Agilent
Protocol Analyzer

User's Guide

Agilent Technologies

Notices

Trademarks

Windows 2000®, Windows XP®, and Microsoft .NET Framework 1.1® are U.S. registered trademarks of Microsoft Corporation.

Installation Guides

You can find the installation guides for different components of the product on the product CD. Agilent recommends you to do not switch on the instrument before you have understood all the applicable installation instructions and have met all the installation prerequisites.

Where to find more information

You can find more information about Protocol Analyzer from the following link:

http://www.agilent.com/find/spt

For further assistance, you can search for a local contact on the following link:

http://www.agilent.com/find/assist

Warranty

Technology Licenses

Restricted Rights Legend

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Safety Symbols on Instruments

Indicates warning or caution. If you see this symbol on a product, you must refer to the manuals for specific Warning or Caution information to avoid personal injury or damage to the product.

Frame or chassis ground terminal. Typically connects to the equipment's metal frame.

Indicates hazardous voltages and potential for electrical shock.

Indicates that antistatic precautions should be taken.

Indicates hot surface. Please do not touch.

Indicates laser radiation turned on.

CSA is the Canadian certification mark to demonstrate compliance with the Safety requirements.

CE compliance marking to the EU Safety and EMC Directives.

ISM GRP-1A classification according to the international EMC standard.

ICES/NMB-001 compliance marking to the Canadian EMC standard.

Environmental Information

	This product complies with the WEEE Directive (2002/96/EC) marking requirements. The affixed label indicates that you must not discard this electrical/electronic product in domestic household waste. *Product Category:* *With reference to the equipment types in the WEEE Directive Annex I, this product is classed as a "Monitoring and Control instrumentation" product.* **Do not dispose in domestic household waste.** **To return unwanted products, contact your local Agilent office, or see www.agilent.com/environment/product/ for more information.**

Printing History

Agilent Technologies, Inc. can issue revisions between the product releases to reflect the latest and correct information in the guide. Agilent Technologies, Inc. also reserves its right to not issue a new edition of the guide for every system release.

The name of the guide and its part number are:

Manual Name: Agilent Protocol Analyzer - User's Guide

Manual Part Number: E2960-91050

The edition number of the guide, publishing time of the guide, and applicable release number of the product are given in the following table.

Edition	Published	Applicable Release
2	March, 2007	6.3

Printed In Germany

Agilent Technologies
Herrenberger Strasse 130
D-71034 Boeblingen, Germany

Contents

5   Triggers

Index

1

Introduction

About Protocol Analyzer   **12**
About Starting and Closing Protocol Analyzer   **14**

This chapter introduces you to the Protocol Analyzer application and provides information on accessing and exiting the Protocol Analyzer GUI.

Agilent Technologies

About Protocol Analyzer

Agilent Protocol Analyzer is an advanced verification system that allows you to capture the data traffic generated by various protocols, such as PCI Express (PCIe), Advanced Switching Interconnect (ASI), and Fibre Channel (FC). It also enables you to view and analyze the captured data to identify problems, find their root cause, and troubleshoot them. This makes Protocol Analyzer a very effective tool to control as well as speed the development and testing of the PCIe, ASI, and FC protocols.

A brief list of the features of Protocol Analyzer is given below:

- Provides full support for Gen1 and Gen2 specifications of PCIe. That is, provides x1, x2, x4, x8, and x16 link widths with 2.5 Gbps/lane to 5.0 Gbps/lane for PCIe

- Provides upto x8 link width with 2.5 Gbps/lane for ASI, and 4 Gbps/lane for FC.

- Provides 2 GB of trace memory.

- Provides a trigger sequencer with sophisticated trigger capabilities and storage qualifications. This helps to monitor desired type of traffic and data patterns.

- Enables to trigger on protocol errors and on the electrical idle condition.

- Provides non-intrusive traffic capturing.

- Supports for filtering the captured trace to help you expedite analyzing the traffic by removing undesired fields from the trace.

- Provides support for manual as well as automatic selection of the speed.

- Provides various probing options for the different types of applications.

- Provides a multiplexer to map physical lanes into logical lanes for managing various pin configurations on a mid-bus probe.

- Provides multi-port display for better insight into the system.

- Provides GUI for trigger setup, search, filter, and error detection.

- Provides easy visibility into protocol transactions. For example, it displays the traffic activity, port link status, and trace content simultaneously.

- Provides tabular traffic display that helps to expedite the debug process.

- Supports cross-triggering with Agilent Logic Analyzer.

NOTE	Protocol Analyzer has two interfaces: GUI and API. This guide covers only the GUI aspect of the Protocol Analyzer application. For information on API, please refer to the online help. Also, this guide covers the Protocol Analyzer GUI only. To understand the hardware aspect of Protocol Analyzer, please refer to:

- *Agilent Midbus Probe, User's Guide*
- *Agilent System Protocol Tester, Installation Guide*
- *Agilent System Protocol Tester, Hardware and Probing Guide*

About Starting and Closing Protocol Analyzer

Before you get started with Protocol Analyzer, you need to know how to access it.

In this section, you will learn about:

- Understanding Protocol Analyzer Session
- Accessing Protocol Analyzer
- Exiting Protocol Analyzer

Understanding Protocol Analyzer Session

In the context of Protocol Analyzer, a *session* represents the components, such as Controller PC, serial I/O modules, and probe, involved in a test. A session forms the basis of communication between the controller PC and the serial I/O modules.

Figure 1 displays the components involved in a Protocol Analyzer session. It also displays that more than one client can be associated with one session.
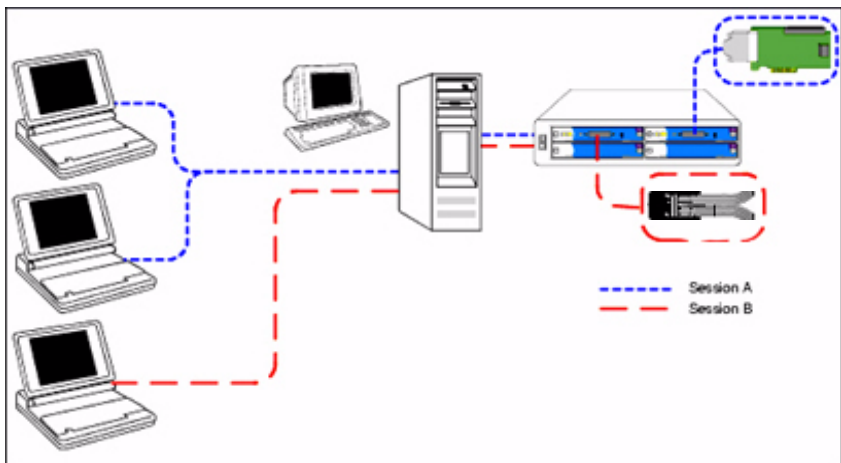
Figure 1   Protocol Analyzer Sessions and Components

In Protocol Analyzer, there are two types of sessions:

- **Online**: In *online session,* you capture real-time packets to analyze. Starting an online session establishes communication between the client and the controller PC, and also loads the necessary firmware on the desired serial I/O module. Therefore, to start an online session, ensure that at least one serial I/O module is connected with the Controller PC. Ending an online session releases the serial I/O module, thus enabling it to be used for a new session.

- **Offline**: In *offline session*, you do not need to connect the Controller PC with any I/O module. Instead, you only need to open the file containing the earlier captured Protocol Analyzer data. You generally start an offline session when you want to view the packet data saved in a file on a computer, and do not want to establish connection with any external hardware device.

> **NOTE** Some options in an offline session are disabled due to their dependency on the connected hardware.

Protocol Analyzer does not enable you to lock a session (online or offline). Therefore, it is possible for multiple Protocol Analyzer instances to concurrently access a single session.

> **NOTE** The controller PC does not protect against meaningless, or even conflicting requests. Therefore, it is recommended that only one user should *own* a particular session at a time.

Accessing Protocol Analyzer

Accessing Protocol Analyzer requires you to specify whether you want to connect to a new or an existing session, name of the session, and the name of the server where you want to start the session. Accessing Protocol Analyzer also requires you to specify the port to use if you are trying to connect to a new session.

To specify all required inputs, Protocol Analyzer provides two dialog boxes: Select type of connection (Figure 2) and Port Selection (Figure 3).
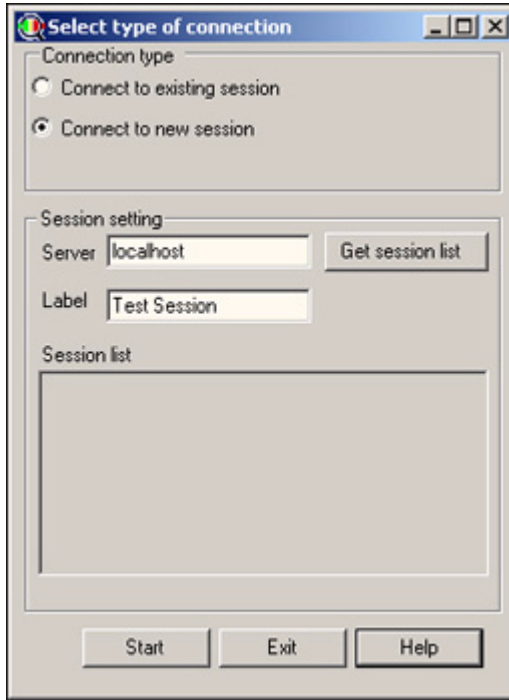
Figure 2   Select type of connection dialog box

Table 1 briefly describes the components of the Select type of connection dialog box.

Table 1   Components of the Select type of connection dialog box

Component	Description
Connect to existing session	Select **Connect to existing session** if you want to use an existing session of Protocol Analyzer on a known server. The existing session can be either initiated by the API or by another GUI since multiple GUIs can share the same session.
Connect to new session	Select **Connect to new session** if you want to create a new Protocol Analyzer session on a known server.
Server	Specifies the name or IP address of the server, where you want to start a new or join an existing Protocol Analyzer session. Its default value is **localhost**.
Get session list	Click **Get session list** to retrieve a list of existing Protocol Analyzer sessions from the server you specified in the **Server** text field. This button works only if you have selected the **Connect to existing session** option.

Table 1   Components of the Select type of connection dialog box

Component	Description
Label	Specifies the name of the session. By default, it takes the user name that you use to log on to your computer.
Session list	Displays a list of sessions existing on the server you specified in the **Server** text field.
Start	Click **Start** to start a new Protocol Analyzer instance.
Exit	Click **Exit** to close the dialog box without starting the Protocol Analyzer application.
Help	Click **Help** to display the online help.

Figure 3 displays the Port Selection dialog box.
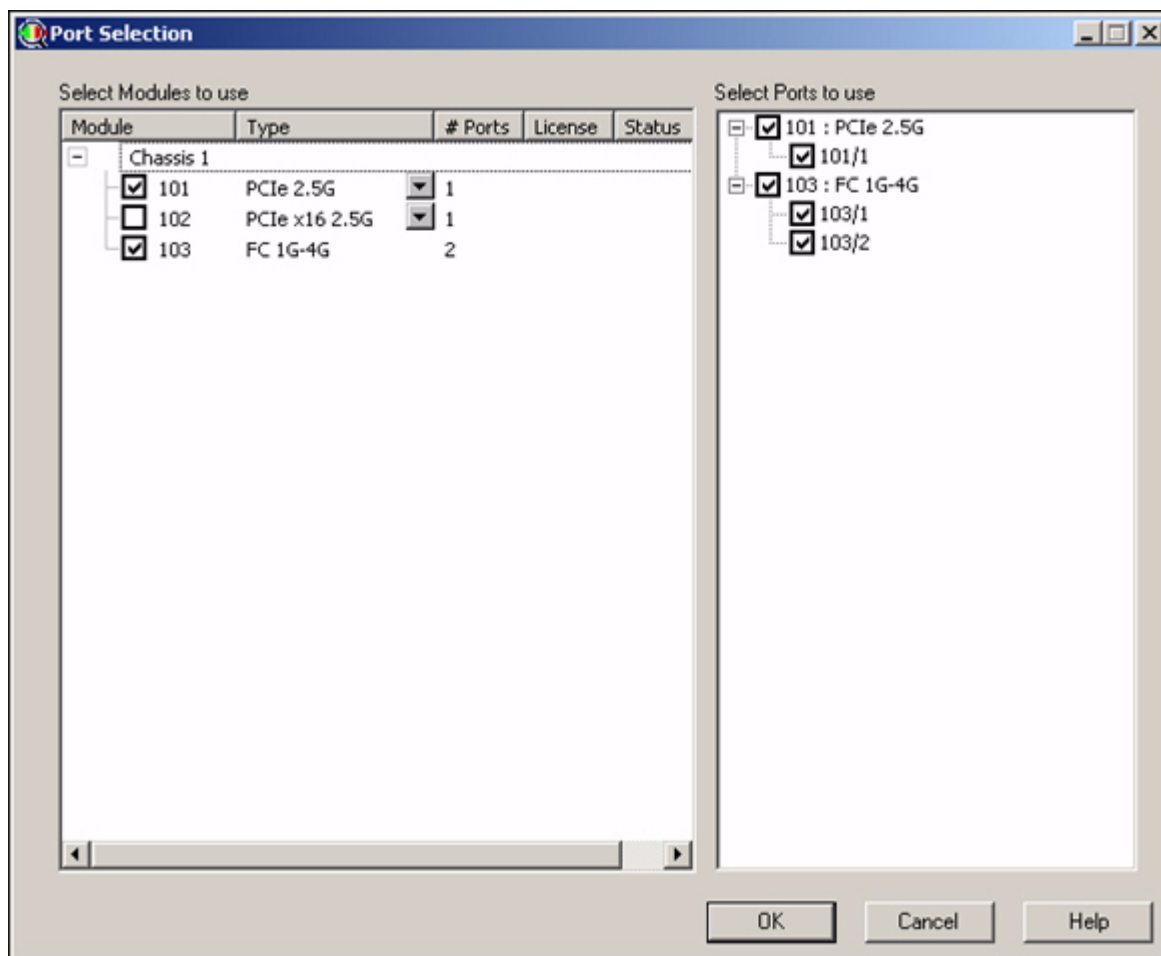
Figure 3   Port Selection dialog box

Table 2 briefly describes the components of the Port Selection dialog box.

