event.

Quick Find/Filter/Hide

Use the Quick Find feature to find the next or previous wire event that contains similar data values to the one you are viewing. Double-click an exchange, or select **Quick Find/Filter/Hide** from the context menu to open the **Quick Find/Filter/Hide** dialog. Searching and filtering are supported only for exchanges not for wire events. See "Navigating a Trace" on page 234 for instructions on using the **QuickFind/Filter/Hide** dialog.

Detailed Find/Filter/Hide

Use this feature to search the wire events in an exchange using a template from the template library tree as a criterion.

Columns

Exchanges View supports multiple columns to decode and display various details for each exchange or wire event. Some of the columns in **Exchanges View** are common with those in the event grid; others are unique to **Exchanges View**. Some of the columns provide information only for the exchange and others for both the exchange and the wire event. You can add or delete columns for exchanges or wire events just as you can in the event grid by right-clicking a column and selecting **Insert Column** or **Delete Column**. The following are the default columns for **Exchanges View**.

Bookmark

This column displays bookmarks corresponding to the exchange or wire event. Whenever bookmarks are modified, those changes are reflected in this column. Similarly, you can edit the bookmarks in place in this column and the changes are reflected in other grids and Bookmark Event drop-down menu.

Side A/Side B

This column displays the command and status for each exchange or PDU. Exchanges have both the command and status on the same line while PDUs have text only on Side A or Side B.

Timestamp

This column shows the same information that is displayed in the event grid for wire event in an exchange. If not all wire events in an exchange are displayed, this column may be blank. Timestamp format is the same in the event grid, **DWORD** tab, and **Exchanges View**. Selecting any of the timestamp format changes the format in all the panes.

Exchange Age (us)

This column is shown for exchanges. It displays the total duration (age) of an exchange. For pending exchanges, this column shows the duration from the beginning of the exchange until the end of the capture. Age can only be displayed until microseconds; nanoseconds cannot be displayed in this column even if the time format selected has nanoseconds in it. The time format is the same as the Delta Time columns in the event grid the DWORD tab. If not all of the wire events within an exchange are displayed, this column may be blank.

Delta Time

This column is shown for wire events. It shows the time elapsed since the previous wire event within the same exchange. The time format is the same as the Delta Time columns in the event grid the DWORD tab.

Cmd

This column corresponds to the command name that initiated the exchange, usually a read or a write. This column is shown for exchanges.

LBA

This indicates the Target Logical Block Address for the command. This column is shown for exchanges. If the command is a read, then the drive will start reading consecutive blocks starting at that address. If it is a write, then the drive will start writing consecutive blocks starting at that address.

Summary

The summary column is shown for both exchange and wire events. This column shows decoded information for the exchange or wire event. If an alias is applied, the alias is displayed instead of the decoded information. The **Summary** column can be added to, moved, expanded, or deleted just like any other column.

Tag

This displays the queue tag for SATA or task tag for SAS of the first frame of a particular command. This column is shown for exchanges.

LUN

This indicates the SCSI Logical Unit Number for the drive. Each drive on a SCSI bus has its own LUN. This column is shown for exchanges.

Source

This displays the address of the host that initiated the command. This column is shown for exchanges. Both the Actual Source Address and Hashed Source Address are displayed.

Destination

This displays the address of the target of the command. This column is shown for exchanges. Both the Actual Destination Address and Hashed Destination Address are displayed.

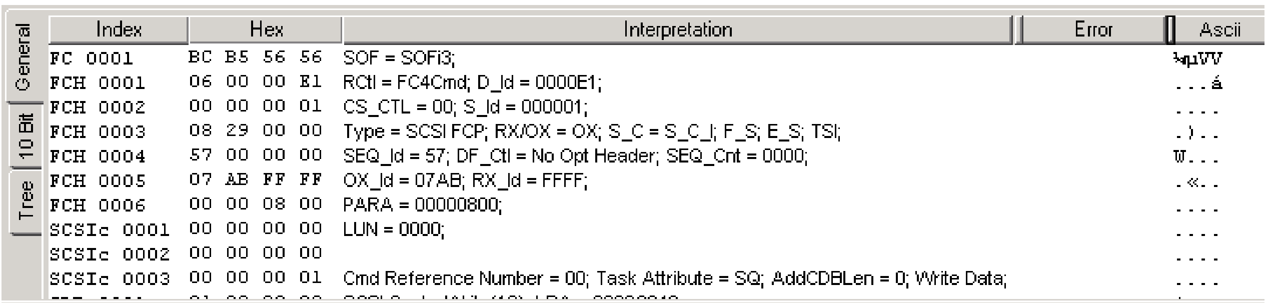
Context Menu Options

All context menu options are common to Exchanges View and the event grid. For an explanation of all the context menu options in **Exchanges View**, see "Context Menu Options for Columns" on page 296.

Using the Details Pane

Press the **Show Details Pane** button to toggle between show and hide of the Details Pane. The **Inspector** tab is the default view. For SAS/SATA traffic, a **DWord** tab is also available in the Details pane. For PCIe traffic, a **LaneView** tab is available in the Details pane. An example of the **Inspector** tab is shown below.

Figure 145: Inspector Tab



For traces containing SAS/SATA traffic, the Details Pane has two major tabs: the **Inspector** tab and the **Dword** tab. See “Dword View” on page 332 for information on the **Dword** tab for SAS/SATA. For traces that do not contain SAS/SATA traffic, no **Dword** tab is displayed. For traces containing PCIe traffic, a **LaneView** tab is displayed. See “LaneView” on page 334 for information on the **LaneView** tab for PCIe. For traces containing no SAS/ SATA or PCIe traffic, the Details Pane shows the **Inspector** tab only. The **Inspector**, **Dword**, and **LaneView** tabs are sometimes referred to as “views”.

Inspector View

The **Inspector** view shows you a detailed interpretation of all the raw data of an event. It shows all the data interpreted in the most detail possible with Xgig TraceView. You are always viewing a single event from the spreadsheet display within the **Inspector** view. To change events, select a new event in the spreadsheet display.

In the **Inspector** view, three different tabs are available for event data. Select the tab at the left to change the view. If all three tabs are not visible, increase the size of the Details Pane to see all three tabs. The three tabs are briefly described below.

For the PCIe protocol, the **Inspector** view displays the bytes for all the lanes, but it decodes only one lane for ordered sets, the lane selected in TraceView’s toolbar. The decoded lane bytes are black, while the undecoded lanes are gray. The **Inspector** view tabs show one byte per lane per line for ordered sets and four bytes per line for DLLPs and TLPs.

For the PCIe protocol, the **Hex** column in the **Inspector** view highlights comma characters and sync bits, and it displays electrical idles and other special characters as shown below.

Table 27: Hex Values for PCIe

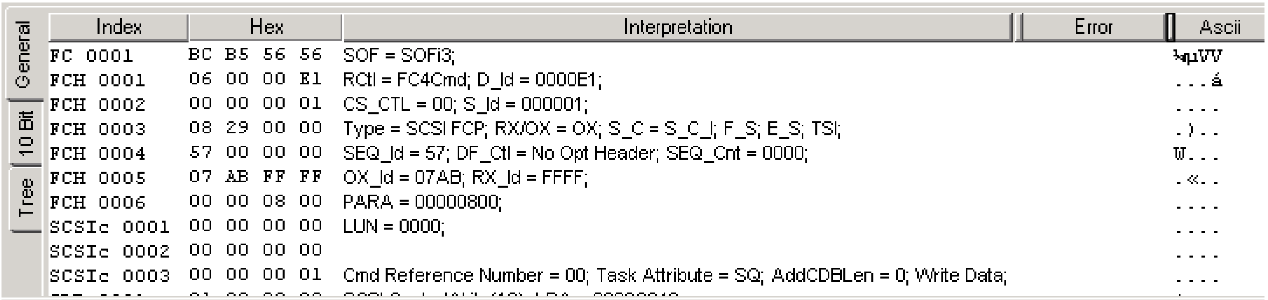
Hex Column	Description
AA	2 hex digits with a white background represent a regular 8B character.
BC	K character at Gen 1/2
2D	Gen3 Start of an Ordered Set Block : The 2 sync bits are represented with the background (white meaning 0, gray meaning 1), and the byte following the 2 sync bits is represented by the hex number, i.e. 2D.
2D	Gen3 Start of a Data Block with sync bits 10. Note that the Data Block sync bits are not shown in the inspector window, they are only shown in the LaneView.
2D	Gen3 Sync bits 11 at the beginning of a block: This is a sync bit error.
2D	Gen3 Sync bits 00 at the beginning of a block: This is a sync bit error.
2D (italic)	Gen3 scrambled data after sync bit errors (the data was not descrambled, it is what appeared on the wire).
__ (underscores	Electrical Idle
(blank)	No Data captured
??	Gen 1/2 Code Violation or Loss of Sync (not used for Gen3)
..	Gen 1/2 10B data that was not descrambled, so we don't know the representation in 8B.

For non-OS events in the PCIe protocol, the **Inspector** view displays four bytes per line. Also, Gen2 TLPs are shifted by one byte position so that their content is DWORD-aligned, and Gen3 TLP and DLLP packets on 8x lanes are shifted by four bytes when they start on lane 4.

General Tab (default)

Shows the hex values for the data and a general interpretation of the data for the protocol being used. Error data is flagged and the ASCII equivalents of the hex data are shown. The **General** tab provides 'fly-over' help that expands the description of the elements found in the event. For example, if you pass the cursor over 'SOF = SOFi3' a pop-up window will display 'Start of Frame = Start of Frame Initiate Class 3.' To disable the display of tooltips, right-click anywhere in the Interpretation pane, and select **Tooltips > Disable**.

Figure 146: Inspector View, General Tab



Index	Hex	Interpretation	Error	Ascii
FC 0001	BC B5 56 56	SOF = SOFi3;		¼µVV
FCH 0001	06 00 00 E1	RCtl = FC4Cmd; D_Id = 0000E1;		...á
FCH 0002	00 00 00 01	CS_CTL = 00; S_Id = 000001;		....
FCH 0003	08 29 00 00	Type = SCSI FCP; RX/OX = OX; S_C = S_C_I; F_S; E_S; TSI;		.)..
FCH 0004	57 00 00 00	SEQ_Id = 57; DF_Ctl = No Opt Header; SEQ_Cnt = 0000;		W...
FCH 0005	07 AB FF FF	OX_Id = 07AB; RX_Id = FFFF;		.«..
FCH 0006	00 00 08 00	PARA = 00000800;		....
SCSIc 0001	00 00 00 00	LUN = 0000;		....
SCSIc 0002	00 00 00 00			....
SCSIc 0003	00 00 00 01	Cmd Reference Number = 00; Task Attribute = SQ; AddCDBLen = 0; Write Data;		....

10 Bit Tab

This tab shows the hex values for the data and a bit-by-bit display of the encoded 40G data in 10-bit increments. Errors are flagged and the K/D symbols calculated for the data are shown. The **10-Bit** tab is generally used when you are trying to debug physical equipment problems. The **10-Bit** column will be blank if the data is unavailable.

For the PCIe protocol, the **10-Bit** tab contains the hex values of the encoded data, errors, and K/D symbols for the data for traces with PCIe events at 2.5 and 5.0 GT/s, which have 8B/10bit physical layer encoding, respectively. The 10-bit column in this tab remains blank unless there are errors.

For the SAS/SATA protocols or for 8Gbps Fibre Channel traces, the **10-Bit** tab will contain a column showing the scrambled form of the data. This column displays only when the original data is in scrambled form. For 8Gbps or 4Gbps traces captured by the 8Gbps Fibre Channel blade, the scrambled data are only generated if the descrambler is on during capture. If the **Link Speed** is set to **8.5000 Gbps Fibre Channel** or **4.2500 Gbps FC (scrambling On)** during capture, the scrambled data is generated and the scrambled form will display in the **10-Bit** tab.

66 Bit Tab

The Inspector 10 Bit tab has been replaced by a 66 Bit tab for all 16G FC traces, for all 10GigE traces captured using Xgig1000 10G ports, and for all 10GigE 40G traces captured using the Xgig1000 40G ports. The 66 Bit tab displays 66B transmission words for all 66B events.

The **66B** column displays the raw 66 bits in hexadecimal form where the first hex digit represents the 2-bit Sync field, and the following 16 hex digits represent the following 64 bits. The hexadecimal value captured for each 66 bit event is the user-friendly representation of these events as shown in the protocol specifications. The value is captured after de-scrambling and bit-swapping each field individually. Note that for Sync Error and Block Type Error 66-bit events, each byte within the 66 bits is being bit-swapped individually.

You can change the 66bit data representation in the 66B column by selecting one of the following menu options from the View > Data Inspector > 66 Bit Representation:

- **Display Bit-Swapped Fields (Hex)**: All the fields in the 66 bit transmission words are bit-swapped before being presented to the user. The 66 bits are represented by 17 hexadecimal digits where the first digit represents the 2 Sync bits. This is the default behavior.

- **Display Bit-Swapped Fields (Binary)**: All the fields in the 66 bit transmission words are bit-swapped before being presented to the user. The 66 bits are represented in binary mode by 66 bits, where the first 2 bits are the Sync bits.
- **Display In Transmission Order (Hex)**: The 66 bits are presented in the order they were captured on the wire without being bit-swapped. The 66 bits are represented by 17 hexadecimal digits where the first digit represents the 2 Sync bits.
- **Display In Transmission Order (Binary)**: The 66 bits are presented in the order they were captured on the wire without being bit-swapped. The 66 bits are represented in binary mode by 66 bits, where the first 2 bits are the Sync bits.

The **Interpretation** column decodes each field of the 66 bits according to the spec. If a field contains a value that is invalid according to the specification, it is marked with (Unexpected Value Found). For example, if a Control field has the value 0x7C, it is decoded as follows:

Control = 0x7C (Unexpected Value Found);

This way, the user can find which specific field of a 66-bit event made the hardware mark it with an error. This is especially important for the “Control” field which can be found up to 8 times in a 66-bit event, the decodes tells you which occurrence of the Control field triggered the “Control Char Error” as generated by the Xgig hardware.

Since every line in TraceView's grid displays one 32-bit word, or multiple 32-bit words. 66B events map to two 32-bit words. **Inspector** view displays the full 66B event on the line of the first corresponding 32-bit, and a text message on the next line telling the user to look at the previous line for the full 66B event. So, for a BB_SCr-Idle 66B transmission word, TraceView displays the full 66B transmission word in the Inspector window 66B tab for the BB_SCr line. Then, for the Idle line, the **Inspector** view’s 66B column tells the user that this DWORD is the second half of a transmission word, look at the previous line the full 66B transmission word.

For frames, **Inspector** view’s 66B column displays all the 66B words that are part of the frame. If the frame is truncated, it displays how many transmission words have been truncated. Misaligned truncation points are re-aligned by truncating the frames at the 66B transmission word boundaries.

The **66B** tab also handles rep-counted primitives. The Interpretation column lists how many primitives have been rep-counted in the Transmission Word.

When a filter is applied on a capture, the 2nd half of a transmission word can be missing. In that case, the 66B displays a message to that effect, and it omits displaying the full 66B transmission word. The same issue can happen at the end of a trace where the second half of a transmission word is not captured.

The Errors column displays the full list of all the errors detected for the 66B events.

The Control/Data Characters column displays the 64B form with comma characters, as visible in the Events view Side A/B columns.

The Inspector View’s **General** and **Tree** tabs show the 64-bit form with comma characters in the Interpretation column. The Hex column shows the hexadecimal representation of the 64 bits.

Sync Tab

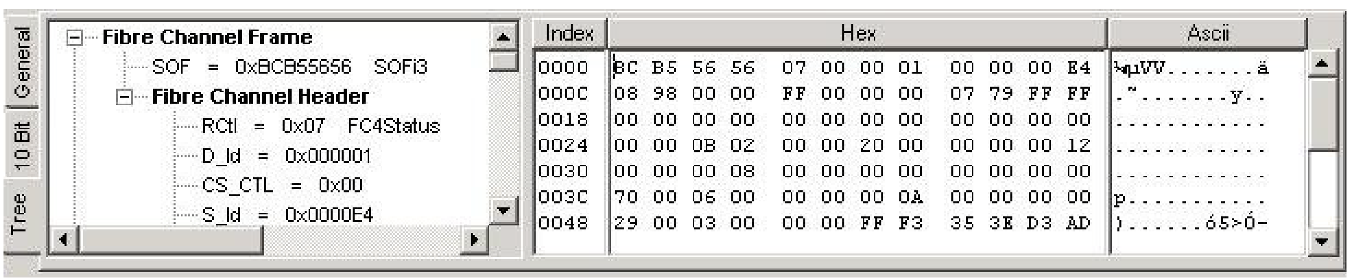
The Sync tab is shown for PCIe traces with Gen 3 PCIe events at 8.0 GT/s. This tab shows the sync bits for ordered set events. However, the Sync tab refers you to LaneView for other Gen3 PCIe events, such as packets and non-OS events because the Inspector does not display these events as one byte per lane per line like it displays OS events. However, LaneView displays all events as one byte per lane per line, so it is more appropriate to look at sync bits for all events.

Tree Tab

Shows the tree structure of the data when mapped to the protocol interpretation being used. You can see the structure of the frame and values associated with all protocol elements discovered within the frame. For example, the display of a Fibre Channel frame shows the start of frame type derived from the SOF value, end of frame values including CRC, as well as the interpretation of fields within the header. If you click one of the elements in the tree structure, the corresponding hex data will highlight as well.

The Tree Tab is composed of two areas which can be resized as needed. The left portion shows the tree view of decoded protocols for the current event. The right portion shows the hex values for the event and their ASCII or EBCDIC representation. The hexadecimal area can be resized for a display of anywhere between 4 and 32 bytes of data per line. Move the slider in the middle of the pane to resize the two areas. The **Index** values change as the slider moves, showing more or less of the hex data on each line.

Figure 147: Inspector View, Tree Tab



Creating Columns From Inspector View Fields

You can drag and drop any field from **Inspector** view to the column header row of one of the other grids to create a column in that grid.

Context Menu Options for Inspector View

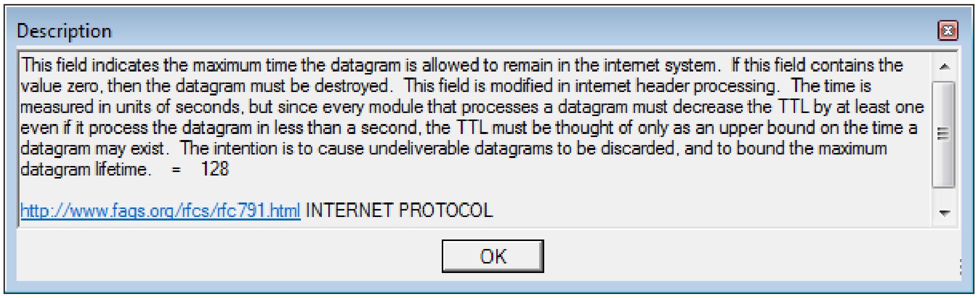
The right-click menu in TraceView is context-sensitive. The following features are available in the tabs of Inspector view.

Copy All Columns

To copy the text from the Inspector pane into tab-separated multi-line text format, right-click in the pane, and select **Copy All Columns** from the context menu. You can paste this into a text editor. This option does not copy the Errors or ASCII columns. Note that the ASCII column is only found on the General tab. This option is available for all three tabs.

Description

To display tooltip information for a field in a dialog with a hyperlink to the protocol specification document, right-click a field, and select **Description**. An example is shown below. This option is available for the **General** and **Tree** tabs.



Show/Hide Off Field Values

To show or hide 0-valued bit fields in the **General** tab of the Inspector pane, right-click in the Interpretation column, and select **Show/Hide Off Field Values** from the context menu.

Alias

To add, delete, or manage aliases, in the **General** and **Tree** tabs of the Inspector pane, right-click in the Interpretation column, and select **Alias** from the context menu. Then, select the desired action from the drop-down menu.

Field Information

To show the offset, length, and value of a field and the different names used by the field throughout the application in the **General** and **Tree** tabs of the Inspector pane, right-click a field, and select **Field Information** from the context menu.

Quick Find/Filter/Hide in Events View

You can access the Quick/Find/Filter/Hide dialog and search for data in the events grid based on fields in **Inspector** View.

Creating a Template For a Field

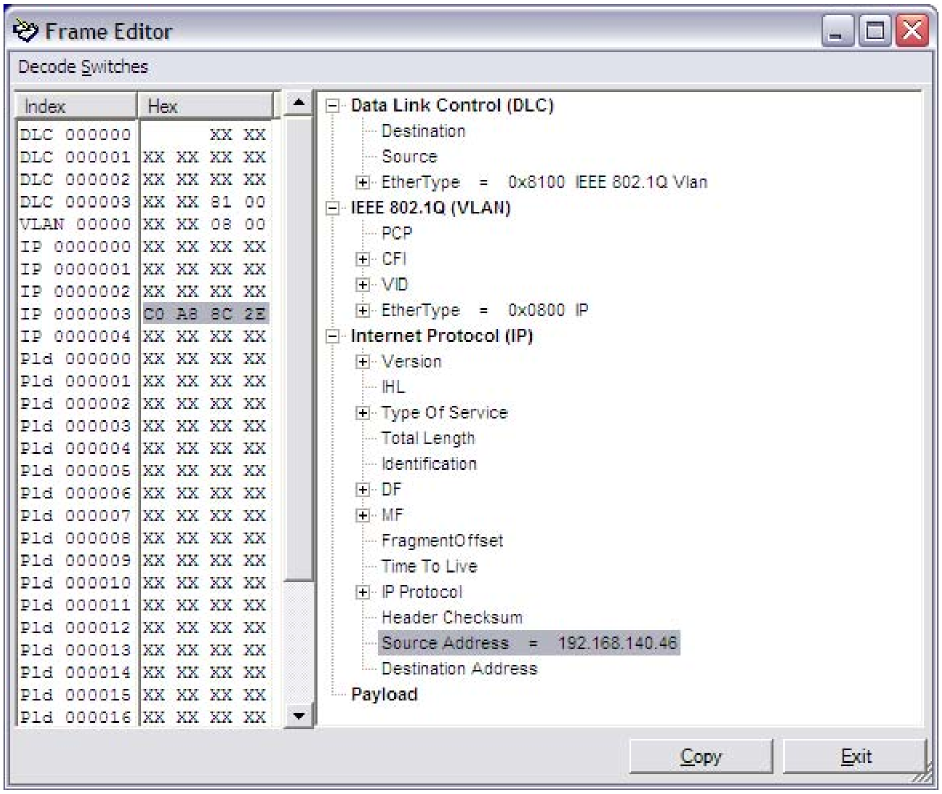
You can create a template based on a field in the Interpretation column of the **General** tab or the **Tree** view of the **Tree** tab using the **Create Template For This Field** context menu option. This option is available for the **General** and **Tree** tabs. Selecting this option creates a template that includes the current field and any other fields required to reach this field.

This template is suitable for use as a trigger in TraceControl. Creating a template based on a field can be beneficial if you want to trigger on an event but do not want to create the template from scratch. You can insert a template based on a field into the template User Library tree for TraceControl, TraceView, Maestro BERT, or Maestro Jammer.

To create a template from a field, right-click a field, and select **Create Template For This Field**.

The following is an example of a template created to search for a specific IP Source Address in a VLAN frame. The template matches a first EtherType = 0x8100 for the VLAN header, then a 2nd EtherType=0x0800 for the IP header, and then the IP Source Address.

Figure 148: Create Template For This Field Dialog



To manually define the frame, type hexadecimal values directly into the center column of the window. To set individual bits in any field, double-click the hex entry to open the Binary Editor. In the hex view, partially defined hex characters appear as question marks: `X001=?`

You can also apply decode switches (if available for the template) by using the **Decode Switches** menu at the top of the dialog. For more information on the Decode Switches menu in this editor, see **"Decode Switches Menu" on page 331**

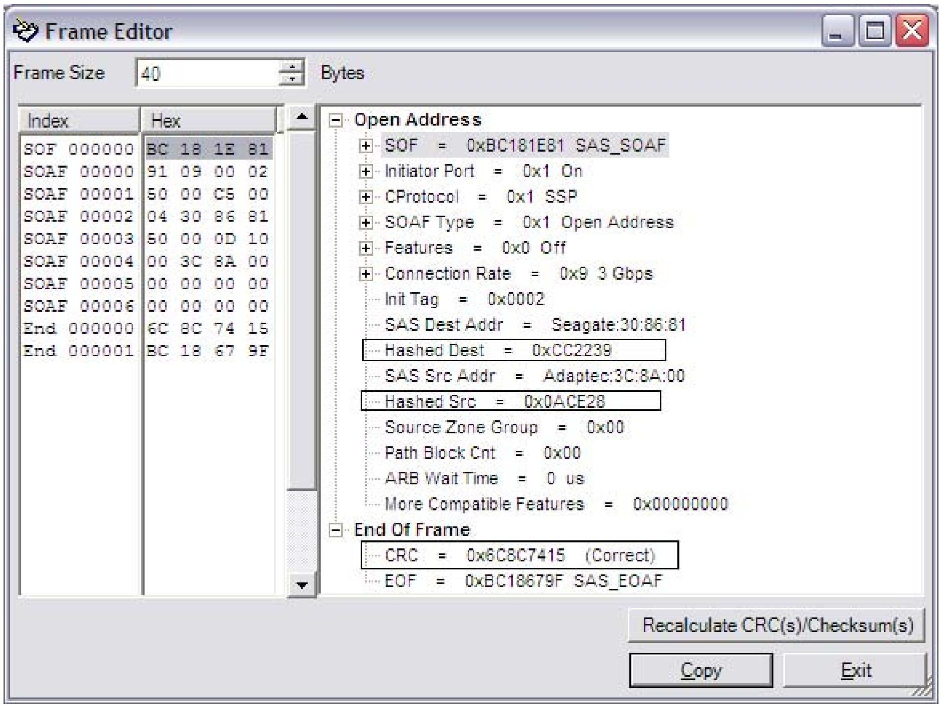
Once you have finished editing the template, click **Copy**, then paste the template into the desired product's template User Library tree by selecting **Paste** from the context menu.

Editing a Frame

You can edit the contents of a frame. The Edit Frame option is available for the **General** and **Tree** tabs. This option provides an editor that allows you to manually edit the header and the payload of a frame, apply decode switches (if available), and recalculate the CRC and Checksum values. You can use this option to gauge the effects of payload values on CRC and Checksum values and to create a frame template for use in Maestro BERT or Maestro Jammer's template User Library tree.

The example below is a SAS Open frame. For this type of frame, the editor shows the computed hashed source/destination field values as the user modifies the Source/Destination addresses. Note that the software has recalculated the CRC.

Figure 149: Edit Frame Dialog SAS Open Frame



The frame size is indicated at the top of the window. You can adjust the frame size within the limits defined by the protocol and frame content.

To manually define the frame, type hexadecimal values directly into the center column of the window. To set individual bits in any field, double-click the hex entry to open the Binary Editor. In the hex view, partially defined hex characters appear as question marks: `X001=?`

The software automatically recalculates the applicable CRCs, and checksums each time you change the frame. If the CRC or checksum is incorrect, an entry is displayed in the frame contents next to the incorrect CRC or checksum showing the correct value of the CRC. To apply the correct recalculation of the CRC and checksum, click the **Recalculate CRC(s)/Checksum(s)** button at the bottom of the window.

Decode Switches Menu

Some templates allow you to specify decode switches. If the template you are creating has this option, the **Decode Switches** menu appears in the upper left corner of the window. The decode switches provide detailed contextual options for decode; for example, further decode of response and data frames. The Decode Switches menu is context sensitive and will only show the decode options available for the specific template you are creating.

The **Decode Switches** menu is intended to help you create a user-defined template. When creating a User Library template, Decode Switches are stored inside the template so they are still ON the next time you open this particular template.

Decode switches allow you to further decode Response and Data frames that can't be decoded without knowing what the associated command frame is. For more information about decode switches, see "Decode Switches" on page 385.

Once you have finished editing the template, click **Copy**, then paste the template into the desired product's template User Library tree by selecting **Paste** from the context menu.

Dword View

The **Dword** view is only available for traces containing SAS/SATA traffic. This view shows each 32-bit Dword interpreted in its own row. The Dword view shows all the Dwords of an event as the Inspector does, yet considers each as an event on its own; all ports' Dwords are interlaced as individual events as in the main spreadsheet. This provides for better timing comparisons between traffic on different ports. In addition, the Dword view shows all captured Dwords, whereas the main spreadsheet does not show unimportant Dwords such as SATA_HOLDs or Scrambled Idle Dwords.

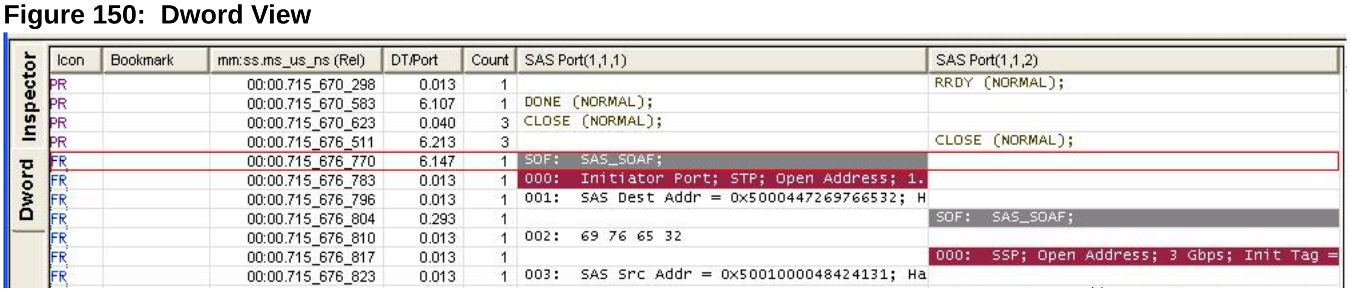
Dword view shows optical OOB events for 12G SAS when devices are connected with optical cable. Dword displays OOB_IDLE rather than DC_IDLE for optical OOB.

By default, the Dword view and TraceView main event grid are synchronized and Sync Scroll Grid button is turned on. Press the **Sync Scroll Grids** button to toggle between synchronizing the grids and having the grids scroll independently.

Several options are available for the display of a data column in Dword view. Right-click a data column header, and select the type of display. Data can be displayed in **10 Bit Data**, **KChar**, **Scrambled Data, Hex,** or **ASCII** format. You can insert a column if you need to display the data in two or more formats within the grid. See "Insert New Column" on page 305 for information on inserting a new column in Dword view.

You can enlarge or reduce the size of the font in the Dword view by using the  and  zoom buttons.

Figure 150: Dword View



The Dword view has some of the same capabilities as the main spreadsheet view. You can insert or delete columns, and you can set the type of display for some columns. For example, in the timestamp field you can set the time as **Calendar Time**, **Time Relative to Capture**, or **Time Relative to Event** by clicking the right mouse on the column. Bookmarks are supported within the **Dword** view. There is a bookmark column in which you can enter a bookmark name. See "Working With Columns" on page 292 for more information on column functions. See "Bookmarks" on page 247 for more information on using bookmarks.

For non-SAS/SATA captures, the Dword view is unavailable. For mixed protocol traces such as SAS and FC, only the SAS ports will appear in the Dword view. Note that Dword view is not available for traces converted from Bus Doctor or I-tech formats.

The display of the Dword tab is based on current port selection. If a mixed protocol domain is opened, if you select a port group with only FC/GE ports the Dword tab is hidden. If the selected port group contains at least one SAS port, the Dword tab is visible. The tab will display or disappear as you change the ports that are selected.

Show EBCDIC/ASCII Representations

By default, the hexadecimal values of each word are also shown, interpreted as ASCII characters. The ASCII characters display in the last column of the **General** and **Tree** tabs. You can change the display of this last column to EBCDIC format. Hex values will be interpreted as EBCDIC characters.

To change the representation, select **View > Data Inspector > Show EBCDIC character set**. Select **View > Data Inspector > Show ASCII character set** to return the display to ASCII characters.

Find/Filter/Hide in Dword View

Quick Find/Filter/Hide operations can be performed in Dword view, although they are more limited than the Quick/Find/Filter/Hide operations available from the main spreadsheet display. Only **Field** or **Fixed hex** options are available in Dword view. See “Quick Find” on page 236 for more information on using Quick Find/Filter/Hide. Activating the Quick Find/Filter/Hide dialog for Dword view is the same as main event view. Double-click a row in the Dword view and the Quick Find/Filter/Hide dialog will appear with contents matching the row.

A filter or hide operation from the main spreadsheet does not affect the Dword display. All Dwords within the trace remain in the display when a filter/hide operation is performed. Conversely, a filter or hide operation from the Dword spreadsheet does not affect the main spreadsheet display. All events within the trace remain in the main spreadsheet display when a DWORD filter/hide operation is performed. For example, if you hide OOBs in the main event view, the Dword view will continue to show OOBs.

Words in a frame are treated as just hex values when using Find/Filter/Hide in the Dword view. If you double-clicks on an SOAF in the Dword view and filters for the SOAF then all hex values matching the SOAF will be selected when the filter is applied rather than showing all frames that match with an SOAF.

Filtering can also be performed on the Dword view by setting up a port group to limit the number of ports that will display. See “Setup Port Groupings” on page 231 for more information on setting up and using port groups.

Show Frame Word Offset

When this context menu option is selected, a three-digit decimal word offset is shown at the beginning of each Dword view line belonging to a frame.

LaneView

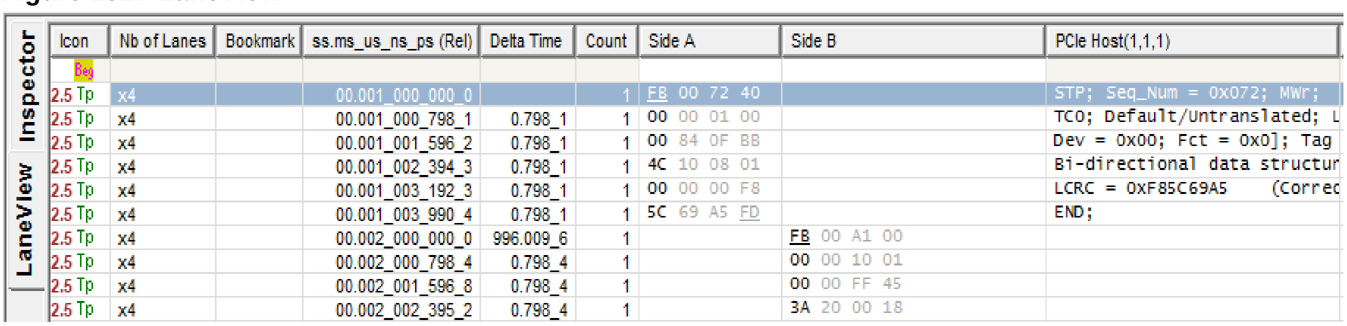
LaneView is visible only for PCIe traces. This tab displays one byte per row per lane. It shows the data by lanes, and there is a column that shows how many lanes are in the trace. LaneView always shows the data column wide enough to show contents for x8 traffic. LaneView displays decodes corresponding to the selected column for ordered sets. Decodes for ordered sets are displayed only on the row on which K character occurs for the selected lane. Contents of the selected column will be highlighted and other columns are grayed out. Lane view displays D chars, K chars, electrical idles, no data, and code violations. Gen2 Unknown OS events are shown in LaneView instead of Inspector because the **Inspector** view is not able to decode misaligned lane events.