Table 2   Components of the Port Selection dialog box

Component	Description
Module	The **Module** column provides a list of modules in the form of check boxes. These check boxes are organized under the expandable list of chassis to which they belong. Here, select a module on which you want to start a new session. A module, which is already associated with a session, appears disabled.
Type	The **Type** column enables you to select the type of protocol to use for each port, such as PCIe, ASI, or FC. This column also shows: • The speed of the port, such as 2.5G or 4G, at which it captures the data. • The link width of the PCIe ports, such as x8 or x16.
# Ports	The **# Ports** column displays the number of ports available for each module.
License	The **License** column displays the license details of each module.
Status	The **Status** column displays the status of each module. This column displays the following messages: • **Rebooting**: This message indicates that the serial I/O module is restarting. • **Ready**: This message indicates that you can now add port to the session. • *Session_Name*: *Session_Name* is the name of the session. This message indicates that the *Session_Name* session is now connected with the port.
Select Ports to use	Select the port to use from the **Select Ports to use** list box.
OK	Click **OK** to start an instance of Protocol Analyzer on the selected port. Clicking OK may start the new Protocol Analyzer instance after a few seconds delay. This is because depending on the selected protocol, appropriate software is first downloaded for the new Protocol Analyzer instance.
Cancel	Click **Cancel** to close the Port Selection dialog box without selecting any port.
Help	Click **Help** to display online help.

To find more information about your licensed software, view the Software Packages Management dialog box. To access this dialog box, click **File > Software Packages**.

To access Protocol Analyzer

1 On the Windows task bar, click **Start > Programs > Agilent System Protocol Tester > Protocol Analyzer**.

The Select type of connection dialog box appears.

2 Do one of the followings:

   a Click **Connect to existing session** to use an existing Protocol Analyzer session.

   b Click **Connect to new session** to start a new Protocol Analyzer session.

3 Type the name or IP address of the server, where you want to start a new or join an existing Protocol Analyzer session, in the **Server** text field.

4 Type in the session name in the **Label** text box.

5 If you are trying to use an existing Protocol Analyzer session, do the following:

   a Click **Get session list**. A list of sessions that are currently running on the server specified in the Server text field is displayed in **Session list**.

   b Select the required session from **Session list**.

   c Click **Start**. The main Protocol Analyzer window appears.

6 If you are trying to create a new Protocol Analyzer session, do the following:

   a Click **Start**. The Port Selection dialog box appears.

   b Select a module check box from the **Module** column.

   c Select an appropriate option from the **Type** drop-down list.

   d Click **OK**. The main Protocol Analyzer window appears.

Exiting Protocol Analyzer

To exit from Protocol Analyzer:

1 Click **File > Exit**.

The Exit dialog box appears (Figure 4).
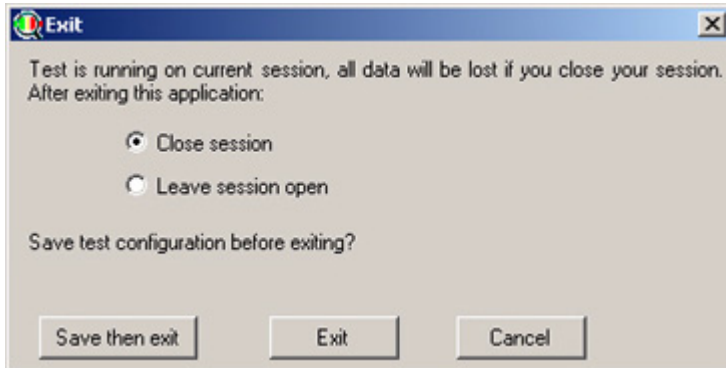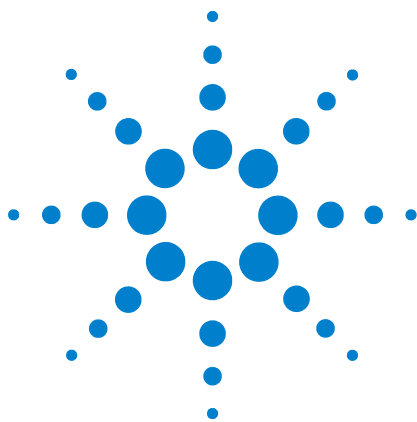
Figure 4 Exit dialog box

2 Do one of the following:

a Select **Close session** to remove the associated session before to closing the Protocol Analyzer window.

b Select **Leave session open** to close the Protocol Analyzer window without removing its associated session.

3 Do one of the following:

a Click **Save then exit**, to save the test configuration before exiting.

b Click **Exit**, to exit without saving the test configuration.

c Click **Cancel**, to quit Exit dialog box and return to Protocol Analyzer.

NOTE Closing a session automatically makes all the GUI interfaces that are connected to it, inaccessible.

2

Getting Started

This chapter briefly introduces you to the main screen components of the Protocol Analyzer application. This chapter also introduces you to loading and saving the Protocol Analyzer data.

Agilent Technologies

About the Protocol Analyzer Components

Protocol Analyzer provides various components that you can use to access its various features.

Figure 5 displays the Protocol Analyzer application window with its main components.
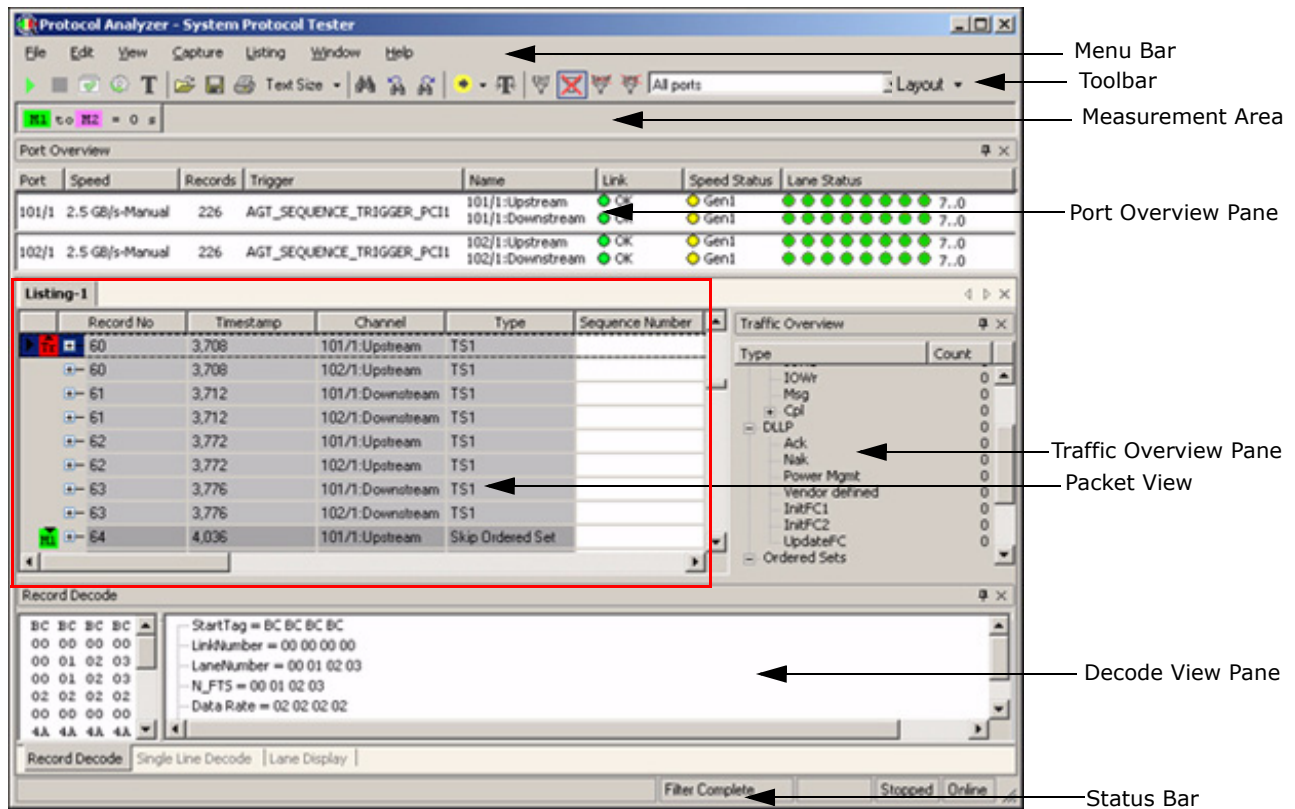
Figure 5   Protocol Analyzer window

This section covers the following topics:

- Protocol Analyzer Window
- Menu Bar
- Toolbar
- Panes

Protocol Analyzer Window

The main components of the Protocol Analyzer window are briefly described below:

- **Menu Bar and Toolbar**: They provide easy and quick access to the features of the Protocol Analyzer application.
- **Measurement Area**: It displays the time gap between two markers.
- **Packet View**: It displays detailed information about all the traced packets.
- **Panes**: They display information about traffic, hardware status, decoded form of the packet data, and the port on which Protocol Analyzer is running.
- **Status Bar**: It displays the current status of the various Protocol Analyzer activities, such as if it is online or offline, and if it is running, triggered, or stopped.

| NOTE | Menu bar, toolbar, and panes are described separately in the following sections. For more information on the Measurement area and the Packet view, refer to Customizing Protocol Analyzer on page 45. |

Menu Bar

In Protocol Analyzer, menu bar provides the following menus:

- File menu
- Edit menu
- View menu
- Capture menu
- Listing menu
- Window menu
- Help menu

File menu

Table 3 provides a brief description of the File menu commands.

Table 3   File menu commands

Menu command	Description
Open	Displays the Open dialog box that enables you to open the configuration (.xml) file and/or the binary (.pad) file.
Save As	Displays the Save As dialog box that enables you to save the configuration (.xml) file and/or the binary (.pad) file.
Text Export	Displays the Save As dialog box that enables you to save the trace to a file in text format.
Close	Closes the currently active listing tab in the Packet view.
Page Setup	Displays the Page Setup dialog box that enables you to specify the page settings for printing the trace.
Print	Displays the Print dialog box that enables you to print the traced data.
Software Packages	Displays the Software Package Management dialog box that shows you a list of already installed software packages, and allows you to install new software packages. To install a new software package using this dialog box: **1** Select the new software package to be installed from the Select Package drop-down list. **2** Type the license key of the new software package in the Enter License Key text box. **3** Click **Apply**.
Exit	Closes the Protocol Analyzer application.

NOTE The File menu also provides quick links to the most recently opened configuration and binary files.

Edit menu

Table 4 provides a brief description of the Edit menu commands.

Table 4   Edit menu commands

Menu command	Description
Copy	Enables you to copy the Protocol Analyzer data to clipboard. For example, you can copy one or more Transaction layer data packet records and paste them in Protocol Exerciser to generate same or similar type of data packets.
Find	Displays the Find dialog box that enables you to specify the criteria to search data packets.
Find Previous	Searches the previous occurrence of the data packet using the search criteria specified in the Find dialog box.
Find Next	Searches the next occurrence of the data packet using the search criteria specified in the Find dialog box.
New Marker	Creates a new marker at the beginning of a selected data packet or frame.
Delete Marker	Removes the selected marker.
Marker Properties	Displays the Properties of marker dialog box that you can use to view and modify the properties of a marker.

NOTE   You cannot delete, edit, or rename system markers.

View menu

Table 5 provides a brief description of the View menu commands.

Table 5   View menu command

Menu command	Description
Filter	Provides sub-menu commands that enable you to create filters on data packets trace, as well as remove filters.
Goto	Provides sub-menu commands that enable you to move on to a trigger, marker, or a particular timestamp in the Packet view.
Text Size	Provides sub-menu commands to set the text size of the data packet records shown in the Packet view to Smallest, Smaller, Medium, Larger, and Largest. The default text size is Medium.
Record Decode View	Displays the Record Decode pane.
Single Line Decode View	Displays the Single Line Decode pane.
Raw View	Displays the Raw Display pane.
Lane View	Displays the Lane Display pane.
Port Overview	Displays the Port Overview pane.
Port Management	Displays the Port Selection dialog box that enables you to select the ports of a module for your test application.
Realtime Statistics	Displays the Realtime Statistics dialog box that shows the graphical representation of the data traffic. This menu command is not available for FC and Gen2.

NOTE   For more information on the Record Decode, Single Line Decode, Raw Display, Lane Display, and Port Overview panes, refer to their respective sections given below.

Capture menu

Table 6 provides a brief description of the Capture menu commands.

Table 6   Capture menu commands

Menu commands	Description
Start	Starts capturing data packets.
Stop	Stops capturing data packets.
Trigger Setup	Displays the Trigger Setup dialog box.
Hardware Setup	Displays the Hardware Setup pane.

Listing menu

Table 7 provides a brief description of the Listing menu commands.

Table 7   Listing menu commands

Menu commands	Description
Duplicate	Creates a duplicate of the currently active listing. This enables you to experiment with the duplicate data, while the original data is preserved in the original listing. Creating a duplicate of a listing also copies the filters applied on the original listing to the duplicate listing.
Delete	Deletes the currently active listing.
Rename	Displays a dialog box, where you can specify the new name for the currently active listing.
Properties	Displays the Properties dialog box, which you can use to specify how the data should be displayed in the Packet view.

Window menu

Table 8 provides a brief description of the Window menu commands.

Table 8   Window menu commands

Menu commands	Description
New Window	Creates a new listing in the Packet view, and displays the data of the previously active listing in this new listing.
Tile Tabbed	Creates separate tabs for each listing in the Packet view. This is also the default alignment used by Protocol Analyzer.
Tile Horizontal	Horizontally aligns the listings in the Packet view.
Tile Vertical	Vertically aligns the listings in the Packet view.
Default Window Arrangement	Resets the GUI settings of the Protocol Analyzer application to default.

Protocol Analyzer provides two more menu commands to arrange listings in the Packet view. These menu commands are *Prominent* and *Rebalance*. Selecting *Prominent* for a listing hides all other listings and displays only the underlying listing in the main Protocol Analyzer window. Selecting *Rebalance* assigns equal space to all the listings on the main Protocol Analyzer window. You can access these menu commands from a short-cut menu, which appears on right-clicking the listing title in the Packet view.

Use Prominent and Rebalance only when listings in the Packet view are aligned horizontally or vertically to each other.

NOTE   The Window menu also displays a list of currently opened listings, with a check-mark sign in front of the currently active listing.

Help menu

Table 9 provides a brief description of the Help menu commands.

Table 9   Help menu commands

Menu command	Description
Help Topics	Displays the online help for Protocol Analyzer.
Session Information	Displays the Session Information message box with the current session information.
About	Displays the information about the System Protocol Tester system.

Toolbar

Toolbar provides a quick access to the features of the Protocol Analyzer application (Figure 6).

Figure 6   Toolbar

Table 10 specifies the names of all toolbar icons.

Table 10   Toolbar icons

Icon	Name
	Start hardware capturing
	Stop hardware capturing
	Show port setup
	Show hardware setup
	Show Trigger Setup
	Open trace file
	Save trace to file

Table 10   Toolbar icons

Icon	Name
	Print
	Find packets
	Find previous occurrence
	Fine next occurrence
	Goto marker
	Goto trigger
	Open Filter Dialog
	Disable Filters
Text Size	Zoom factor for packet views
Layout	Viewer Layout
	Filter all Skip Ordered Sets
	Filter all Update Flow Control Packets, Ordered Sets, and Training Sequences
OS	Enable/Disable Ordered Set Filters
All ports	Channel Selector

NOTE	Toolbar also shows the [icon] icon to enable filters. This icon appears when you click the **Disable Filters** icon.

NOTE	Out of the toolbar icons given in the above table, the **Filter all Skip Ordered Sets** and **Filter all Update Flow Control Packets, Ordered Sets, and Training Sequences** icons are not displayed for FC. On the other hand, the **Enable/Disable Ordered Set Filters** icon is displayed only for FC.

Panes

Protocol Analyzer provides the following panes:

- Port Overview
- Traffic Overview
- Hardware Status
- Decode View

Port Overview

To access the Port Overview pane:

- Click **View > Port Overview**.

  The Port Overview pane appears (Figure 7).

Figure 7   Port Overview pane

Port Overview displays the data of the ports that are connected with the current Protocol Analyzer session.

Table 11 provides a brief description of the data displayed in the Port Overview pane.

Table 11 Port Overview pane

Column	Description
Port	This column displays the ID of those ports, which are connected with the current Protocol Analyzer session.
Speed	This column displays the per lane speed at which the port will capture the data.
Records	This column displays the number of records captured in the buffer.
Trigger	This column displays the most recently applied trigger.

Table 11   Port Overview pane

Column	Description
Name	This column displays module and port numbers along with the name of the streams or channels from which the port will capture the data. For example, 101/1: Upstream or 102/1A. Since a port on x16 link width captures data from a single stream or channel, this column displays only the name of the underlying stream or channel. This column also allows you to change the name of a stream or channel. To do this: **1** Right-click the stream or channel whose name you want to change. **2** Click the **Change name** shortcut menu command from the right-click menu. The New Name dialog box appears. **3** Type the new name in the text box. **4** Click **OK**. This is useful if you are working with multiple ports, and each port is connected to a different DUT.
Link	This column displays the following messages to show the status of each link: • **No Laser**: This message means that laser is turned off and the port is not capturing data. This message is shown with a red colored bullet (●). This message applies to the Fibre Channel protocol only. • **LOS**: This message means loss of synchronization and the port is not capturing data. This message is shown with a red colored bullet (●). • **OK**: This message means that a connection has been established between a probe card and DUT. This message is shown with a green colored bullet (●).
Speed Status	This column displays the following messages to show the speed status of the link: • **Not Detected**: This message means that Protocol Analyzer is not able to detect the speed of the link. It may be because the link is not configured or is electrical idle. This message is shown with a red colored bullet (●). • **Gen1**: This message means that the speed of the link is 2.5 Gb/s. This message is shown with a yellow colored bullet (○). • **Gen2**: This message means that the speed of the link is 5 Gb/s. This message is shown with a green colored bullet (●).

Table 11   Port Overview pane

Column	Description
Lane Status	This column displays the status of the lane by using different colored bullets. These bullets are: • **Red**: This colored bullets means that there are no signals or the lane is electrically idle. • **Orange**: This colored bullet marks the presence of invalid signals on the lane. • **Green**: This colored bullet means that the data on the lane is deskewed. • **Yellow**: This colored bullet means that the data on the lane is skewed. It corresponds to *blinking-green* on the front panel LEDs of the N5306A I/O module. • **Grey**: This colored bullet means that the lane is not configured. For example, if you are using x4 link width, then first four bullets of the lane would be green and rest of the bullets would be grey colored bullets.
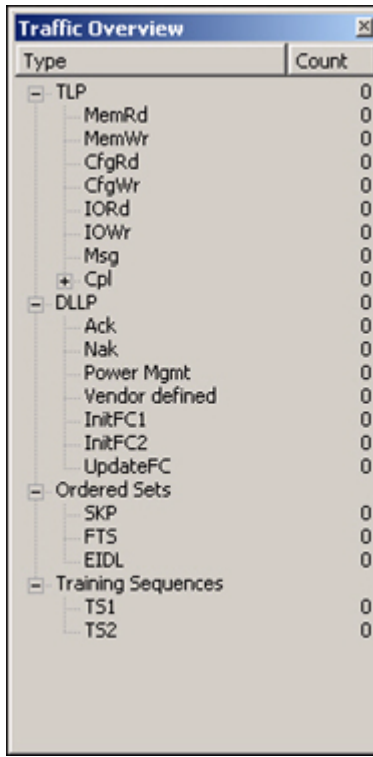
NOTE   In the Port Overview pane, the File column replaces the Trigger, Link, Speed Status, and Lane Status columns when you try to view the offline data. The File column displays the complete path of the file that you have opened to view the offline data.

Traffic Overview

To access the Traffic Overview pane:

• Click **View > Traffic Overview**.

The Traffic Overview pane appears (Figure 8).

Figure 8   Traffic Overview pane

The Traffic Overview pane displays the following information:

- **Type**: This column displays the packets that belong to the underlying protocol, such as PCIe or ASI. Also, these packets are arranged by their type, such as TLP and DLLP.

- **Count**: This column displays the number of occurrences of each packet in the trace.

NOTE	Traffic overview information is not needed for Fibre Channel. Therefore, the Traffic Overview pane is not displayed when you start Protocol Analyzer for Fibre Channel.

Hardware Status

To access the Hardware Status pane:

• Click **View > Hardware Status**.

The Hardware Status pane appears (Figure 9).

For the x8 Link Width   For the x16 Link Width
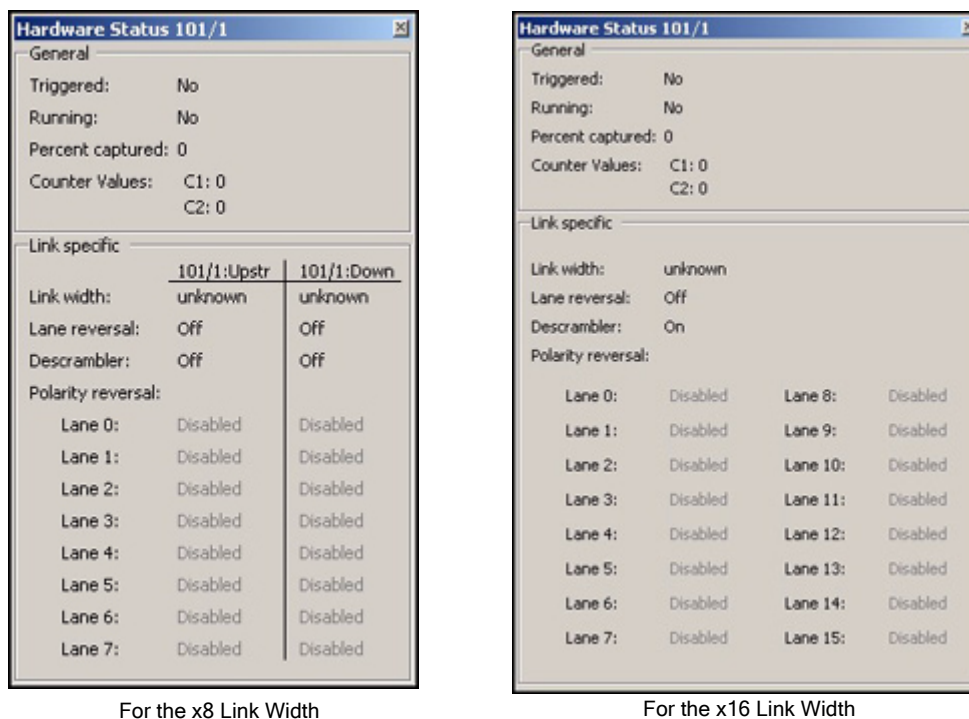
Figure 9   Hardware Status pane

The Hardware Status pane displays the following information:

• **General**: This section shows information about Protocol Analyzer, such as if it is triggered or not, and whether it is running or not. This section also shows the percentage of trace memory filled and the status of the counters (C1 and C2) that Protocol Analyzer provides for triggers.

• **Link specific**: This section shows the status information of the link width, lane reversal, descrambler, and polarity reversal. In this section, the display for polarity reversal is different for the x16 and x8 link widths.

Protocol Analyzer does not allow you to set these values; rather it automatically picks these values during the link training activity.

> **NOTE**   Hardware status information is not needed for Fibre Channel. Therefore, the Hardware Status pane is not displayed when you start Protocol Analyzer for Fibre Channel.

Decode View

The Decode View pane displays the detailed data of the packet you selected in the Packet view. It is named as Decode View, because it displays the packet data in hexadecimal, selected base, and in its decoded form.

Decode View has the following nested panes:

- **Record Decode**: It displays the decoded data in a vertical record hierarchy format. You can access it by clicking the **Record Decode View** menu command in the View menu.

- **Single Line Decode**: It wraps the decoded data, for each row of hexadecimal data, in a single line. You can access it by clicking the **Single Line Decode** menu command in the View menu.

- **Raw Display**: It displays the data of the selected packet in its raw 10 bit form. You can access it by clicking the **Raw View** menu command in the View menu.

  The Raw Display pane is available only for FC.

- **Lane View**: It displays the raw data in a lane-wise format. You can access it by clicking the **Lane View** menu command in the View menu.

  Some important points about the Lane View pane are:

  - When logical idles are transferred, the Lane View pane displays **idle** with grey color in the background.

  - When a link is in the *electrical idle* state, the Lane View pane displays the data with orange color in the background. The data shown for the lane in this state might be the garbage data, i.e. not useful to the user.

  - The Lane View pane is available only when you are using the PCIe Gen2 hardware.

> **NOTE**   *Electrical idle* is a function of a lane or channel, not of an entire link. Therefore, the electrical idle state is shown per lane.

Figure 10 displays the Decode View panes.

Record Decode   **Single Line Decode**

Raw View

Lane View
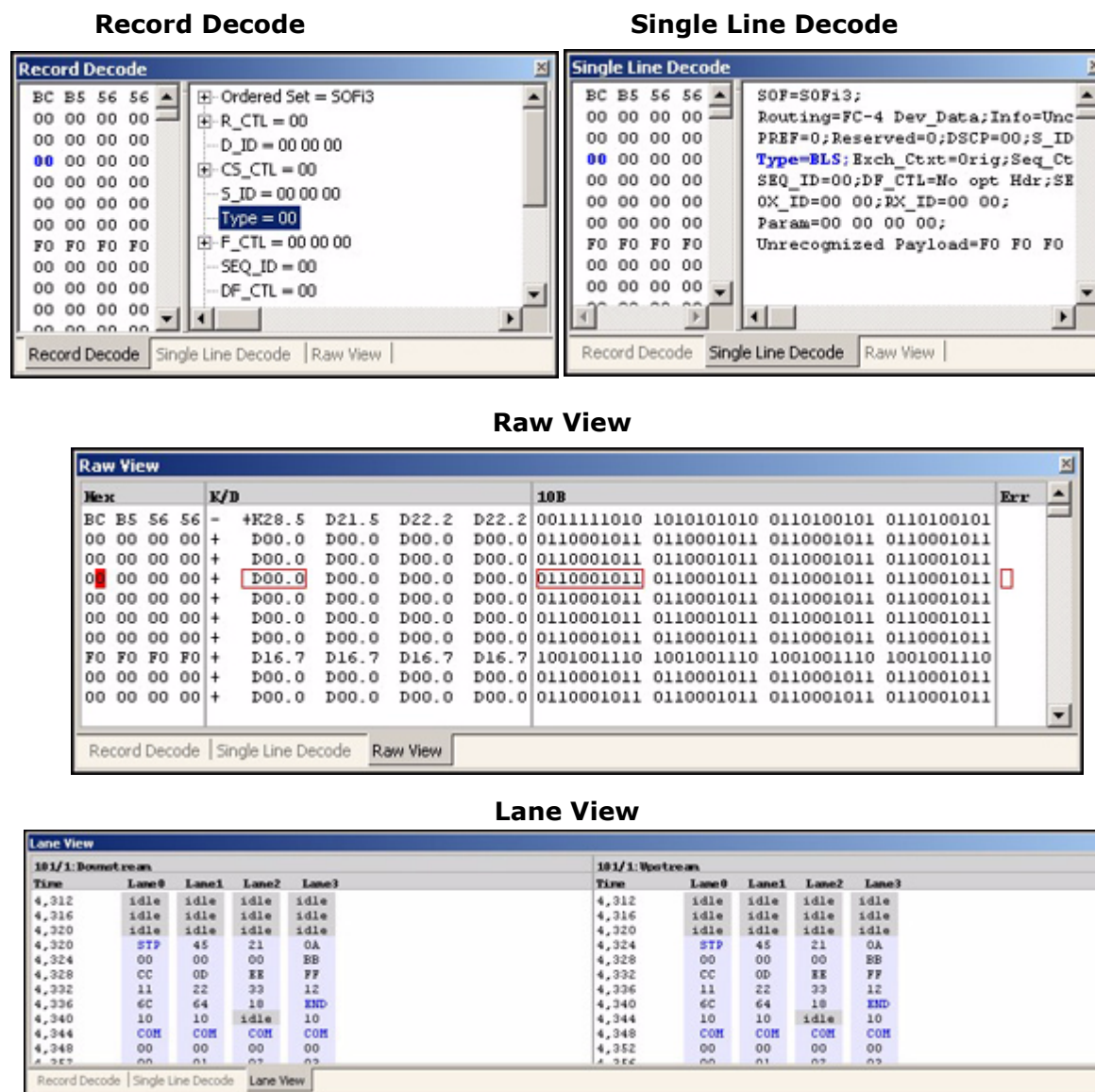
Figure 10   Decode View panes

About Loading and Saving the Protocol Analyzer Data

Before starting to use Protocol Analyzer, it is important to understand how to maintain the data that you have captured to analyze. Protocol Analyzer provides features that allow you to save the analyzed data to a file and load it back to the application.