To synchronize LaneView and the TraceView main event grid, click the **Sync Scroll Grids** button in TraceView's toolbar. Use this button to toggle between synchronizing the grids and having the grids scroll independently.

Several options are available for the display of a data column in LaneView. Right-click a data column header, and select the type of display. Data can be displayed in **10 Bit Data**, **KChar**, **Scrambled Data, Hex,** or **ASCII** format. You can insert a column if you need to display the data in two or more formats within the grid. See "Insert New Column" on page 305 for information on inserting a new column in LaneView.

You can enlarge or reduce the size of the font in the LaneView by using the  and  zoom buttons.

Figure 151: LaneView



LaneView has some of the same capabilities as the main spreadsheet view. You can insert or delete columns, and you can set the type of display for some columns. For example, in the timestamp field you can set the time as **Calendar Time**, **Time Relative to Capture**, or **Time Relative to Event** by clicking the right mouse on the column. Bookmarks are supported within LaneView. There is a bookmark column in which you can enter a bookmark name. See "Working With Columns" on page 292 for more information on column functions. See "Bookmarks" on page 247 for more information on using bookmarks.

Show EBCDIC/ASCII Representations

By default, the hexadecimal values of each word are also shown, interpreted as ASCII characters. The ASCII characters display in the last column of the **General** and **Tree** tabs. You can change the display of this last column to EBCDIC format. Hex values will be interpreted as EBCDIC characters.

To change the representation, select **View > Data Inspector > Show EBCDIC character set**. Select **View > Data Inspector > Show ASCII character set** to return the display to ASCII characters.

Find/Filter/Hide in LaneView

Quick Find/Filter/Hide operations can be performed in LaneView, although they are more limited than the Quick/Find/Filter/Hide operations available from the main spreadsheet display because it can only search on the information of a single row. When an event spans multiple rows, like a packet, it is not possible to search for a specific field of the packet. You must use the main event view instead. LaneView allows searching for K chars and sync bits in one lane, in any lane, or in all lanes. LaneView also allows you to search on the "Event Type", "Ordered Set" or "Non-OS" type when all the lanes are synchronized together. This view also supports several other fields, like "Count", "Port, and "Errors/Warnings".

Only **Field** or **Fixed hex** options are available in LaneView. See “Quick Find” on page 236 for more information on using Quick Find/Filter/Hide. Activating the Quick Find/Filter/Hide dialog for LaneView is the same as main event view. Double-click a row in the LaneView and the Quick Find/Filter/Hide dialog will appear with contents matching the row.

A filter or hide operation from the main spreadsheet does not affect the LaneView display. All Dwords within the trace remain in the display when a filter/hide operation is performed. Conversely, a filter or hide operation from the Dword spreadsheet does not affect the main spreadsheet display. All events within the trace remain in the main spreadsheet display when a DWORD filter/hide operation is performed.

Words in a frame are treated as just hex values when using Find/Filter/Hide in LaneView.

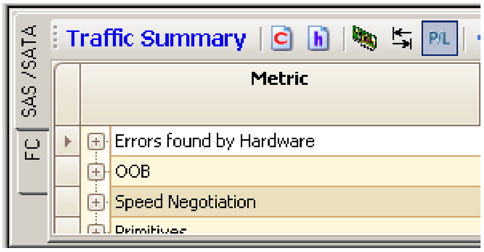
Filtering can also be performed in LaneView by setting up a port group to limit the number of ports that will display. See “Setup Port Groupings” on page 231 for more information on setting up and using port groups.

Show Frame Word Offset

When this context menu option is selected, a three-digit decimal word offset is shown at the beginning of each LaneView line belonging to a frame.

Using the Traffic Summary Pane

The Traffic Summary pane shows metrics of errors, OOB events, speed negotiation events, primitives, ordered sets, and frames in a hierarchy. There is one Traffic Summary panel per physical layer protocol. If a trace contains Traffic Summary data for more than one protocol, the panel will contain a tab for each protocol.



For each panel, you can expand or collapse the tree to see the counts at different levels of granularity. For each of the metrics, the count for each port is shown in a separate column.

Traffic Summary data is generated on the blade when the trace is captured. The Traffic Summary data remains in the hardware as long as the trace data remains in the hardware. When you extract a subsection of the trace, the relevant traffic summary data is also extracted. Only traces captured using Xgig Analyzer 4.3 or higher for SAS/SATA and 4.5 or higher for Fibre Channel will contain the Traffic Summary data. If the trace does not have Traffic Summary data, the Traffic Summary pane will not display and the **Traffic Summary** option in the **View** menu will be grayed out. Traffic Summary data capture is supported for 6G and 12G SAS/SATA traffic and for Fibre Channel traffic captured on an 8G Xgig blade, a 16G Xgig5000 blade, or 16G ports on Xgig1000 systems.

You can select a cell in the metrics grid and use the toolbar controls to navigate to any occurrence of that event. You can also go to any arbitrary occurrence just by typing the number of the occurrence in the toolbar. When you navigate to an event, both the main decode grid and the Dword grid will be scrolled to the point of time at which that event occurred.

Use the **Show Pane** option from the **View > Traffic Summary** menu to show/hide the Traffic Summary pane.

Two examples of the TraceView main window are shown below. Figure 152 shows a SAS/SATA trace. See "Traffic Summary SAS/SATA Counters" on page 342 for a description of Traffic Summary SAS/SATA metrics. Figure 153 shows a Fibre Channel trace. See "Traffic Summary Fibre Channel Counters" on page 355 for a description of Fibre Channel Traffic Summary metrics.

Figure 152: Traffic Summary Example for SAS/SATA

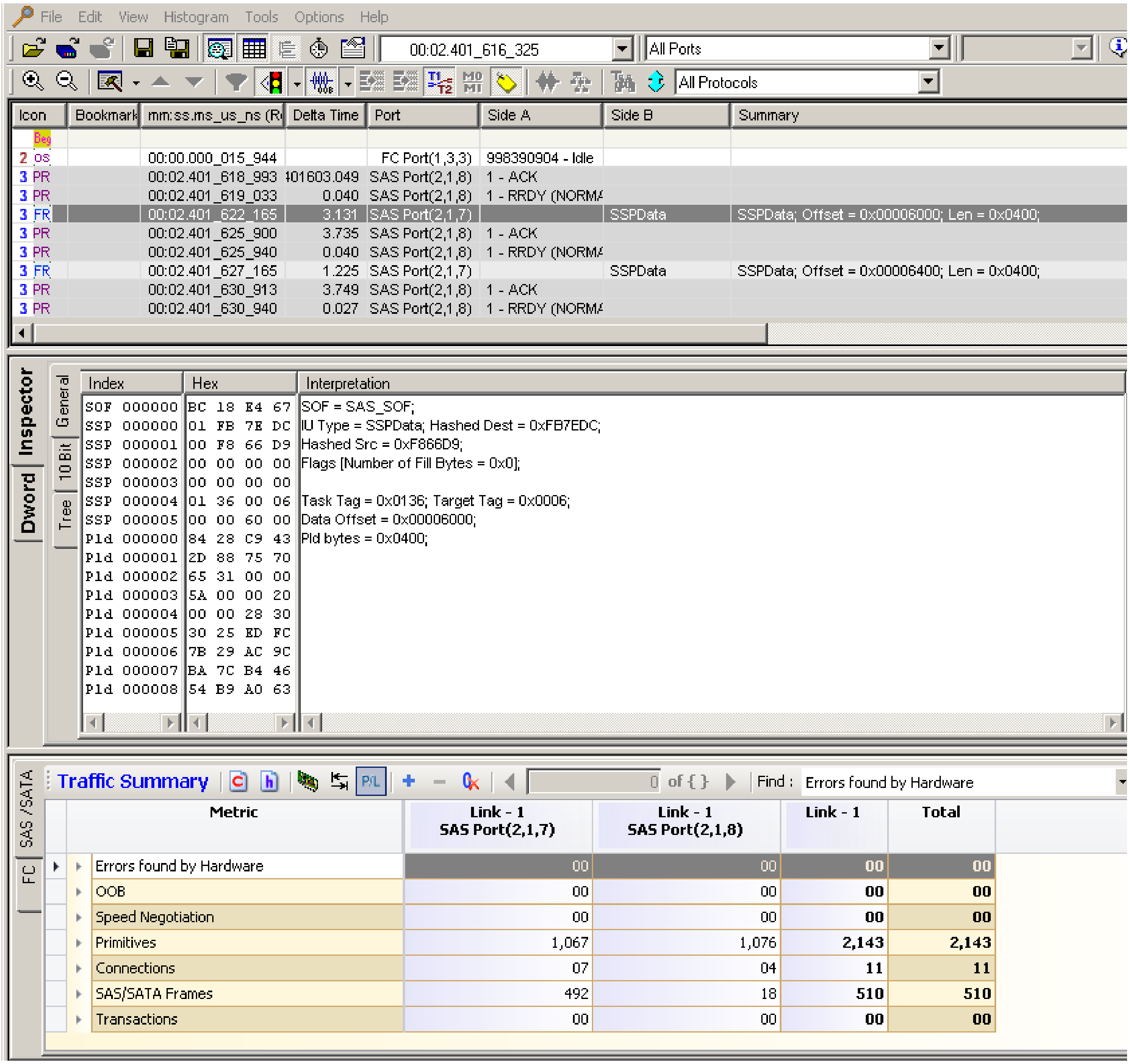
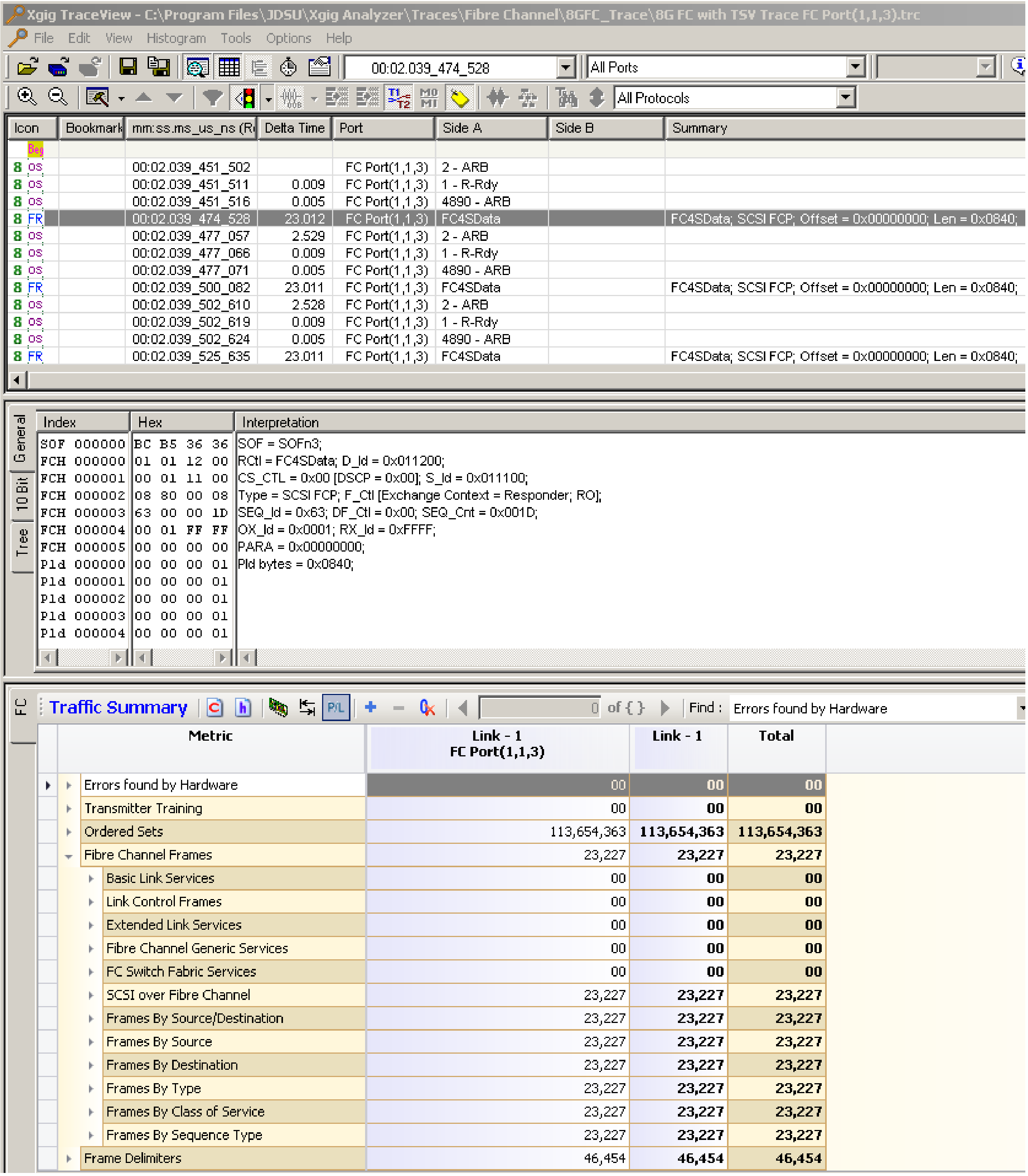


Figure 153: Traffic Summary Example for Fibre Channel



Traffic Summary Toolbar, Buttons, and Menus

Figure 154 shows the toolbar and Figure 155 shows the menu items available when you select

Traffic Summary from the **View** menu of TraceView. Select **Show Pane** from the **Traffic Summary** menu to show the Traffic Summary pane. See Table 28 for a description of all controls.

Figure 154: Traffic Summary Toolbar

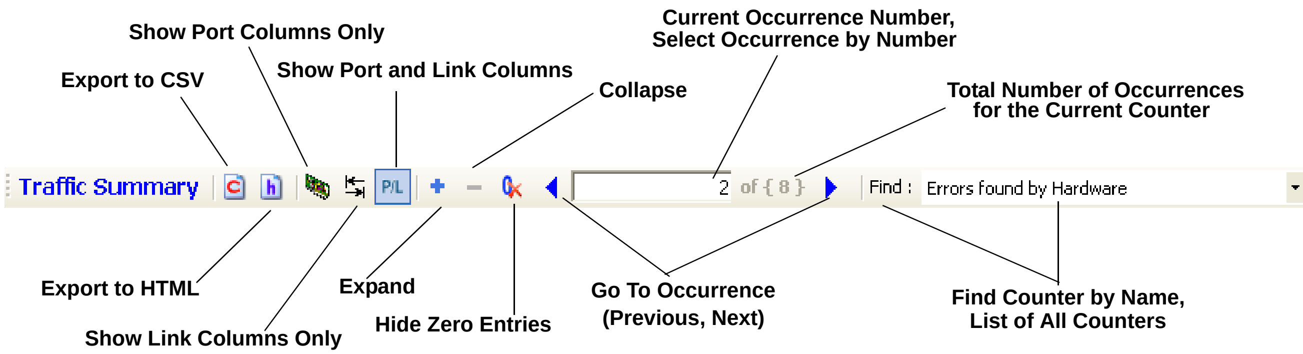


Figure 155: Traffic Summary Menu Options

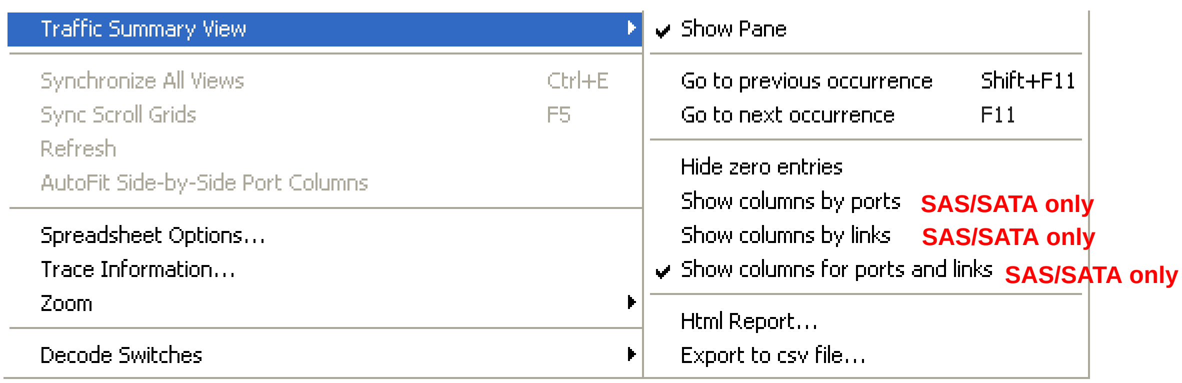


Table 28: Button and Menu Item Controls for Traffic Summary Pane

Button	Menu Item	Description
	Export to csv file	Produces a Traffic Statistic Summary as a Comma Separated Value (.csv) file. This report contains all possible metrics and columns. CSV files can be imported to Microsoft Excel.
	HTML Report	Produces a Traffic Statistic Summary as an HTML report. The report contains all possible metrics and columns. Links are available in the report to review metrics that are either up or down within the metric hierarchy.
	Show columns by ports	Controls the columns displayed for all metrics. Show columns by ports will show the counts by port only. For example, **Link -1 SAS Port(1,1,1)** and **Link -1 SAS Port(1,1,2)**.
	Show columns by links	Controls the columns displayed for all metrics. Show columns by links will show the counts by link only. For example, **Link -1**.
	Show columns for ports and links	Controls the columns displayed for all metrics. Show columns by ports and links will show the counts by both ports and links. For example, **Link -1 SAS Port(1,1,1)**, **Link -1 SAS Port(1,1,2)** and **Link -1**.

Table 28: Button and Menu Item Controls for Traffic Summary Pane (continued)

		Show all the sub-categories of metrics that are displayed for this type of metric. If there are no branches in the tree for the currently selected metric or the branches are already displayed, the button is grayed out.
		Hide all the sub-categories of metrics that are displayed for this type of metric. If there are no branches in the tree for the currently selected metric or the branches are not displayed, the button is grayed out.
	Hide zero entries	Show/hide all metrics that have a value of zero.
	Go to previous occurrence Shift +F11 Go to next occurrence F11	These controls allow you to go to the previous (back arrow, Shift +F11) and next (forward arrow, F11) occurrence of the event. If the value of the metric is zero or navigation is not allowed, the buttons and menu items are grayed out. If the current location is the first/last occurrence, the back/forward button and previous/next menu item are grayed out. The selection box in the toolbar, called the Event Number box, allows you to select the number of the occurrence for the currently selected metric and syncs the main grid to that location in the trace. The total number of occurrences is indicated after the Event Number box, and this maximum value changes based on the number of occurrences for the current metric. To enter a value, place the cursor in the field, type in the value, and press Enter. If the value of the metric is zero or navigation is not allowed for this counter, the selection field is grayed out. See "Navigating to Events Using Traffic Summary Counters" on page 340 for more information on navigation.
		The **Find:** field lists all Traffic Summary counters in alphabetical order. If you know the name of the counter, select the counter name from the list in the pull-down box and press Enter. The row containing the selected counter is displayed and highlighted.

Navigating to Events Using Traffic Summary Counters

As described in Table 28, "Button and Menu Item Controls for Traffic Summary Pane," on page 339, there are several different ways of navigating to an event. To start navigating, first make sure you have selected a cell (counter) within the Traffic Summary display. The valid events to navigate to are always bounded by 1 as the first event and by the count value as listed in the Traffic Summary pane for the counter. The current number of the event is displayed in a box in the toolbar, called the Event Number box, between the triangle-shaped arrow buttons; the total number of events is indicated with the text "**of {nn}**" where nn is the total number of events.

If a counter value is zero, the navigation features are disabled. If you enter a value in the box that is greater than the counter value, you will go to the last occurrence of the event.

Navigating to Events With No Repeat Counts

For events that do not have repeat counts, such as frames, the events for the counter are numbered consecutively as they are discovered in the trace, and you can navigate to each numbered event by using the triangle-shaped arrow buttons in the toolbar, shortcut keys (Shift +F11 and F11), or by entering the event number in the box between the forward and back arrow buttons. Many primitive events are also numbered and listed in this way.

Navigating to Events With Repeat Counts

In TraceView, some events that can repeat consecutively many times in a trace are displayed as a single event with a repeat count. The display in Traffic Summary view is slightly different for events that have repeat counts. See Table 29 for a list of these events. For these events, each occurrence represents a range (a number of repeated events greater than one). For example, if the primitive event repeats 55 times, then the second value that you can navigate to is the numbered event 56, which is the start of another series of that event with a different location in the trace. All events are counted, but for navigation you can only go to the start or end numbers for repeated primitives.

When navigating using “next occurrence” or “previous occurrence” controls, the count numbers displayed are slightly different depending on the direction you are navigating. Since each consecutive occurrence represents a range, you will go to the event corresponding to number at the top of the range when navigating down (next occurrence) and you will go to the event corresponding to the number at the bottom of the range when navigating up (previous occurrence). The simplified example below shows how navigation and event numbers in the Event Number box change based on the direction of navigation.

Assume that the counter value for a primitive is 100, and there are four distinct occurrences of the repeated primitive within the trace. The first occurrence repeats 10 times (range 1-10), the next 20 times (range 11-30), the next 30 times (range 31-60), and the last 40 times (range 61-100). The Event Number box will display 1 when you initially select the counter, and the sequence of numbers as you navigate down are 1, 11, 31, and 61. When you navigate using next occurrence, the Event Number box will show 11, and the current location is the start of the next occurrence of the primitive with a repeat count. Navigating again using next occurrence, the Event Number box will show 31. If you enter a numeric value for navigation greater than or equal to the counter value (100), you will go to the last occurrence. If you enter a numeric value for navigation less than or equal to the counter value (100), you will go to the first event that starts the occurrence. For example, if you enter 55 you will go to the third occurrence of the repeated primitive, which in this example starts at count 31.

When you reach the end of the number of occurrences and reverse the direction of navigation, the navigation numbers and the exact location that navigation takes you to will change. When navigating up, the next number is now the highest value in the range. Using the same example, when you navigate up (previous occurrence) the sequence is as follows: 61, 60, 30, and 10. You can therefore navigate to the beginning or end of each repeated primitive sequence, depending on whether you start from the top or the bottom of the list of occurrences.

Table 29: Primitive and Other Events with Repeat Counts

SAS/SATA Primitive Events	SAS/SATA Primitive Events	SAS/SATA Primitive Events	Other Events
ACK	NOTIFY	SAS_SOAF	Code or Disparity Error
AIP	OPEN_ACCEPT	SAS_SOF	Framing Error
ALIGN	OPEN_REJECT	SATA_CONT	Loss of Sync
CREDIT_BLOCKED	SAS_EOAF	SATA_DMAT	Primitive Error
DONE	SAS_EOF	SATA_EOF	Multiplexing Alignment Error
MUX	SAS_ERROR	SATA_ERROR	Fibre Channel Ordered Set
NAK	SAS_RRDY	SATA_SOF	

Traffic Summary SAS/SATA Counters

The major categories of metrics in Traffic Summary are summarized below.

- **Errors found by Hardware**
  This category includes all errors found by the Xgig hardware, including any connection conflicts.
- **OOB**
  This category includes metrics for all OOB events except Speed Negotiation events.
- **Speed Negotiation**
  This category includes metrics for all Speed Negotiation events.
- **Primitives**
  This category includes metrics for all primitives within SMP, SSP, or STP connections, as well as all SAS/SATA primitives that are not connection-oriented.
- **Connections**
  This category includes connection counts. Counts are categorized, based on the open protocol, as SSP, STP, or SMP connections. The counts are further categorized as accepted or rejected connections, and rejected connections are categorized by type.
- **SAS/SATA Frames**
  This category includes metrics for all SAS/SATA frames. This includes Address Frames, SSP, STP, and SMP frames (request and response), all SATA frames, as well as counts of unknown frames for each type.
- **Transactions**
  This category counts SATA/SSP/ATAPI Exchanges based on the request size.

Traffic Summary SAS/SATA Error Counters

The following table describes the error counters found by the hardware that are counted in the Traffic Summary pane.

Table 30: Traffic Summary SAS/SATA Error Counters

Error Counter	Description
Errors Found by Hardware	A summary count of all errors below. If multiple errors occur on a single event, it is only counted once by this counter.
Code or Disparity Error	Counts all occurrences where a code violation or disparity error is detected by the hardware.
CRC Error	Counts all CRC errors.
Framing Error	Counts all occurrences where a frame is abnormally terminated or an EOF is found outside of a frame.
Loss of Sync	Counts all occurrences where there is a Loss of Sync or Loss of Signal.
Primitive Error	Counts all occurrences where a Dword is detected that has a K character but is not a standard primitive.
Primitive Sequence Error	Counts all occurrences where a Primitive Sequence is malformed.
Connection Conflict	Counts open collisions when both channels see OPEN address frames at the same time.
Multiplexing Alignment Error	Increments when a multiplexing alignment error occurs. These errors can occur only when the signal through the port contains two logical channels. Every other Dword on the physical port must belong to a single logical channel.

Traffic Summary SAS/SATA OOB Counters

The following table describes the SAS/SATA OOB counters within the Traffic Summary pane of TraceView. TraceView uses timing values and other criterion to determine events reported for speed negotiation using OOB signals.

Table 31: Traffic Summary SAS/SATA OOB Counters

OOB Counters	Description
Valid COM Events	
COMINIT/ COMRESET	This counter increments when the timing of the first, second, third, and fourth D.C. idle time of a received COMINIT/ COMRESET OOB signal is within the range 255 to 465 ns.
COMSAS	This counter increments when the timing of the first, second, third, and fourth D.C. idle time of a received COMSAS OOB signal is within the range 700 to 1525 ns.
COMWAKE	This counter increments when the timing of the first, second, third, and fourth D.C. idle time of a received COMWAKE OOB signal is within the range 70 to 160 ns.
SATA Port Selection OOB	This counter increments when a SATA Port Selection OOB signal is detected.
Invalid COM Events	
COMINIT/ COMRESET (incorrect timing)	This counter increments when the timing of the second or third or fourth D.C. idle time of a received COMINIT/ COMRESET OOB signal is not within the range specified in 255 to 465 ns.
COMSAS (incorrect timing)	This counter increments when the timing of the second or third or fourth D.C. idle time of a received COMSAS OOB signal is not within the range 700 to 1525 ns.
COMWAKE (incorrect timing)	This counter increments when the timing of the second or third or fourth D.C. idle time of a received COMWAKE OOB signal is not within the range 70 to 160 ns.

Traffic Summary SAS/SATA Speed Negotiation Counters

The following table describes the SAS/SATA Speed Negotiation counters within the Traffic Summary pane of TraceView. TraceView uses timing values and other criterion to determine events reported for speed negotiation using OOB signals.

Table 32: Traffic Summary SAS/SATA Speed Negotiation Counters

Speed Negotiation Counters	Description
Valid Speed Negotiation	
Valid SNW-1	This counter increments when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 1.5 Gbps during SNW-1 window of the SAS speed negotiation sequence.
Valid SNW-2	This counter increments when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
Valid SNW-3	This counter increments when the analyzer receives one or more SAS-2 SNW-3 phy capabilities bits transmitted as COMWAKE OOB signals during SNW-3 window of the SAS speed negotiation sequence.
Valid Final-SNW (1.5 Gbps)	This counter increments when a Final-SNW event at 1.5 Gbps is detected. A valid Final-SNW event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 1.5 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Valid Final-SNW (3.0 Gbps)	This counter increments when a Final-SNW event at 3.0Gbps is detected. A valid Final-SNW event is set when the analyzer receives ALIGN(1) primitives from both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Valid Train SNW	This counter increments when any Valid Train SNW event is detected, regardless of the speed or parameters set for the speed negotiation.
ATT (Actual Training time) within spec	This counter increments when an ATT within spec event is detected. An ATT within spec event is set when the measured value of ATT is within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
RCDT (Rate Change Delay Time) within spec	This counter increments when an RDCT within spec event is detected. A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a SAS speed negotiation window time. An RDCT within spec event is set when the measured RCDT value lies within this range: 492.5 us < RCDT < 507.5 us.
SNTT (Speed Negotiation Transmit time) within spec	This counter increments when an SNTT within spec event is detected. A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. An SNTT within spec event is set when the measured SNTT time lies within this range: 102.5 us < SNTT < 117.5 us
SATA 1.5 Gbps speed detected	This counter increments when ALIGN(0) primitives are detected from host and drive at 1.5 Gbps on a SATA link.
SATA 3.0 Gbps speed detected	This counter increments when ALIGN(0) primitives are detected from host and drive at 3.0 Gbps on a SATA link.
SATA 6.0 Gbps speed detected	This counter increments when ALIGN(0) primitives are detected from host and drive at 6.0 Gbps on a SATA link.

Table 32: Traffic Summary SAS/SATA Speed Negotiation Counters

Speed Negotiation Counters	Description
Invalid Speed Negotiation	
Invalid SNW-1	This counter increments when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 1.5 Gbps during SNW-1 window of the SAS speed negotiation sequence.
Invalid SNW-2	This counter increments when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps during SNW-2 window of the SAS speed negotiation sequence.
Invalid SNW-3	This counter increments when the analyzer receives no SAS-2 SNW-3 phy capabilities bits during SNW-3 window of the SAS speed negotiation sequence.
Invalid Final-SNW (1.5 Gbps)	This counter increments when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 1.5 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Invalid Final-SNW (3.0 Gbps)	This counter increments when the analyzer does not receive ALIGN(1) primitives from one or both ends of a SAS link at 3.0 Gbps rate during Final-SNW window of the SAS speed negotiation sequence.
Invalid Train-SNW	This counter increments when any Invalid Train-SNW event is detected, regardless of the speed or parameters set for the speed negotiation.
ATT (Actual Training time) outside spec	This counter increments when an ATT outside spec event is detected. The event is set when the measured value of ATT is not within TLT (Training Lock Time) which is defined to be 28497920 OOBI or ~ 18.998613 ms.
RCDT (Rate Change Delay Time) outside spec	This counter increments when an RDCT outside spec event is detected. A SAS device shall send D.C Idle for 750000 OOBI (nominal value = 500 us) during the RCDT phase of a speed negotiation window time. The event is set when the measured RCDT time falls within this range RCDT time <= 492.5 us or RCDT time >= 507.5 us.
SNTT (Speed Negotiation Transmit time) outside spec	This counter increments when an SNTT outside spec event is detected. A SAS device shall send ALIGN(0) or ALIGN(1) for 163840 OOBI (nominal value = 109.2 us) during the SNTT phase of a SAS speed negotiation window time. The event is set when the measured SNTT time <= 102.5 us or SNTT time >= 117.5 us.
SATA speed negotiation failed	This event is set when speed negotiation is not successful on a SATA link.
Phy Reset	
SAS Phy Reset	The counter increments when the physical link is reset.

Traffic Summary SAS/SATA Primitive Counters

All SAS/SATA primitive sequences will only be counted once per sequence. Refer to the CurrentProtocolVersions.txt document in the installation directory for information on the SAS/SATA spec. The three primary types of metrics as follows:

- **Primitives Outside Connections**
  These are all primitives that are outside of established SSP, SMP, or STP connections, such as ALIGNs, OPEN_ACCEPTs, and CLOSEs.
- **Primitives Inside SSP/SMP Connection**
  Serial SCSI Protocol (SSP) is the foundation for supporting SAS disk drives.Serial Management Protocol (SMP) is the foundation for managing SAS Expanders. These metrics count the SAS primitives within SSP or SMP connections, such as RRDY, DONE, and NAK.
- **Primitives Inside STP Connection**
  Serial Tunneling Protocol (STP) is the foundation for supporting SATA devices within SAS storage enclosure subsystems. These metrics count the SATA primitives within STP connections, such as SATA_R_RDY and SATA_HOLD.

When there are multiple primitives of the same type, for example ALIGNs, there is a metric in the hierarchy that counts all primitives of that type. In this case, they are ALIGN(0), ALIGN(1), ALIGN(2), ALIGN(3). Counters that break out the metric into the specific primitives are listed under the primitive type.

In SAS/SATA traces, if the analyzer does not capture the beginning of a Primitive Sequence then that sequence will not be included in the Traffic Summary Counters. If you are not sure if a sequence is being counted, look for a beginning of a sequence icon in the DWord View. If none are marked as such then the sequence will not be included in the Traffic Summary counters.

Traffic Summary SAS/SATA Connection Counters

SAS/SATA Connection counters provide a count of all successful connections by counting OPEN_ACCEPT primitives. Connection counters also provide counts of all failed attempts to establish connections by counting all forms of the OPEN_REJECT primitive. Each OPEN_ACCEPT or OPEN_REJECT is categorized as belonging to the STP, SMP, or STP protocol based the Connection Protocol Type field found in the associated OPEN_ADDRESS frame. The metrics are listed by protocol as follows:

- **SSP Connections**
  Serial SCSI Protocol (SSP) is the foundation protocol for supporting SAS disk drives. Counters include Accepted Connections and all types of Rejected Connections.
- **SMP Connections**
  Serial Management Protocol (SMP) is the foundation protocol for managing SAS Expanders. Counters include Accepted Connections and all types of Rejected Connections.
- **STP Connections**
  Serial Tunneling Protocol (STP) is the foundation protocol for supporting SATA devices within SAS storage enclosure subsystems. Counters include Accepted Connections and all types of Rejected Connections.

Traffic Summary SAS/SATA Frame Counters

TraceView counts various SAS/SATA frames.The frame counter metrics are divided into the categories as described in the SAS/SATA spec. Refer to the CurrentProtocolVersions.txt document in the installation directory for information. Details for counters in each category are provided in the following sections.