In this section, you will learn about:

- Saving the Data
- Loading the Data

Saving the Data

There are two ways to save the Protocol Analyzer data. One way allows you to save the data in the XML and binary format, and the other way allows you to save the data in text format.

In this section, you will learn about:

- Saving the Data in XML and Binary Format
- Saving the Data in Text Format

Saving the Data in XML and Binary Format

When you try to save the data in XML and binary format, the GUI settings of the Protocol Analyzer application are saved in the `.xml` file, and the trace data is saved in the `.pad` (binary) file.

You do not have to create a `.pad` file separately. It is automatically created by Protocol Analyzer while creating the XML file.

For `.pad` files, Protocol Analyzer uses the following naming convention:

`<XML_FileName><Module_Number>_<Port_Number>.pad`

For example, you create an XML file named `TraceData.xml` to save the data of the module `102` and the port `1`. As a consequence, Protocol Analyzer creates the following `.pad` file:

`TraceData102_1.pad`

You should not rename the `.pad` file. This is because, the XML file internally refers to it by its automatically generated name.

To save the data in XML and binary format:

1 Select **File > Save As**.

The Save As dialog box displays (Figure 11).
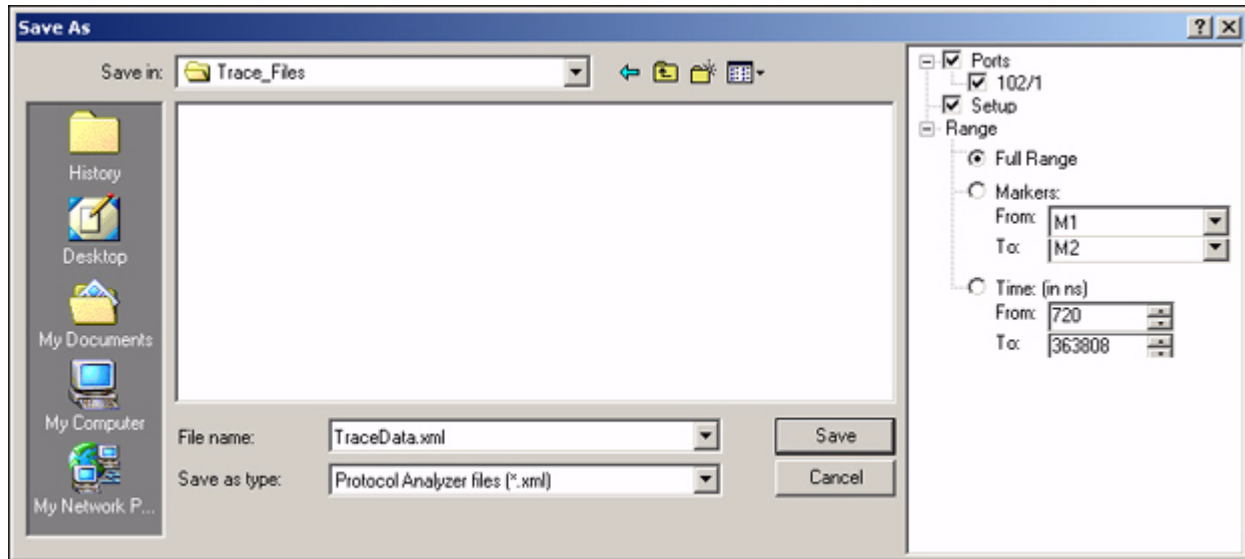
Figure 11   Save As dialog box - XML and Binary Format

2 Browse to the location where you want to save the data.

3 Type the name of the file in the **File name** text box.

4 Select **Protocol Analyzer files (*.xml)** from the **Save as type** drop-down list.

5 Expand the **Port** check box list.

A nested check box list of ports, to which the current Protocol Analyzer session is connected, is displayed.

6 Select the desired ports.

Selecting multiple ports instruct Protocol Analyzer to create a separate `.pad` file for each selected port.

7 Select the **Setup** check box if you want to save the setup information.

8 Expand **Range**. This displays a list of option buttons to specify the data range to be saved.

9 Do one of the following:

   a Select **Full Range** to save the complete traced data.

   b Select **Markers** to save a range of records between two markers. Here, you also need to specify the starting and ending markers in the **From** and **To** text boxes.

   c Select **Time** to save a range of packet records that were captured during the specified range of time. Here, you need to specify the start timestamp and end timestamp in the **From** and **To** text boxes.

10 Click **Save** to save the Protocol Analyzer data.

NOTE	If you only want to save the GUI settings of Protocol Analyzer and not any binary data, then do not select the Port check box.

Saving the Data in Text Format

Saving the data in text format creates a `.csv` file that contains the packet data in decoded form.

Some important points about the resulting text file are:

- All entries, except the entries for summary columns, in this file are separated by semicolon.

  A *summary column* contains multiple fields along with their respective values.

- Entries for the summary columns are separated by commas.

- All lines contain same number of commas (if any) and semicolons. If there is an empty field, it is represented by an empty string followed by a comma or semicolon, which ever is applicable.

- The first line lists field names.

- All the following lines are field values.

- Field names in the text file matches the collapsed view of the columns on screen.

- Second line onwards, each line represents a single packet data.

An example of how data is saved in a text file is given below. The italicized content represents the fields and values of a summary column.

```
Record No;Timestamp;Channel;Type;Tag;Seq No,Tag,Length;

0;3,012;101/1:Downstream;Ack;11;1 84,11,0 01;

1;3,060;101/1:Downstream;Ack;10;1 85,10,0 01;
```

The advantage of saving the data in text format is that you can edit the data using any text editor application.

To save the data in text format:

1 Click **File > Text Export**.

The Save As dialog box appears (Figure 12).
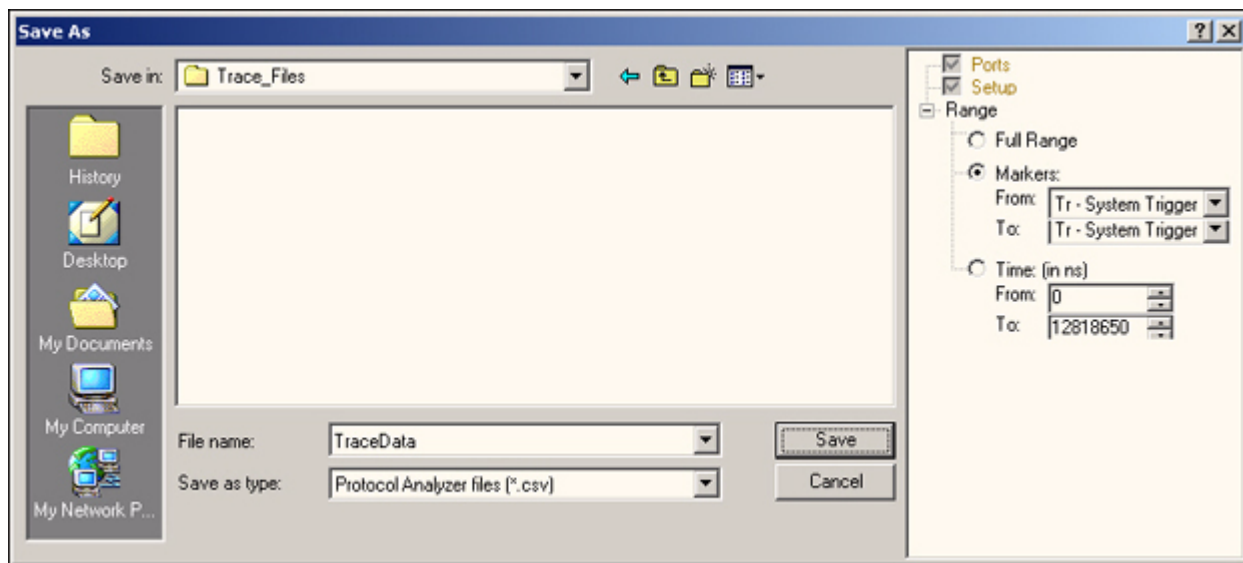
Figure 12   Save As dialog box - Text Format

2 Browse to the location where you want to save the data.

3 Type in the name of the file in the **File name** text box.

4 Select **Protocol Analyzer files (*.csv)** from the **Save as type** drop-down list.

5 Expand the **Port** check box list. A nested check box list of ports, to which the current Protocol Analyzer session is connected, is displayed.

6 Select the desired ports.

7 Expand **Range**. This displays a list of option buttons to specify the data range to be saved.

8 Do one of the following:

a Select **Full Range** to save the complete trace data.

b Select **Records** to save only a range of packet records. Here, you also need to specify the start range and end range of records in the **From** and **To** text boxes.

c Select **Time** to save a range of packet records that were captured during the specified range of time. Here, you need to specify the start timestamp and end timestamp in the **From** and **To** text boxes.

9 Click **Save** to save the Protocol Analyzer data.

NOTE	The performance of the process, which saves data in text format, degrades with the increasing size of trace.

Loading the Data

Once you have saved the trace data to a file, you can open it to load it again in Protocol Analyzer. You generally do this to compare the previously captured data with the data you have just captured.

Protocol Analyzer enables you to load the data only from the XML file and/or the binary file. It does not allow you to load the data from the text (.csv) file.

To load the data in Protocol Analyzer:

1 Click **File > Open**.

The Open dialog box appears (Figure 13).
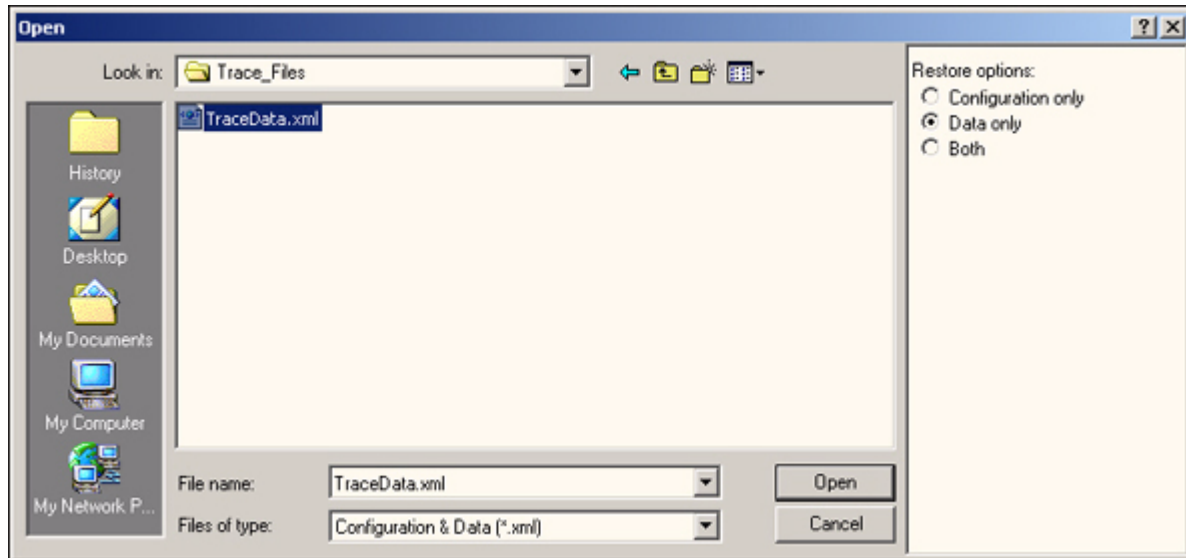
Figure 13   Open dialog box

2 Do one of the following:

   a Click **Configuration only** if you want to load the contents of the XML file without loading the binary file (`.pad`) it references.

   b Click **Data only** if you want to load the contents of the binary file without loading the contents of the XML file.

   c Click **Both** if you want load the contents of the XML and binary files.

3 Browse to the target location and select the desired file.

4 Click **Open** to load the data from selected file.

| NOTE | When you want to load GUI settings only, ensure that |

- Protocol Analyzer is not in offline mode.
- Protocol Analyzer has the same hardware configuration that existed when you saved the GUI settings you want to load now.
- Data in the Packet view is loaded from an online I/O module and not from a `.pad` file.

3

Customizing Protocol Analyzer

This chapter provides information on how to manage floating windows and set the preferences for the Protocol Analyzer GUI. This chapter also provides information on how to create, edit, jump to, measure time between, and delete markers.

Managing Windows

The main Protocol Analyzer window contains many floating windows. These windows can float anywhere on the desktop, or you can dock them together with other windows on the main Protocol Analyzer window. In the default window arrangement, all windows are properly docked on the main Protocol Analyzer window.

In this section, you will learn:

- To Display a Floating Window
- To Hide a Floating Window
- To Auto-Hide a Floating Window
- To Change a Docked Window to a Floating Window
- To Dock a Floating Window
- To Set the Default Windows Arrangement

To Display a Floating Window

- Click **View > *menu_command_for_floating_window***.

  Here, *menu_command_for_floating_window* represents the name of the menu command to access the floating window. For example, Port Overview is a floating window. To display it, click the **View > Port Overview** menu command.

To Hide a Floating Window

- Click the ⊠ icon on the title bar of the floating window.

  You can also hide a floating window by clicking its menu command in the View menu.

To Auto-Hide a Floating Window

- Click the 🔲 icon on the title bar of the floating window.

  This automatically hides the floating window when you are not using it. This also displays a new 🔲 icon on the title bar of the floating window.

  To display the window again, place the cursor over the tab displayed for the hidden window, or click its menu command in the View menu.

To Change a Docked Window to a Floating Window

- Double-click the title bar of the docked window.

To Dock a Floating Window

- Double-click the title bar of the floating window.

To Set the Default Windows Arrangement

- Click **Window > Default Window Arrangement**.

Setting Preferences

By default, Protocol Analyzer displays packet data using predefined columns, fields, time format, and color settings. There may be a situation when you want to make some changes to these predefined settings to match your data display needs. To make such changes, Protocol Analyzer provides the Properties dialog box (Figure 14). This dialog box allows you to make changes to the way data packets are displayed in the Packet view.

To access the Properties dialog box:

• Click **Listing > Properties**.

   The Properties dialog box appears (Figure 14).
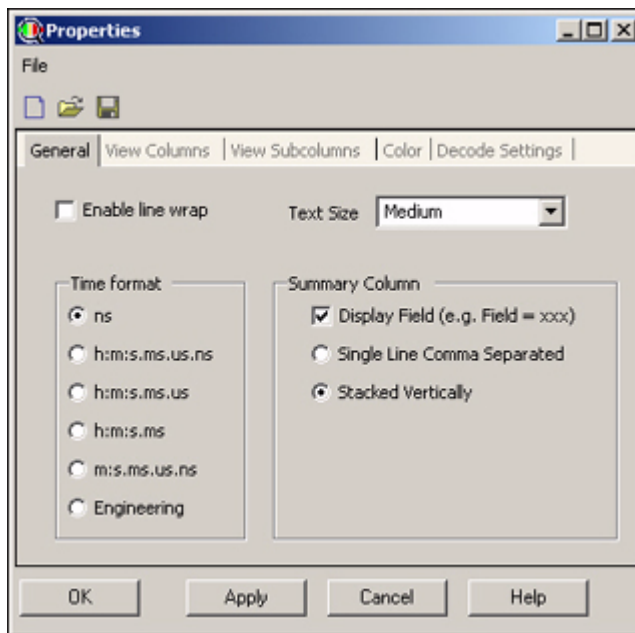
Figure 14   Properties dialog box

NOTE	You can also access this dialog box directly from the Packet view. There, right-click anywhere in the Packet view, and then click the **Viewer Properties** short-cut menu command.

Table 12 briefly describes the common components of the Properties dialog box.

Table 12 Components of the Properties dialog box

Component	Description

File	The **File** menu provides the following menu commands:
	• **Open**: Select **Open** to display the Open dialog box, using which you can load the saved `*.vly` file into the Properties dialog box. You generally load an already saved file to make some changes to it.
	• **Save As**: Select **Save As** to display the Save As dialog box, using which you can save the current settings of the Properties dialog box for later references.
	• **Set As Default**: Select **Set As Default** to save the current settings in the Properties dialog box as default. This means, whenever you need to apply these settings to a listing in the Packet view, you only have to:
	  • Select **File > My Default Layout** to open your default settings in the Properties dialog box.
	  • Click **Apply**.
	• **My Default Layout**: Select **My Default Layout** to open your default settings in the Properties dialog box.
	• **Restore Factory Default**: Select **Restore Factory Default** to revert to the setting that was originally existing when you first opened the Properties dialog box after installing the Protocol Analyzer application. The factory default setting is different from the setting that you saved using the Set As Default menu command.
	The File menu also provides quick links to the most recently opened Viewer Properties Configuration (*.vly) files.

Toolbar	**Toolbar** provides icons for My Default Layout (⬚), Open (📂), and Save As (💾).
General	The **General** tab enables you to apply line wrap to the content displayed, and specify the time format to be used to display the timestamp details in the Packet view.
View Columns	The **View Columns** tab enables you to specify columns and their order to be displayed in the Packet view.
View Subcolumns	The **View Subcolumns** tab enables you to specify the fields and their order to be displayed in the Packet view.
Color	The **Color** tab enables you to specify the background and foreground color settings for the data displayed in the Packet view.

Table 12 Components of the Properties dialog box

Component	Description
Decode Settings	The **Decode Settings** tab enables you to specify an appropriate SCSI command for FC.
OK	Click **OK** to close the Properties dialog box after saving the changes made in it.
Apply	Click **Apply** to implement the changes made in the Properties dialog box.
Cancel	Click **Cancel** to close the Properties dialog box without saving any changes.
Help	Click **Help** to display online help.

Some of the common components of the Properties dialog box are also accessible from the toolbar on the main Protocol Analyzer window. There, the toolbar has the *Layout* icon, which you can click to view a drop-down list of options, such as Open, Save as, My Default, and User Layout. User Layout further expands to display a list of most recently saved `*.vly` files, if any.

The Layout icon also provides predefined setting options, such as Virtual_Frame_Tagging (for FC), Link_Training and Config_Accesses (for PCIe), which you can choose as per the needs of the trace shown in the packet view. For example, if trace contains link initialization data, then you can choose Link_Training option. These options are nothing but predefined `vly` files.

In this section, you will learn about:

- Setting Up Line Wrap, Text Size, and Time Format
- Setting Columns
- Setting Subcolumns
- Setting Colors
- Setting The SCSI Decode Mode
- Setting Listing Properties

Setting Up Line Wrap, Text Size, and Time Format

To specify the line wrap, text size, and time format settings, use the General tab (Figure 14).

Table 13 briefly describes the components of the General tab.

Table 13 Components of the General tab

Component	Description
Enable line wrap	Selecting **Enable line wrap** limit the packet content to the display without extending the display to the right.
Text Size	The **Text Size** drop-down list provides options, such as Smallest, Smaller, Medium, Larger, and Largest, which you can choose to change the size of the text displayed in the Packet view.
Time format	The **Time format** section provides options to specify the time format to be used to display the timestamp details in the Packet view.
Summary Column	The **Summary Column** section provides options to display the Summary column, with comma-separated or vertically stacked list of the fields and their values, in the Packet view.

NOTE	To directly access the General tab for changing the timestamp format, right-click anywhere in the Timestamp column in the Packet view, and click the **Timestamp Format** short-cut menu command.

NOTE	You can also change the origin of the timestamp to any row or marker in the Packet view. When you do this, the timestamp of the underlying row becomes zero. Also, the timestamp of all rows prior or after to this row are accordingly affected.

To change the timestamp origin, right-click in the Timestamp column, and click the **Timestamp Origin** short-cut menu command. This displays a set of sub-menu commands. Here, select an appropriate sub-menu command to change the timestamp origin. To revert back to the original timestamp settings, right-click in the Timestamp column, and click the **Timestamp Origin > Reset** short-cut menu command.

Setting Columns

There may be a situation when, instead of all columns, you want to view only a few columns in the Packet view. You may also want to organize them in a particular order. To do all this, you can use the View Columns tab (Figure 15).
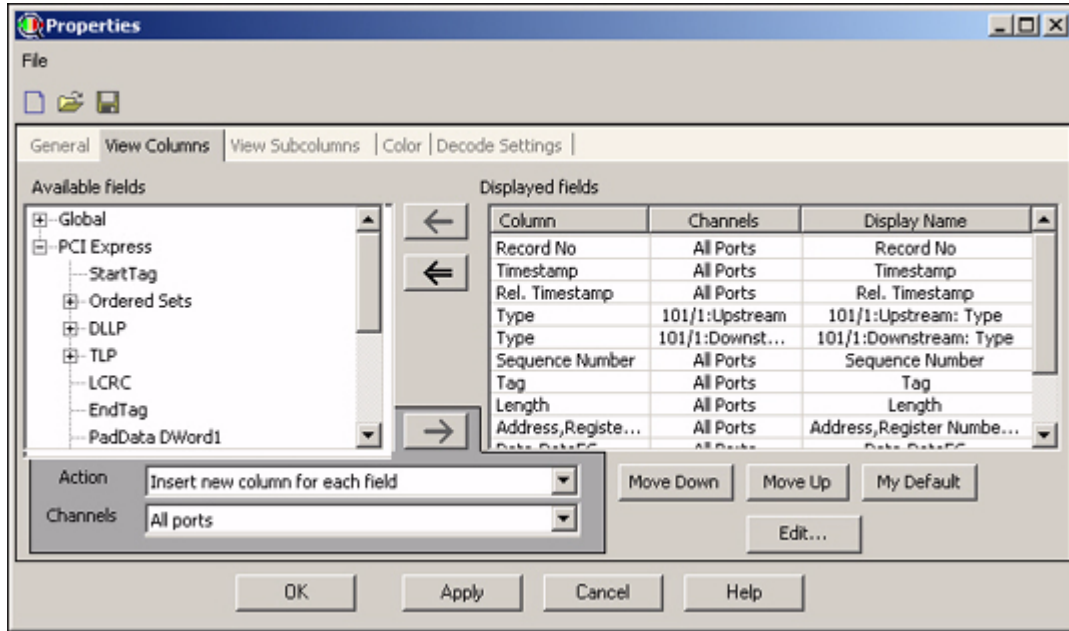
Figure 15   View Columns tab

Table 14 briefly describes the components of the View Columns tab.

Table 14   Components of the View Columns tab

Component	Description
Displayed fields	The **Displayed fields** list box contains the columns that are displayed in the Packet view. In this list box: • The **Column** column displays a list of fields to be displayed in the Packet view. • The **Channels** column specifies the channels, for which the corresponding field displays the data in the Packet view. • The **Display Name** column shows the title text that appears for each column in the Packet view.
Available fields	The **Available fields** list box contains the columns that are not displayed in the Packet view.

Table 14 Components of the View Columns tab

Component	Description
Action	The **Action** drop-down list provides the following options:
	• **Insert new column for each field**: Select this option if you want to add a new column in Displayed fields for each column selected from Available fields.
	• **Insert one summary column for field(s)**: Select this option if you want to add a new column in Displayed fields for the columns selected from Available fields.
	• **Append field(s) to existing column(s)**: Select this option if you want to append one or more selected columns from Available fields to the column selected in Displayed fields. The resulting column will then be displayed as a summary column in the Packet view.
	• **Distribute field(s) over all ports**: Select this option if you want to display the value of the column selected from Available fields for all ports. For example, the **101** module has two ports, **1** and **2**, for the present session. In this situation, selecting this option with **SOF** field adds **101/1:SOF** and **101/2:SOF** columns in Displayed fields.
	• **Distribute field(s) over all channels**: Select this option if you want to display the value of the column selected from Available fields for all channels. For example, **101** module has two ports for the present session, and each port has two channels. In this situation, selecting this option with **SOF** field adds **101/1A:SOF**, **101/1B:SOF**, **101/2A:SOF**, and **101/2B:SOF** columns in the Displayed fields list box.
	• **Modify channel filter for selected column(s)**: Select this option if you want to change the channel filter settings of the one or more columns given in the Displayed fields list box. For example, you had set all the columns to be displayed to all ports. Now, you want to show some of these columns for a single port. In order to do this, select this option. Then, select the desired columns in the Displayed fields list box, along with the desired port from the Channels drop-down list. Finally, click **Select** to modify the channel filter for the selected columns.
Channels	The **Channels** drop-down list provides options to select ports, on which you want to apply the action selected in the Action drop-down list.
Deselect	Click **Deselect** to move the column selected in the Displayed fields list box to the Available fields list box.
Deselect All	Click **Deselect All** to move all the columns from the Displayed fields list box to the Available fields list box.

Table 14 Components of the View Columns tab

Component	Description
Select	Click **Select** to move the column you selected in the Available fields list box to the Displayed fields list box.
Move Down	Click **Move Down** to move the selected column by one place down in the Displayed fields list box.
Move Up	Click **Move Up** to move the selected column by one place up in the Displayed fields list box.
Default	Click **Default** to restore the default settings of the View Columns tab.
Edit	Click **Edit** to display the Edit Column dialog box for the column selected in the Displayed fields list box. Using this dialog box, you can change the selected column to a summary column by adding more fields, change the order of the fields in the column by moving them up or down, and change display base of the individual fields from hexadecimal to binary, decimal, or string.

Setting Subcolumns

Like columns, you can also choose to display only required sub columns and organize them in a particular order in the Packet view. To do this, use the View Subcolumns tab (Figure 16).
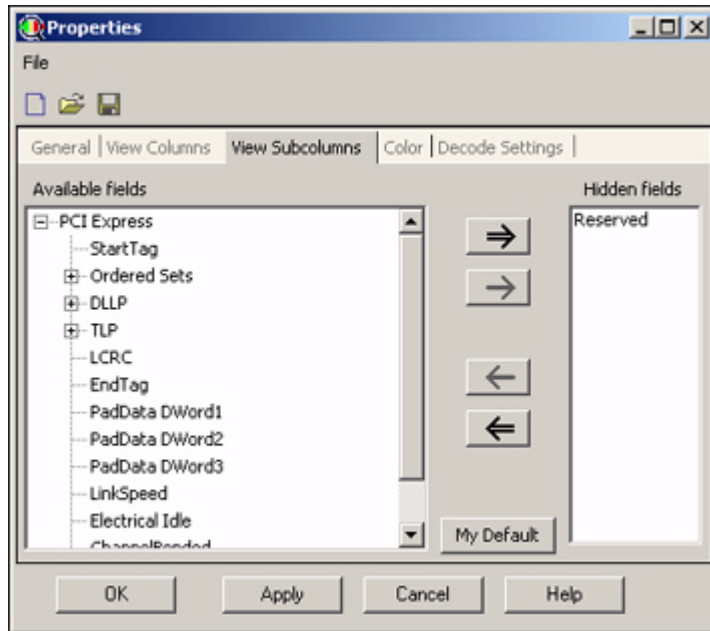
Figure 16   View Subcolumns tab

Table 15 briefly describes the components of the View Subcolumns tab.