- **Address Frames**
  Address frames are indicated by counting identify or open events. Open events are broken down by protocol and by source/destination address.
- **SSP Frames**
  Serial SCSI Protocol (SSP) is the foundation protocol for supporting SAS disk drives. Counters include SSP Data, XRdy, Command, Response, Task Management, Vendor Specific, and Reserved frame types. Individual types of SSP Responses and Task Management frames are broken down into separate counters, including counters for specific SSP response codes.
- **SMP Frames**
  SMP request and response frames are counted by each type of request or response.
- **SATA Frames**
  Counters include all types of SATA frames. Counters are included for all types of SATA errors as indicated by the SATA error bits. Note that frames be counted more than once within the FIS error counters if they have more than one error bit set.

Unknown Counters for SAS/SATA Frames

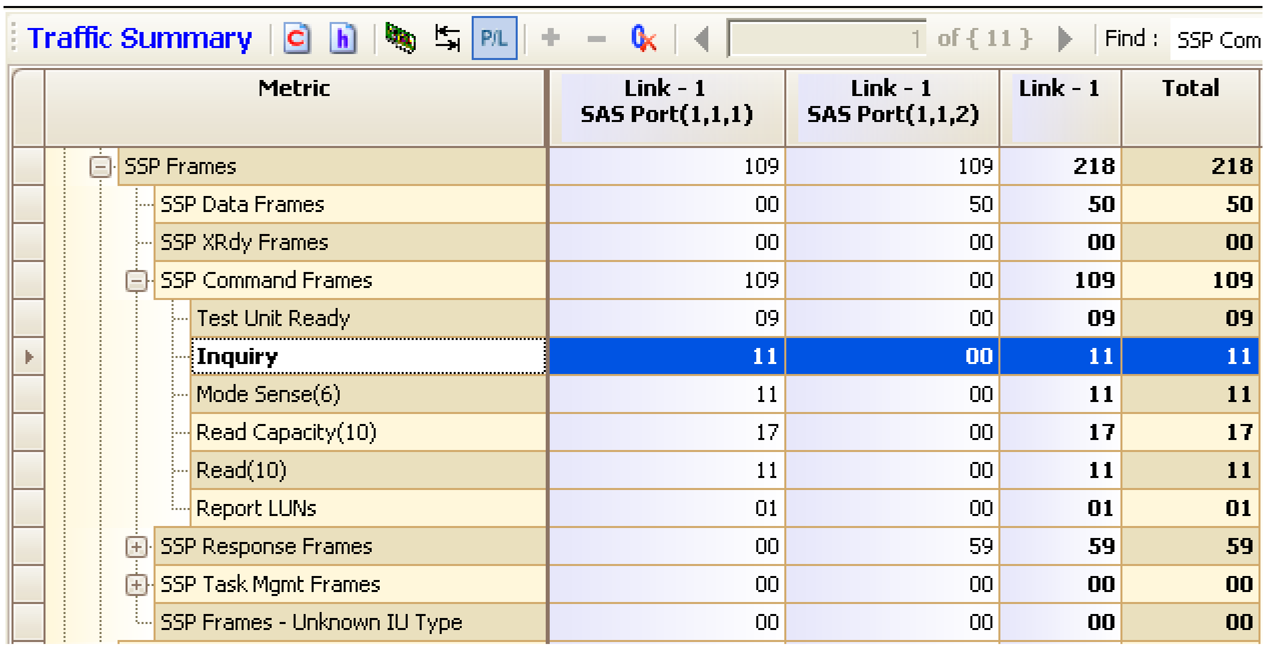
Where appropriate, there are counters for unknown frames types or unknown responses. Unknown counters count all frames that can be recognized as belonging to a general category, but cannot be counted in any of the other specific categories. For frame types this includes frames that are invalid, obsolete, reserved, or vendor-specific. Unknown counters are incremented based on how much information can be gathered from the decode. For example, if a frame is recognized as an SSP-type frame but its sub-type is not recognized (Data, XRdy, Command, Response, or Task Management), it is counted in the **SSP Frames - Unknown IU Type** counter. However, if the frame is recognized as a SSP Task Management frame, yet the specific Task Management function is unrecognized, it is counted in **Unknown Task Mgmt Function** counter. This counter is shown in the lower level of the tree under **SSP Task Mgmt Frames**.

Dynamic Counters for SAS/SATA Command Frames

Frame counters for commands are dynamic, meaning frame counters are added for different command types. The primary counter for the type of frame is always counted and displayed, but the specific command counters only appear if a frame with a specific SCSI command is encountered in the decode. For each type of frame, a breakdown of the commands are counted in the added dynamic counter(s) in a sub-level of the Traffic Summary hierarchy. The primary counter is always the total of all dynamic counters that are within its branch in the hierarchy. Dynamic counters are added for two types of frame counters, the SSP counter **SSP Command Frames** and the SATA counter **Reg: Host -> Dev Command FIS**.

See Figure 156 for an example of dynamic command frame counters. In the example, the decode encountered six different types of SSP command frames. No other SSP command frames events were encountered in the decode. Therefore, these six types of SSP command frames are listed and counted within **SSP Command Frames**.

Figure 156: Example of Dynamic Command Frame Counters



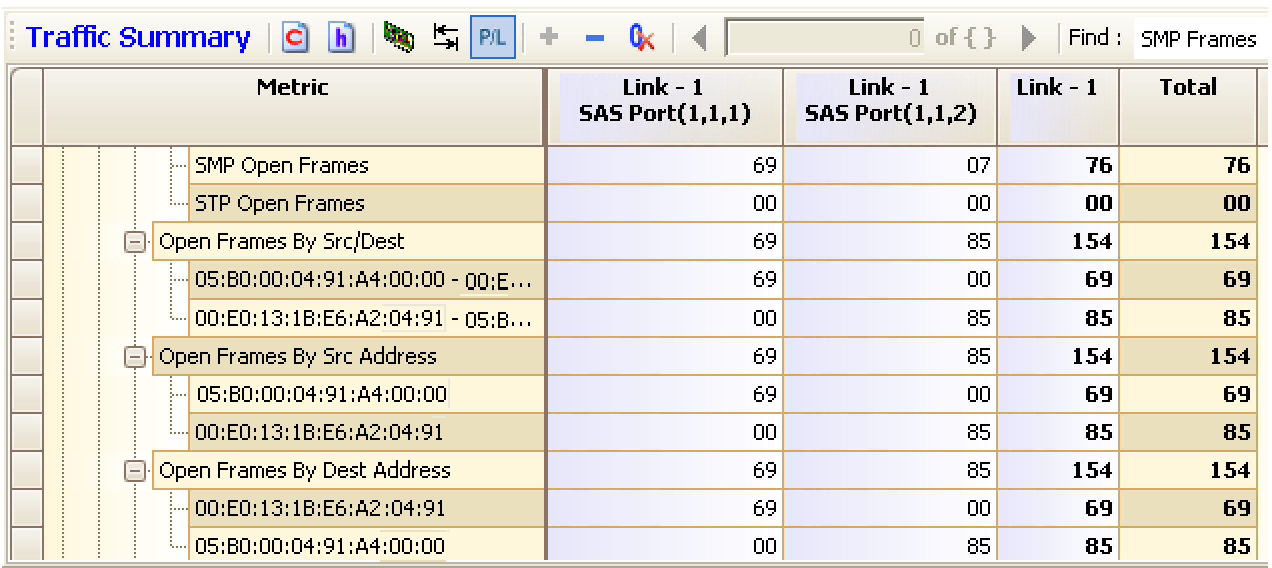
Metric	Link - 1 SAS Port(1,1,1)	Link - 1 SAS Port(1,1,2)	Link - 1	Total
SSP Frames	109	109	218	218
SSP Data Frames	00	50	50	50
SSP XRdy Frames	00	00	00	00
SSP Command Frames	109	00	109	109
Test Unit Ready	09	00	09	09
Inquiry	11	00	11	11
Mode Sense(6)	11	00	11	11
Read Capacity(10)	17	00	17	17
Read(10)	11	00	11	11
Report LUNs	01	00	01	01
SSP Response Frames	00	59	59	59
SSP Task Mgmt Frames	00	00	00	00
SSP Frames - Unknown IU Type	00	00	00	00

Dynamic Counters for SAS/SATA Source and Destination Addresses

Address counters for source/destination addresses are dynamic, meaning counters are added for each source address, destination address, or source/destination address-pair encountered in the decode. The primary counter (for example, **Open Frames by Src Address**) is always counted and displayed, but the sub-level counters of specific addresses only appear if an open frame with a specific address or address-pair is encountered in the decode. This provides a count of open frames by each address or address-pair. The primary counter is always the total of all dynamic counters that are within its branch in the hierarchy.

The figure below shows an example of the open frame address counters displayed when addresses and address-pairs are found in the decode. In the example only a single conversation is represented. The list of source and destination addresses could be very long if many conversations are encountered.

Figure 157: Example of Dynamic Address Counters



Metric	Link - 1 SAS Port(1,1,1)	Link - 1 SAS Port(1,1,2)	Link - 1	Total
SMP Open Frames	69	07	76	76
STP Open Frames	00	00	00	00
Open Frames By Src/Dest	69	85	154	154
05:B0:00:04:91:A4:00:00 - 00:E...	69	00	69	69
00:E0:13:1B:E6:A2:04:91 - 05:B...	00	85	85	85
Open Frames By Src Address	69	85	154	154
05:B0:00:04:91:A4:00:00	69	00	69	69
00:E0:13:1B:E6:A2:04:91	00	85	85	85
Open Frames By Dest Address	69	85	154	154
00:E0:13:1B:E6:A2:04:91	69	00	69	69
05:B0:00:04:91:A4:00:00	00	85	85	85

Address Frame Counters

Table 33: Traffic Summary Frame Address Counters

Frame Address Counters	Event Description
Address Frames	Counts all Open Address and Identify SOAF Frames.
Identify Frames	Counts Identify SOAF frames.
Open Frames	Total count of the three open frame counters described below.
SSP Open Frames	Counts Open Address SOAF frames for the SSP protocol.
SMP Open Frames	Counts Open Address SOAF frames for the SMP protocol.
STP Open Frames	Counts Open Address SOAF frames for the STP protocol.
Open Frames by Src/Dest	Counts all Open Address SOAF frames that have a source and destination address. Expand the tree under this counter for counts by specific source-destination address pairs.
Open Frames by Src Address	Counts all Open Address SOAF frames that have a source address. Expand the tree under this counter for counts by specific source address.
Open Frames by Dest Address	Counts all Open Address SOAF frames that have a destination address. Expand the tree under this counter for counts by specific destination address.
Address Frames - Unknown	Counts all occurrences where an Open Address or Identify frame is invalid, obsolete, reserved, or vendor specific.

SSP Frame Counters

SSP frame counters include SSP Data, XRdy, Command, Response, Task Management, and Unknown frame types. Individual types of SSP Responses and Task Management frames are broken down into separate counters, including counters for specific SSP response codes.

SMP Frame Counters

SMP request and response frames are counted by each type of request or response. Unknown SMP requests and responses are also counted. SATA Frame Counters

Counters include all types of SATA frames. Counters are included for all types of SATA errors as indicated by the SATA error bits. Note that frames can be counted more than once within the FIS error counters if they have more than one error bit set.

Traffic Summary SAS/SATA Transaction Counters

SAS/SATA Transaction counters provide a count of all SSP/ATAPI/SATA transactions by counting all SSP/ATAPI/SATA events with request sizes. The transaction counters include all the Read/Write commands for SSP/ATAPI/SATA; counters are added based on each unique request size.

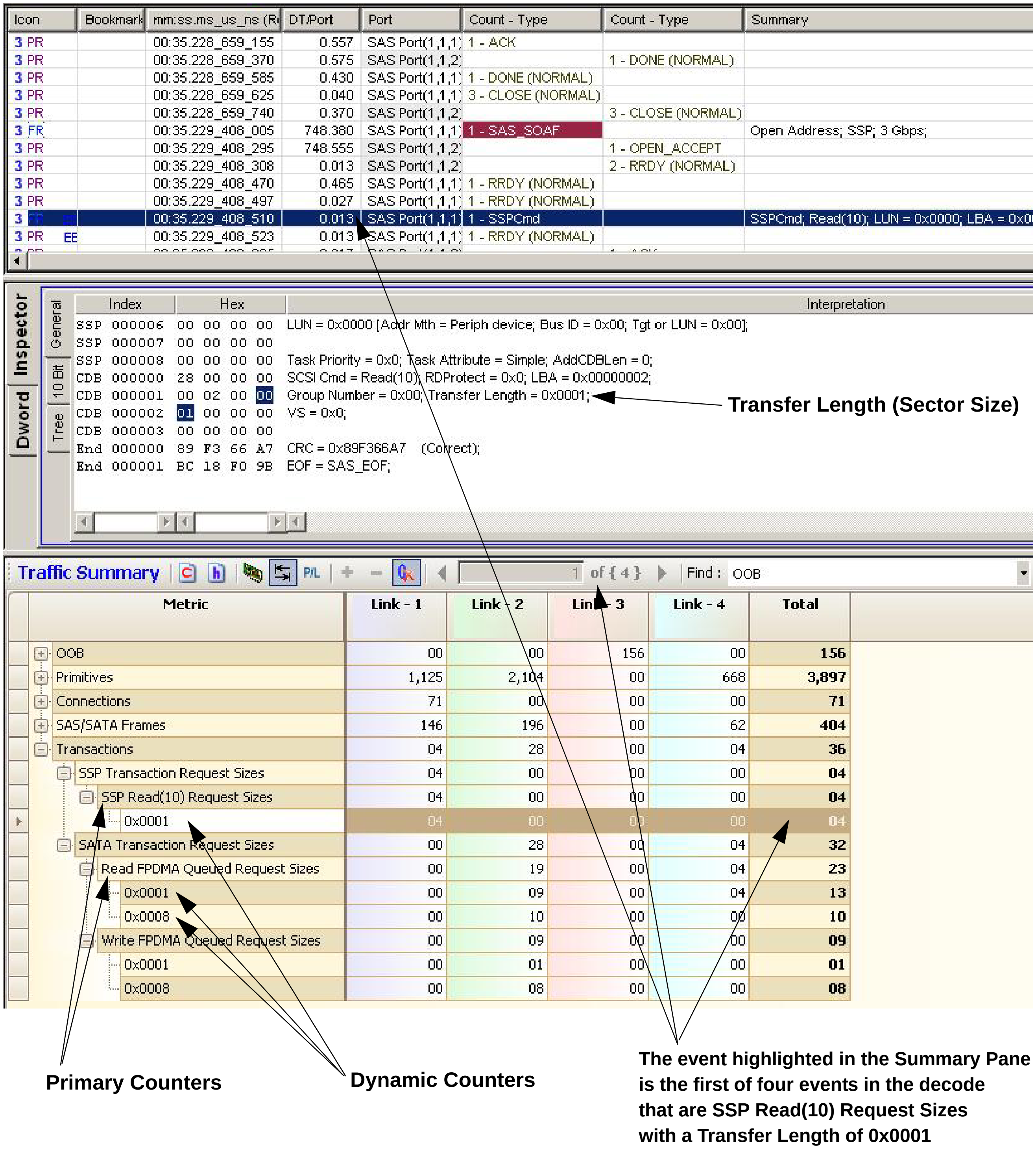
The metrics are listed by protocol as follows:

- **SSP Transaction Request Sizes**
  Serial SCSI Protocol (SSP) is the foundation protocol for supporting SAS disk drives. Counters include all types of request size events for read, write, and write and verify. See the T10 committee web site, http://www.t10.org/drafts.htm, for up to date SSP specifications. Refer to the CurrentProtocolVersions.txt document in the installation directory for information on the SAS/SATA specification.
- **ATAPI Transaction Request Sizes**
  AT Attachment with Packet Interface (ATAPI) is the older standard interface used to connect storage devices such as hard disks, solid-state drives, and CD-ROM drives inside personal computers. Counters include all types request size events for read, write, and write and verify. See the T13 committee web site, http://www.t13.org/, for up to date ATAPI specifications. Refer to the CurrentProtocolVersions.txt document in the installation directory for information on the SAS/SATA specification.
- **SATA Transaction Request Sizes**
  Counters include all types of SATA request size events for both read and write. See the T13 committee web site, http://www.serialata.org/, for up to date SATA specifications. Refer to the CurrentProtocolVersions.txt document in the installation directory for information on the SAS/SATA specification.

Transaction counters are dynamic, meaning transaction counters are added for different request sizes. The primary counter for the type of frame is always counted and displayed, but the sub-level counters of request sizes only appear if a frame with a specific request size is encountered in the decode. For each type of frame, a breakdown of the request sizes are counted in the added dynamic counter(s) in a sub-level of the Traffic Summary hierarchy. The primary counter is always the total of all dynamic counters that are within its branch in the hierarchy.

See Figure 158 for an example of dynamic transaction counters based on request size. In the example, the decode encountered **SSP Read(10) Request Sizes** with a Transfer Length of 0x0001. No other events of this type with a different Transfer Length were found, so therefore only one dynamic counter (**0x0001**) is added in the sub-level for that counter. The first event of this type is currently selected and highlighted in the decode. For the counter **Read FPDMA Queued Request Sizes**, two dynamic counters were added, **0x0001** and **0x0008**. This is because requests of this type were encountered with two different transfer lengths. Note that the values for the sub-level counters (**0x0001** = 13 and **0x0008** = 10) add up to the count for the primary counter (**Read FPDMA Queued Request Sizes** = 23).

Figure 158: Transaction Request Size Dynamic Counters



Traffic Summary Fibre Channel Counters

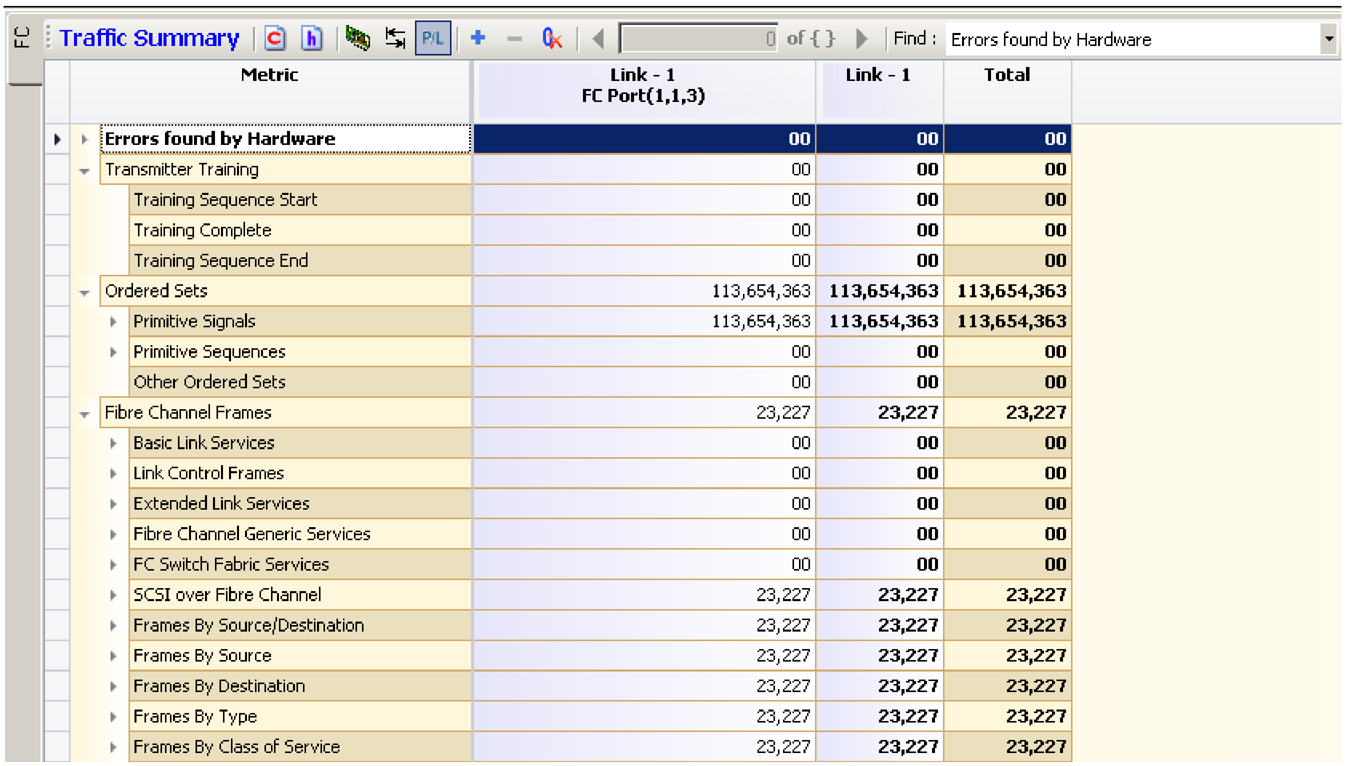
The major categories of metrics in Traffic Summary are summarized below.

- **Errors found by Hardware**
  This category includes all errors found by the Xgig hardware.
- **Ordered Sets**
  This category includes metrics for all primitive signals, primitive sequences, and unknown Ordered Sets.
- **Fibre Channel Frames**
  This category includes metrics for all Fibre Channel frames. This includes Basic Link Services, Link Control Frames, Extended Link Services, Fibre Channel, FC Switch, SCSI over Fibre Channel, and Frames by source/destination, type, class of service, and sequence type.
- **Frame Delimiters**
  This category includes metrics for start of frame (SOF) and end of frame (EOF) ordered sets.
- **Training Transmission**

  This category includes metrics for 16G FC training frames.

An example of the Traffic Summary pane with FC traffic is shown below.

Figure 159: Traffic Summary Pane with FC Traffic



Metric	Link - 1 FC Port(1,1,3)	Link - 1	Total
Errors found by Hardware	00	00	00
Transmitter Training	00	00	00
Training Sequence Start	00	00	00
Training Complete	00	00	00
Training Sequence End	00	00	00
Ordered Sets	113,654,363	113,654,363	113,654,363
Primitive Signals	113,654,363	113,654,363	113,654,363
Primitive Sequences	00	00	00
Other Ordered Sets	00	00	00
Fibre Channel Frames	23,227	23,227	23,227
Basic Link Services	00	00	00
Link Control Frames	00	00	00
Extended Link Services	00	00	00
Fibre Channel Generic Services	00	00	00
FC Switch Fabric Services	00	00	00
SCSI over Fibre Channel	23,227	23,227	23,227
Frames By Source/Destination	23,227	23,227	23,227
Frames By Source	23,227	23,227	23,227
Frames By Destination	23,227	23,227	23,227
Frames By Type	23,227	23,227	23,227
Frames By Class of Service	23,227	23,227	23,227

Traffic Summary FC Error Counters

The following table describes the FC error counters found by the hardware that are counted in the Traffic Summary pane.

Table 34: Traffic Summary FC Error Counters

Error Counter	Description
Errors Found by Hardware	A summary count of all errors below. If multiple errors occur on a single event, they are counted multiple times by this counter.
Code or Disparity Error	Counts all occurrences where a code violation or disparity error is detected by the hardware.
CRC Error	Counts all CRC errors.
Loss of Sync	Counts all occurrences where there is a Loss of Sync or Loss of Signal.
Sync Error	Counts all 66B Sync Errors
O Code Error	Counts all 66B O Code Errors
Block Type Error	Counts all 66B Block Type Errors
Control Char Error	Counts all 66B Control Char Errors
Reserved Bit Error	Counts all 66B Reserved Bit Errors

Traffic Summary FC Ordered Set Counters

- The following figures show the Ordered Set counters within the Traffic Summary pane of TraceView. Refer to the CurrentProtocolVersions.txt document in the installation directory for information on the Fibre Channel specification.

Ordered Sets are divided into three groups, Primitive Signals, Primitive Sequences, and Unknown Ordered Sets.

- **Primitives Signals**
  This metric contains one counter for each Primitive Signal as defined in T11/1861D draft for Fibre Channel.
- **Primitives Sequences**
  This metric contains one counter for each Primitive Sequence as defined in T11/1861D draft for Fibre Channel.
- **Unknown Ordered Sets**
  This metric contains one counter for all unknowns primitives starting with a K character.

  When there are multiple primitives of the same type, for example ARB, there is a metric in the hierarchy that counts all primitives of that type. In this case, they are ARB(FF), ARB(x,y), ARB(AL_PA). Counters that break out the metric into the specific primitives are listed under the primitive type.

Traffic Summary FC Frame Counters

TraceView counts various Fibre Channel frames. The frame counter metrics are divided into the categories summarized below. Details for counters in each category are provided in the following sections.

The Traffic Summary for Fibre Channel provides counters for various metrics. Specifically, Traffic Summary provides the following counters for each of the Fibre Channel frames.

- **Basic Link Services**
  one counter per request, accept, and reject reason
- **Link Control Frames**
  one counter per link control frame
- **Extended Link Services**
  one counter per request, accept, and reject reason
- **Fibre Channel Generic Services**
  one counter per request, accept, and reject reason
- **FC Switch Fabric Services**
  one counter per request, accept, and reject reason
- **SCSI over Fibre Channel**
  - **SCSI Commands**
    one counter per 8-bit SCSI opcode
  - **SCSI Task Management**
    one counter per SCSI Task Management IU
  - **SCSI Responses**
    - SCSI Status
      one counter per SCSI status
    - SCSI Response Codes
      one counter per FCP response code
  - **FCP_CONF Frames**
    FCP_CONF frames
- **Frames by Source/Destination**

  up to 126 pairs of S_Id - D_Id values
- **Frames by Type**
  256 counters for all possible 8-bit Fibre Channel Header Type values defining payload type
- **Frames by Class of Service**
  five counters for SOF class
- **Frames by Sequence Type**
  four counters for SOF type

Frame Delimiters

This metric contains one counter for each Start of Frame (SOF) and one for each End of Frame (EOF).

Dynamic Counters for SCSI Command Frames

Some commands, such as SCSI commands, are dynamic. Frame counters for commands are dynamic, meaning frame counters are added for different command types. The primary counter for the type of frame is always counted and displayed, but the specific command counters only appear if a frame with a specific SCSI command is encountered in the trace. A breakdown of the commands is added to the dynamic counter(s) in a sub-level of the Traffic Summary hierarchy. The primary counter is always the total of all dynamic counters that are within its branch in the hierarchy. Dynamic counters are added for the SCSI over Fibre Channel counter **SCSI Commands**.

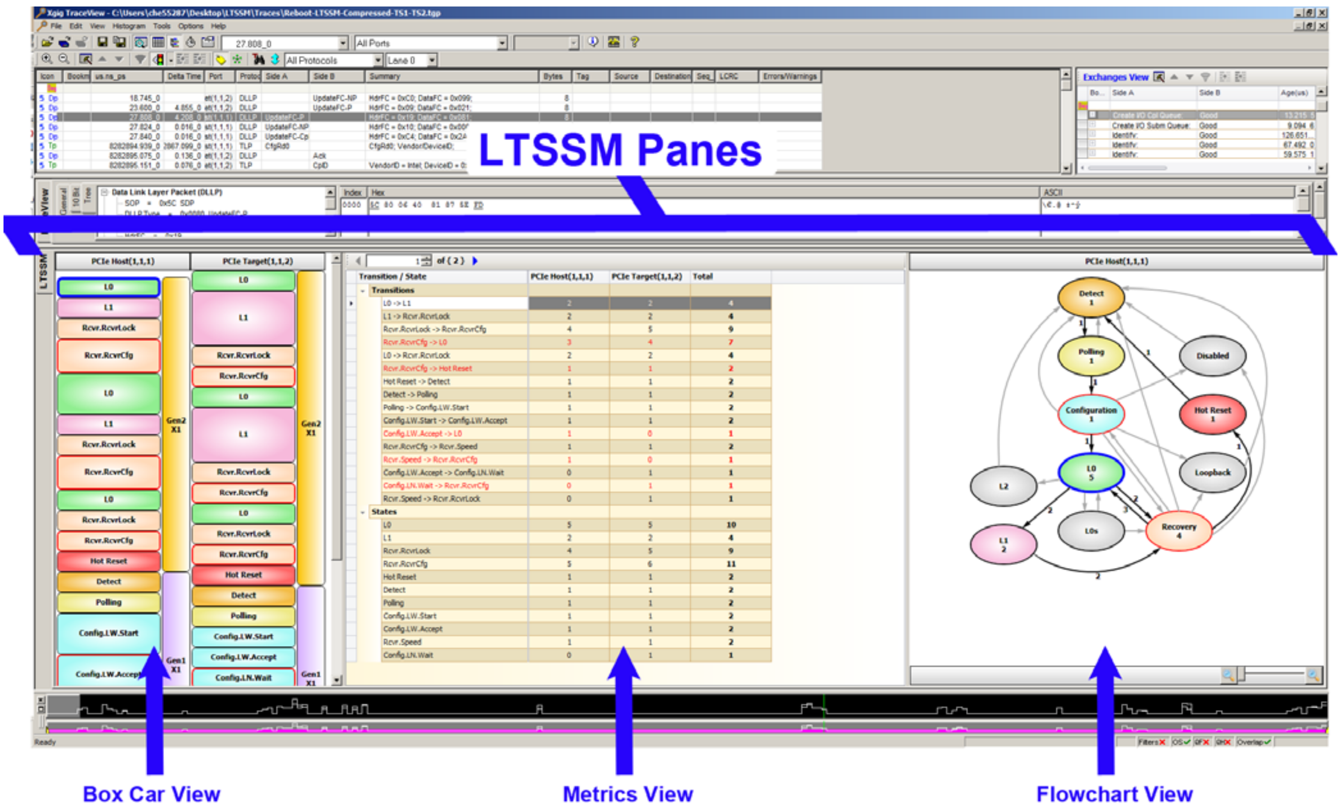
Dynamic Counters for Source and Destination Addresses

Counters for source/destination addresses are dynamic, meaning counters are added for each source address, destination address, or source/destination address-pair encountered in the trace. The primary counter (for example, **Frames by Source**) is always counted and displayed, but the sub-level counters of specific addresses only appear a frame with a specific address or address-pair is encountered in the decode. This provides a count of frames by each address or address-pair. The primary counter is always the total of all dynamic counters that are within its branch in the hierarchy.

Using the LTSSM Panes for PCIe

The LTSSM panes consists of three separate LTSSM views that display the PCIe handshake meta-data. The three separate LTSSM views are the Box Car view, the Metrics view, and the Flowchart view. These views interact with one another and also with the event view and the Lane View (page 334) to display the handshake between the host and the target.

Figure 160: LTSSM Views



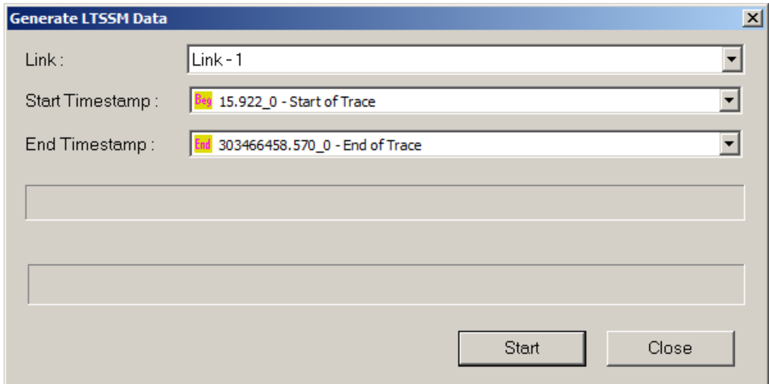
The port/link names are shown in the view headings. When you edit the port/link name aliases, LTSSM reflects the new names for the column headings.

Caution: LTSSM debugging gets the best results when all of the data is captured and data is not filtered before it is processed. To capture the best results, use the Xgig TraceControl configuration file named “PCXIe_Capture LTSSM and All Errors.tcc”. Refer to “Loading a Configuration” on page 78 for instructions on loading a configuration file.

Generating LTSSM Data

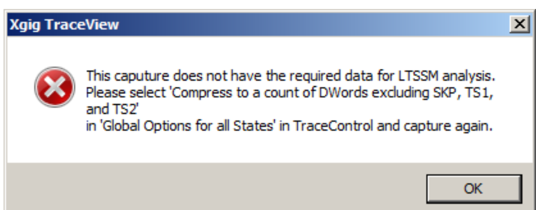
When a new capture is opened in TraceView, LTSSM data is not generated until you select **Generate LTSSM Data...** from the **File** menu to open the **Generate LTSSM Data** dialog box. This dialog box is displayed to allow you to select the link, and the starting and ending times. Click the **Start** button to start generating the LTSSM data.

Figure 161: Generate LTSSM Data Dialog Box



When you click the **Start** button, filter settings used for the capture are validated. If the settings are not correct an error dialog is displayed describing which filter setting to use in TraceControl to recapture the trace. The LTSSM generation will not be allowed to proceed until the recapture is performed using the correct filter setting.

Figure 162: Error Message

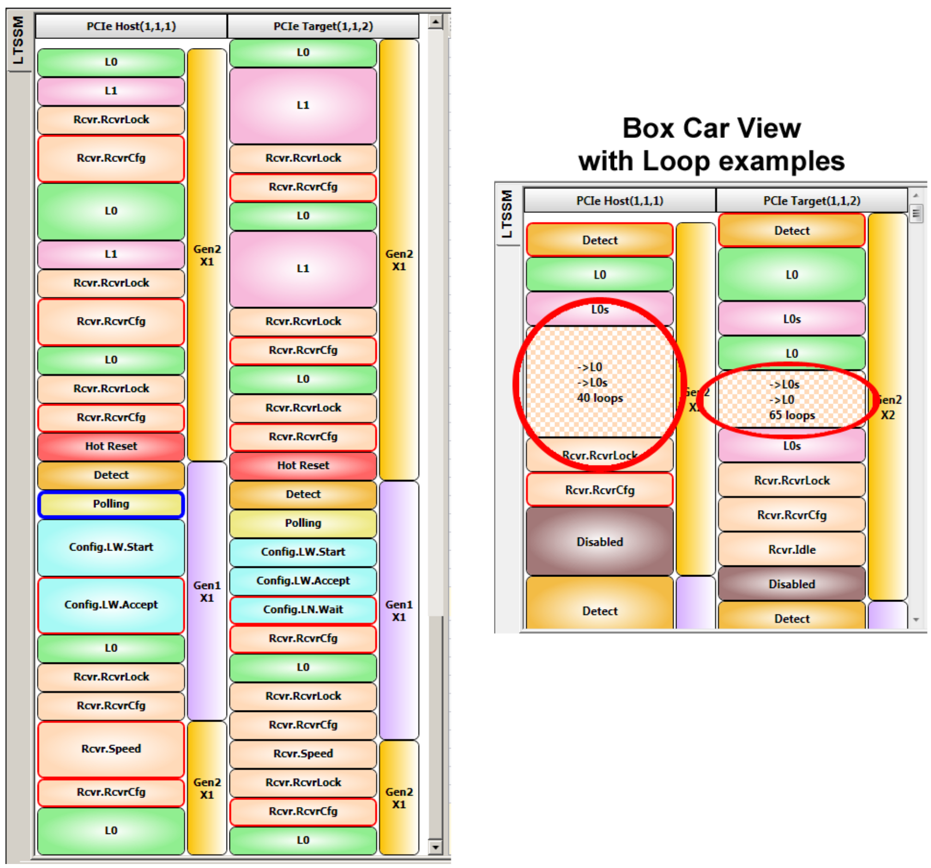


If the filter settings are valid LTSSM engine will start processing the trace in the background a progress dialog is displayed.