Table 15   Components of the View Subcolumns tab

Component	Description
Hidden fields	The **Hidden fields** list box contains the sub columns that are not displayed in the Packet view.
Available fields	The **Available fields** list box contains the sub columns that are displayed in the Packet view.
Select All	Click **Select All** to move all the sub columns from the Available fields list box to the Hidden fields list box.
Select	Click **Select** to move the sub columns you selected in the Available fields list box to the Hidden fields list box.
Deselect	Click **Deselect** to move the sub columns selected in the Hidden fields list box to the Available fields list box.
Deselect All	Click **Deselect All** to move all the sub columns from the Hidden fields list box to the Available fields list box.
Default	Click **Default** to restore the default settings of the View Subcolumns tab.

Setting Colors

The Properties dialog box has the Color tab (Figure 17), which enables you to specify the background and foreground colors of the data appearing in the Packet view.
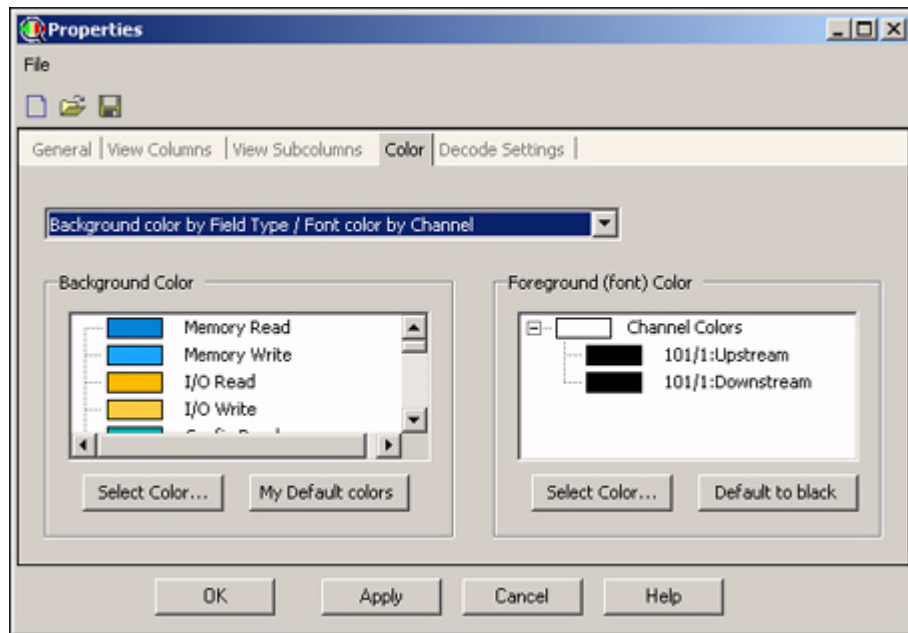
Figure 17   Color tab

Table 16 briefly describes the components of the Color tab.

Table 16   Components of the Color tab

Component	Description

Color Settings	The **Color Settings** drop-down list provides the following options:
	• **Background color by Field Type/Font color by Channel**: Select this option if you want to specify different:
	  • Background color for each field type.
	  • Foreground color for each channel.
	• **Background color by Field Type/Auto font color (black or white)**: Select this option if you want to:
	  • Specify different background color for each field.
	  • Automatically assigned black or white color to the foreground text.
	• **Background color by Channel/Font color by Field Type**: Select this option if you want to specify different:
	  • Background color for each channel.
	  • Foreground color for each field type.
	• **Background color by Channel/Auto font color (black or white)**: Select this option if you want to:
	  • Specify different background color for each channel.
	  • Automatically assigned black or white color to the foreground text.

Background Color	In the **Background Color** section: • A list box displays a list of available field types or channels, depending on the option selected from the Color Settings drop-down list. Here, select a field type or channel whose background color you want to change. • Click **Select Color** to display the Color dialog box. In this dialog box, select a basic color or define a custom color, and use it as a background color of the selected field type or channel. • Click **Default Colors** to restore the default background color settings of the field types or channels.

Table 16 Components of the Color tab

Component	Description
Foreground Color	In the **Foreground Color** section: • A list box displays a list of available field types or channels, depending on the option selected from the Color Settings drop-down list. Here, select a field type or channel whose foreground color you want to change. • Click **Select Color** to display the Color dialog box. In this dialog box, select a basic color or define a custom color, and use it as a foreground color of the selected field type or channel. • Click **Default Colors** to restore the default foreground color settings of the field types or channels.

Setting The SCSI Decode Mode

To specify an appropriate SCSI command, use the Decode Settings tab (Figure 18). This tab provides the SCSI Decode Mode drop-down list that has options to specify an appropriate SCSI command, such as SBC2, SSC2, SCC2, and MMC3.
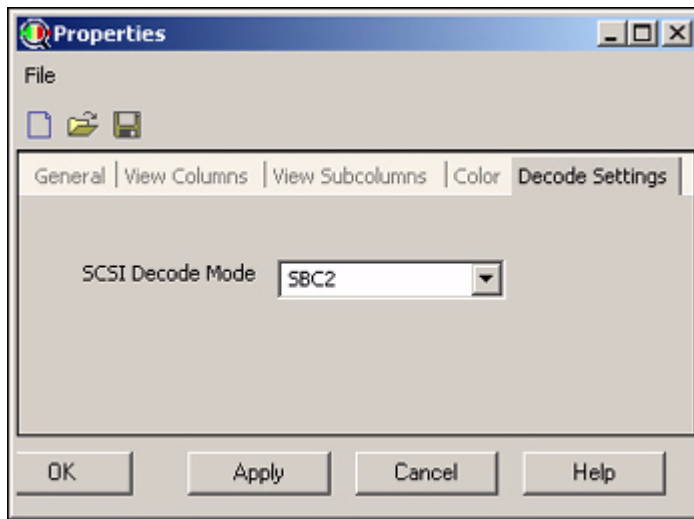
Figure 18 Decode Settings

NOTE	The Decode Settings tab is displayed on for FC.

Setting Listing Properties

Consider that you are working on a listing that currently displays the following details (columns) about the captured data in the Packet view:

- Record No
- Channel
- Ordered Set

Now, you also want to include a summary column to display the timestamp and size of the data packet. You also want that:

- Information inside the summary column should be vertically stacked.
- Displayed in the `fieldName = value` format.

To Customize Listing Properties

1 Click the **Listing > Properties** menu command.

The Listing Properties dialog box appears.

2 Select the **General** tab.

3 Select **Display Field**.

This ensure that the information in the summary column is displayed in the `fieldName = value` format.

4 Select **Stacked Vertically**.

This ensures that the information in the summary column is vertically stacked.

5 Select the **View Columns** tab.

6 Select **Insert one summary column for field(s)** from the Action drop-down list.

7 To select the timestamp and size fields, do the following:

a Expand **Global** inside the **Available fields** list box.

b Select **Timestamp**.

c Press and hold-down the [**ctrl**] key on your computer's keyboard, and select **Size (Bytes)**.

8 Click **Select**.

This creates a new summary column for timestamp and size fields, in the Displayed fields list box (Figure 19).
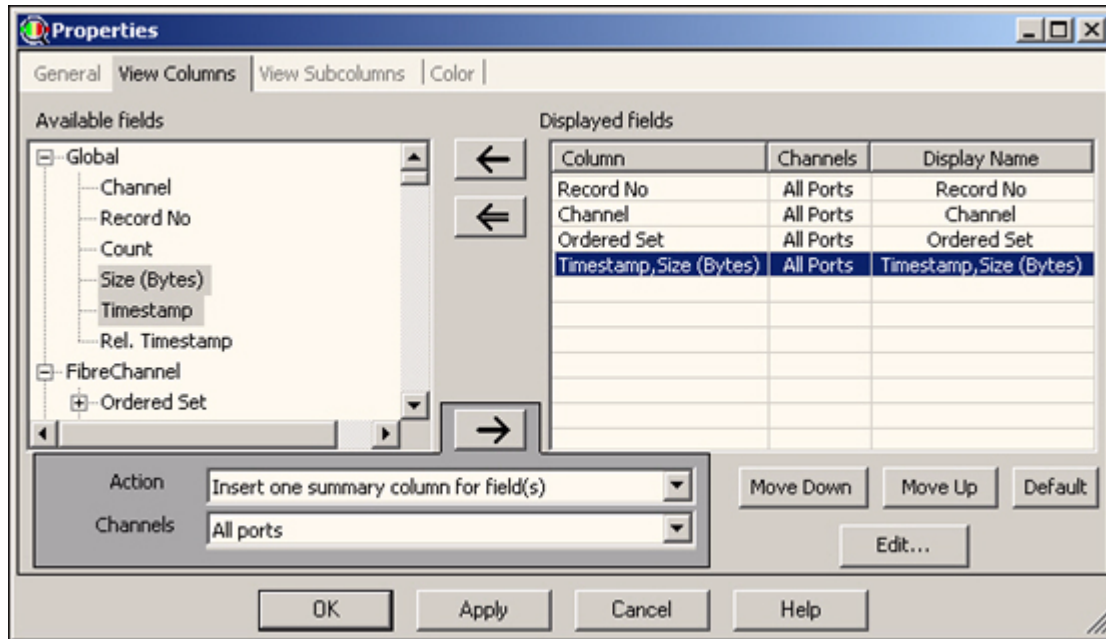
Figure 19   Properties dialog box

9 Click **Apply**.

10 Click **OK**.

The final result is shown in Figure 20.

Customized Listing
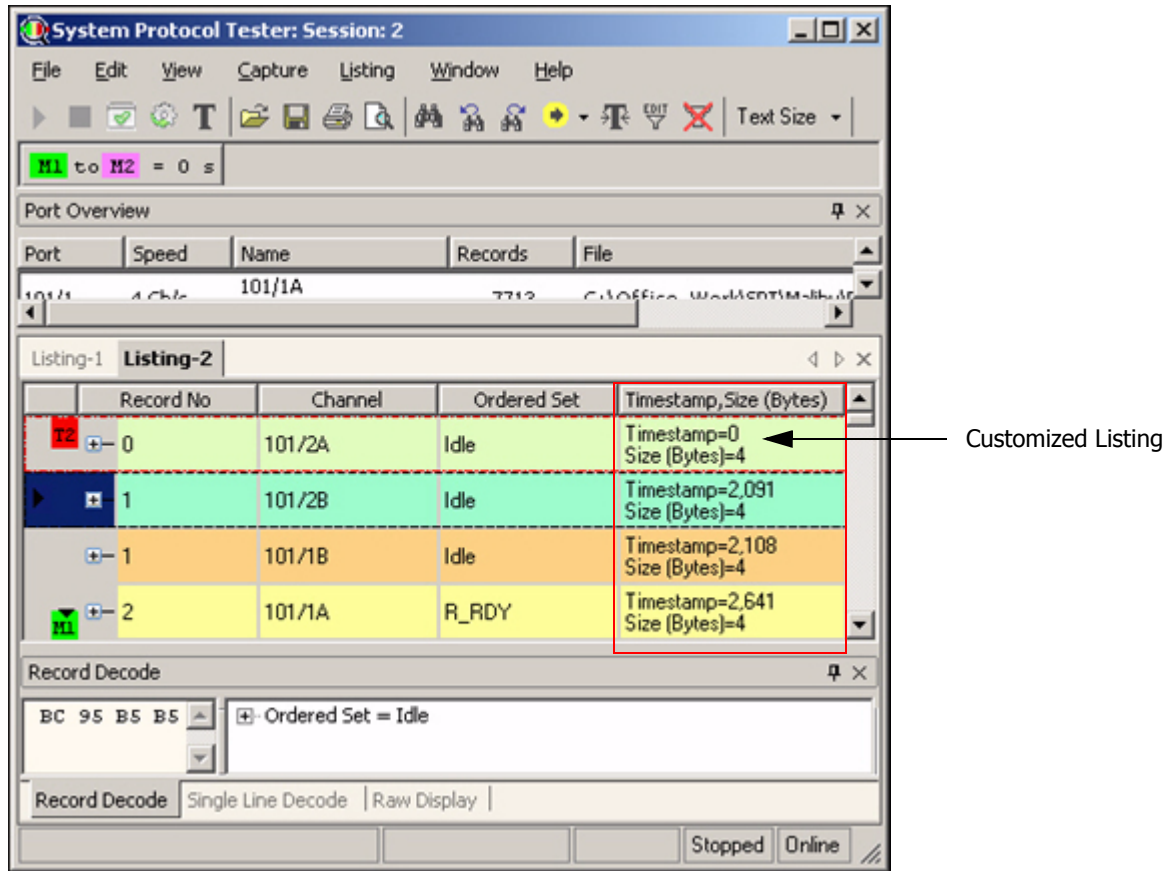
Figure 20   Customized Listing

Marking Packets

In Protocol Analyzer, you can create markers to bookmark packets in the Packet view. Creating markers help you to easily jump to the marked packets, and to measure the time difference between the marked data packets.

In Protocol Analyzer, you can create, edit, and delete markers.

In this section, you will learn:

- To Create a Marker
- To Edit a Marker
- To Jump to a Marker
- To Measure the Time Difference between Markers
- To Delete a Marker

To Create a Marker

1 Select the packet, for which you want to create a marker, in the Packet view.

2 Click **Edit > New Marker**.

NOTE   You can also create a new marker:

- By double-clicking on the left of a packet's expand (or collapse) button.
- By right-clicking on the left of a packet's expand (or collapse) button, and then selecting the **New Marker** shortcut menu command.

To Edit a Marker

1 Select the marker that you want to edit.

2 Click **Edit > Marker Properties**.

The Properties of marker dialog box appears (Figure 21).
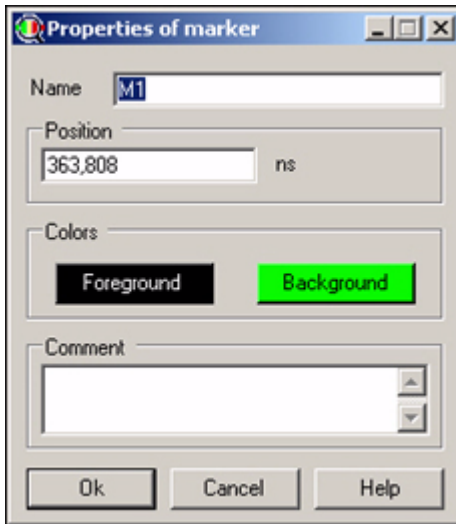
Figure 21   Properties of marker dialog box

3 Do the following as desired:

a Type in the new name of the marker in the **Name** text box.

b Specify the new position of the marker in the **Position** section. This section shows the position of the marker in nanoseconds (ns).

c Specify the new foreground and background colors of the marker in the **Colors** section. This section has two command buttons: Foreground and Background. Clicking these buttons display the Color dialog box, from where you can choose the desired foreground or background color.

d Type in a comment about the marker, if any, in the **Comment** text area.

e Click **OK**.

To Jump to a Marker

- Click **View > Goto > Marker >** *Marker_Name*.

  Here, *Marker_Name* is the name of the marker to which you want to jump.

  You can also click the [icon] icon on the toolbar and jump to the desired marker by selecting it from the drop-down list.

To Measure the Time Difference between Markers

1 Click anywhere on the Measurement area.

  A shortcut menu appears.

2 Click the **New measurement** shortcut menu command.

  The Properties of Measurement dialog box appears (Figure 22).
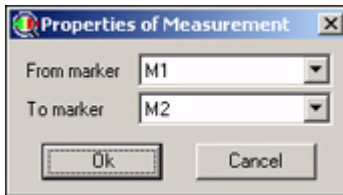
Figure 22   Properties of Measurement dialog box

3 Select the first marker from the **From marker** drop-down list.

4 Select the second marker from the **To marker** drop-down list.

5 Click **OK**.

  The measured time difference between the two specified markers is displayed in the Measurement area.

  Using the above procedure, you can add multiple measurements to the Measurement area. The resulting time difference for all measurements will always be displayed in nanoseconds.

NOTE	You can delete an existing measurement by just clicking it on the Measurement area, and then clicking the **Delete** shortcut menu command.
	You can also delete all existing measurements by clicking anywhere on the Measurement area, and then clicking the **Delete All** shortcut menu command.

To Delete a Marker

1 Select the marker, which you want to delete, in the Packet view.

2 Click **Edit > Delete Marker**.

NOTE	You can also delete a marker by right-clicking on the marker name, and then selecting the **Delete Marker** shortcut menu command.

Correlating Timestamps of Traces from Two Protocol Analyzers - Example

Consider that you there is a situation where you have two Protocol Exercisers (`Ex1` and `Ex2`) and Protocol Analyzers (`An1` and `An2`) arranged in the following manner:

`Ex1 -> An1 -> An2 -> Ex2`

In the above setup, `Ex1` is the *source* of a packet's origin and `Ex2` is the *destination* point. The two Protocol Analyzer devices are hooked between `Ex1` and `Ex2`.

Now for a particular packet that originates from `Ex1`, you want to find out the time difference between when it is seen by `An1` and when it is seen by `An2`.

The following procedure provides step-by-step instructions to correlate the timestamps of the traces from `An1` and `An2` in the above mentioned setup.

To Correlate the Timestamps of a Packet Captured by An1 and An2

1 Add `An1` and `An2` to the same chassis.

   To successfully complete this step, refer *Setting Up the Hardware* in *Agilent System Protocol Tester, Installation Guide*.

2 Add `An1` and `An2` to the same session.

   Adding both Protocol Analyzers to the same session ensures that they start simultaneously and their timestamps correlate directly.

   The successful completion of this step displays the main Protocol Analyzer window.

3 Click the **Capture > Start** menu command.

   The successful completion of this step displays the captured data in the Packet view.

4 Create two new markers in the Packet view:

   a Create first marker on the desired packet captured by `An1`.

   b Create second marker on that same packet captured by `An2`.

5 Measure the time difference between these two markers.

To successfully complete this step, refer To Measure the Time Difference between Markers.

The result of this activity is displayed in the Measurement area.

NOTE	The final result of the above activity shows inaccuracy of 16 +X nanoseconds (ns). Here, the value of X depends on the underlying link width in the following manner:

- For the x8 link width, X = 8 ns
- For the x4 link width, X = 16 ns
- For the x2 link width, X = 32 ns
- For the x1 link width, X = 64 ns

Out of the inaccuracy of 16 + X ns, you can eliminate the inaccuracy of 16 ns by sending *External Trigger Out* signals from both Protocol Analyzers to an Oscilloscope. However, you must ensure sending External Trigger Out signals from the front panel of chassis. This is because, sending External Trigger Out signals from the back panel of chassis produces inaccuracy of approximately 2 microseconds (us).

For information on External Trigger Out, refer to Chapter 5, "Triggers.

4

Capturing, Filtering, and Finding the Data

This chapter provides information on how to setup hardware and capture data for different protocols. This chapter also provides information on how to create and use filters in Protocol Analyzer and how to find records from the Packet view.

About Setting Up the Hardware

Once you have installed the Protocol Analyzer, you can start using it to capture data. At this stage, Protocol Analyzer captures the data using the default settings in Hardware Setup dialog box, such as default **x1** link width.

There may be a situation when the default link width of Protocol Analyzer does not match the negotiated link width of transmitter and receiver. This prevents Protocol Analyzer from properly decoding the data packets, which results in displaying the garbage data on the screen. To avoid this situation, ensure that the link width of Protocol Analyzer is always same as the negotiated link width of transmitter and receiver. To do this, use the Hardware Setup dialog box (Figure 23). This dialog box also enables you to specify other hardware settings, such as trace memory size, clock source, and capture mode.

To access this dialog box:

*   Click **Capture > Hardware Setup**.

    The Hardware Setup dialog box appears (Figure 23).
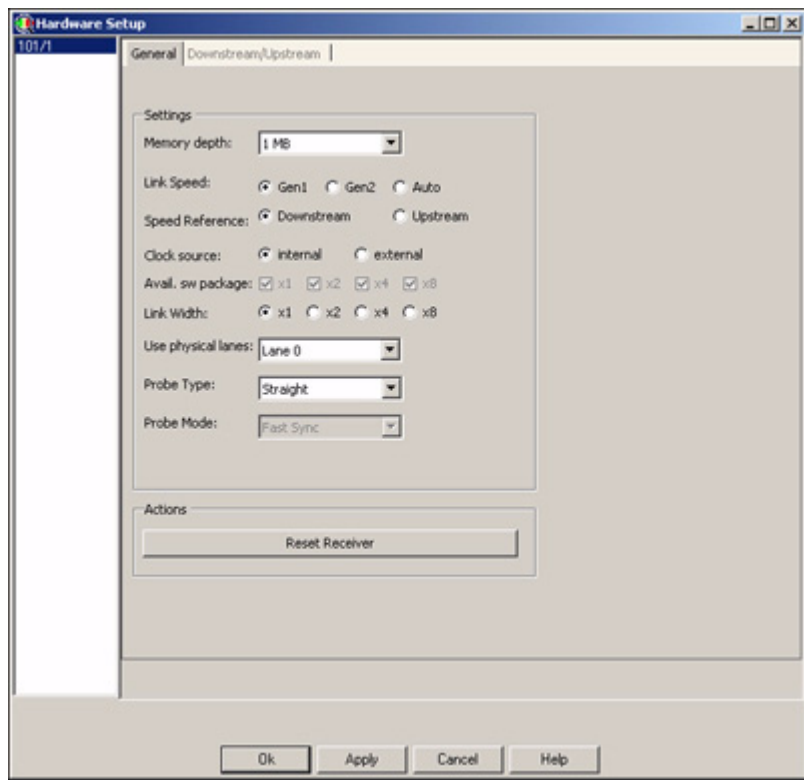
Figure 23   Hardware Setup dialog box

The Hardware Setup dialog box provides a different set of options for different protocols. The Hardware Setup dialog box is also different for the x16 link width, when compared with x8 or lower link widths.

In the following sections, you will learn about:

- Setting Up the Hardware for PCI Express
- Setting Up the Hardware for ASI
- Setting Up the Hardware for Fibre Channel
- Setting Up the Hardware for x16

Setting Up the Hardware for PCI Express

Figure 24 displays the Hardware Setup dialog box for the PCI Express protocol.
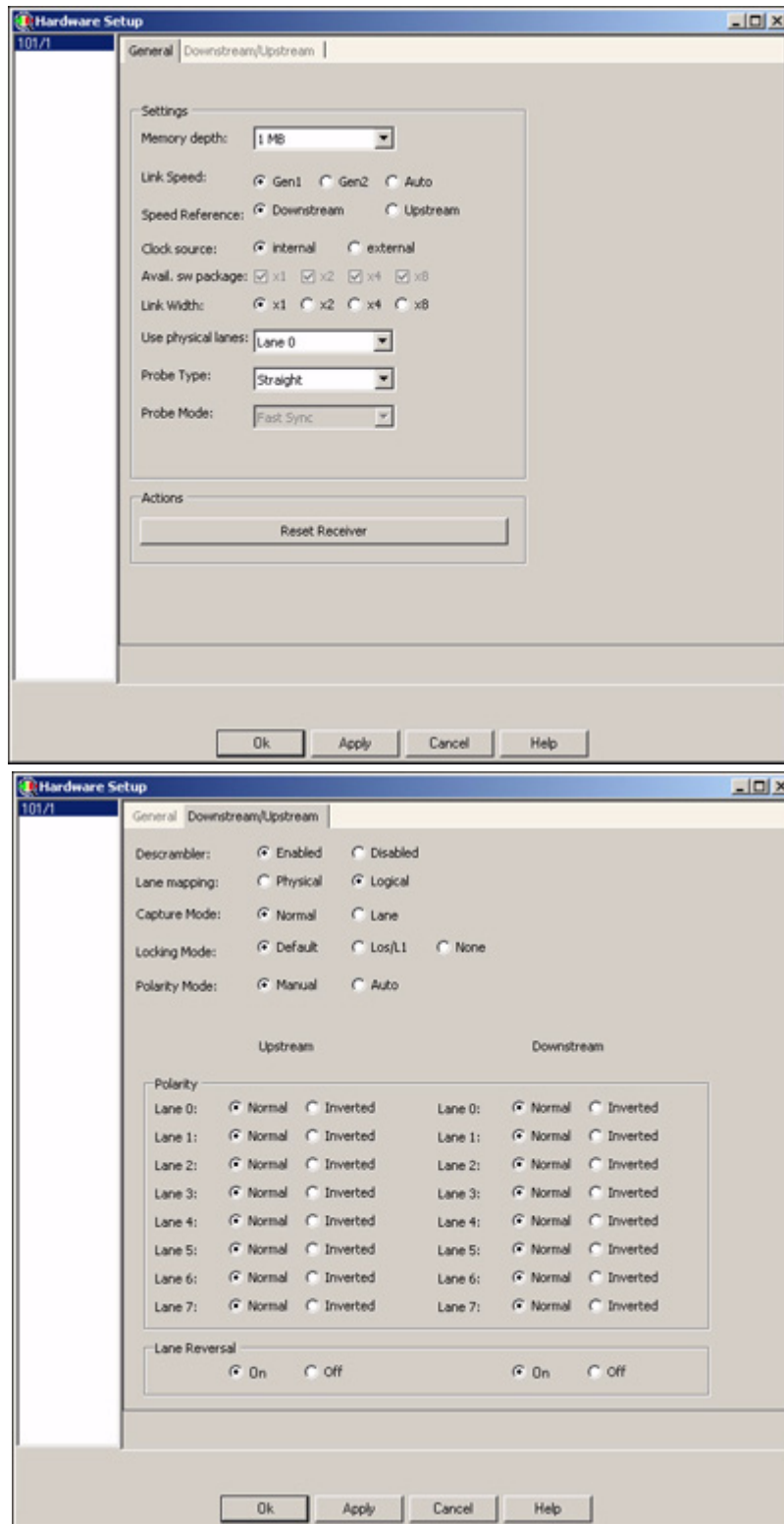
Figure 24   Hardware Setup dialog box for PCI Express

As shown in Figure 24, the Hardware Setup dialog box for PCI Express has two tabs: General and Downstream/Upstream.

Table 17 briefly describes the components of the General tab.

Table 17 Components of the General tab

Component	Description
Memory depth	Click the **Memory depth** drop-down list to select the size of the trace memory, where all the captured data is stored. This drop-down list allows you to choose between 1 KB and 2 GB of trace memory size. The default size is 1 MB. You can increase the memory depth to save more number of records in the trace, however it may increase the *file save time* and *data upload time* considerably. Therefore, it is very important to carefully decide upon the memory depth requirements.
Link Speed	Displays the following option buttons: • **Gen1**: Select **Gen1** if you want Protocol Analyzer to capture data at the 2.5 Gb/s speed. • **Gen2**: Select **Gen2** if you want Protocol Analyzer to capture data at the 5 Gb/s speed. • **Auto**: Select **Auto** if you want Protocol Analyzer to determine the data capturing speed from data signals. In this setting, the speed detection process takes some time, during which Protocol Analyzer does not captures any data. Protocol Analyzer saves the current speed in the trace memory. Therefore, you can view it as part of the trace data in the Packet view.
Speed Reference	**Speed Reference** provides options, such as *Downstream* and *Upstream*, to specify the speed at which Protocol Analyzer should capture the data for both directions. For example, selecting *Upstream* instructs Protocol Analyzer to use the speed of the upstream port for capturing the data from both upstream and downstream ports. Speed Reference options are not available for x16.