Box Car View

The Box Car view has a column for each side of the link – one for uplink and another for downlink. Each column has two sub-columns that show LTSSM states and sub-states, and the link speed (Gen1, Gen2, and Gen3) with the corresponding lane widths (X4 for example reflects 4 traffic lanes.) All the states in a column are shown in chronological order but their height is not proportional to the time duration of each state. If a sequence is visited repeatedly, it is displayed as a single bubble showing the states visited and the number of loops.

Figure 163: Box Car View



When you click on a state in box car view, it will be highlighted. Its corresponding state in flowchart view will also be highlighted. The first event corresponding to the beginning of the state will be highlighted in event grid and lane view grid. If a state's transition to the next state is invalid according to protocol specification, a red border will be displayed around the state. You can mouse over the states that have a red border to display a tooltip describing its invalid transition.

Also clicking the link speed with the lane width highlights the corresponding event in Event view and Lane view which caused the speed and lane width change.

In the example shown on the right side of Figure 163, the highlighted bubbles show transitions that are caught in a loop between two or more states. The states between which the loop is occurring and the number of loops that occurred are displayed in the bubble. In this case (the red circle and red oval), the looping is between L0 and L0s states and there are 40 loops in the PCIe Host column and 65 loops in the PCIe Target column.

Metrics View

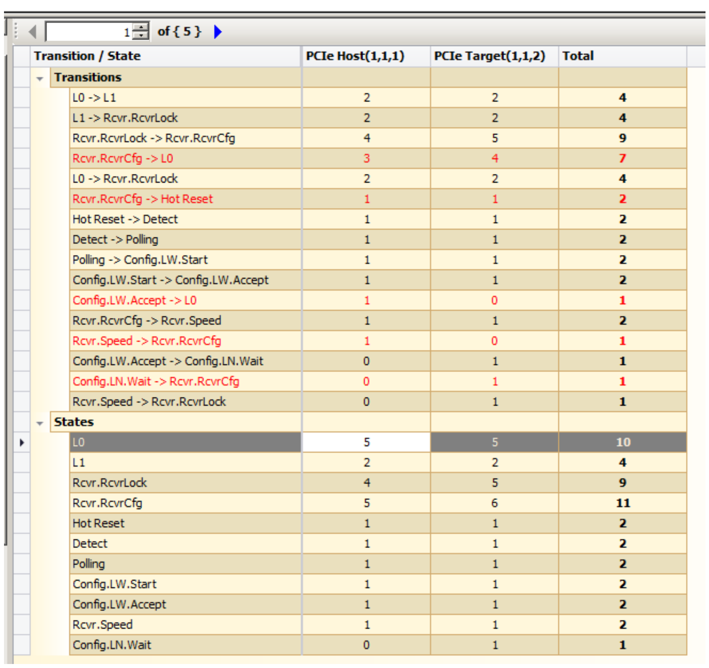
The Metrics view (shown in Figure 164) displays all the transitions and states that have occurred in the trace in a tree list. The two root nodes ‘Transitions’ and ‘States’ have specific children under them which can be used for navigation. Each child node (transition/state) has a count for each side (uplink and downlink) and also an aggregated count. Invalid transitions are displayed with red text.

You can click on a cell with a non-zero value to navigate to the first instance in both event grid and lane view. You can use previous/next buttons to navigate, or input a number in the Event Number box to navigate to a specific instance.

The selection box (at the top of the Metrics View) is called the Event Number box.

The Event Number box allows you to select the number of the occurrence for the currently selected metric and syncs the main grid and Lane view grid to that location in the trace. The total number of occurrences is indicated after the Event Number box, and this maximum value changes based on the number of occurrences for the current metric. To enter a value, place the cursor in the field, type in the value, and press Enter or just click the spinner to increase or decrease the value. If the value of the metric is zero or navigation is not allowed for this counter, the selection field is grayed out.

Figure 164: Metrics View



Transition / State	PCIe Host(1,1,1)	PCIe Target(1,1,2)	Total
Transitions			
L0 -> L1	2	2	4
L1 -> Rcvr.RcvrLock	2	2	4
Rcvr.RcvrLock -> Rcvr.RcvrCfg	4	5	9
Rcvr.RcvrCfg -> L0	3	4	7
L0 -> Rcvr.RcvrLock	2	2	4
Rcvr.RcvrCfg -> Hot Reset	1	1	2
Hot Reset -> Detect	1	1	2
Detect -> Polling	1	1	2
Polling -> Config.LW.Start	1	1	2
Config.LW.Start -> Config.LW.Accept	1	1	2
Config.LW.Accept -> L0	1	0	1
Rcvr.RcvrCfg -> Rcvr.Speed	1	1	2
Rcvr.Speed -> Rcvr.RcvrCfg	1	0	1
Config.LW.Accept -> Config.LN.Wait	0	1	1
Config.LN.Wait -> Rcvr.RcvrCfg	0	1	1
Rcvr.Speed -> Rcvr.RcvrLock	0	1	1
States			
L0	5	5	10
L1	2	2	4
Rcvr.RcvrLock	4	5	9
Rcvr.RcvrCfg	5	6	11
Hot Reset	1	1	2
Detect	1	1	2
Polling	1	1	2
Config.LW.Start	1	1	2
Config.LW.Accept	1	1	2
Rcvr.Speed	1	1	2
Config.LN.Wait	0	1	1

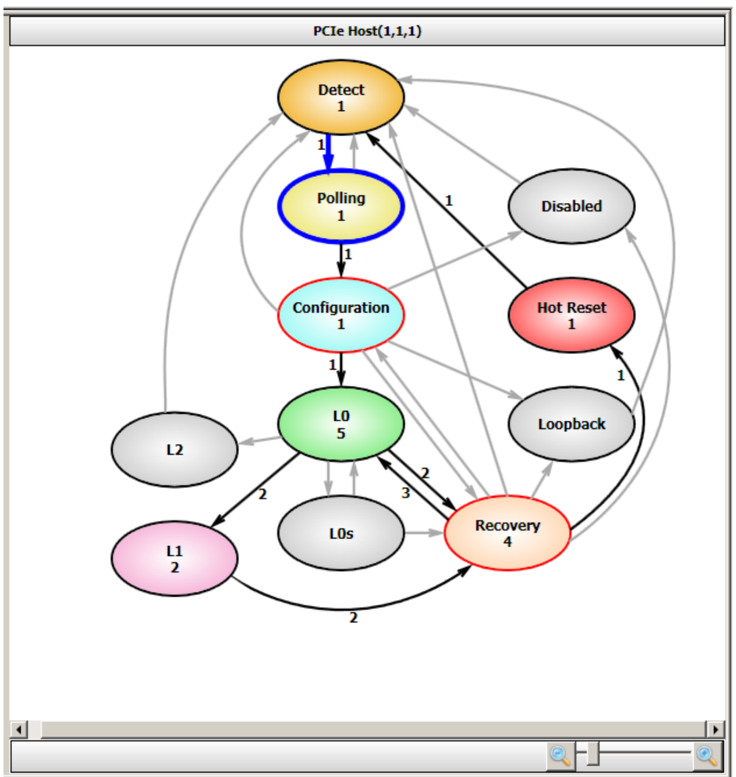
Flowchart View

The Flowchart shows various states possible and transitions between them. States and transitions found are visually differentiated from those that are not found in current trace. For example, states and transitions not found are grayed out. When a state is selected in the Box Car view, the corresponding state bubble is selected in the Flowchart view along with the state transition that caused the state change. Both the state and transition are identified by a thicker border/arrow. Similarly, when an event is selected in the main event grid, the state bubble corresponding to the selected event in the Flowchart view and state box in Box Car view are highlighted.

Invalid states are displayed with a red border. Counts are shown for each state or transition that is not grayed out.

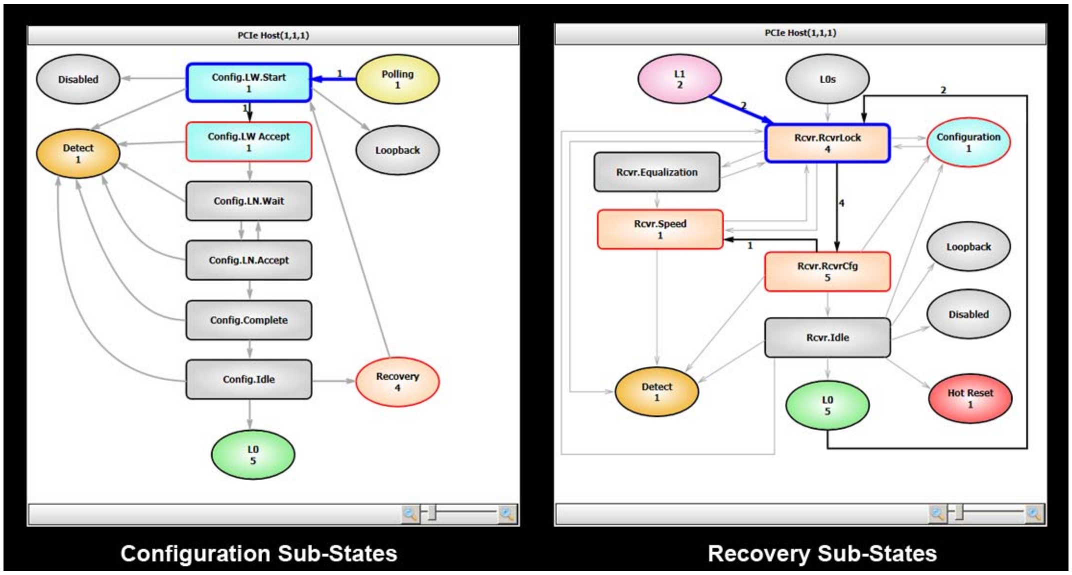
There are three different views for the Flowchart view. One is Overall view. In this view, all the main states are shown. When the selection in Box Car view is a main state, or the selected event in event grid corresponds to a main state, this Flowchart view is displayed.

Figure 165: Flowchart View (Overall View)



Some of the states, Configuration and Recovery, have sub-states. When selection in Box Car view is a sub-state, or a selected event in event grid corresponds to a sub-state, the Flowchart view shows one of the following diagrams. Transitions and states/sub-states are grayed out based on availability. These flowcharts are as described in PCIe specifications.

Figure 166: Flowchart View with Sub-States (Configuration & Recovery)



You can zoom in or out on the Flowchart using the zoom tool at the bottom of the Flowchart view. This tool allows you use the slider or step through the sizes using ‘Zoom In’ or ‘Zoom Out’ buttons..

Chapter 15

Xgig TraceView Histograms

In this chapter:

- Histogram Overview
- Histogram Controls

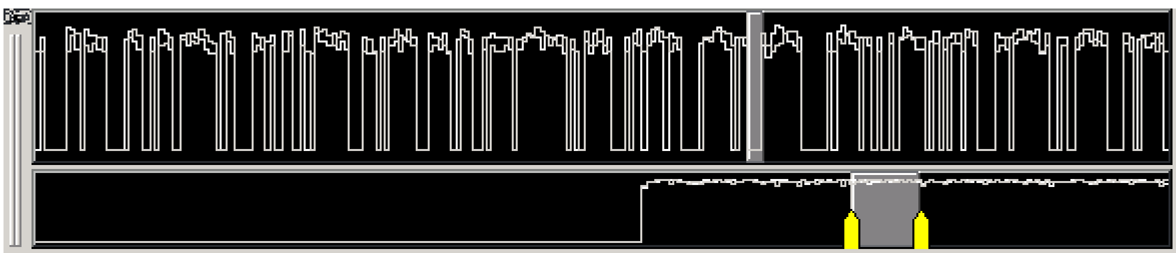
Histogram Overview

The histogram can graphically represent the entire trace from start to end. It also allows you to expand and collapse the view of the trace to look at a graphic display of a detailed portion of the trace. The histogram only represents the trace information for the ports currently selected. If you change the ports that are selected for the current view, the histogram changes to show the data for those ports only. The histogram display is divided into two areas:

- The upper part of the histogram shows a detail area of the trace. The gray area in the upper histogram corresponds to the events shown in the spreadsheet area (listing of events).
- The lower histogram represents the entire trace, or the extent of a trace you want to view. The gray area on the histogram corresponds to the detail area.

An example of the histogram area is show below.

Figure 167: Example Histogram Display



Using the Detail Area Histogram (upper histogram)

Drag the gray area to move around in the trace. The size of the gray area will change depending on how much of the trace is displayed in the listing of events. You can also navigate to an area of the trace by double-clicking on the location in time you want to display.

Using the Entire Trace Histogram (lower histogram)

The gray box on the lower histogram can be resized to zoom into a smaller area in the trace. This is reflected in the upper histogram.

The yellow extent marks can be moved to narrow the view of the trace. Click and drag with the mouse to move the extent marks. By narrowing the extent marks that narrow the gray box that defining the detail area, you can see a graphic display of a very small time slice in the trace in the upper histogram.

If you move the yellow start and/or end extent markers to select custom time extents, data displayed is intersection of user set time extents and time extents determined by the state of T1/T2 button. This is true for event grid, DWORD grid, Exchanges View, and TSV. Depending on custom time extents selected, it is possible for an exchange to be inside the time slice but for some of the frames within that exchange to be outside the time slice. If some of the frames under an expanded exchange fall outside the current time slice, Exchanges View will display place holder frames for each of the frames outside the time slice. An example of a decode for placeholder frames is “frame is clipped by current time extents”. Synchronization is disabled for the placeholder frames.

Histogram Controls

Histogram controls allow you to focus on a smaller area of the trace, change the appearance/scale of the graphs, and show or hide traces.

Upper Histogram Controls

- **Gray Area, Double-Arrow Mouse**
  When you pass the mouse over the gray area, the double-arrow mouse appears. Click and drag to change the time slice that will display in the spreadsheet area.

Lower Histogram Controls

- **Yellow Extent Marks**
  Click and drag the yellow extent mark on either side to decrease or increase the portion of trace data displayed.
- **Gray Area, Double-Arrow Mouse Icon**
  When you pass the mouse over the gray area, the double-arrow mouse appears. Click and drag to change the start of the time slice that will display in the upper histogram.
- **Left Arrow Mouse Icon**
  When you pass the mouse over the left edge of the gray area, the left arrow mouse appears. Click and drag to change the left extent of the detail area.
- **Right Arrow Mouse Icon**
  When you pass the mouse over the right edge of the gray area, the right arrow mouse appears. Click and drag to change the right extent of the detail area.

Right-Click (Either Histogram)

Right-clicking brings up a menu of display options for both histograms. Depending on the data, changing the settings can give you a better visual display or transition points and high/low values.

- **Line Graph or Stair Step (default)**
  A line graph smooths out visual transitions for low to high and high to low.
- **Independent Scale or Absolute Scale (default)**
  Independent scale can show larger visual differential between traces for some trace files.
- **Linear Scale or Logarithmic Scale (default)**
  Linear scale can show larger visual differential between high and low values than the logarithmic scale.

Chapter 16

Xgig TraceView Template Editor

In this chapter:

- Using Template Editor

Using Template Editor

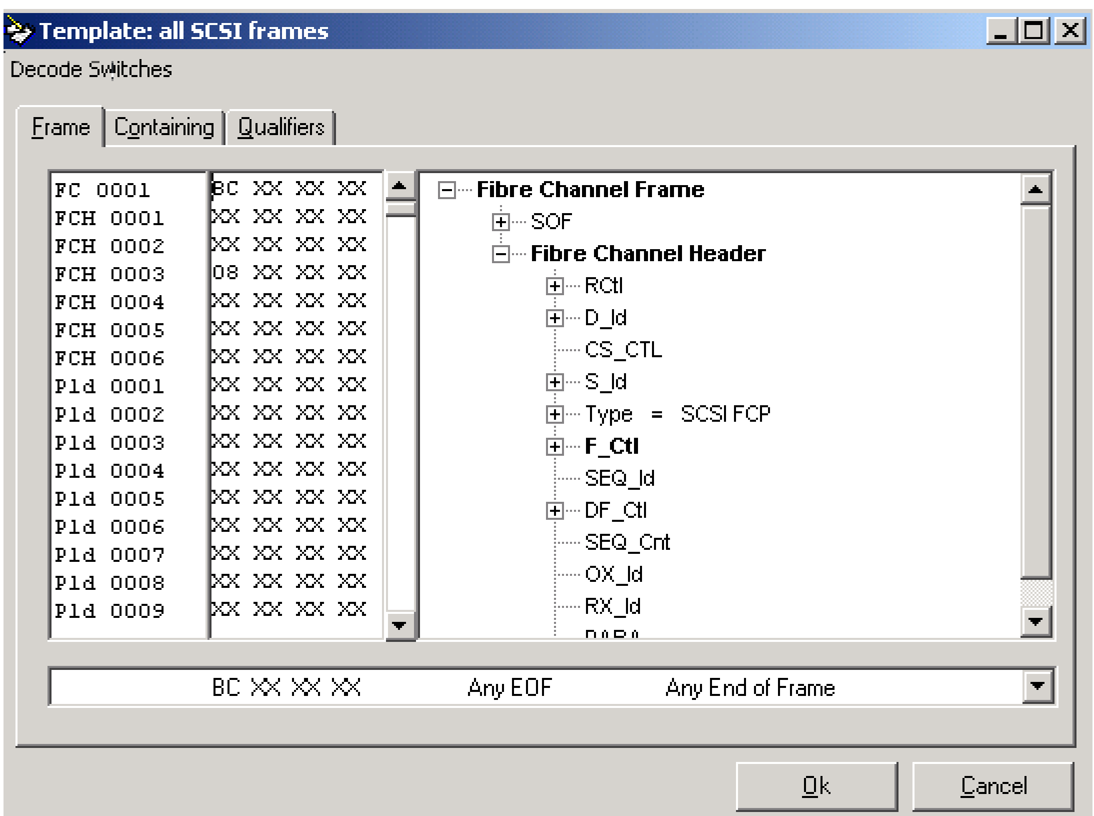
The **Template Editor** available from the Detailed Find/Filter/Color window allows you to customize your own templates. Customized templates can be created before or after drag-and-drop of an editable template to the **Filter**, **Find**, or **Color** tabs of the Detailed Find/Filter/Color window.

A custom template can be based on an error condition, a primitive, or a frame – any of the basic pre-defined template types available in Xgig TraceView.

The **Template Editor** dialog box appears when you double-click any editable template in the Detailed Find/Filter/Color window. The editor uses the template you have selected as the starting point for creating a new template. After you have made all your selections to create the new template, press **OK**. Give the template a unique name to avoid confusion. You can store your new template in any location in the **User Library**.

An example of the Template Editor dialog box is shown in Figure 168. The area on the left shows specific byte values in hexadecimal and the area to the right, called Tree View, shows a hierarchical tree of the fields within the frame.

Figure 168: Template Editor



Pre-Defined and User-Defined Templates

Two types of templates are available from the Available Templates Browser, pre-defined and user-defined templates. Pre-defined templates are found in the **Viavi Library** section, and user-defined templates are found in the **User Library** section. Pre-defined templates cannot be changed or deleted.

User-defined templates are created by the user. They can be identical to the pre-defined templates available in the Viavi Library. The **User Library** section can store the templates you use most often, identified by names you are familiar with.

You can define unique templates that are not available in the Viavi Library. User-defined templates are typically created using a pre-defined template as a starting point. Add the values, patterns, and qualifiers to create a unique template. Double-click any template in the **User Library** section to bring up the **Template Editor** to create and store user-defined templates. Once you have created and saved a user-defined template, you can always access it from the **User Library** area of the browser.

When you create a new template, it is strongly suggested that you copy the template and rename it. This prevents confusion resulting from changing the contents of a template without changing the name.

Making Edits to the Template

To create a user-defined template, edit the template values to change the match pattern. The types of changes you can make to create a new template are:

- **Frame Byte Contents**
  To change the byte contents of the template, select the desired field strings on the right, or enter hex and Xs on the left. You can either **replace** the existing values with those you have selected, or you can **insert** the new values in the location selected, thereby shifting the original value to the next field. Replace is the default function for editing frame byte contents. Pressing the **Insert** key on your keyboard before you type a new value invokes insert mode. To discontinue using the insert mode, press the **Insert** key again, and you will return to the replace mode.
- **Bit-Pattern Definitions**
  Bit level definitions are possible by double-clicking on a byte, which brings up the Binary Editor. Click the bit in the Binary Editor, type in the new value, and click **OK**.
- **Qualifiers (Qualifiers tab)**
  The **Qualifiers** tab allows you to filter specific ports, errors, pre- or post-trigger traces, and specify filter length in bytes.
- **Byte-Pattern Definitions (Containing tab)**
  For frames, the **Containing** tab allows you to specify a byte pattern to be matched anywhere in the frame headers or payload.
- **Primitive group selection**
  Some SAS/SATA primitive templates (names starting with “**Any...**”) define a group of primitives. The template editor allows you to select or de-select individual primitives to include or exclude them in the group.
- **PCIe Address Regions**
  In PCIe and NVMe templates with addresses, you can select PCIe or NVMe regions by name from a drop-down menu at the bottom of the template editor.

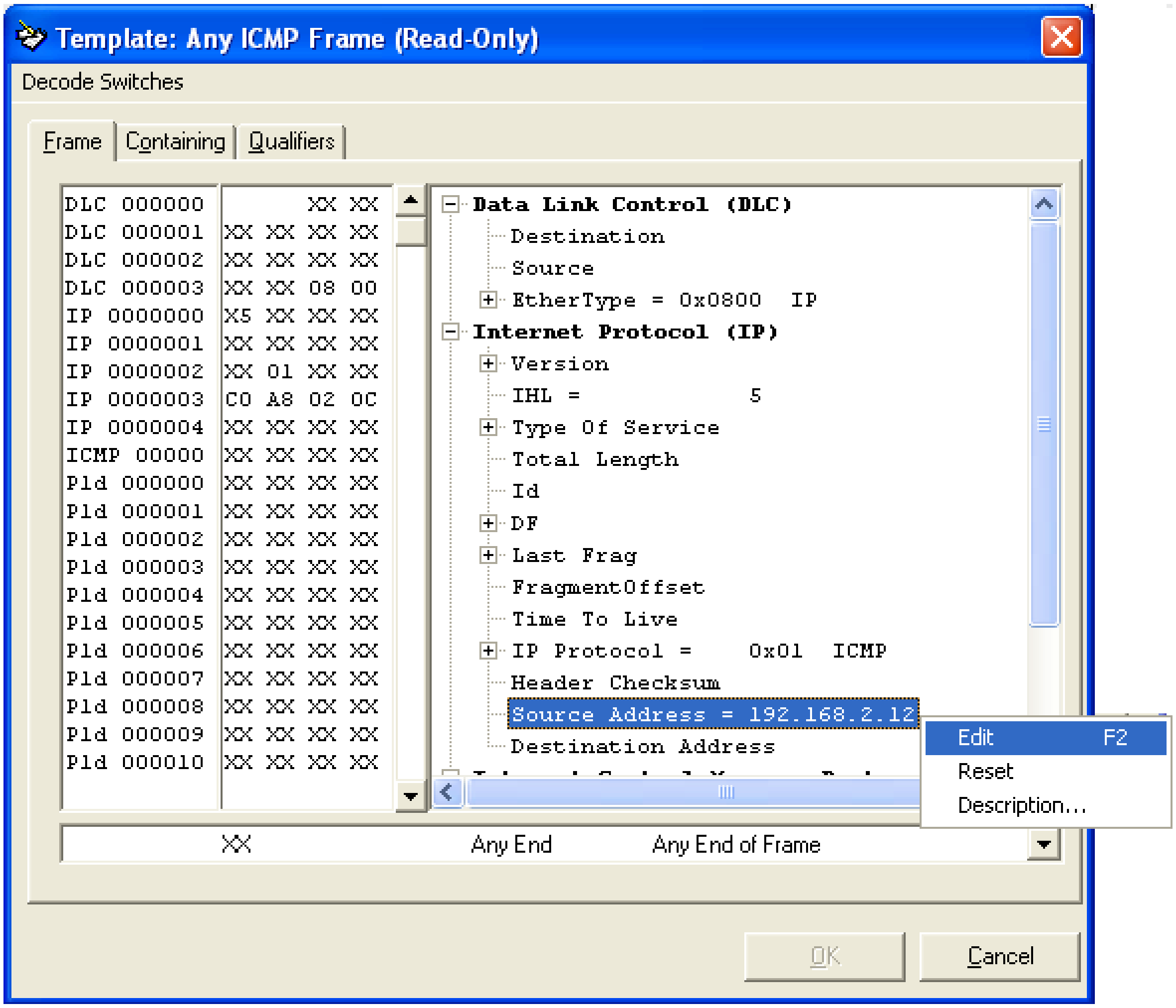
In-Place Field Editing

For editable fields, context menu selections or function key selections allow you to edit the value for field. There are three ways to initiate in-place field editing in the Tree View: press the F2 key, select **Edit** from the context menu, or click the field once to select it, and again to initiate in-place editing. In-place editing can be very useful for fields where the general format is not hexadecimal. For example, IP addresses can be entered in IP dotted notation rather than translated to hexadecimal for direct entry in the byte pattern. Figure 169 shows in-place editing for an IP address.

For the context menu available from each tree node, the menu contains some or all of the following options, depending on the current item selected:

- **Edit**
  This menu item is only available on editable fields. Select **Edit** to directly edit the field value in Tree View (the area on the right in the display). The field format can be hexadecimal, decimal, an IP address, etc.
- **Reset**
  This menu item is only available on editable fields with an equals (=) sign and a value associated to them. It allows resetting the value to don't cares (XXXXX) in the match buffer.
- **Description**
  This menu item is available for all fields and displays a detailed description for that field.

Figure 169: Example of In-Place Editing to Change the IP Address

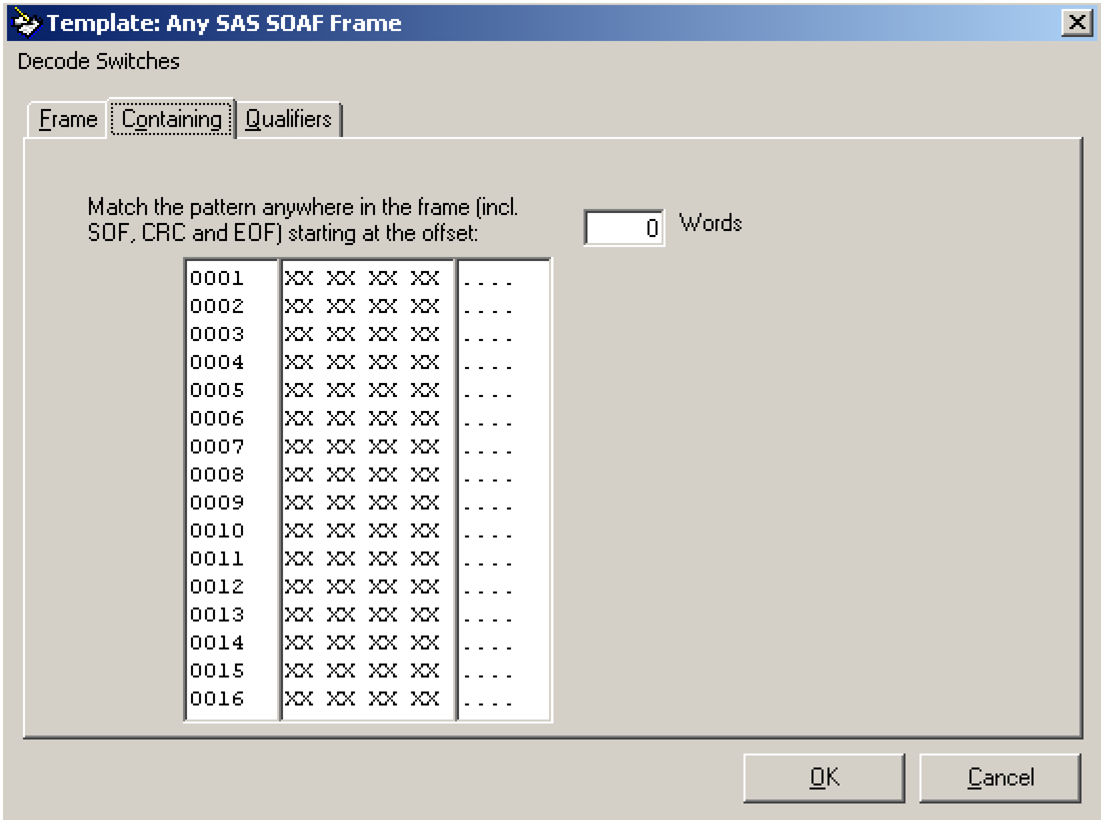


Containing Tab

The **Template Editor** dialog box appears when you double-click any editable template. Some templates have a **Containing** tab. The **Containing** tab allows you to specify a byte pattern to match anywhere in a frame's payload or header. The **Containing** tab is only available for frames.

An example of the Template Editor with the Containing tab visible is shown in Figure 170.

Figure 170: Template Editor, Contains Tab



To create a byte pattern to match:

1. Apply a template by dragging it to one of the boxes in the **Find**, **Filter**, or **Color** tab.
2. Double-click the template to bring up the Template Editor.
3. Click the **Containing** tab.
4. Click the byte you want to change and type in a value.
5. When you have completed the pattern you want to match, click OK.
6. Make sure you rename the new template.

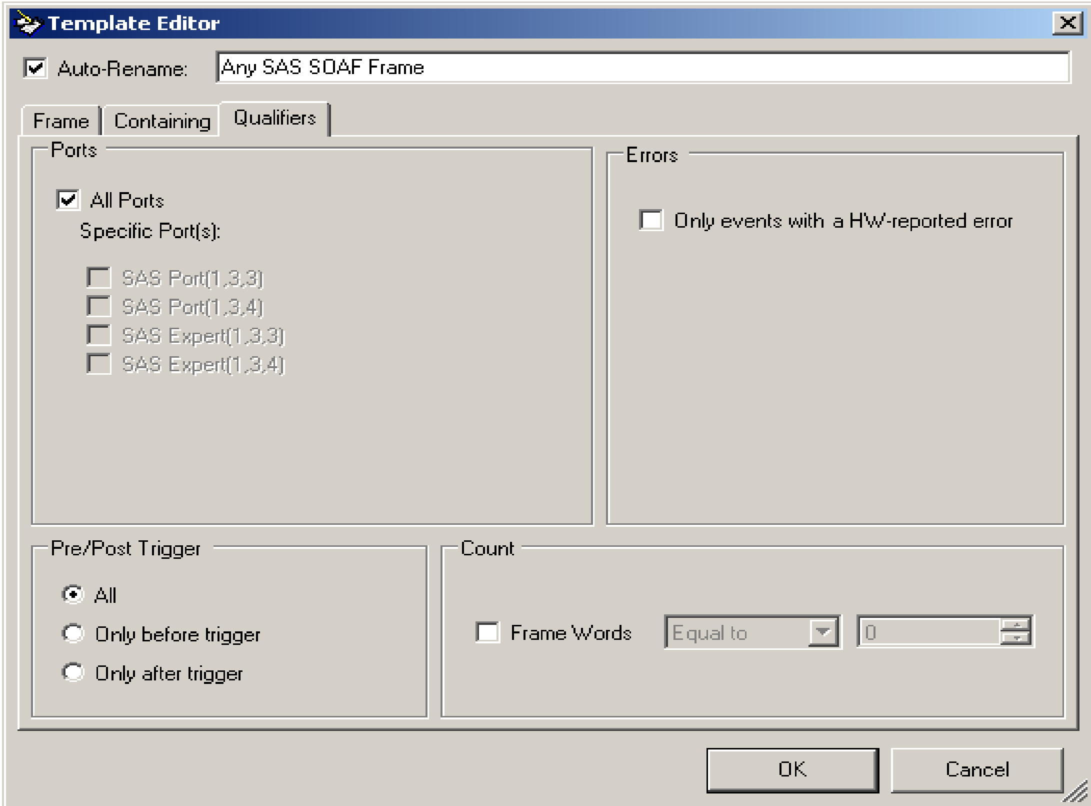
Qualifiers Tab

The **Template Editor** dialog box appears when you double-click any editable template. Some templates have a **Qualifiers** tab. The **Qualifiers** tab allows you to further refine your find or filter for frame, ordered set, or unframed data. Qualifiers are elements that can be useful for find or filter operations but are not a simple pattern match of the data. Matching data or header patterns is performed in the **Containing** tab.

The **Qualifiers** tab cannot be changed for a template until it is dragged to the **Find**, **Filter**, or **Color** tab.

An example of the **Template Editor** with the **Qualifiers** tab visible is shown in Figure 171.

Figure 171: Template Editor, Qualifiers Tab



To add a qualifier:

1 Apply a template by dragging it to one of the boxes in the **Find**, **Filter**, or **Color** tab.

2 Double-click the template to bring up the Template Editor.

3 Click the **Qualifiers** tab.

4 Change the qualifier options. See below for the available options.

5 When you have completed specifying qualifiers, click **OK**.

6 Make sure you rename the new template.

Qualifier Options

Qualifier options are:

- **Port Selection**
  Check **All Ports** if you want to filter or find within all ports. Click next to the port number(s) if you want to filter or find data for a specific port(s).
- **Error Filter**
  Check the **Only events with a HW-reported error** check box to show or find only events with errors.

- **Trace Filter**
  The default is **All**, which applies the filter to all events. Click **Only Before Trigger** to only filter on events before the trigger event. Click **Only After Trigger** to only filter events after the trigger event.
- **Length Filter**
  Click next to **Words** to filter or find a frame based on the length of the frame. The frame length is specified in words. Only frames that are greater than or equal to the specified frame length make this condition true. This option is only available for frame templates.
- **Counter Filter**
  Click next to **Repeat Count** to filter or find a primitive or ordered set based on its repeat count. You may type in a number and select one of the following: **Equal to**, **Not Equal to, Less Than**, or **Greater Than**. This option is only available for primitive and ordered set templates.

Decode Switches in the Template Editor

The **Template Editor** dialog box appears when you double-click any editable template. Some templates have an option in the upper left corner for specifying Decode Switches. The decode switches provide detailed contextual options for decode; for example, further decode of response and data frames. The Decode Switches menu is context sensitive and will only show the decode options available for the specific template you are creating. For example, for Fibre Channel templates, iSCSI options do not display.

The **Decode Switches** menu within the Template Editor is used to help you create a user-defined template. Any Decode Switches used within the Template Editor only apply to the single template you are creating; they do not affect global settings for Decode Switches.When editing a User Library template, Decode Switches are stored inside the template so they are still ON the next time you open this particular template in the Template Editor.

Important: Decode Switches within the Template Editor are not used for searching and filtering, but are only used to assist you in defining a bit pattern. Please refer to the section “Proper Use of Template Editor Decode Switches” on page 377 for a complete description of how to use these switches.

There are many Template-Editor-specific Decode Switches. These decode switches allow you to further decode Response and Data frames that can't be decoded without knowing what is the associated command frame. Below is a description of some of these switches:

- **SCSI Data Interpretation**
  Shows up on SCSI Data frames for SAS, SATA and Fibre Channel. It contains a list of all fixed format SCSI data frames, depending on the settings of the SCSI Interpretations switch.
- **FC-ELS Accept Interpretation**
  Shows up on FC-ELS (Fibre Channel Extended Link Services) Accept frames. It contains a list of the possible Link Services Accept frame formats.
- **FC-4 Link Accept Interpretation**
  Shows up on FC-4 Link Services Accept frames. It contains a list of the possible FC-4 Link Services Accept frame formats.

- **FC-SW Accept Interpretation**
  Shows up on FC-SW (Fibre Channel Switch Fabric Internal Link Service) Accept frames. It contains a list of the possible Switch Link Service Accept frame formats.
- **FC-GS Accept Interpretation**
  Shows up on FC-GS (Fibre Channel Generic Service) Accept frames. It contains a list of the possible Generic Service Accept frame formats.
- **ATA Output Interpretation**
  Shows up on SATA Data and Response (Reg: Host->Dev) FIS. It contains a list of all possible ATA commands.
- **FCLP Data Interpretation**
  Shows up on SCSI Data frames for SAS, SATA and Fibre Channel. It contains a list of all possible FC-AE-FCLP Data frames.

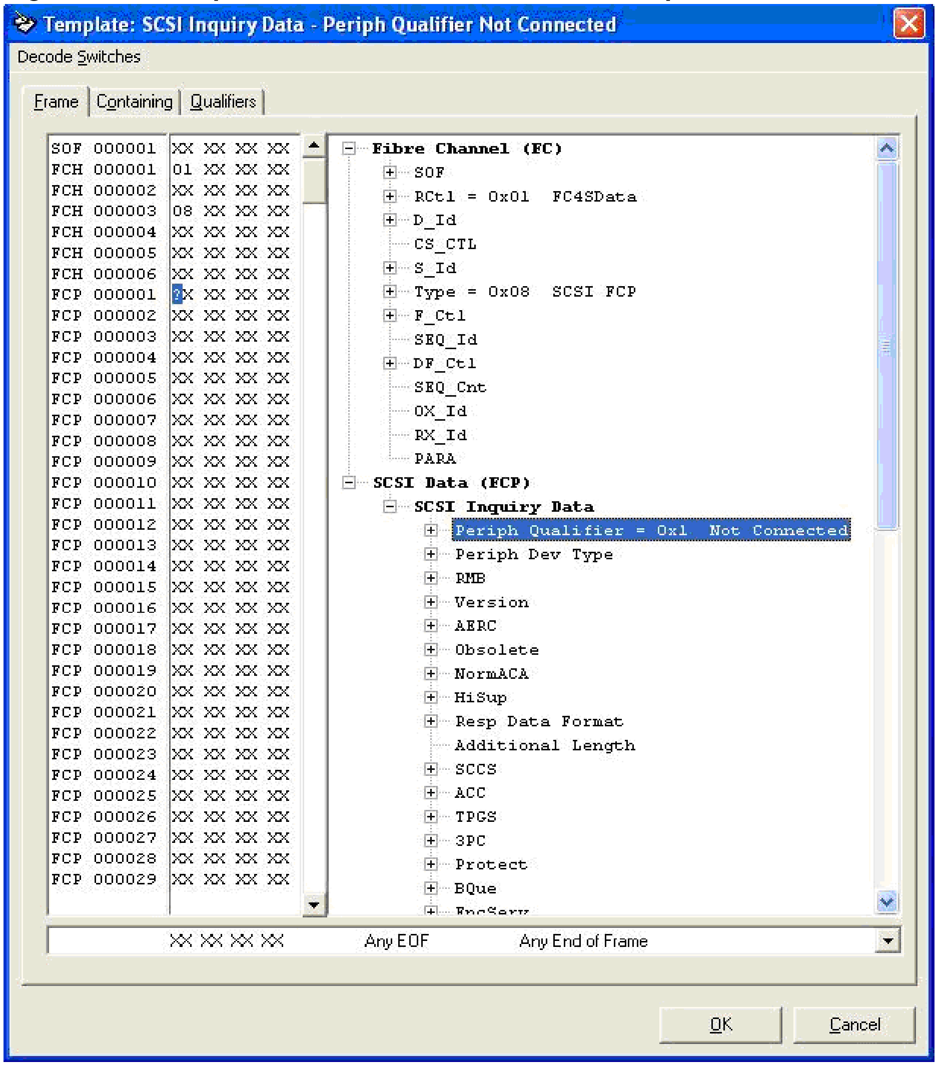
When appropriate, some of the global Decode Switches described in the section “Decode Switches” on page 385 are also visible in the Template Editor.

Proper Use of Template Editor Decode Switches

Be aware that the Decode Switches are a tool to help you create templates, but the switches you set aren't used by TraceControl or TraceView to trigger/filter or search for a specific frame.

For example, assume you create a **SCSI Inquiry Data** template from the **Any SCSI Data** template by setting the switch **SCSI Data Interpretation** to **SCSI Inquiry Data**. You then set the 3-bit **Periph Qualifier** field to **0x1 Not Connected**, you end-up with a template shown in Figure 172.

Figure 172: Template Editor Decode Switches Example



If you use this template as a simple trigger condition in TraceControl, chances are that it will trigger on another SCSI Data frame that isn't a SCSI Inquiry Data frame, but has the first 3-bits in the payload set to 0x1. This “false match” to a value within a non-SCSI Inquiry Data frame happens because the switches are only used to set up the bit pattern for filter/trigger in TraceControl and TraceView. Decode Switches are not used to determine which type of frame to compare to.

The Decodes Switches in the Template Editor can be a critical tool for selecting the proper bit pattern; however, do not mistake this for an absolute method of selecting only those frames that have a particular decode switch value. There are numerous ways to narrow your search/filter further using templates and other capabilities of Xgig Analyzer software. For example, if you have some idea of the traffic pattern, you might be able to specify enough template bits to allow triggering on exactly the desired frame. As another example, you could use a 2-level trigger condition in TraceControl, for example, **Arm on arm condition. Stop capture after trigger condition when armed** (two-level trigger). The Arm condition can be set to the command frame, and the trigger condition can be set to the corresponding data frame. It is often easy to create a template for the command frame that will give you 100% accuracy; after the arm condition is met, you will receive the corresponding data frame shortly after. By using the Arm-Trigger technique, you greatly improve the chances of hitting the right frame.

Chapter 17

Annotated Traces, Expert Traces, and Decode Switches

In this chapter:

- Working with Traces Annotated by Expert
- Working with Expert Traces
- Decode Switches

Working with Traces Annotated by Expert

The Expert program is capable of adding annotations to a trace as it processes it.

The annotations made to the trace by Expert allow TraceView to decode response messages that would be impossible to decode without state information. The following messages are decoded in TraceView after processing the trace in the Expert program:

- SATA Reg:Dev->Host and Data frames (Identify Device, Packet Command, ATA Device Configuration, SCSI CDB inside ATAPI frame, etc.)
- ELS ACC frames (PLOGI, FLOGI, etc.)
- GS Accept frames (GID_FT, GFT_ID, etc.)
- FC-SW Accept frames (LSU, EFP, etc.)
- SCSI Data frames (Inquiry, Mode Sense, Read Capacity, Report LUNS, etc.)
- iSCSI Data and Header Digests
- PCIe Configuration Space
- NVMe/AHCI Registers
- NVMe Commands, Completions, Data and Doorbells
- SATA over PCIe Commands, Responses, Data frames

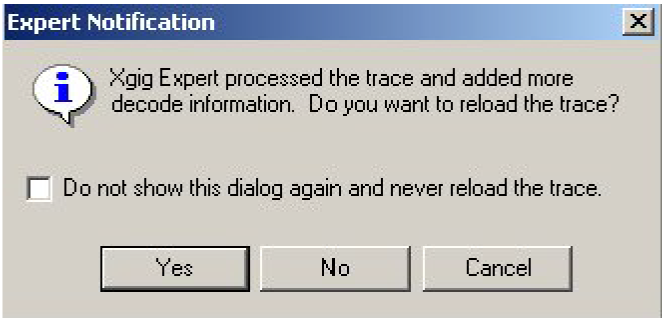
The SCSI Data frame annotations are added for any protocol processed by Expert; for example, SAS, FC, iSCSI, FCIP, or iFCP.

In addition, to increase the number of frames decoded in TraceView, Expert adds address/offset/command information for every SAS, SATA, NVMe, PCIe, AHCI, iSCSI, and Fibre Channel frame. The additional information provides significant advantages for search/filter/hide by address/command information. These Expert Annotations are visible in the **Side A**, **Side B**, **Summary**, **Tag**, **InitTag,** and **LUN** columns of the default configurations, as well as in the Inspector Window. They can also be added as separate columns within the spreadsheet with the Insert Column dialog box. That dialog box has a drop-down list showing all fields and additional annotations for the current event selected. It also has an auto-completion feature allowing you to type the first few letters of a fields and it will provide you common choices. You can also find any field in a Tree View by clicking the **Browse >>** button.

Viewing the Annotations in TraceView

To get the annotations that were created in Expert so that you may view them in TraceView, you must open the trace in Expert and then reload the trace in TraceView. When Expert finishes the annotation of the trace, it notifies TraceView to reload the trace and TraceView pops-up a dialog asking if you want to reload the trace with the annotations. However you do not need to wait for Expert to finish with the complete annotation to view the annotation up to any point in the process. Refer to “Viewing Partial Annotation in TraceView” on page 383 for information.

Figure 173: Reload Trace Dialog Box.



If TraceView is not open the notification message will not appear, but the annotations will be available the next time you load the trace in TraceView.

You can add columns to TraceView's spreadsheet in order to view all the expert annotations in a trace. The **Expert\ExpertAnnotationInfo** column can be found in the Insert Column dialog (see Figure 136 on page 306).

Expert\ExpertAnnotationInfo columns display the annotations from Xgig Expert 3.0 and above. It is strongly recommended that you re-process older traces with the new version of Xgig Expert to add additional expert information to the trace.

Viewing Partial Annotation in TraceView

The processing of annotations in Expert can take an extended period of time. However you can load the annotations that have already been processed by Expert up to any point in time so that they may be viewed immediately in TraceView. While you are viewing the partial annotations in TraceView, Expert continues running in the background until it has finished. You may load partial annotations during the process if need be.

Looking at the bottom of Figure 174, "Partial Annotations in TraceView, note that there are two colored lines; a magenta-colored line and a teal-colored line in the histogram area.

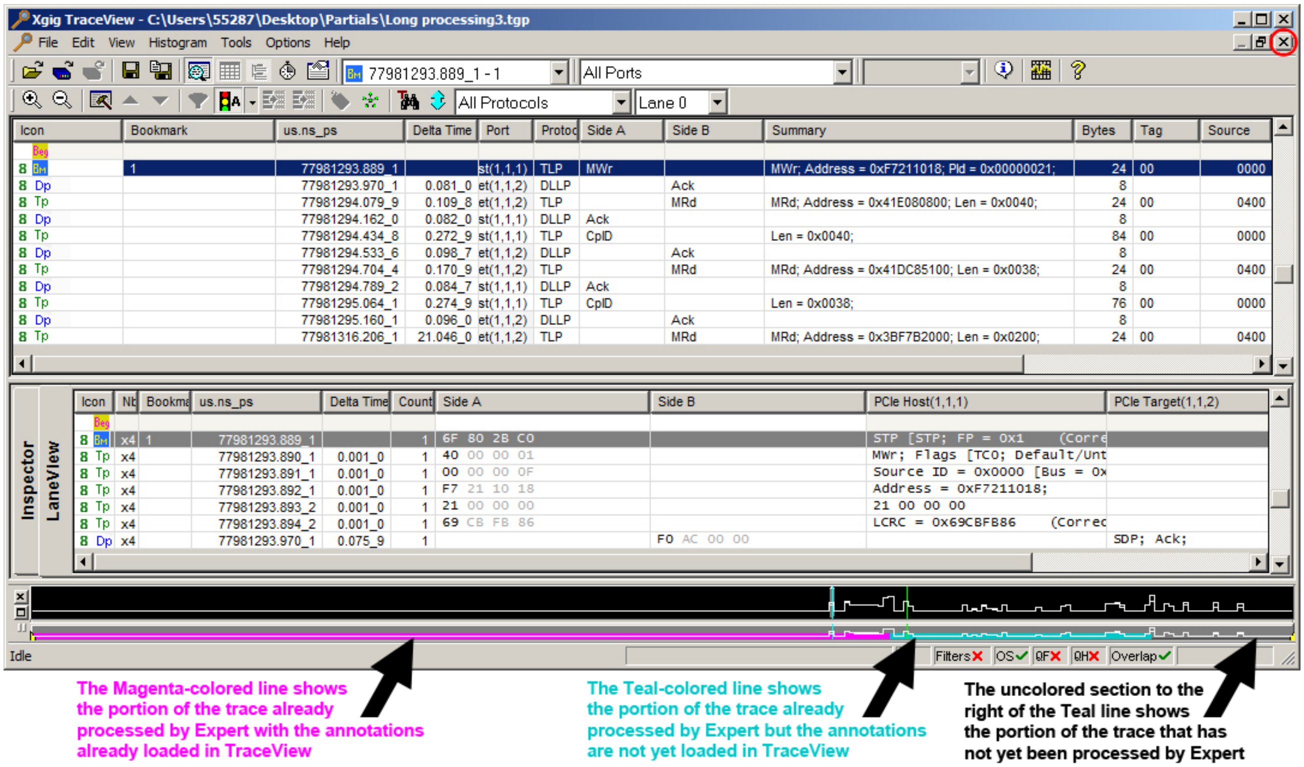
- The magenta-colored line shows the portion of the trace that has already been processed by Expert and the annotations generated by Expert has been loaded into and can currently be seen in TraceView.
- The teal-colored line shows the portion of the trace that has already been processed by Expert that is available to be loaded into TraceView at this point.
- The uncolored area to the right of the teal-colored line shows the portion of the trace that has not yet been processed by Expert.

To update TraceView so that you can view the annotations for the Teal-colored portion of the trace:

1. Close the trace in TraceView by clicking the **Close** button that is circled in red near the top right corner of Figure 174.
2. Open the trace again in TraceView.

Once the trace is reopened, you will note that the magenta-colored line has lengthened toward the right (and the teal-colored portion of the line is now very small) showing you that more annotations are available to be viewed in TraceView.

Figure 174: Partial Annotations in TraceView



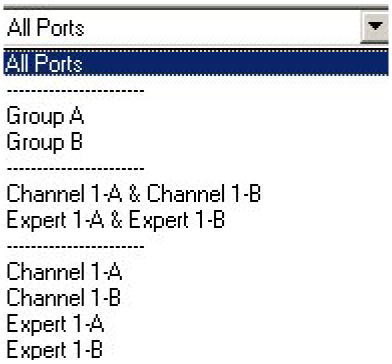
Working with Expert Traces

Expert Trace Files are created by Xgig Expert for any saved trace file (Expert traces are not created for buffer contents). A file will be created for each port in the trace. When you create Expert Trace Files, you will receive a message informing you the files have been created. See the Expert Trace Output section in the Expert on-line help for more information on the types of traces created by Expert.

Important: An Expert Trace is different from an Expert Annotation. The Expert Annotation adds additional decode information to existing events. An Expert Trace actually creates a new trace and adds events to the new trace, such as information about conversations. Expert Annotations are automatically added and an Expert Trace is automatically created when the trace is opened in Expert. The new group file will be the same name as the original group file for the trace with Expert appended to the name. For example, the trace **2drivecomp.tgp** is saved as the Expert Trace **2drivecomp Expert.TGP**.

The Expert Trace can be decoded and viewed in TraceView. When viewing an Expert Trace, you will see additional port selection options from the **Select Ports** pull-down menu. You can select a view of just the original trace, just the new events added by Expert, or both. If you choose to view just the original trace, you will still see the Expert Annotations added by Expert to existing events. Below are examples of the **Select Ports** pull-down when viewing an Expert Trace.

Figure 175: Select Ports for an Expert Trace.



There is a new set of columns specific to Expert traces that can be added and displayed in the TraceView spreadsheet. Select any of the columns from the Insert Column dialog under the Expert\ folder to display information specific to Expert events (i.e., these columns only display the information for expert events and they stay blank for regular frames). However, note that all the columns under **Expert\ExpertAnnotations** are not for Expert traces, but are for Expert annotations (refer to the previous section for more details).

Decode Switches

TraceView automatically recognizes differences between Fibre Channel, SAS, and Ethernet, and will properly decode data from any Viavi analyzer device. However, certain protocols such as SCSI may have different interpretations depending on the type of devices sending and receiving data. Set decode switches so your trace is interpreted correctly by the TraceView decodes. Each decode switch affects the interpretation of a specific protocol.

To set a decode switch, select **Decode Switches** from the **View** menu and navigate to the proper area to set the switch. The decode switches set from the **View > Decode Switches** menu affect the decodes as displayed in the TraceView's main decode grid, DWord View, and Inspector View.

You can also use decode switches from the Template Editor to create very specific templates. See “Decode Switches in the Template Editor” on page 376 for information on using decode switches from the Template Editor.

All decode switches set from the menu are saved in TraceView configuration files, with the exception of the **/C/ Encodings**. The example templates within TraceView software use settings for the decode switches so they will decode traces properly.

The switches are as follows:

- **/C/ Encodings**
- **ATA Cmd Interpretation**
- **DDP Interpretation**
- **FC-AE-FCLP**
- **Viavi Signatures**
- **IP TOS Field Interpretation**
- **LUN Interpretation**

- **OOB/Speed Neg. Interpretation**
- **SATA PM Port Interpretation**
- **SCSI Interpretation**
- **SCSI Data Integrity Field (T10-DIF)**
- **iSER/SRP Interpretation**
- **Reserved/Obsolete Values**
- **OUI Interpretation**
- **Brocade VE Port Frame Decoding**

You can set only one value for each switch. For example, if you set **SCSI Interpretation** to **Direct Access Devices**, no frames are interpreted using the other two settings. See “Working with Traces Annotated by Expert” on page 382 and “Working with Expert Traces” on page 384 for more information on using Expert to provide additional decode information.

/C/ Encodings

This option sets the interpretation the Gigabit Ethernet /C/ primitives sent during the Auto-Negotiation phase. The /C/ primitives contain 16-bits of data, and the interpretation depends of the current phase of the Auto-Negotiation. The TraceView application does not track the state of the Auto-Negotiation, so it does not know what is the proper interpretation for each /C/ primitive. For interpretation of /C/ primitives, select **Decode Switches > /C/ Encodings**. There are two decode choices available:

By default, TraceView assumes that the /C/ primitive contains the **16-bit Config_Reg** data, which corresponds to the **Config_Reg base page encoding** switch. However, when the Next Page bit of the Config_Reg is set to 1, then the next /C/ primitive should be interpreted using the **Next page encoding** switch, until the Next Page bit is set to 0.

SCSI Interpretations

For interpretation of SCSI frames, select **Decode Switches > SCSI Interpretation**. There are many decode choices available for the SCSI protocol:

- **Any SCSI Device**
  Use this option if you do not know what kind of SCSI traffic you have. This option assumes Direct Access Devices such as disks by default, but non-direct access SCSI opcodes are also interpreted as much as possible. This is the default option.
- **Direct Access Devices (SBC)**
  Use this option if your network only uses direct access devices (SBC) such as disks.
- **Sequential Devices (SSC)**
  Select this option if your network only uses sequential devices (SSC) such as tape.
- **Medium Changers (SMC)**
  Select this option if your network only uses medium changers (SMC) such as CD-ROM servers.
- **SCSI Controllers (SCC)**
  Select this option if your network only uses SCSI storage array devices (SCC) – commonly known as RAID devices.

- **Processor Type Devices (SPC-2)**
  Select this option if your network only uses Processor Type Devices (SPC-2).
- **Automation/Drive Interface Devices (ADC)**
  Select this option if your network only uses automation/drive interface devices (ADC).
- **Multi-Media Drives (MMC)**
  Select this option if your network only uses multi-media drives, such as CD and DVD.
- **Simple Streaming Protocol (FC-AV)**
  Decode the Send command FCP_DATA IUs as the Simple Streaming protocol. The Simple Streaming protocol contains the Play, Pause, Resume, etc. commands to control the video transfers over the network. The Simple Streaming protocol messages are carried by SCSI-3 into Send FCP_DATA IUs.

LUN Interpretations

This option sets the interpretation of the LUN structure to either **Assume Single Level LUNS** or **Assume Hierarchical Addressing for LUNs**.

FC-AE-FCLP

FC-AE-FCLP is one of the 5 sub-protocols for FC-AE. FC-AE-FCLP is implemented through Vendor Specific SCSI Opcodes. By default, FC-AE-FCLP is disabled in the TraceView application. You can enable it using the switch **Enable FC-AE-FCLP As Vendor SCSI Opcodes**. You can disable it using the switch **Disable FC-AE-FCLP**.

SCSI DATA Integrity Field (T10-DIF)

The SCSI Block Device protocol specification (SBC-3) defines a protection information model to protect the data from malicious and unintentional corruption. Under that model, the SCSI data frames contain some Data Integrity fields (DIF) at a fixed interval within the data. The interval is typically either 512-bytes or 4096 bytes.

- **512-Byte Blocks ending with Guard/App/Ref Tag**: This switch enables the decoding of the T10 Data Integrity Fields (T10-DIF) in the SCSI Data frames for Fibre Channel and SAS. There are 3 data integrity fields for a total of 8 bytes: 2-byte Logical Block Guard, 2-byte Logical Block Application Tag and 4-byte Logical Block Reference Tag. These DIF fields are decoded in the SCSI data frame following each 512-byte block of data.
- **4096-Byte Blocks ending with Guard/App/Ref Tag**: This switch enables the decoding of the T10 Data Integrity Fields (T10-DIF) in the SCSI Data frames for Fibre Channel and SAS. There are 3 data integrity fields for a total of 8 bytes: 2-byte Logical Block Guard, 2-byte Logical Block Application Tag and 4-byte Logical Block Reference Tag. These DIF fields are decoded in the SCSI data frame following each 4096-byte block of data.
- **No T10-DIF Protection**: This switch disables the decoding of the T10 Data Integrity Fields (T10-DIF). This is the default switch.

Viavi Signatures

Some Viavi traffic generator products add some records into the data portion of the traffic. This is the case for Load Tester and Medusa Labs Test Tools (MLTT). This switch enables decoding of these records. MLTT adds a special record at the beginning of every SCSI data block transferred. The record is typically found at every 512-byte boundary of the SCSI data. Load Tester records are inserted at the beginning of the Fibre Channel payload for every frame. The following choices are available:

- **Don't Decode Viavi Signatures**
  This option disables the decoding of the special records. This is the default setting.
- **Medusa Labs Tools I/O Signature**
  This option enables the decoding of the MLTT Signature records every 512 bytes in the SCSI data. This switch enables decoding of these special records.
- **Medusa Labs Test Tools IO Signature/Timestamp in secs**
  This option is the same as the previous one, except that an additional 32-bit timestamp is decoded at the end of the record. This timestamp is added to the record if specified by command-line arguments within the MLTT tools when the capture is created.
- **Medusa Labs Test Tools IO Signature/Timestamp in ms**
  This option is the same as the previous one, except that an additional 16-bit millisecond resolution timestamp is added after the 32-bit timestamp. This timestamp is also added by command-line argument.
- **Load Tester Signature (at beginning of payload)**
  This option enables the decoding of 24-byte Load Tester records at the beginning of the Fibre Channel payload for every FCoE frame.
- **Load Tester Signature (at end of payload)**
  This option enables the decoding of 24-byte Load Tester records at the end of the Fibre Channel payload for every FCoE frame.
- **Load Tester Truncated Signature**
  This option enables the decoding of a 14-byte Load Tester record at the beginning of the payload for UDP frames only.

SAS/SATA Interpretations

- **ATA Cmd Interpretation**
  Sets the bit length for interpretation of ATA commands within SAS/SATA frames. The original specification for the ATA interface only provides 28-bits with which to address devices. Select **ATA 28 Bit LBA Cmd Mapping** if this type of addressing is used. 48-bit Logical Block Addressing (LBA) is a technology which extends the capacity of IDE ATA/ATAPI. Select **ATA 48 Bit LBA Cmd Mapping** if this type of addressing is used.
- **SATA PM Port Interpretation**
  Port multipliers are silicon-based devices that allow a single Serial ATA port to communicate with multiple drives. **SAS PM Port Interpretation** should be set to **Show PM Port** if a SATA Port Multiplier is available in the configuration. The PM Port field in SATA Frames is decoded when this switch is set; otherwise, this field is reserved. Also, some Port Multiplier specific commands will be decoded when this switch is set.

- **OOB/Speed Negotiation Interpretation**
  Out-of-Band (OOB) signal and speed negotiation happen on a SAS/SATA link during initialization and speed negotiation. The default option, **Show 'OOB' and 'Speed Neg.' in decodes,** uses the text “OOB” or “Speed Neg.” as a prefix to every D.C. Idle and Data Burst event. The other option, **Remove 'OOB' and 'Speed Neg.' from decodes,** omits that prefix to simplify the decodes.

RDMA/iWARP Interpretations

- **DDP Interpretation**
  Sets the interpretation for the Direct Data Placement (DDP) protocol. Select **RDMA Present** if the Remote Direct Memory Access (RDMA) protocol is implemented within DDP for the trace data. Select **DDP Unknown** if DDP is used, but RDMA is not used within DDP. By default, the option **RDMA Present** is assumed.

iSER/SRP Interpretation
iSER/SRP Interpretation Sets the interpretation for the iSER (iSCSI RDMA) or SRP (SCSI RDMA) protocol. Select **iSER Protocol** if this protocol is used in the trace, or select **SRP Protocol** if this one is used instead, or **No iSER/SRP Protocol** if not used. iSER is a recent IETF standard extension to iSCSI that includes support for multiple RDMA-based transports including InfiniBand and Ethernet RDMA. SRP (or SCSI RDMA) is a mapping of SCSI over the InfiniBand protocol. By default, the option **No iSER/SRP Protocol** is assumed.

IP TOS Interpretation

Sets the interpretation for the Layer-3 Type of Service field. Set the interpretation to **TOS** or **Differentiated**. If IP TOS Interpretation is not used or not relevant to your trace analysis, leave all options unchecked.

Reserved/Obsolete Values

Sets the interpretation for bits that are reserved, vendor-specific, retired, not applicable, or obsolete. These bits usually do not add value to the decode, therefore the default is to **Hide Reserved Bits.** However, there are two other options available if you need see these bit values, **Show Reserved Bits** and **Report Invalid Reserved Bits as Errors**.

Information regarding reserved bits displays in the **Tree** view of the **Inspector**. See the figures on the followings pages to see a Tree view of the same frame with each option selected.

Select **Show Reserved Bits** to see all the reserved bit values in the decode. If bits are reserved, they are displayed in the decode with an **R** or **Reserved** for the field name. If the value for a field does not apply for the decode of this particular frame, the field is marked as **Not Applicable**.

Select **Report Invalid Reserved Bits as Errors** to report to all non-zero reserved bits or any field with a **Reserved** interpretation as errors. The decode marks these values as **(Invalid)** in the **Tree** view display. The decode will also display the error **Invalid Reserve Bits** in the **Errors/Warnings** column. You can search/filter hide frames that have invalid reserve bits using the Quick Find dialog using **Invalid Reserve Bits** in the **Errors/Warnings** column.

Figure 176: Hide Reserve Bits (left), Show Reserve Bits (right)

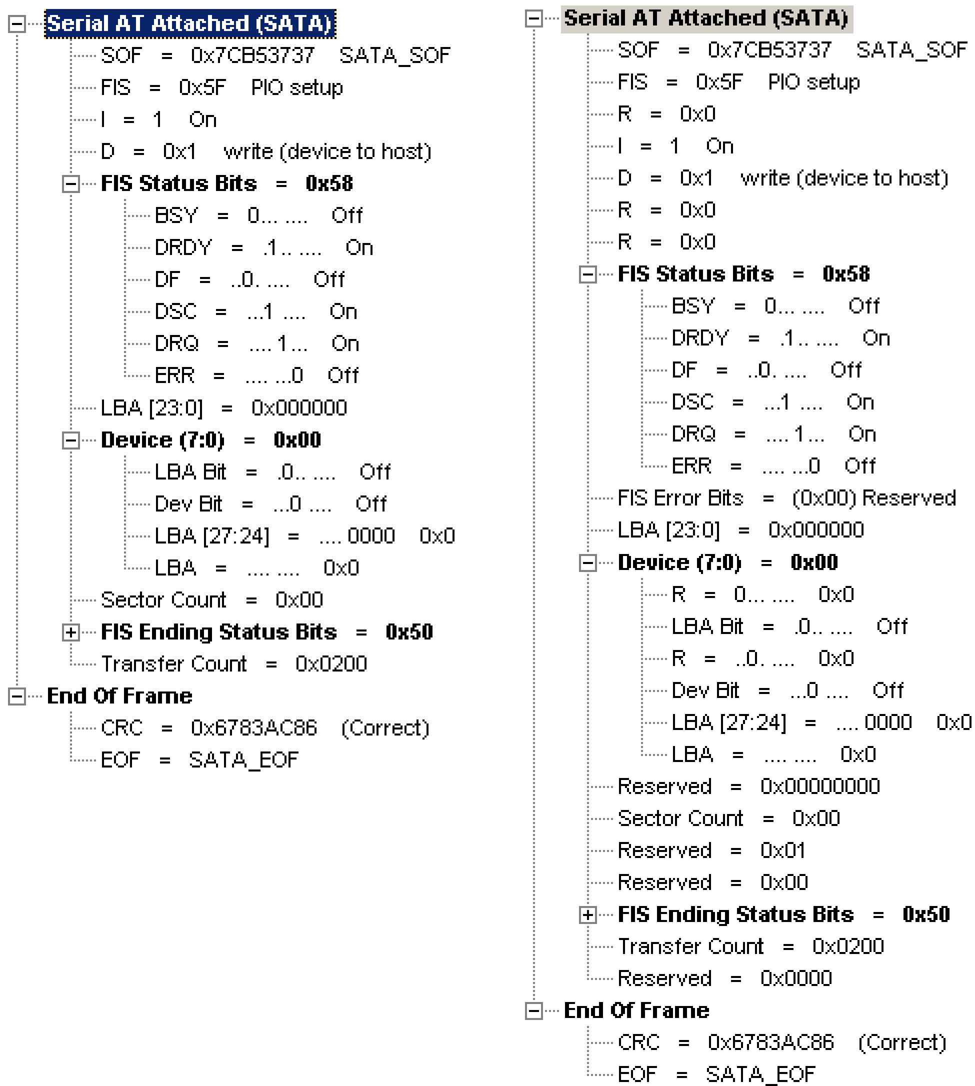
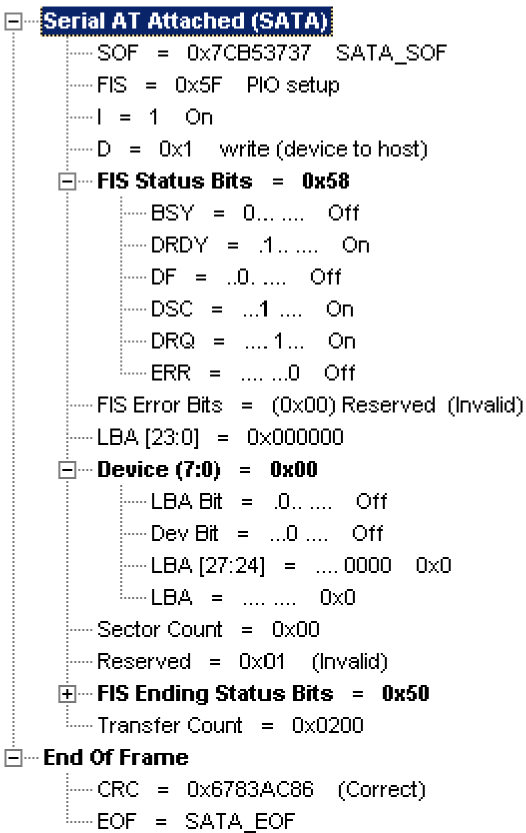
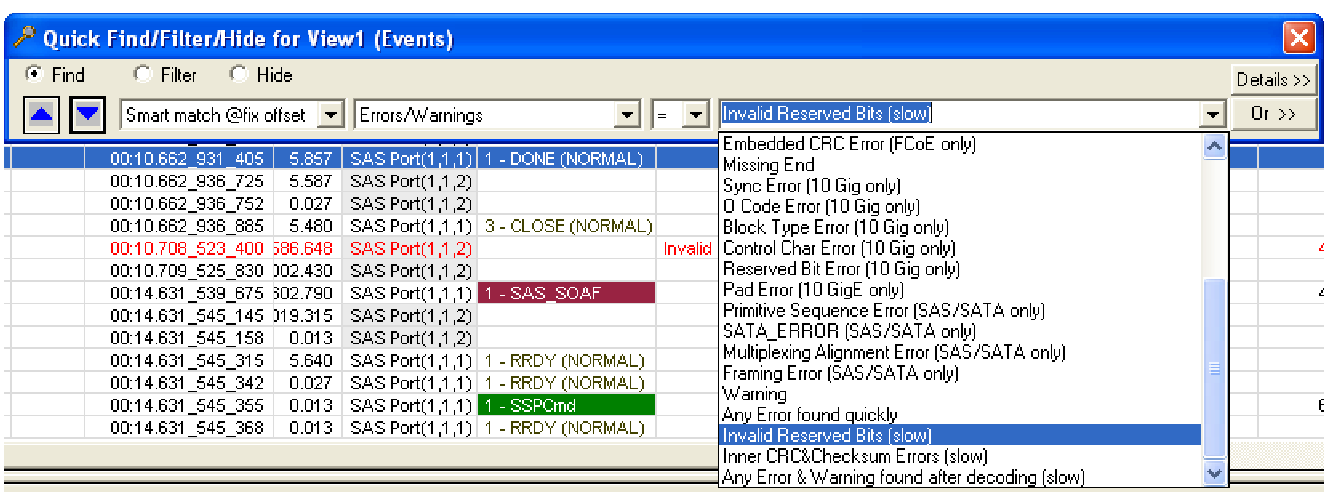


Figure 177: Report Invalid Reserve Bits as Errors



You can use Quick Find/Filter/Hide and the **Errors/Warnings** column to Find/Filter/Hide frames with Invalid Reserve Bits.



OUI Interpretation

World Wide Names and MAC addresses contain a 24-bit Organization Unique Identifier (OUI). This option selects to enable/disable the decoding of vendor names inside World Wide Names and MAC addresses.

- **Display OUI Vendor Names**
  This option enables the display of the vendor names. This is the default value.
- **Display OUIs in Hexadecimal**
  This option disables the display of the vendor names. The 24-bit hexadecimal value is displayed instead.

Brocade VE Port Frame Decoding

This switch is necessary to decode the frames on Brocades's VE Ports, which otherwise look like random data.

- **Disable VE Port Frame Decoding**
  This is the default behavior where we decode the standard Ethernet frames.
- **Skip 8 bytes after DLC.Source**
  This option skips 8 bytes after the Ethernet Source field and then it decodes the EtherType, according to the Brocade VE Port frame format.

Chapter 18

Converting Files from Other Platforms

In this chapter:

- Converting Bus Doctor Files
- Converting I-Tech Files

Converting Bus Doctor Files

Xgig Expert and Xgig TraceView support SAS v1.1 - Serial Attached SCSI and SATA - Serial ATA captures taken from Bus Doctor analyzer platforms. Xgig Expert provides full SAS Link Layer (SL), Serial ATA Tunneled Protocol (STP) and Serial SCSI Protocol (SSP) experts and metrics for both single transmit/receive links as well as wide links of up to 4 lanes (limited only by the RX-252's channel count). The software includes full SATA support and decodes for FPDMA, DMA, PIO and ATAPI on both Native SATA Links and SAS-STP Links.

Only saved trace files can be converted at this time. Converted files are displayed in the TraceView spreadsheet view using the protocol color coding familiar to Bus Doctor users. See “Protocol Display Color Coding” on page 437 for information on colors used for this display. Display colors can be changed as described in “Spreadsheet Options” on page 294.

Supported Bus Doctor trace file formats

Xgig Expert and Xgig TraceView support the following saved capture types:

- RX-252 SAS
- RX-108 SAS and SATA Pods (all varieties)

Data can be captured with either Bus Doctor or Bus Doctor Plus software packages. It is recommended that you use the Bus Doctor Plus version 3.2 or higher versions of the software for trace capture.

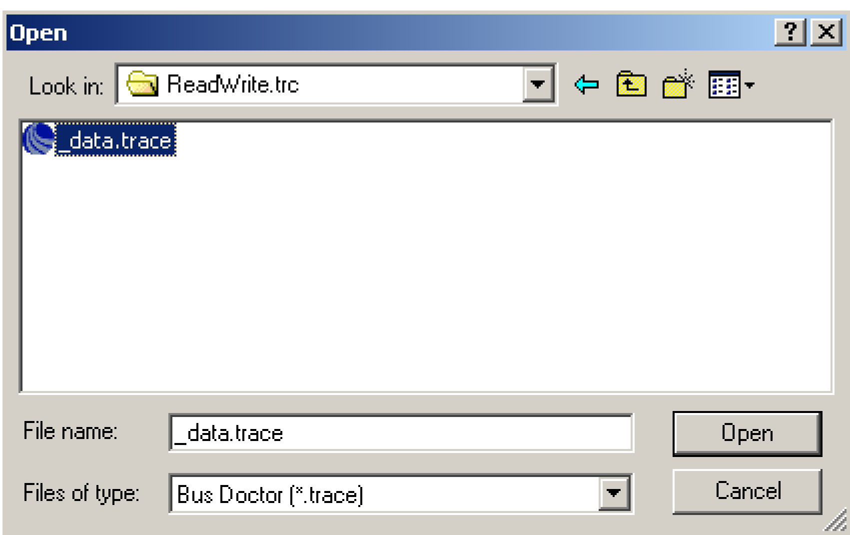
Converting traces

To convert a trace, open the trace with either Xgig Expert or Xgig TraceView:

1 Select **File>Open** from the Xgig application.

2 Change the **Files Of Type** selector to **Bus Doctor (*.trace)** as shown below:

Figure 178: Open Bus Doctor Trace for Conversion



3 Navigate to the directory where the trace is stored.
NOTE: This will vary somewhat for Bus Doctor and Bus Doctor Plus. Bus Doctor files are typically a single *.trace* file. Bus Doctor Plus files are comprised of several files stored within a directory, which contains the file *_data.trace* along with some other supporting files.

4 Double-click the .trace file which you want to convert.

5 If the trace has been previously converted, you will be prompted to overwrite the trace or abort the conversion.

6 The trace will then be converted to Xgig trace format. A screen displays showing the progress of the conversion. Once conversion is complete, the trace automatically opens in the Xgig application.

Opening traces

Once the trace file has been converted, the files can be reopened by simply opening the .TGP file in the same directory where the original trace file was. In the example above, this would be *C:\traces\ReadWrite.trc\ReadWrite.tgp*. This file can be opened with Xgig Expert via the **File>Open** menu or in Xgig TraceView by simply double-clicking on the TGP file in explorer or using **File>Open**.

Converter notes

SAS Scrambled Idle Dwords and SATA/STP Scrambled Primitive Data will be discarded upon conversion. Only primitives with valid K-characters are converted (with the exception of errors).

To greatly speed up conversion and analysis time by Expert, the converter, by default, does not convert SATA_HOLD, SATA_HOLDA, SATA_R_IP, SATA_CONT, or SATA_SYNC primitives.

These primitives are not typically utilized by Expert, other than for a couple of very subtle performance metrics and the trade-off is MUCH faster trace conversion and processing time by Expert and TraceView. If you find it important to see these primitives in the converted trace, utilize the converter from the command line (see below) with the /I switch to re-enable the conversion of these.

The converter also, by default, truncates the frames down to 16 words per frame. The extra data is not utilized by Expert for the most part, and requires significant amounts of overhead/time to process, thus is dropped in the conversion process. If you find it important to see all of the frame data in the converted trace, utilize the converter from the command line (see below) with the /T0 switch to re-enable the full frame conversion without truncation.

TraceView will show COMSAS, COMINIT, COMWAKE, COMRESET and D.C. Idle events as “simulated events” with meaningless 8b data values. These items will be visible and decoded. However, they will be represented as K-character events.

For Bus Doctor traces, the clock rate information from the trace is not converted (because of some limitations in the original capture). SAS traces are assumed to be 3.0Gbps unless converted from the command line conversion utility with the /R30 switch to select 1.5Gbps.

The converter utility can be run as a stand-alone executable from a CMD window and supports many options and additional features that are not available when converting from the GUI application. The executable is called *IOConverter.exe* and exists in the program installation directory (normally *C:\Program Files\Viavi\Xgig Analyzer*). For detailed information on the IOConverter, run IOConverter.exe /h from the command line.

Channel mappings and nomenclature

Converted traces use a “Port” naming convention that is common to the Xgig platform architecture. When an RX-252 analyzer trace is converted, the following names are utilized in the Xgig format:

Table 35: Bus Doctor to Xgig Port Name Conversion

Bus Doctor Name	Xgig Port Name	Port Name Meaning
L1 I->T	SAS_Port 0	Initiator transmit port for Link 1
L1 T->I	SAS_Port 1	Target transmit port for Link 1
L2 I->T	SAS_Port 2	Initiator transmit port for Link 2
L2 T->I	SAS_Port 3	Target transmit port for Link 2
L3 I->T	SAS_Port 4	Initiator transmit port for Link 3
L3 T->I	SAS_Port 5	Target transmit port for Link 3
L4 I->T	SAS_Port 6	Initiator transmit port for Link 4
L4 T->I	SAS_Port 7	Target transmit port for Link 4

In the Xgig trace format, each port (or channel) represents a single transmitter. Each port is saved to a separate file (with the .BUS extension for SAS traces, .TRC for Fibre Channel trace and .GBE for Gigabit Ethernet traces). Additionally each of the filenames/locations are placed into a .TGP file (Trace Group File), which is the file type that is opened by default in both Xgig Expert and Xgig TraceView.

Converting I-Tech Files

Xgig Expert and Xgig TraceView support SAS v1.1 - Serial Attached SCSI and SATA - Serial ATA captures taken from I-Tech analyzer platforms. Xgig Expert provides full SAS Link Layer (SL), Serial ATA Tunneled Protocol (STP) and Serial SCSI Protocol (SSP) experts and metrics for both single transmit/receive links as well as wide links of up to 4 lanes. The software now includes full SATA support and decodes for FPDMA, DMA, PIO and ATAPI on both Native SATA Links and SAS-STP Links.

Only saved trace files can be converted at this time.

Supported I-Tech trace file formats

Xgig Expert and Xgig TraceView support the following saved capture types:

- I-Tech PowerFrame MP, Fibre Channel, and SAS Blades capturing Fibre Channel or SAS/ SATA traffic

- I-Tech Satellite Fibre Channel captures

I-Tech Data can be captured using the Satellite software. It is recommended to use version 2.10.1 or higher of this software for capture.

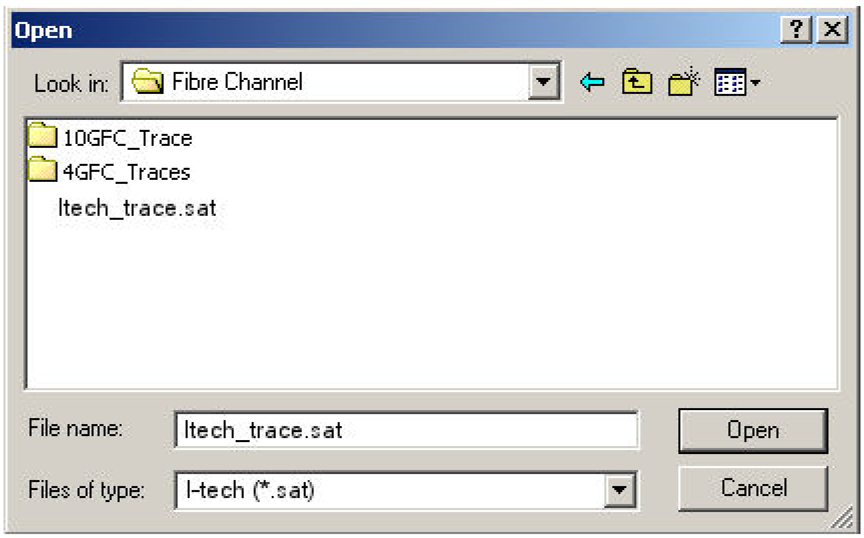
Converting I-Tech traces

To convert a trace, open the trace with either Xgig Expert or Xgig TraceView:

1 Select **File>Open** from the Xgig application.

2 Change the **Files Of Type** selector to **I-Tech (*.SAT)** as shown below:

Figure 179: Open I-Tech Trace for Conversion



3 Navigate to the directory where the trace is stored.

4 Double-click the .SAT file which you want to convert.

5 If the trace has been previously converted, you will be prompted to overwrite the trace or abort the conversion.

6 The trace will then be converted to Xgig trace format. A screen displays showing the progress of the conversion. Once conversion is complete, the trace automatically opens in the Xgig application.

Opening traces

Once the trace file has been converted, the files can be reopened by simply opening the .TGP file in the same directory where the original .sat file was. This file can be opened with Xgig Expert via the **File>Open** menu or in Xgig TraceView by simply double-clicking on the TGP file in explorer or using **File>Open**.

Converter notes

SAS Scrambled Idle Dwords and SATA/STP Scrambled Primitive Data will be discarded upon conversion. Only primitives with valid K-characters are converted (with the exception of errors).

To greatly speed up conversion and analysis time by Expert, the converter, by default, does not convert SATA_HOLD, SATA_HOLDA, SATA_R_IP, SATA_CONT, or SATA_SYNC primitives.

These primitives are not typically utilized by Expert, other than for a couple of very subtle performance metrics and the trade-off is MUCH faster trace conversion and processing time by Expert and TraceView. If you find it important to see these primitives in the converted trace, utilize the converter from the command line (see below) with the /I switch to re-enable the conversion of these.

The converter also, by default, truncates the frames down to 16 words per frame. The extra data is not utilized by Expert for the most part, and requires significant amounts of overhead/time to process, thus is dropped in the conversion process. If you find it important to see all of the frame data in the converted trace, utilize the converter from the command line (see below) with the /T0 switch to re-enable the full frame conversion without truncation.

TraceView will show COMSAS, COMINIT, COMWAKE, COMRESET and D.C. Idle events as “simulated events” with meaningless 8b data values. These items will be visible and decoded. However, they will be represented as K-character events.

The converter utility can be run as a stand-alone executable from a CMD window and supports many options and additional features that are not available when converting from the GUI application. The executable is called *IOConverter.exe* and exists in the program installation directory (normally *C:\Program Files\ViaviViavi\Xgig Analyzer*). For detailed information on the IOConverter, run IOConverter.exe /h from the command line.

I-Tech specific notes

The I-Tech analyzer provides a mechanism for truncating frames in the capture to a user specified number of bytes. Use of this option causes primitives within frames to be discarded automatically, thus risking the potential of missing critical primitives such as R_RDY, ACK, etc. It also captures in such a fashion that the conversion process would be unable to determine an accurate length of the payload data in frames, which is critical to Expert and cannot be overlooked. Therefore, conversion of SAS/SATA captures with truncated frames within them is disallowed.

I-Tech captures of OOB sequences work very differently than Bus Doctor captures of the same sequences. The I-Tech analyzer captures the OOB bursts and does not mark a record for the completed or failed OOB sequence. To accommodate this, the converter only inserts completed OOB summary events into the Xgig capture - the individual OOB events will not be shown.

In I-Tech, code violations and disparity errors do not store the 10b data (for Fibre Channel or SAS/SATA capture formats) and error bytes are represented by a value of XX in the I-Tech viewer, but have a valid data value of 0x23 behind them. Converted disparity errors and code violations will show the error, but will have a hex value of 0x23 in the byte of the error, since the 10b data is not present.

The I-Tech analyzer does not store information on the running disparity of the captured data, so the resulting display of 10b data in Xgig will have incorrect running disparity values.

I-Tech traces store full information on the capture data rate accurately, so the /R switch from the command line is not necessary. The converter will automatically set the correct capture rates in the trace.

Channel mappings and nomenclature

Converted traces use a "Port" naming convention that is common to the Xgig platform architecture. When an I-Tech analyzer trace is converted, the following names are utilized in the Xgig format:

Table 36: I-Tech to Xgig Port Name Conversion

I-Tech Name	Xgig Port Name	Port Name Meaning
Channel 1A	SAS_Port 0	Initiator transmit port for Link 1
Channel 1B	SAS_Port 1	Target transmit port for Link 1
Channel 1C	SAS_Port 2	Initiator transmit port for Link 2
Channel 1D	SAS_Port 3	Target transmit port for Link 2
Channel 2A	SAS_Port 4	Initiator transmit port for Link 3
Channel 2B	SAS_Port 5	Target transmit port for Link 3
Channel 2C	SAS_Port 6	Initiator transmit port for Link 4
Etc.....	Etc......	Etc.....
N/A	SAS_Port 32	Primitives embedded within Initiator Frames for Link 1
N/A	SAS_Port 33	Primitives embedded within Target Frames for Link 1
N/A	SAS_Port 34	Primitives embedded within Initiator Frames for Link 2
N/A	SAS_Port 35	Primitives embedded within Target Frames for Link 2
N/A	SAS_Port 36	Primitives embedded within Initiator Frames for Link 3
N/A	SAS_Port 37	Primitives embedded within Target Frames for Link 3
N/A	SAS_Port 38	Primitives embedded within Initiator Frames for Link 4
Etc.....	Etc......	Etc.....

Ports 32-63 may or not be created following conversion, depending upon the data within the trace. These ports are only created as necessary. These ports will not be visible in Xgig Expert and it will handle them automatically. The conversion program that imports I-tech SAS/SATA capture files does not currently support primitive sequences within a frame (for example, ALIGN, RRDY, SATA_HOLD, SATA_HOLDA). The occurrence of any primitives within a frame will be placed in an additional port number that is 32 higher than the original port number.

In the Xgig trace format, each port (or channel) represents a single transmitter. Each port is saved to a separate file (with the .BUS extension for SAS traces, .TRC for Fibre Channel trace and .GBE for Gigabit Ethernet traces). Additionally each of the filenames/locations are placed into a .TGP file (Trace Group File), which is the file type that is opened by default in both Xgig Expert and Xgig TraceView.

Chapter 19

Xgig TraceView Tools

In this chapter:

- Get Information on Decodes
- Delta Calculator
- Copy Event Data (Filter on Data Events)
- Export to Text File
- Print the Selected View
- Show Capture Configuration
- Get Trace Information
- Timestamp Options
- TraceView Options
- TCP/UDP Port Mappings
- WWN and MAC Address Decoding

Get Information on Decodes

Changes to the decodes are documented in the file CurrentProtocolVersions.txt. Refer to this file to check for any specific decode improvement. The file is located in the installation directory, typically C:\Program Files\ViaviViavi\Xgig Analyzer\CurrentProtocols\CurrentProtocolVersions.txt. There is also a file located in the installation directory named **XgigProtocolList.txt** which is a complete list of protocols supported by the current release.

Delta Calculator

The **Delta Calculator** feature calculates the delta time between any two events in a trace. The delta time between events can help determine the timing properties of your application or provide general performance information. For example, if you know the approximate quantity of data between events, then the delta time between those same events can give you an evaluation of performance.

You can establish bookmarks at the events for which you want to calculate the delta time.

To use the Delta Calculator with a pre-defined bookmark:

1. Click the Delta Calculator  button in the toolbar or double-click the timestamp. The Delta Calculator dialog box appears.
2. Select the pull down tab under Delta Start Time and select a bookmark.
3. Select the pull down tab under Delta Stop Time and select a bookmark. The delta time displays in the Delta Calculator dialog box.

To use the Delta Calculator with timestamps from the spreadsheet:

1. Click the Delta Calculator  button in the toolbar or double-click the timestamp. The Delta Calculator dialog box appears.
2. Select the pull down tab under Delta Start Time.
3. Click the row in the spreadsheet. Its timestamp appears in the Delta Start Time box.
4. Select the pull down tab under Delta Stop Time.
5. Click the row in the spreadsheet. Its timestamp appears in the Delta Stop Time box.
6. The delta time displays in the Delta Calculator dialog box.
7. The delta time between the two events will display even if the stop time is earlier than the start time.

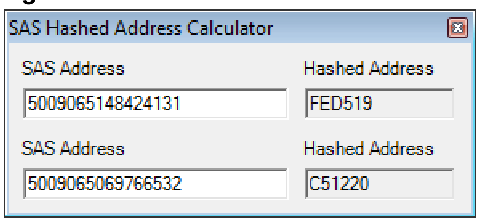
SAS Hashed Address Calculator

The **Hash Calculator** feature creates a 3-byte hashed value of the SAS address or unique World Wide Name. This name/address is an 8-byte hexadecimal value that displays in SAS traces as a 3-byte hashed value. For example, if you know the SAS address or WWN, you can create the 3-byte hashed value and search/filter for that value in the trace.

To use the Hash Calculator:

1. Select **Hash Calculator** from the **Tools** menu. The **SAS Hashed Address Calculator** dialog box appears.
2. Type or paste the text of the WWN in hexadecimal in the **SAS Address** field.
3. The hashed value for the WWN will appear in the **Hashed Address** field.
4. You can copy the values from these fields and paste them into other TraceView dialogs for search/filter.

Figure 180: SAS Hashed Address Calculator



Copy Event Data (Filter on Data Events)

Select **Copy Event Data** from the **Edit** menu to copy the currently selected event's data to the clipboard. Only the currently selected event is copied.

Copy Event Data is useful to copy an event and paste it as a template into the Xgig Maestro BERT software, or any other generator software supporting this feature. For the Xgig Analyzer specifically, Copy Event Data could be used for creating filters or finds based on event data within the trace.

Once event data has been copied, it can be used as a template in either TraceView or TraceControl. In TraceView the template allows you to quickly search for complex events. In TraceControl the template allows you to create trigger conditions for events discovered in TraceView. The copied event data can be pasted anywhere templates can be edited.

To create a filter template based on copied data:

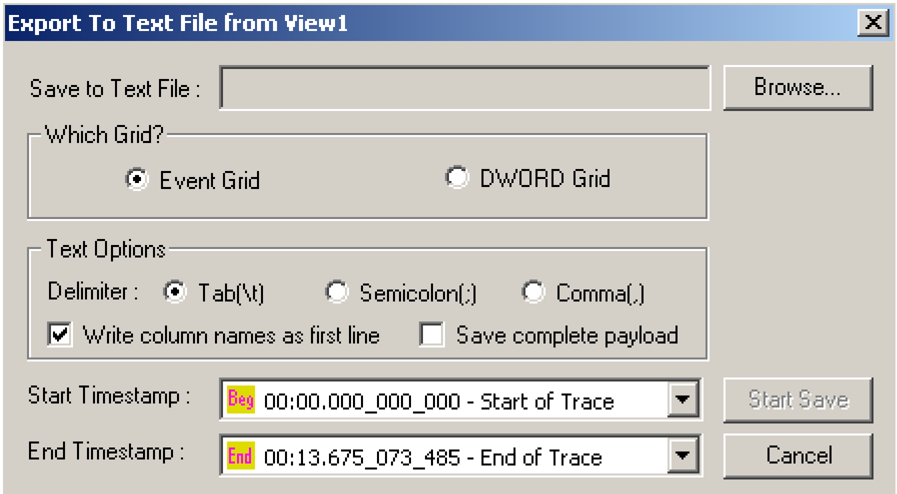
1. Copy trace data by selecting the data and selecting **Copy Event Data** from the **Edit** menu.
2. Go to **Detailed Find/Filter/Color** and right-click n in the **Find**, **Filter**, or **Color** tab.
3. Select **Paste** to create a new filter template based on the copied data.

Export to Text File

You can save your trace as a text file. Select the **Export**  button or select **Export to Text File…** from the **File** menu.

Use the **Grid Options** to select the type of events to export. Use the **Text Options** to set the format of the text data. Use the **Start timestamp:** and **End Timestamp:** fields to set the extent of the trace data to export.

Figure 181: Export to Text File



Grid Options

You can select events from either the main **Event Grid** or **Dword** view.

Text Options

Select a delimiter of **Tab (\t)**, **Semicolon (;)** or **Comma (,)** as the character to separate column data within the exported text.

Select **Write column names as first line** to place the column names as the first text line in the exported file.

If you have the **Summary** column displayed and this column's display option set to **Display Raw Data**, the **Save complete payload** option includes the entire payload/frame information for each event. For Fibre Channel frames, the raw payload data is saved, skipping the Fibre Channel header. For Gigabit Ethernet, the entire frame is saved. If the **Save complete payload** option is not selected, only the first 32 bytes of the data are exported.

The exported file contains the data interpretation as displayed in the **Summary** column. For example, if **Display Short Interpretation** is selected, short summary information is exported to the file. If **Display Raw Data** is selected, raw data is exported. If the **Summary** column is not included in the column display, payload/frame data from the **Summary** field is not included in the exported file.

Set the Beginning and End Points for Export

Set the limits of the trace data to export in the **Start Timestamp:** and **End Timestamp:** fields. The timestamp values to use as the beginning and end points of the export operation are available from each pull-down menu. Two defaults are provided, **Start of Trace** and **End of Trace**.

You can set the limits of the trace data to export by clicking on events in the spreadsheet. Click an event and its timestamp is entered in the **Start Timestamp:** field. Click the **End Timestamp:** field and then on another event in the trace. Its timestamp is entered in the **End Timestamp:** field.

Other timestamps are made available in the pull-down menus by adding bookmarks. Select a timestamp in the trace, right-click the bookmarks column, and select **Bookmark Editor…** to create a bookmark. Once the bookmark is created, the bookmark name appears in the pull-down menus for the **Start Timestamp:** and **End Timestamp:** fields.

Print the Selected View

Select **Print** from the **File** menu to print whichever view you have currently selected (the main spreadsheet or Dword view). All columns for the events that appear in the display will print.

If you want to print a display with many columns, set the printer to print in landscape mode.

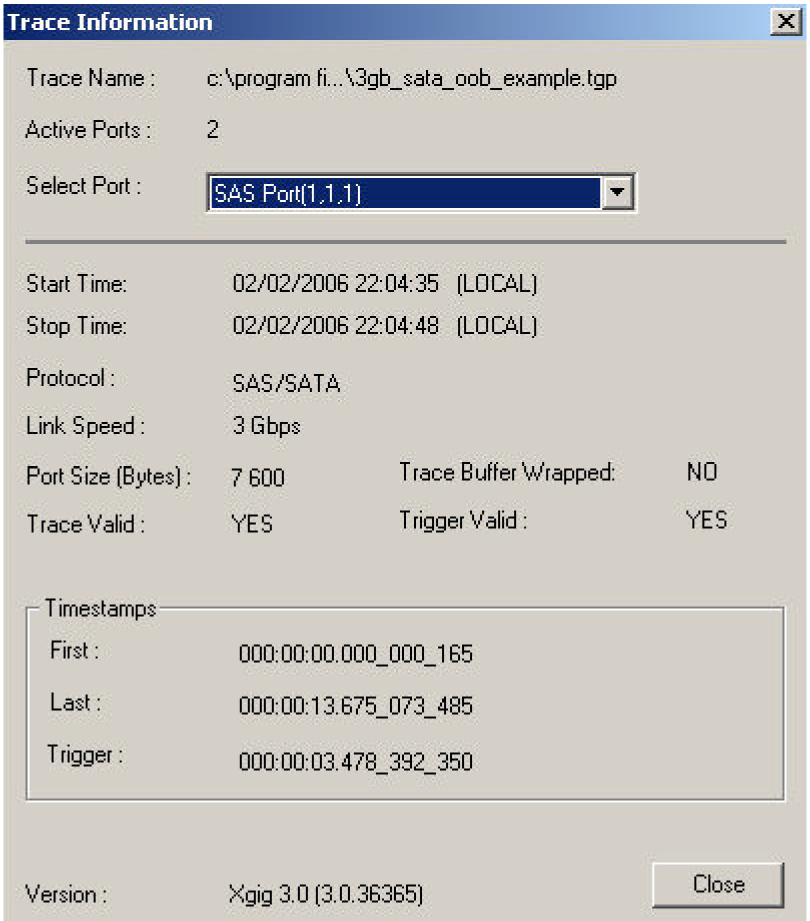
Show Capture Configuration

Select **Show Capture Configuration** for the **File** menu to open a dialog that shows a read only version of the capture configuration defined in TraceControl. If the currently opened trace does not contain a capture configuration, this menu will be grayed out.

Get Trace Information

Press the **Trace Information**  button to display critical information about the current trace. The dialog is also displayed by using the **View > Trace Information...** menu.

Figure 182: Trace Information Message Box



Timestamp Options

Select **Options > Timestamp Format...** from the menu bar to change the format for the timestamp in columns that display a time value. You can select various displays of the date or select an option that displays no date. You can select the granularity of time (milliseconds, microseconds, nanoseconds). An option is also available to convert UTC time values to local time if the trace is from the Xgig chassis. The default option in the Timestamp Format window is **mm/dd hh:mm:ss.ms_us_ns**.

There are also three different ways to reference timestamps in the display. Set this option be right-clicking on a timestamp column or field:

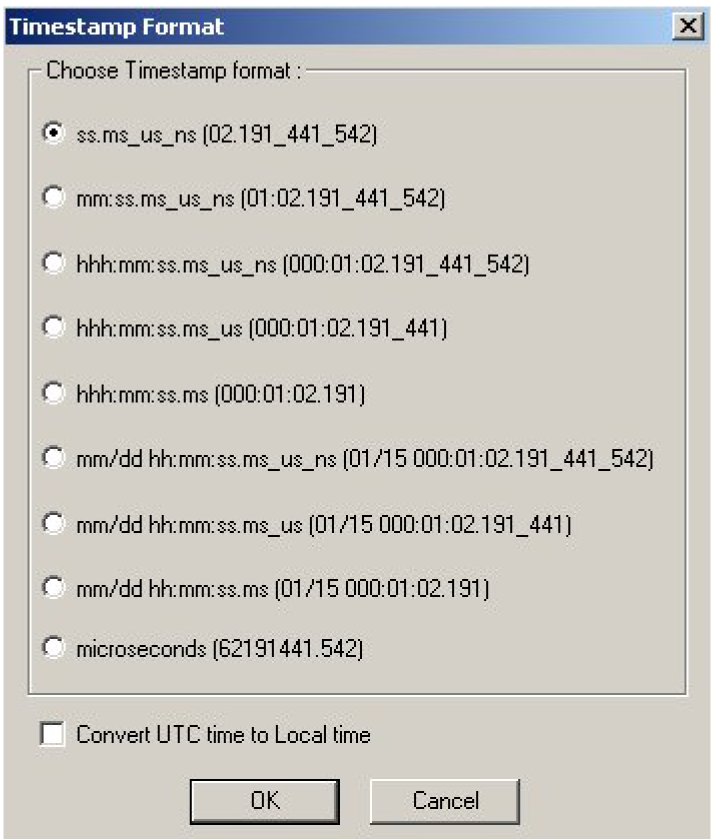
- **Display Calendar Time**
  Sets the timestamp to display as a calendar time based on the system clock at the time of capture.
- **Display Time Relative to Capture**
  Sets the timestamp to display as a time relative to the start time of the capture (first event equals time zero).

- **Display Time Relative to Event**
  Sets the timestamp to display as an time relative to the currently selected event (current event equals time zero).

There are several rules regarding changing the timestamps in TraceView:

- When the timestamp is set to any non-mm/dd format and you change from relative to calendar, mm/dd is added to the timestamp display. For example, 00:00:00.012 becomes 05/22 00:00:00.012.
- When the timestamp is set to the microsecond format and you change from relative to calendar, the timestamp format will change to the **mm/dd hh:mm:ss.ms_us_ns** format.
- When TraceView is set to show calendar time and the timestamp is changed to show any timestamp format without mm/dd, the timestamp changes to **Time Relative to Capture**.
- Xgig hardware supports the conversion between UTC and LOCAL time. UTC time conversion is not available in older trace files.
- All dialogs and displays in TraceView update immediately when the timestamp is changed.

Figure 183: Timestamp Options



TraceView Options

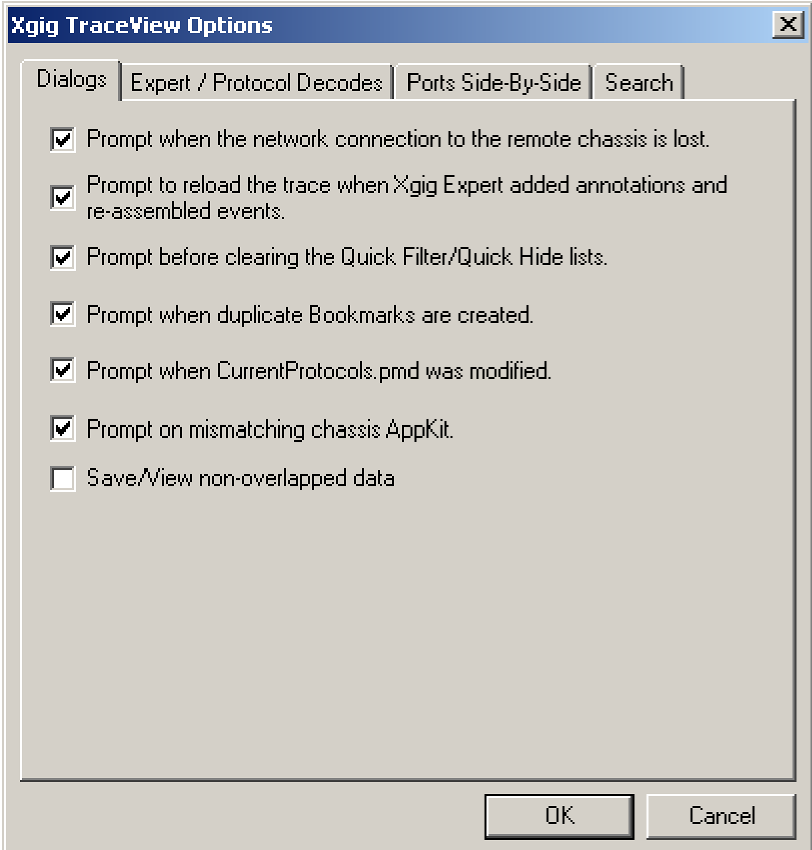
Select **Options > Xgig TraceView Options...** from the menu bar to set configuration options for TraceView. There are three tabs in the **Xgig TraceView Options** dialog:

- **Dialogs** tab
  Use these settings to prevent TraceView from displaying certain dialog messages.
- **Expert/Protocol Decodes** tab
  Use these settings to set the level of integration with Xgig Expert.
- **Ports Side-by-Side Configuration** tab
  Use these settings to set configuration options in the port side-by-side display of trace data, including the option to display one Dword per line.
- **Search** tab
  Use these settings to control the search methods used in the **Quick Find** dialog.

Dialogs Tab

- **Prompt when the network connection to the remote chassis is lost**
  If enabled, TraceView will present a dialog when the connection to the Xgig chassis is lost and you are viewing data directly from an Xgig blade hardware buffer.
- **Prompt to reload the trace when Xgig Expert added more decode information**
  If enabled, TraceView presents a dialog box to reload the trace after a trace has been examined by the Expert application. The Expert application can add more detailed decode information, but you must reload the trace to see this information in TraceView.
- **Prompt before clearing the Quick Filter/Quick Hide lists**
  If enabled, TraceView presents a confirmation message when you press the **Clear** button in the Quick Filter List or Quick Hide List dialog box.
- **Prompt when duplicate Bookmarks are created**
  If enabled, TraceView presents a confirmation message when you attempt to create a bookmark for an event that has already been bookmarked.
- **Prompt when CurrentProtocols.pmd was modified**
  If enabled, TraceView presents a dialog box alerting the user that the compiled decode library used for searching might match different events than what is being decoded and shown in the user interface.
- **Prompt on mismatching chassis AppKit**
  If enabled, TraceView presents a dialog box alerting the user that the compiled decode library on the chassis might match different events than what is being decoded and shown in the user interface.
- **Save/View non-overlapped data**
  By default, this is unchecked. This check box controls two different things. First, it shows/hides the **T1/T2** button in TraceView's menu bar. Secondly, it excludes/includes non-overlapped data while saving. The **T1/T2** button is displayed only when the check box is checked. Once the **T1/T2** button is visible, you can click it so that it is not depressed to view non-overlapped data, or click it so that it is depressed to see overlapped data.

Figure 184: Xgig TraceView Options Dialog Box, Dialogs Tab



Expert/Protocol Decodes Tab

The following options are available for decodes:

- **Show OOB Begin/End markers**
  If this option remains unselected, OOB Begin/End markers are not displayed by TraceView. For certain applications, such looking for a particular speed negotiation window or OOB signal, you may wish to turn on the display of these markers.

  The Begin/End markers enable you to easily see the demarcation between the OOB Sequence and Speed Negotiation Sequence at a high level. Inside of an OOB sequence, the markers show the begin and end limits of different OOB signals. Inside of a Speed Negotiation sequence, the markers show the begin and end limits of different speed negotiation windows. Navigate to a particular OOB signal or speed negotiation window by syncing to these markers. This is especially useful because speed negotiation windows are typically long and contain many events.

  For Begin/End markers to display, you need to display advanced OOB events in the main event grid display. Select **Show Advanced OOB Events** from the OOB toolbar icon pull-down to show these events.

The following options are available for annotations for new traces:

- **Prompt to launch Expert on new traces to add annotations, re-assembled PDUs, and exchange events**

  Selecting this option will bring up a pop up dialog asking if you would like to add annotations using Expert when you open a new trace.

- **Automatically launch Expert on new traces**
  This is the default setting. Selecting this option will automatically launch Xgig Expert in the background when TraceView is launched. Remove the selection of this option if you do not want Xgig Expert to launch when TraceView is launched.

- **Don’t prompt nor launch Expert on new traces**

  Selecting this option means that Expert will not automatically be run for new traces nor will you be prompted if you want to run Expert.

The following options are available for incompatible annotations.

- **Prompt to launch Expert on incompatible annotations and re-assembled events**

  This is the default setting. Selecting this option will bring up a pop up dialog asking if you would like to launch Expert or not. Then you have the choice to run Expert, or TraceView will hide all expert annotations and exchange events.

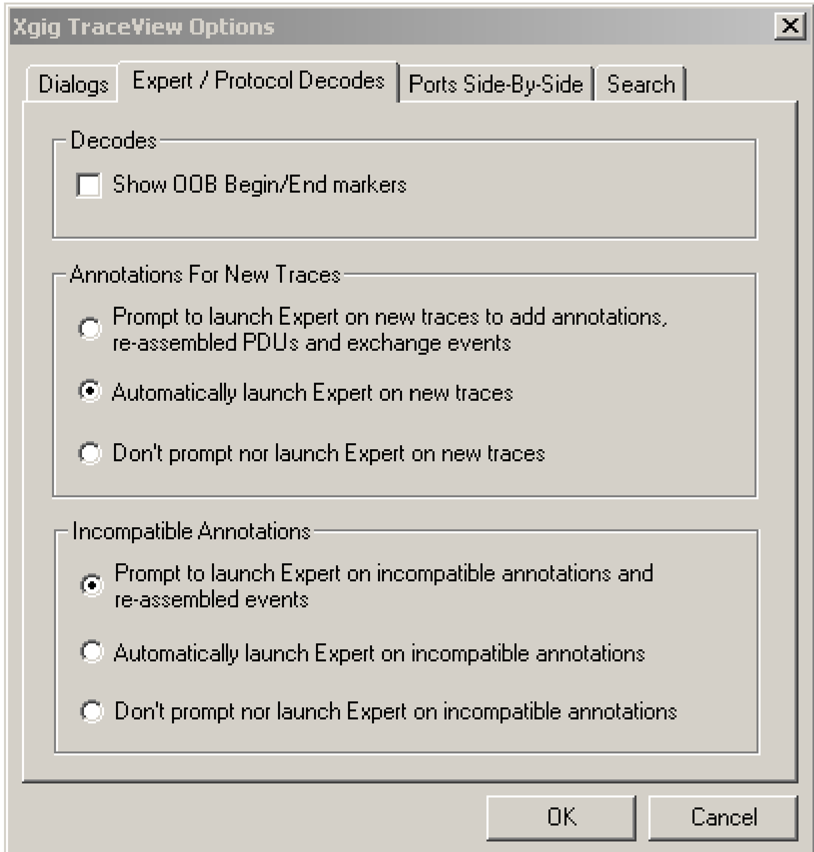
- **Automatically launch Expert on incompatible annotations**

  This is the default setting. Selecting this option will automatically launch Expert in the background when TraceView opens an incompatible trace.

- **Don’t prompt nor launch Expert on incompatible annotations**

  Selecting this option means that TraceView will automatically hide all expert annotations and exchange events on incompatible traces without prompting you.

Figure 185: Xgig TraceView Options Dialog Box, Expert/Protocol Decodes Tab



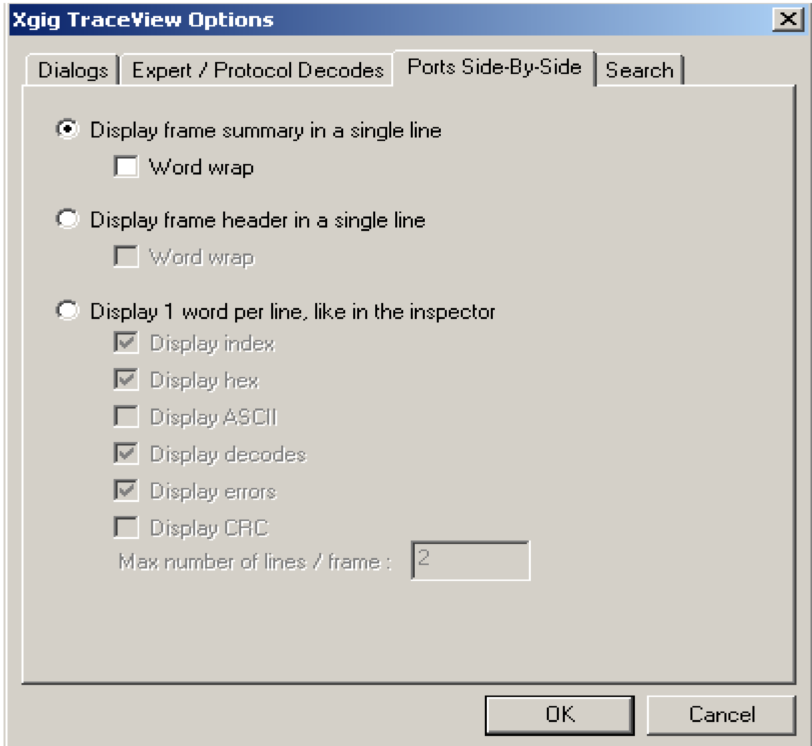
Ports Side-by-Side Configuration Tab

The **Ports Side-By-Side Configuration** tab provides three mutually exclusive options for setting the Port Side-By-Side view.

- **Display frame summary in a single line**
  Select this option to display a frame summary only as a separate row within the spreadsheet for Port Side-By-Side view.
- **Display frame header in a single line**
  Select this option to display each frame header as a separate row within the spreadsheet for Port Side-By-Side view. Frame summaries are also displayed as a separate row.
- **Display 1 word per line like in the inspector**
  Select this option to display each Dword as a separate row within the spreadsheet for Port Side-By Side view. Partial information for each Dword may be displayed. Use the check boxes under this option to set the options you want to display. You can also set the maximum number lines for a single frame. For example, if the maximum number is set to 10, only the first 10 Dwords for that frame will be displayed.

In Port Side-By-Side configuration, frame summaries, frame headers, or Dwords are displayed separately for logical links within a multiplexed port.

Figure 186: Xgig TraceView Options Dialog Box, Ports Side-by-Side Configuration Tab



Search Tab

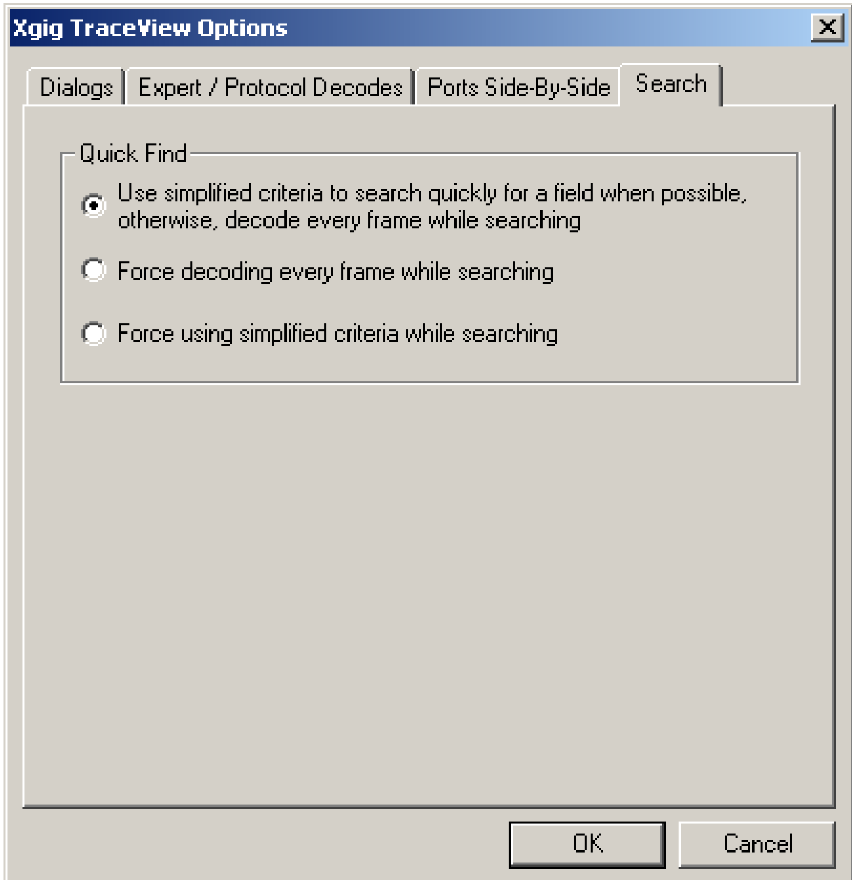
The following search options are available for the Quick Find dialog:

- **Use simplified criteria to search quickly for a field when possible, otherwise, decode every frame while searching**
  When you select this option, Quick Find will automatically perform a simplified search, when the **Field** search is selected, when possible and appropriate. Otherwise, it will perform a compiled decode search.

- **Force decoding of every frame while searching**
  When you select this option, the **Field** search option is replaced by **Factory search** and **Simplified search**, and **Factory search** is selected by default.

- **Force using simplified criteria while searching**
  When you select this option, the **Field** search option is replaced by **Factory search** and **Simplified search**, and **Simplified search** is selected by default.

Figure 187: Xgig TraceView Options Dialog Box, Search Tab



TCP/UDP Port Mappings

You can change the default TCP/UDP port mapping in TraceView and Expert by adding a file `UserTCPUDPServices.txt` file in the installation folder of the Xgig Analyzer. The file format is the same as in `TCPUDPServices.txt`, which is also found in the Xgig Analyzer folder. The easiest method for creating entries is to copy lines from `TCPUDPServices.txt`, paste them in `UserTCPUDPServices.txt`, remove the beginning #, and then modify them. TraceView and Expert loads both files every time they are launched.

For example, assume you want to display port 3260 as HTTP rather than as iSCSI. The default `TCPUDPServices.txt` file defines the TCP port 3260 as iSCSI:

3260 tcp iSCSI iSCSI

Copy the line into `UserTCPUDPServices.txt`, remove the beginning #, and change the mapping to HTTP:

3260 tcp HTTP HTTP

TraceView will now display the decode of port 3260 as HTTP.

Port mappings should only be changed by adding entries to the `UserTCPUDPServices.txt` file.

WWN and MAC Address Decoding

World Wide Names and MAC addresses contain a 24-bit Organization Unique Identifier (OUI). A configuration file, OUI.txt, can be used to set the value of the 24-bit Organization Unique Identifiers (OUI). This configuration file is available in the installation folder of the Xgig Analyzer. 24-bit numbers found in the decode are mapped to the corresponding vendor name by the Xgig applications. You can change the default OUI number mappings by editing the OUI.txt. The content of the file is read at the Xgig applications startup. Open the file in a text editor for more information.

It is also possible to disable the OUI vendor name decoding entirely using the **OUI Interpretation** Decode Switch. Refer to "Decode Switches" on page 385 for more information.

Chapter 20

Xgig Trace View Hints and Tips

In this chapter:

- Trace View Hints and Tips
- Toolbar
- Keyboard Shortcuts

TraceView Hints and Tips

Configuration and Views

Most options are available from the pull down menu. However, some options are only available from the context menu in the spreadsheet view. For example, creating a bookmark or inserting a column.

- You can choose to save the configuration information with a trace file. Select the **Save Viewer Configuration** box when saving the trace.
- Configuration files are independent of traces. You can apply a configuration file you have already developed to a new trace.
- You can view a trace’s configuration file by selecting **File**, **View Capture Configuration**. This opens a read only copy of the TraceControl configuration. You can see the General Settings tab as well as the Capture and Trigger setup tab.
- Use the **Protocol Layer** drop-down menu in the menu bar to view a trace’s protocol layers.
- Use the **Details** Pane to view hex or bit values for information. Use the tabs on the left of the pane to select different views.
- Use the **Dword** tab in the Details Pane to see SAS/SATA traces Dword-by-Dword.
- To return to the “last viewed” trace in the same domain, open TraceView and press the **Open Last Domain**  button.
- The TraceView application automatically saves the current configuration upon exiting and uses it next time.
- Hide the **Histogram** and **Inspector** panes to increase the number of events being viewed.

Navigate, Search

- Drag-and-drop templates from the **Available Templates Browser** to the **Find** tab to setup searches.
- Double-click templates you drag to the **Find** tab if you need to set up a custom template. Creating custom templates works as in TraceControl.
- Right-click a field in the spreadsheet display and select **Quick Find/Filter/Hide** to quickly search for similar items. You can also double-click a field to invoke the **Quick Find/Filter/Hide** dialog.
- Double-click in the **Bookmark** column and type a label to mark an event so you can find it later.
- You can quickly navigate to bookmarks, timestamps, and the trigger position.

Filter and Hide

- Drag-and-drop templates from the **Available Templates Browser** to the **Filter** tab to set display filters.
- Double-click templates you drag to the **Filter** tab if you need to set up a custom template. Creating custom templates works as in TraceControl.

- Right-click a field, and select **Quick Find/Filter/Hide** to quickly hide similar items.
- Check the **Filter Status Area** at the lower right to see the status of all filter operations.
- Right-click a field, and select **Copy Event Data**. Go to **Detailed Find/Filter/Color**, and right-click in the **Find**, **Filter**, or **Color** tab. Select **Paste** to create a new template based on the copied data.
- Click the **Overlapping Data** button to show only events among many devices that occurred in the same time window.
- Click the **Ordered Sets** button to show/hide ordered sets and primitives. Set the options for this button to see only certain subsets of all ordered sets or primitives.
- You can copy the hex data in the Details Pane to paste in the **Template Editor**.

Columns

- To get a menu for column display, right-click column headers.
- To get a menu for column operations, right-click column values
- TraceView has a list of columns to choose from. The column you need is probably in the list.
- You can add information to a column by selecting **Add to this Column**, so it contains exactly the information you want.
- TraceView's list of pre-defined columns includes special composite columns called field groups. Field groups are columns full of useful decode information.
- Select the **Ports Side-by-Side** configuration from the **File > Load Configuration > Default Ports Side-by-Side** menu to see all ports as columns.
- Select **Autofit Side-by-Side Port Columns** from the **View** menu to fit all port columns in the display when in the **Ports Side-by-Side** configuration.

Histograms

- Use the yellow extent markers to zoom in on a specific area of the trace.
- Resize the gray areas in the histograms to further narrow the area of trace to look at.
- The upper histogram is a complete histogram of the gray area in the lower histogram.
- The gray area in the upper histogram represents the events displaying in the spreadsheet.

Tools

- Use **Export to Text File** to export a trace or parts of a trace to a text file. Use **Save As** to save a subset of a trace file.
- To establish an alias for any value in the display, right-click a field, select **Set Alias** .
- For SAS, use the **Hash Calculator** tool to calculate a 3-byte hashed address from an 8-byte World Wide Name.

Toolbar

The toolbar provides shortcuts to commonly used functions.

Figure 188: TraceView Toolbar

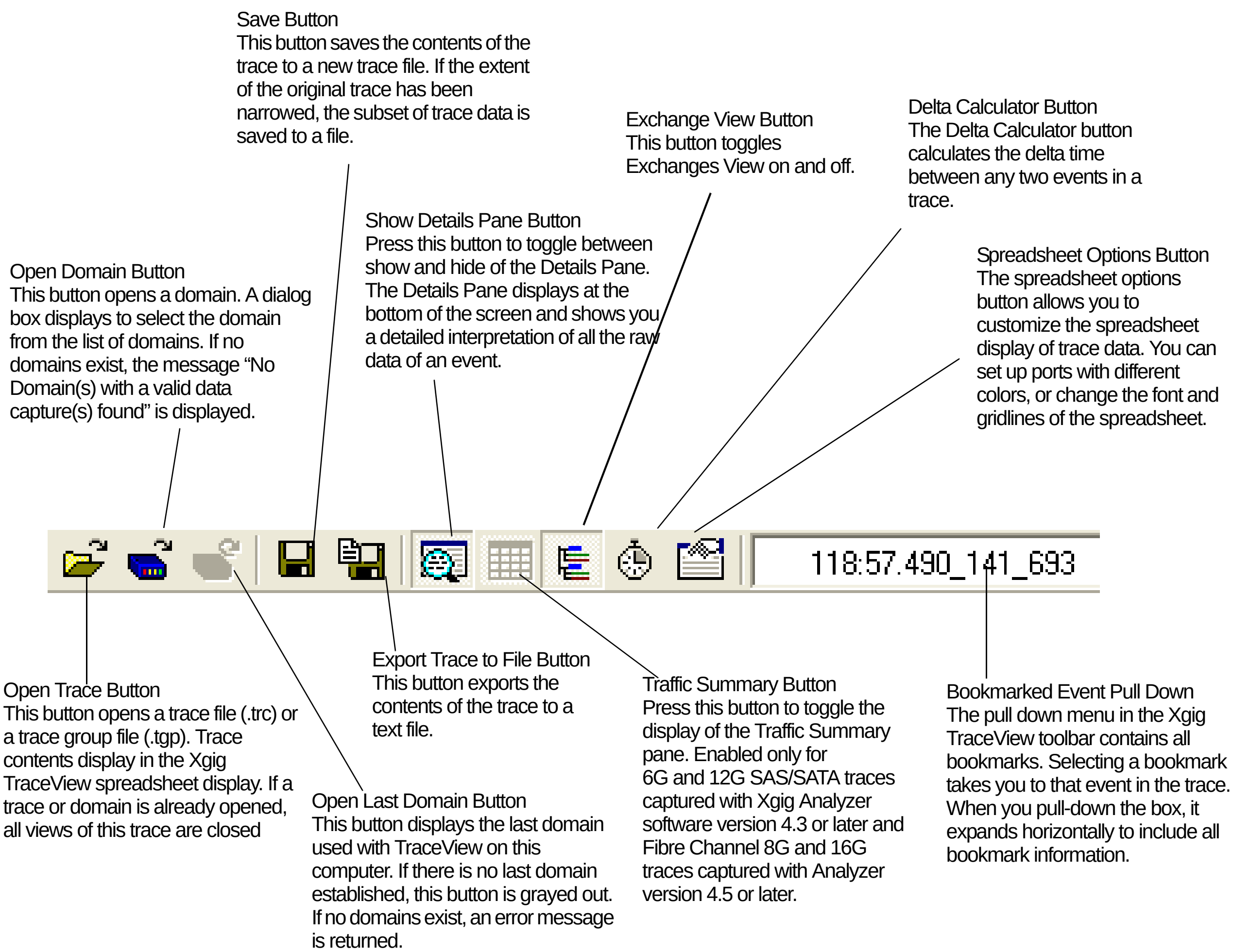


Figure 189: TraceView Toolbar (continued)

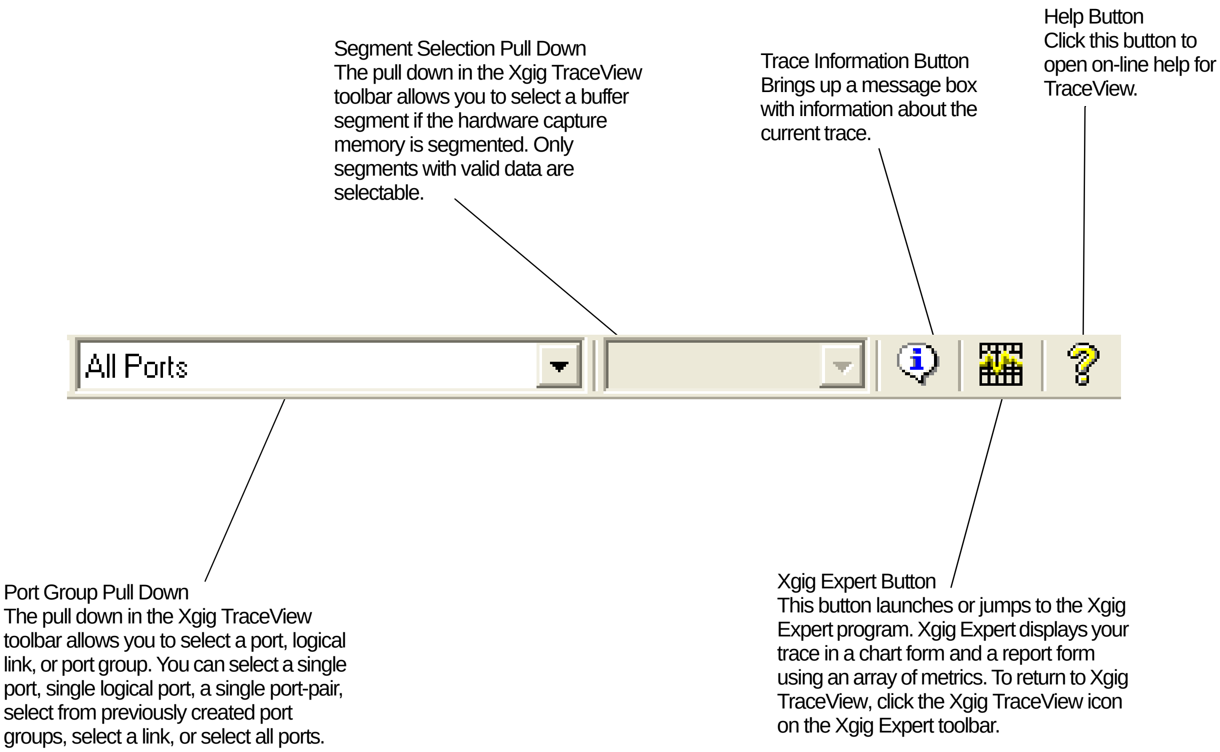


Figure 190: TraceView Navigation Toolbar

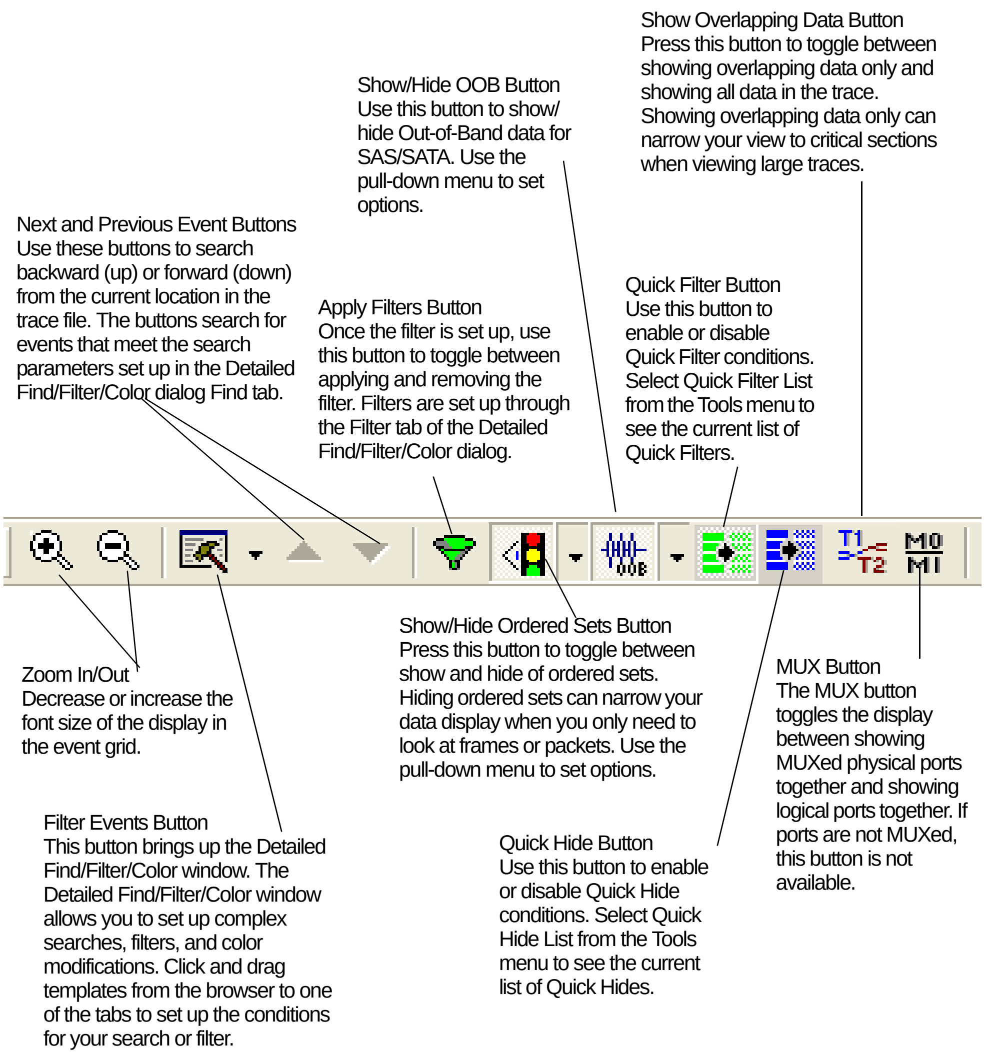
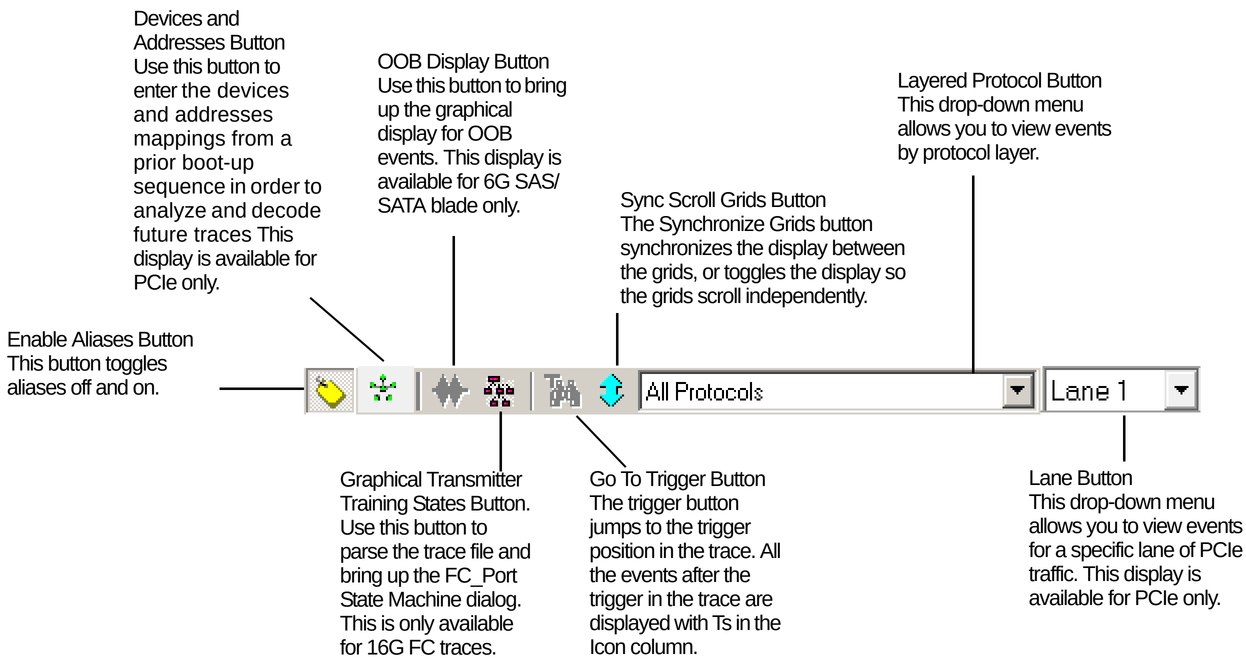


Figure 191: Trace Navigation Toolbar (continued)



Keyboard Shortcuts

Table 37:   Keyboard Shortcuts, TraceView

Key	Description
Ctrl +N	Open a New View
Ctrl +O	Open Trace File
Ctrl +D	Open Domain
Ctrl +P	Print
Ctrl + +	Zoom In
Ctrl + –	Zoom Out
Ctrl +C	Copy Event Data
Ctrl + F3	Quick Find/Filter/Hide
Shift +F3	Detailed Find Previous
Ctrl + E	Synchronize all views
F1	Help
F2	Apply filters

Table 37: Keyboard Shortcuts, TraceView

F3	Detailed Find Next
F4	Show / Hide Ordered Sets
F5	Sync Scroll Grids
F7	Go to Trigger
F8	Show / Hide OOB
F9	Go to Expert
Shift +F11	In Traffic Summary, Go to previous occurrence
F11	In Traffic Summary, Go to next occurrence
Keyboard Shortcuts When Selecting Column Data...	
Ctrl +Q	Quick Find/Filter/Hide
Ctrl +R	Set Alias
Ctrl +C	Copy Event Data
Keyboard Shortcuts from Bookmark Column Only...	
Ctrl +R	Bookmark
Ctrl+1	Set Global Cursor 1
Ctrl+2	Set Global Cursor 2
Keyboard Shortcuts From the Available Template Browser...	
Enter	Open…
Ctrl +C	Copy
Ctrl +X	Cut
Ctrl +V	Paste
Del	Delete
F2	Rename

PART FIVE: Using Xgig Expert

Chapter 21

Xgig Expert

In this chapter:

- Key Features of Xgig Expert
- Opening a Trace
- Switching to TraceView

Key Features of Xgig Expert

Xgig Expert  is an analysis tool for Fibre Channel, FCP-SCSI, Gigabit Ethernet, IP, TCP, iFCP, FCIP, iSCSI, SAS, SATA, PCIe, NVMe, and AHCI traffic. Xgig Expert automatically identifies protocol violations and errors within the trace as well as providing a rich set of metrics for performance and behavioral analysis. Traces from Gigabit Ethernet topology, SAS/SATA topology, or Fibre Channel topology (Arbitrated Loop, Public Loop, Switch Fabric, etc.) are supported and automatically analyzed when opened.

You can launch Xgig Expert from Xgig TraceControl, from Xgig TraceView, or from the desktop. To invoke Xgig Expert from Xgig TraceControl or Xgig TraceView, select the Xgig Expert icon from the toolbar.

The Xgig Expert on-line help system has extensive information on how to run the Expert program. Also refer to the *Xgig Expert: Analysis Tool for Fibre Channel Networks, A Case Study and User's Guide* for an extended example of using Xgig Expert software.

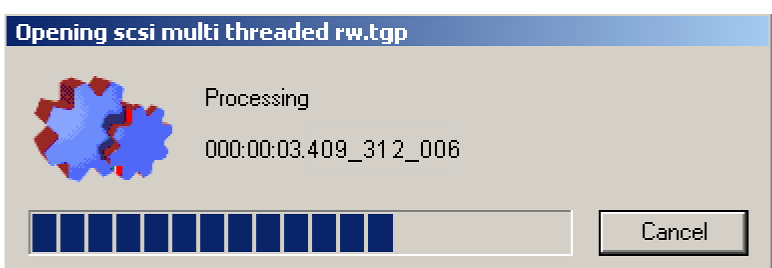
Some key features of Xgig Expert are listed below:

- The **Graph View** button allows you see key metrics over time as line graphs. Data rate is given in megabytes/ per second as well as I/O per second. The queue depth is plotted for all initiators and all targets over the length of the trace.
- The **Add Counters** button (**+**) shows a window which displays the wide range of metrics available in Xgig Expert.
- The **Report View** button allows you to create a report with performance statistics taken over the entire length of the trace.
- **Debug View** shows the topology and details for categories of debug events.

Opening a Trace

The **Opening Trace** screen appears while Xgig Expert calculates statistics for the selected trace file or the selected domain

Figure 192: Opening Trace Progress Message.



After analyzing the trace, Xgig Expert opens **Debug View**, showing the topology and details for categories of debug events.

Switching to TraceView

To switch to Xgig TraceView application, from the Xgig Expert **View** menu select **Go to Xgig TraceView** or click the Xgig TraceView icon on the toolbar. TraceView automatically jumps to the timestamp nearest to the currently selected item in Expert. You can also right-click a timestamp in the **Timestamp** window of Xgig Expert and select **Copy**. Switch to Xgig TraceView, paste the timestamp into the **Timestamp** box of TraceView, and press **Enter**.

Figure 193: Xgig Expert Main View

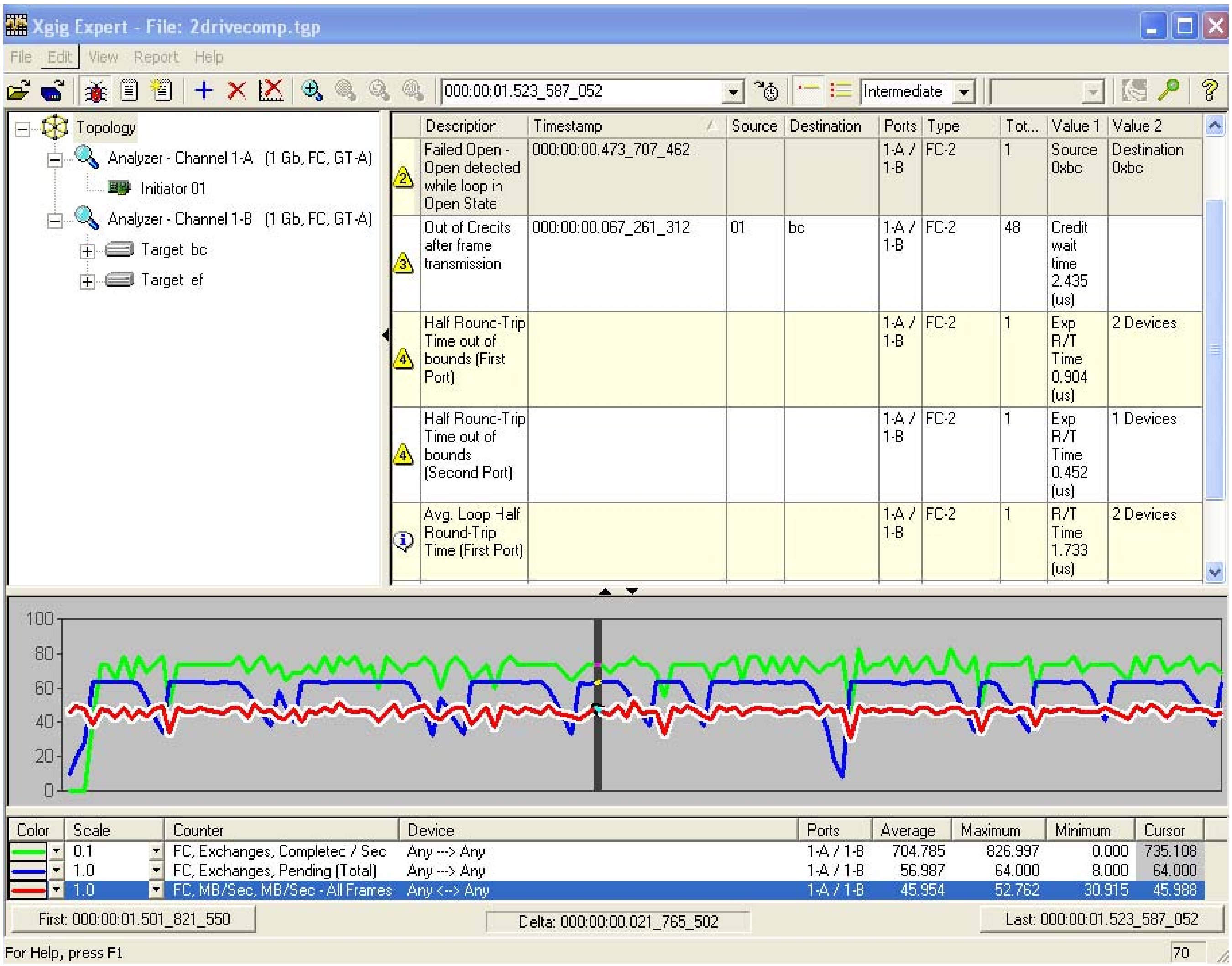
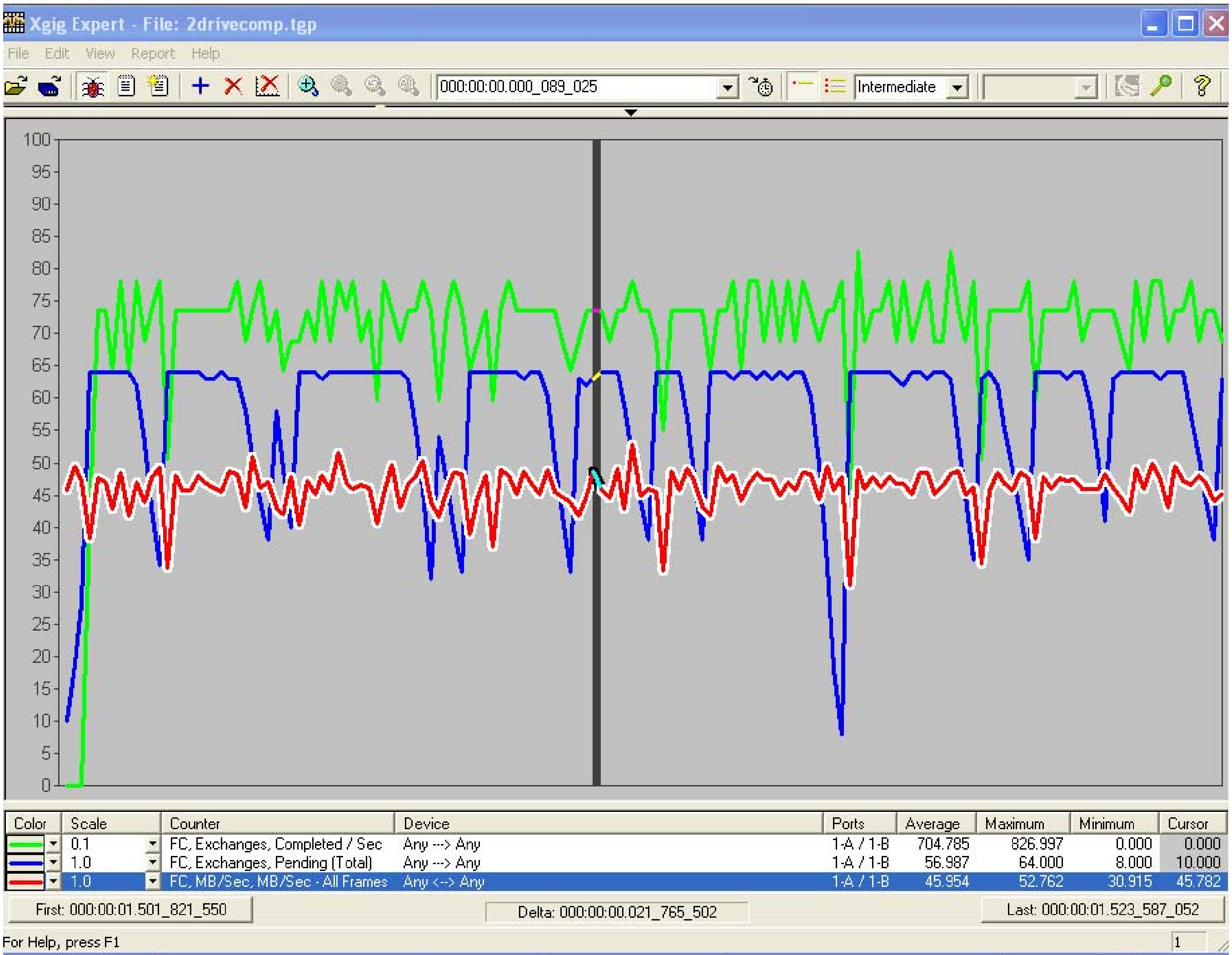


Figure 194: Xgig Expert Graph View



PART SIX: Appendices

Appendix A

Analyzer File Formats

The following file formats are defined for Xgig Analyzer.

.trc extension -- Single-port Trace Files for Fibre Channel or SAS/SATA

A .trc file contains all the data collected by a single Fibre Channel or SAS/SATA analyzer hardware port.

.gbe extension -- Single-port Trace Files For GigE

A .gbe file contains all the data collected by a single Gigabit Ethernet analyzer hardware port.

.alias extension -- Aliases file for a trace

An .alias file is a file containing all of the aliases for a trace file. It has the same name as the trace file.

.tgp extension -- Trace Group Files

Trace group files (.tgp) are a collection of trace files (.bus, .trc, or .gbe) for the Xgig Analyzer. The trace group file only contains a list of .trc or .gbe files that are to be displayed. When opened in TraceView, all the data in the listed files are interleaved by timestamp when displayed.

.bus extension -- Single-port Trace Files for SAS/SATA

A .bus file contains all the data collected by a single SAS/SATA Bus Doctor analyzer phy, after conversion from Bus Doctor format to Xgig format.

.cfg extension -- Xgig TraceView Configuration files

Xgig TraceView configuration files (.cfg) control the display of the data. The columns, colors, searches, filters, views, and groups, are all saved in the configuration file. Aliases and bookmarks are saved directly in the trace file and are available regardless of the configuration file. The Xgig TraceView program looks for a Xgig TraceView configuration file of the same name as the .tgp or .trc file that it is opening. If this file cannot be found, the program will open the last configuration used. If there is no last configuration used, the program opens a default configuration file.

.tcc extension -- Xgig TraceControl Configuration files

The Xgig TraceControl configuration file (.tcc) controls all configuration for capturing traces. This includes the information you can specify from the Xgig TraceControl Configuration screen such as link speed setting, signal regeneration setting, trace size options, capture options, and trigger options.

.ffg extension -- Filter Group Configuration files

The Filter Group configuration file (.ffg) saves all configuration information applied to the **Find**, **Filter**, and **Color** tabs in the Detailed Find/Filter/Color window. Any changes made to the templates using the **Frame**, **Qualifiers**, or **Containing** tabs will be saved in the .ffg file.

.hst extension -- Capture File Format for Surveyor

The .hst file format is used by the Viavi Surveyor application. TraceView can save or open files in this format. TraceControl can save traces from Xgig hardware into this format.

.pcapng extension -- Capture File Format as PCapNg File

The .pcapng file format can be saved by TraceControl and TraceView to save trace trace information to be used by applications other than Xgig Analyzer. One of these applications is WireSharkfiles

.cap extension -- Capture File Format for Surveyor

The .cap file format is used by the Viavi Surveyor application. TraceView can save or open files in this format.

Appendix B
Connection and Wiring Examples

In this appendix:

- Connecting the Xgig Blade
- Connecting the Xgig Blade Through a Tap

The following examples show two ways to connect Xgig Multi-Function Blades to the network. There are many other possibilities. After reading this section, if you need help with a special configuration contact Customer Support.

Warning: Do not look directly into the end of a fiber or the connector. Exposure to laser radiation can cause eye injury.

Make sure that you connect the blade ports to the correct media type — Fibre Channel ports to Fibre Channel links, GigE ports to GigE links, or SAS/SATA ports to SAS/SATA links.

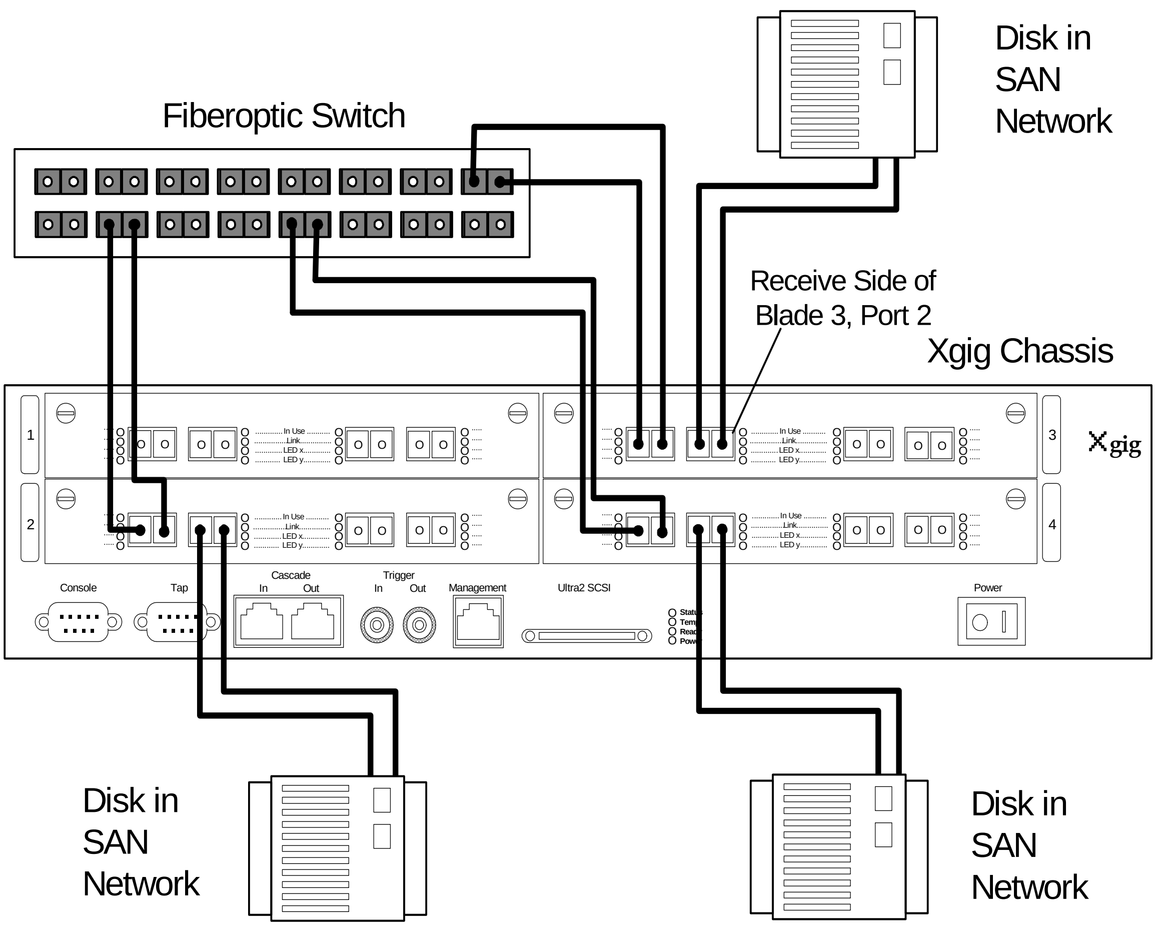
Example Direct Connection, Fibre Channel Network

The following configuration shows a single Xgig Four Slot Chassis with four Xgig Multi-Function Blades. In the example, three links are monitored via direct connection to the Fibre Channel ports.

The four blades can be used to set up eight Fibre Channel links for analysis and monitoring purposes. The number of links to be monitored can be increased up to a maximum of 32 by cascading 4 chassis together. The receive side for each analyzer port is always on the right.

To directly connect to Fibre Channel ports, each side of the link must be connected to the same port-pair. Port-pairs are defined by adjacent ports (port 1 and port 2, or, port 3 and port 4) on the same blade. In the example below, each link is connected to port 1 and to port 2 on an Xgig Multi-Function Blade.

Figure 195: Xgig Direct Connection



Some examples of unusable connections follow.

- You cannot connect one side of the link to blade 1, port 1 and connect the other side of the link to blade 2, port 1.
- You cannot connect one side of the link to blade 1, port 2 and connect the other side of the link to blade 1, port 3.

Example Connection Through Taps, Fibre Channel Network

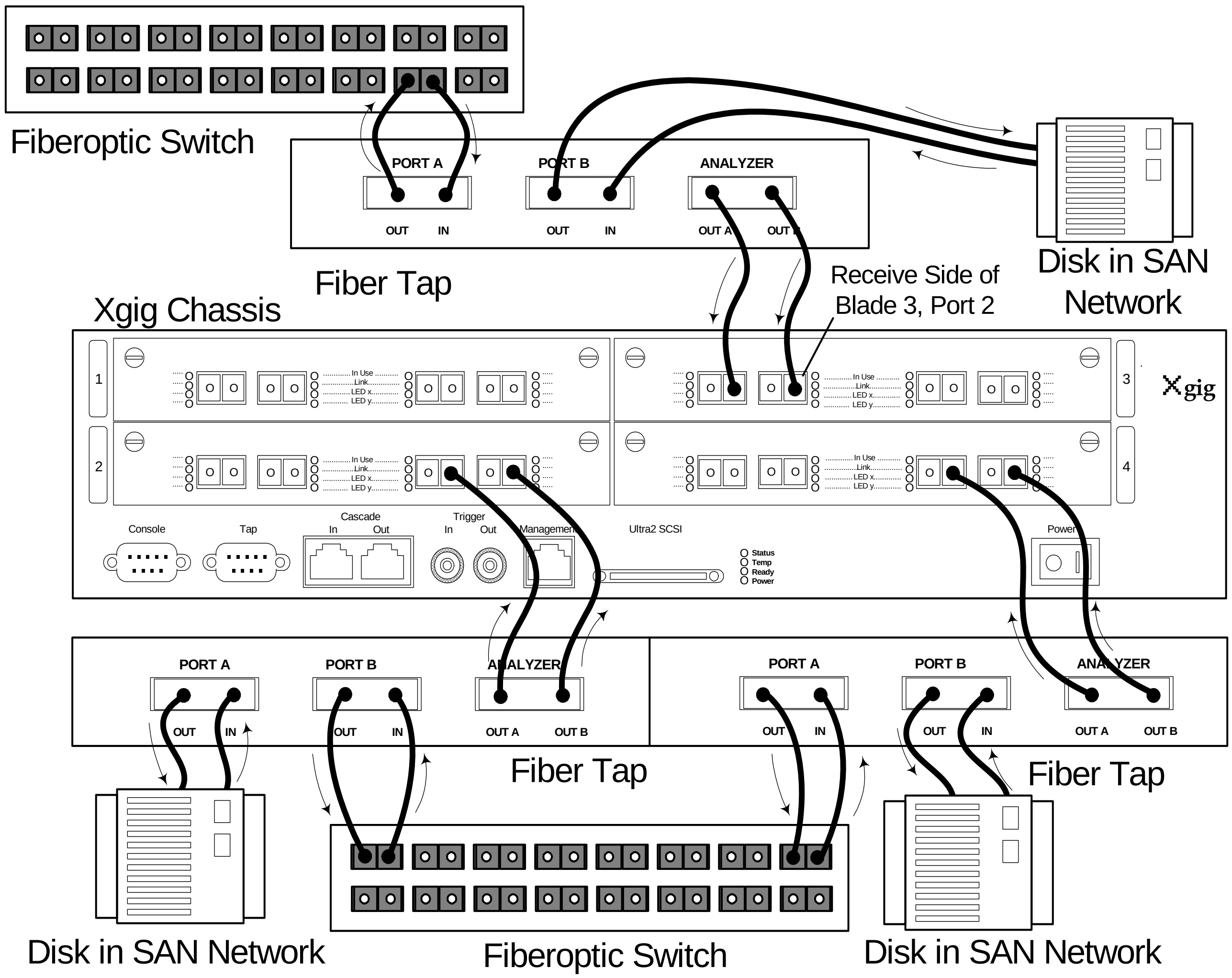
The following configuration shows an Xgig Four Slot Chassis with four Xgig Multi-Function blades. Three links are monitored using three single-port fiber taps.

The tap ports are connected to the Rx ports on the Xgig Multi-Function blades in the Xgig chassis. Use the Receive side (right side) of the ports ONLY when passively monitoring a link with the Xgig Multi-Function blades.

To correctly monitor both directions of a Fibre Channel link through a tap, each side of the link must be connected to the receiving ports of the same port-pair. Domain creation is performed using the TraceControl program.

By attaching both tap ports to the ports of an Xgig Multi-Function Blade port-pair, you can guarantee that the ports are part of the same domain. For example, connect one side of the link from the tap to Chassis 1, Blade 2, Port 3 and one side to Chassis 1, Blade 2, Port 4, as shown in Figure 196.

Figure 196: Xgig Analyzer Connection Through Taps



The small arrows in the figure show the data flow.

Appendix C

Protocol Display Color Coding

Protocol color coding is applied based on the protocol detected by TraceView. Types of frames and ordered sets are displayed using distinctive colors. You must select the **Use Color Coding Based On Protocol (Bus Doctor)** from the **Spreadsheet Options** dialog box to have protocol color schemes applied to the decode.

Fibre Channel, iSCSI, SAS/SATA, and NVMe protocols are supported for color coding in this release.

The protocol-based color scheme is the same color scheme used by Viavi’s Bus Doctor Plus bus analyzer product. For SAS, color is applied on the **count-OS-IU Type** column. For SATA, color is applied on the **count-OS-IU Type-FIS** column. For FC, color is applied on the **count-OS-Rctl** column. For Dword view and in port side-by-side view, the port column is colored. Primitives (including SOF and EOF) not shown as separate events in the spreadsheet display do not have an assigned color. However, since these primitive events show on separate lines in Dword view, they will have an assigned color in Dword view. For visibility, an event with an error has its text colored in red throughout all columns. For NVMe, command, status, and data entries are colored in the Side A and Side B columns in the main event grid.

Colors in the Dword view will be applied to the summary cell of the Dword matching the field code or event type.

Colors are assigned for each protocol as described in the following tables.

Table 38: iSCSI Color Coding

Item	**Background Color**	**RGB Components**	**Foreground Color**	**RGB Components**
Any Error		255, 255, 255		255, 0, 0
BHSopI* = SCSI Cmd		0, 0, 128		255, 255, 255
BHSopT* = SCSI Resp		0, 128, 0		255, 255, 255
BHSopI = Login Cmd		153, 35, 66		255, 255, 255
BHSopT = Login Resp		0, 128, 128		255, 255, 255
Everything else		255, 255, 255		0, 0, 0

* BHSopI and BHSopT: Basic Header Segment Opcode for initiator/target

Table 39: Fibre Channel Color Coding

Item	Background Color	RGB Components	Foreground Color	RGB Components
Any Error		255, 255, 255		255, 0, 0
Ordered Sets		255, 255, 255		128,128,0
FCP_CMND(RCtl=06), FCP_RSP(RCtl=07)		0, 128, 0		255, 255, 255
Loop Init Sequence		255, 102, 0		255, 255, 255
Extended Link Services(RCtl=22-23)		0, 128, 128		255, 255, 255
Everything else		255, 255, 255		0, 0, 0

Table 40: SAS/SATA Color Coding

Item	Background Color	RGB Components	Foreground Color	RGB Components
Any Error		255, 255, 255		255, 0, 0
SATA_EOF, EOF, EOAF		128, 128, 128		255, 255, 255
SATA_SOF, SOF, SOAF		0, 0, 0		255, 255, 255
Remaining Primitives		255, 255, 255		128,128,0
SATA_FIS27		153, 35, 66		255, 255, 255
SATA_FIS34		255, 255, 0		0, 0, 0
SATA_FIS39		0, 0, 128		255, 255, 255
SATA_FIS41		0, 128, 0		255, 255, 255
SATA_FIS46		0, 128, 0		255, 255, 255
SATA_FIS58		0, 128, 128		255, 255, 255
SATA_FIS5F		51, 204, 204		0, 0, 0
SATA_FISA1		224, 224, 224		0, 0, 0
SSP_IU01		0, 128, 0		255, 255, 255
SSP_IU05		0, 128, 0		255, 255, 255
SSP_IU06		0, 128, 0		255, 255, 255
SSP_IU07		0, 128, 0		255, 255, 255
SSP_IU16		0, 128, 0		255, 255, 255
SSP_IU40		0, 0, 128		255, 255, 255
SSP_IU41		0, 0, 128		255, 255, 255
AF0		153, 35, 66		255, 255, 255
AF1		153, 35, 66		255, 255, 255
Vendor Specific (UIF0-FF)		0, 128, 0		255, 255, 255
Everything else		255, 255, 255		0, 0, 0

Table 41: NVMe Color Coding

Item	Background Color	RGB Components	Foreground Color	RGB Components
NVMe Command		153, 35, 66		255, 255, 255
NVMe Status		255, 255, 0		0, 0, 0
NVMe Data		0, 128, 0		255, 255, 255

Appendix D

Xgig Chassis Trigger/Stop from the Command Line

You can Trigger or Stop captures at the Xgig chassis from the command line of remote clients.The domain being triggered/stopped needs to be created using TraceControl. However, without TraceControl installed on the client work station, the user or a high-level application can stop or trigger all ports in a domain with a simple command line interface.

The remote command line operations are supported through a free utility which is downloaded from the Internet. The syntax for the command line described in this Appendix must be followed for the utility to work with Xgig chassis.

Requirements

- Xgig Chassis (server) must have Xgig Server Appkit Version 3.2.x or greater
- An HTTP utility that will perform an HTTP POST operation.
  For example, **Wget.exe** V1.10 or better can be installed on the client.**Wget.exe** supports a "-post-data" parameter on the client work station where the command line interface will be used. **Wget.exe** is free and can be downloaded at http://users.ugent.be/~bpuype/wget/
- The client work station that runs **wget.exe** must have access through the network to the Xgig Chassis being controlled. The machine that runs **wget.exe** does not need to have the TraceControl Application software installed.
- Domain(s) must be created prior using the command line using TraceControl application software.

Command Line Interface

The command line interface is used to issue the stop/trigger on the running domain in the Sync Group. Command can be applied for intra-chassis or inter-chassis domains as long as the domain name is specified. The parameters enclosed in braces <> are user-supplied values that are required to complete the command option. The command line parameters enclosed in brackets [ ] are optional.

The **wget** options described here are those relevant to using the command to control Xgig. There are other options available for the **wget** command. Refer to the **wget** documentation available on the http://users.ugent.be/~bpuype/wget/ web site.

Important: Passwords specified in the command are the administrative passwords for the Xgig Chassis, not the user names and passwords used to log in as a client of Xgig.

Command Syntax:
wget [-O-] "--post-data=Parameters=/<MODE> \"<DOMAIN_NAME>\" [/PASSWORD \"<SLAVE_USERNAME:SLAVE_PASSWORD>\"] " http://<MASTER_USERNAME:MASTER_PASSWORD>@<HOST>/cgi-bin/domaincontrol.pl

Example:
wget -O- "--post-data=Parameters=/TRIGGER \"My Domain\" /PASSWORD \"MySlave:MySlavePassword\"" http://MyUserName:MyPassword@MyChassis/cgi-bin/domaincontrol.pl

Parameter Descriptions

-O-
This optional parameter causes the output/result from the Xgig chassis to display on the standard output device.

/MODE:
The MODE can be either **STOP** or **TRIGGER**. With the **STOP** option, the capture running on the specified domain will stop immediately. With the **TRIGGER** option, the capture running on the specified domain will trigger immediately and will stop after post-fill is satisfied. The mode is case insensitive and is a required field.

Note: In a SAS domain, the analyzer can be stopped with either TRIGGER or STOP commands; however, a non-SAS domain (Fibre Channel, Ethernet) may not stop unless you use the command with the /MODE option set to STOP.

\"<DOMAIN_NAME>**\"**
The Domain Name to be stopped or triggered. For Sync Groups with duplicated domain names for running capture domains, the first matching domain in the Sync Group data base will be selected. The Domain Name must be enclosed in **\"** and **\"** (for example, **\"My Domain\"**); the Domain Name can have spaces within the name. The Domain Name is case sensitive and is a required field.

/PASSWORD **\"<**SLAVE_USERNAME>:<SLAVE_PASSWORD>**\"**
This option is required only if the specified DOMAIN_NAME contains ports on a single slave chassis of the Sync Group. This option is ignored if the requested domain contains ports on more than one chassis or in the master chassis.

If the /PASSWORD is specified, the slave user name and password must be enclosed by **\"** and **\"** and separated by a colon. User name and password are case sensitive. Example: **/PASSWORD \"My Slave:MySlavePassword\"**

Note: If the ports within the domain are located in a single chassis other than the master of the Sync Group AND the **/PASSWORD** option is not specified, the default user name and password **JDSU:JDSUsnt** is used. The master chassis will forward the request to the chassis that is associated with the domain.

<MASTER_USERNAME>:
User name to access the Master chassis of the Sync Group. User name and password are case sensitive. This is a required field.

<MASTER_PASSWORD>
Password to access the Master chassis of the Sync Group. User name and password are case sensitive. This is a required field.

<HOST>
Xgig Chassis name or IP address of the Master chassis in the Sync Group. This is a required field.

Examples of Using Wget

Stop Example

Assume you wish to stop a domain named "My Domain (1,1,1)" in the Sync Group. This domain is created as inter-chassis domain with ports located in 2 or more chassis. The following are the chassis name and the user name and password:
Master chassis name is "MyChassis"
User name to access Master chassis is "MyUserName"
Password to access Master chassis is "MyPassword"

The following command will stop the capture for the domain:

```
wget -O- "--post-data=Parameters=/Stop \"My Domain (1,1,1)\"" http://MyUserName:MyPassword@MyChassis/
cgi-bin/domaincontrol.pl
```

Trigger Example

Assume you wish to trigger the domain "My Domain (1,2,1)" in the Sync Group. This domain is created as an intra-chassis domain with all ports are located in the Master Chassis. The following are the chassis name and the user name and password:
Master chassis name is "MyChassis"
User name to access Master chassis is "MyUserName"
Password to access Master chassis is "MyPassword"

The following command will trigger the capture for the domain:

```
wget -O- "--post-data=Parameters=/Trigger \"My Domain (1,2,1)\"" http://MyUserName:MyPassword@MyChassis/
cgi-bin/domaincontrol.pl
```

Trigger Example for Ports on Slave Chassis

Assume you wish to trigger the domain "My Domain (2,1,1)" in the Sync Group. This domain is created as an intra-chassis domain and contains only ports that are located in a single slave chassis. The following are the chassis name and the user name(s) and password(s):
Master chassis name is "MyChassis"
User name to access Master chassis is "MyUserName"
Password to access Master chassis is "MyPassword"
User name to access Slave chassis is "SlaveUserName"
Password to access Slave chassis is "SlavePassword"

The slave user name and password is required to forward the request to the slave chassis. The following command will trigger the capture for the domain:

```
wget -O- "--post-data=Parameters=/TRIGGER \"My Domain (2,1,1)\" /PASSWORD
\"SlaveUserName:SlavePassword\""  http://MyUserName:MyPassword@MyChassis/cgi-bin/domaincontrol.pl
```

Output Samples

Output appears on the standard output device if the **-O-** option is used in the command line.

Example Output, Ports on Master and on Slave Chassis

The domain in this output sample is a inter-chassis domain (composed of ports from more than one chassis in the Sync Group).   The user name to access the Master Chassis is "JDSU", and the password is "JDSUsnt".

Note that the variable DomainType is used to indicate if the domain is an intra-chassis domain (Local) or an inter-chassis domain (Global).

```
C:\>wget -O- "--post-data=Parameters=/TRIGGER \"My Domain (1,4,1)\" http://JDSU:JDSUsnt@xgigsim-7/cgi-bin/
domaincontrol.pl

--10:30:48--  http://JDSU:*password*@xgigsim-7/cgi-bin/domaincontrol.pl

      => `-'

Resolving xgigsim-7... 10.11.7.84

Connecting to xgigsim-7|10.11.7.84|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

[<=>                                          ] 0          --.--K/s

Domain      = My Domain (1,4,1)

Option      = TRIGGER

SyncChannel  = 0

DomainType   = Global

CurrRunState = Capture is Running

PostExeState = Triggered

Status      = Executed

   [ <=>                                      ] 187        --.--K/s


10:30:49 (14.51 MB/s) - `-' saved [187]
```

Example Output, Ports on Slave Chassis

This output is for a command to a intra-chassis domain with all ports on slave chassis (2nd chassis). In this example command:

- My Domain (2,1,1) is a local domain which contains ports within the slave chassis (2nd chassis).
- The slave password is not provided in the command line. Therefore, the master chassis uses the default user name and password when forwarding the request to the 2nd chassis.

```
C:\>wget -O- "--post-data=Parameters=/TRIGGER \"My Domain (2,1,1)\"" http://JDSU:JDSUsnt@xgigsim-7/cgi-bin/
    domaincontrol.pl

--10:30:45--  http://JDSU:*password*@xgigsim-7/cgi-bin/domaincontrol.pl

      => `-'

Resolving xgigsim-7... 10.11.7.84

Connecting to xgigsim-7|10.11.7.84|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]


  [<=>                                    ] 0         --.--K/s

Domain     = My Domain (2,1,1)

Option     = TRIGGER

ForwardingTo = XGIGSIM-6 (10.11.7.70)


Option     = TRIGGERSYNC

SyncChannel  = 120

DomainType   = Local

ReqChassis   = 2

MyChassis    = 2

DomainValue  = 0

CurrRunState = Capture is Running

PostExeState = Triggered

Status     = Executed

  [ <=>                                   ] 314       --.--K/s


10:30:46 (23.30 MB/s) - `-' saved [314]
```

Example Script

Complete command example scripts (.cmd files) are installed with the Xgig Analyzer Software and are located in \Program Files\Viavi\Xgig Analyzer\Scripts. An example script is shown below.

```
@echo off
set domain=%1
set chassis=%2
set mode=%3

if '%chassis%'=='' goto end_usage
if '%domain%'=='' goto end_usage
if '%3'=='' set mode=TRIGGER

wget -O- "--post-data=Parameters=/%mode% \%domain%" http://JDSU:JDSUsnt@%chassis%/cgi-bin/domaincontrol.pl
goto end_all

:end_usage
echo ==============================================================================================
echo TriggerAnalyzer.cmd - Remote triggering for Xgig Analyzer domains via HTTP.
echo ==============================================================================================
echo Usage:
echo This batch file requires two parameters:
echo 1. The Domain Name to trigger/stop (eg: "My Domain (1,1,1)" - note the quotes are required with spaces!)
echo 2. The Chassis Name or IP Address (eg: Xgig02005584 or 10.22.10.5)
echo Optional Parameter:
echo 3. Mode to use: STOP or TRIGGER - defaults to TRIGGER
echo ==============================================================================================
echo Example:
echo TriggerAnalyzer "My Domain (1,1,1)" Xgig02005584
echo Translates to:
echo wget -O- "--post-data=Parameters=/TRIGGER \"My Domain (1,1,1)" http://JDSU:JDSUsnt@Xgig02005584/cgi-bin/
domaincontrol.pl
echo ==============================================================================================
echo NOTES:
echo 1. In a SAS domain, the analyzer can be stopped with either TRIGGER or STOP commands, however,
echo    a non-SAS domain (i.e. Fibre Channel, Ethernet) will not stop if sent TRIGGER and the analyzer mode
echo    (set by TC) is not configured for "Stop after trigger".  In this situation, it would be necessary
echo    to use the STOP command!
echo 2. This batch file assumes the use of default username and passwords on the chassis and would need
echo    to be modified accordingly if non-default values are utilized.
echo 3. This tool requires the utility wget.exe version 1.10 or newer, which can be downloaded from:
echo    http://users.ugent.be/~bpuype/wget/
echo 4. For full documentation on this feature see the Xgig Analyzer Users Guide (XgigAnalyzerUG.pdf).

:end_all
```

INDEX

Symbols

Numbers

A

B

C

December 2015
English

Viavi Solutions

North America:	**1.844.GO VIAVI / 1.844.468.4284**
Latin America	**+52 55 5543 6644**
EMEA	**+49 7121 862273**
APAC	**+1 512 201 6534**
All Other Regions:	**viavisolutions.com/contacts**
email	**customer.care@viavisolutions.com**