Table 17   Components of the General tab

Component	Description
Clock source	Displays the following option buttons: • **internal:** Select **internal** to select an internal clock source, which is a recommended source for both types of systems (using SSC as well as not using SSC). You should select this option button if the data rate is in the range of 2.5 GB/s or 5 GB/s +/- 50 ppm. Analyzer will not require any input clock in this mode. • **external:** Select **external** to select an external clock source. Use external clock only if internal clock does not satisfy your needs. An external clock needs to be provided to Analyzer in this mode.
Avail. sw package	Displays the disabled check boxes of link width. A selected check box means the link width is available to you. A cleared check box means the link width is not available to you.
Link Width	Displays the option buttons for the available link width. Here, select the link width that matches the negotiated link width of transmitter and receiver.
Use physical lanes	The **Use physical lane** drop-down list provides options to select a desired pin(s) configuration on the mid-bus probe. Options displayed here depends on the link width selected in the General tab. For example, if you are using the x8 mode and you selected the x4 link width in the General tab, then the Use physical lane drop-down list displays the following options: • **Lane 0 ... 3** • **Lane 4 ... 7** Similarly, if you are using the x16 mode and you selected the x8 link width in the General tab, then the physical lane drop-down list displays the following options: • **Lane 0 ... 7** • **Lane 8 ... 15**
Probe Type	The **Probe Type** drop-down list provides the following probe type options: • Straight • N5307A SlotInterposer These options are displayed only when you select the x1 link width. For x2, x4, and x8 link widths, this drop-down list is disabled, and the Straight probe type is used by default.

Table 17 Components of the General tab

Component	Description
Probe Mode	The **Probe Mode** drop-down list enables you to specify how you want to capture the data traffic in Protocol Analyzer. This drop-down list provides the following options: • **Standard**: Analyzer can be used for all analysis purposes. If electrical idle is broken on a lane, the analyzer will resume capturing. This mode should be used in all cases except when debugging around electrical idle. • **Fast Sync**: This mode is optimized to analyze around power-up, link-training, or L0s states, where faster reaction times of Analyzer are needed, and less focus is placed on signal integrity. The Analyzer will take less time to resume capturing after break of electrical idle, but there is a probability to record false errors.
OK	Click **OK** to close the Hardware Setup dialog box after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in this tab to the hardware.
Cancel	Click **Cancel** to close the Hardware Setup dialog box without saving any changes.
Help	Click **Help** to display online help.

| NOTE | If you have selected Automatic in the Link Speed drop-down list, then the *Speed* column in the Packet view may shows *Unknown* on every speed change even before the underlying device has sent its EIOS (Electrical Idle Ordered Sets) and goes to the *electrical idle* state.

Clicking **Reset Receiver** also resets the changes made to the hardware setup. As a result of this, the *Link width* attribute in the Hardware Status dialog box displays *unknown* until the next link training.

Click Reset Receiver if Analyzer Receiver does not recover in case of Power Management scenarios. |

Table 18 briefly describes the components of the Upstream/Downstream tab.

Table 18   Components of the Upstream/Downstream tab

Component	Description
Descrambler	Displays the following option buttons: • **Enabled**: Selecting **Enabled** activates the descrambler algorithm. This algorithm is used to generate the de-scrambled packet stream from an incoming scrambled packet stream. • **Disabled**: Selecting **Disabled** deactivates the descrambler algorithm. You generally select this option when DUT is transmitting the non-scrambled data. This is because selecting Disabled, when DUT is transmitting scrambled data, displays the garbage data.
Lane mapping	Displays the following option buttons: • **Physical**: Selecting **Physical** displays the actual physical status of the lane. For example, you are using the x8 mode, selected the x4 link width, and have specified to use **4 ... 7** physical lanes. In this case, selecting Physical displays the lane status as **4 ... 7**. • **Logical**: Selecting **Logical** always displays that *0 ... (Link Width - 1)* lanes are in use, irrespective of the actual physical status of the lane. For example, you are using the x8 mode, selected the x4 link width, and have specified to use **4 ... 7** physical lanes. In this case, selecting Logical displays the lane status as **0 ... 3**. The current lane settings are immediately displayed in the Polarity section of the Hardware Setup dialog box, Lane Status column of the Port Overview pane, and Hardware Status dialog box. However, the Lane Display pane does not reflect the current lane settings until the next Protocol Analyzer run.
Capture Mode	Displays the following option buttons: • **Normal**: Selecting **Normal** captures data only when all the configured lanes are out of the Loss of Sync (LOS) condition, that is, each lane is having valid data. In this mode, channel bonding may not exist when data capturing starts. However, Protocol Analyzer ensures that channel bonding occurs before data capturing ends. • **Lane**: Selecting **Lane** captures data by each lane. This means, if only one lane is out of the LOS condition, then its data is captured in the trace. In this mode, channel bonding may not exist at all.

Table 18   Components of the Upstream/Downstream tab

Component	Description
Locking Mode	Displays the following options: • **Default**: Select this option only when you have selected the Auto option button in the General tab. • **L0s/L1**: Select this option only when you have selected the Gen1 or Gen2 option button in the General tab. • **None**: This option is not in use yet.
Polarity Mode	Displays the following option buttons: • **Manual**: Selecting **Manual** enables you to set the polarity of the individual lanes to the **Normal** or **Inverted** state. • **Auto**: Selecting **Auto** sets the polarity of the lanes automatically during the initial link training.
Lane reversal	Displays the following option buttons for each stream: • **On**: Select **On** to activate lane reversal. • **Off**: Select **Off** to deactivate lane reversal.
OK	Click **OK** to close the Hardware Setup dialog box after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in this tab to the hardware.
Cancel	Click **Cancel** to close the Hardware Setup dialog box without saving any changes.
Help	Click **Help** to display online help.

Setting Up the Hardware for ASI

Figure 25 displays the Hardware Setup dialog box for the ASI protocol.
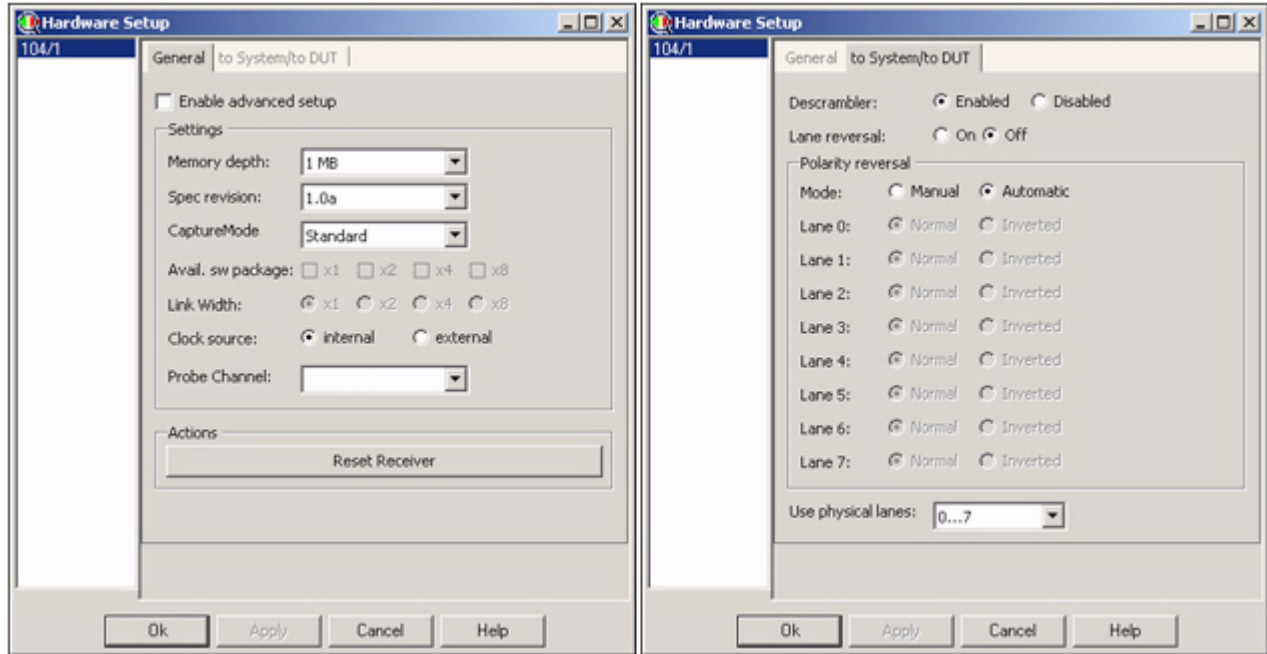
Figure 25 Hardware Setup dialog box for ASI

As shown in Figure 25, the Hardware Setup dialog box for ASI has two tabs: General and to System/to DUT.

Table 19 briefly describes the components of the General tab.

Table 19 Components of the General tab

Component	Description
Port Selector	The **Port Selector** list displays a list of available ports for ASI. Select the port for which you intend to specify hardware settings.
Enable advanced setup	Select **Enable advanced setup** to display separate tabs for *to DUT* and *to System*. This enables you to apply different hardware settings for *to DUT* and *to System*.

Table 19 Components of the General tab

Component	Description
Memory depth	Click the **Memory depth** drop-down list to select the size of the trace memory, where all the captured data is stored. This drop-down list allows you to choose between 1 KB and 1 GB of trace memory size. The default size is 1 MB. You can increase the memory depth to save more number of records in the trace, however it may increase the *file save time* and *data upload time* considerably. Therefore, it is very important to carefully decide upon the memory depth requirements.
Spec revision	Click the **Spec revision** drop-down list to select the revision number (1.0 or 1.0a) of the ASI protocol specification.
Capture Mode	The **Capture Mode** drop-down list enables you to specify how you want to capture the data traffic in Protocol Analyzer. This drop-down list provides the following options: • **Standard**: Analyzer can be used for all analysis purposes. If electrical idle is broken on a lane, the analyzer will resume capturing. This mode should be used in all cases except when debugging around electrical idle. • **Fast Sync**: This mode is optimized to analyze around power-up, link-training, or L0s states, where faster reaction times of Analyzer are needed, and less focus is placed on signal integrity. The Analyzer will take less time to resume capturing after break of electrical idle, but there is a probability to record false errors.
Avail. sw package	Displays the disabled check boxes of link width. A selected check box means the link width is available to you. A cleared check box means the link width is not available to you.
Link Width	Displays the option buttons for the available link width. Here, select the link width that matches the negotiated link width of transmitter and receiver.

Table 19   Components of the General tab

Component	Description
Clock source	Displays the following option buttons: • **internal:** Select **internal** to select an internal clock source. You should select this option button if the data rate is in the range of 2.5 GB/s or 5 GB/s +/- 50 ppm. Note that there is no input clock in this mode. • **external:** Select **external** to select an external clock source. You should select this option button if the device under test uses SSC or the data rate is in the range of 2.5 GB/s +/- 300 ppm (+0% / -0.5% if using SSC). The clock rate for external mode should be between 100 MHz +/- 300 ppm (+0% / -0.5% if using SSC)
Probe Channel	The **Probe Channel** drop-down list provides options for the available channels. Here, select a channel that matches the negotiated link width of transmitter and receiver. This drop-down list is available when you are using the ATCA probe board or the midbus footprint.
Reset Receiver	Click **Reset Receiver** to reset the receiver circuit of Protocol Analyzer to the default state. Clicking this button deletes all the changes you made to the default state of the receiver circuit.
OK	Click **OK** to close the Hardware Setup dialog box after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in this tab to the hardware.
Cancel	Click **Cancel** to close the Hardware Setup dialog box without saving any changes.
Help	Click **Help** to display online help.

Table 20 briefly describes the components of the to System/to DUT tab.

Table 20   Components of the to System/to DUT tab

Component	Description
Descrambler	Displays the following option buttons: • **Enabled**: Selecting **Enabled** activates the de-scrambler algorithm. This algorithm is used to generate the de-scrambled packet stream from an incoming scrambled packet stream. • **Disabled**: Selecting **Disabled** deactivates the descrambler algorithm. You generally select this option when DUT is transmitting the non-scrambled data. This is because selecting Disabled, when DUT is transmitting the scrambled data, displays the garbage data.
Lane reversal	Displays the following option buttons: • **On**: Select **On** to activate lane reversal. • **Off**: Select **Off** to deactivate lane reversal.
Polarity reversal	Displays the following option buttons: • **Manual**: Selecting **Manual** enables you to set the polarity of the individual lanes to the **Normal** or **Inverted** state. • **Automatic**: Selecting **Automatic** sets the polarity of the lanes automatically during the initial link training.
Use physical lanes	The **Use physical lane** drop-down list enables you to specify the number of physical lanes to use. This drop-down list provides the following options: • **0 ... 7**: Selecting **0 ... 7** maps 0 ... 7 physical lanes with 0 ... 7 channels of Protocol Analyzer. • **4 ... 7**: Selecting **4 ... 7** maps 4 ... 7 physical lanes with 4 ... 7 channels of Protocol Analyzer. If you select the x1, x2, or x4 lane width in the General tab, then selecting 4 ... 7 maps 0 ... 3 physical lanes with 0 ... 3 channels of Protocol Analyzer.
OK	Click **OK** to close the Hardware Setup dialog box after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in this tab to the hardware.
Cancel	Click **Cancel** to close the Hardware Setup dialog box without saving any changes.
Help	Click **Help** to display online help.

Setting Up the Hardware for Fibre Channel

Figure 26 displays the Hardware Setup dialog box for the Fibre Channel protocol.
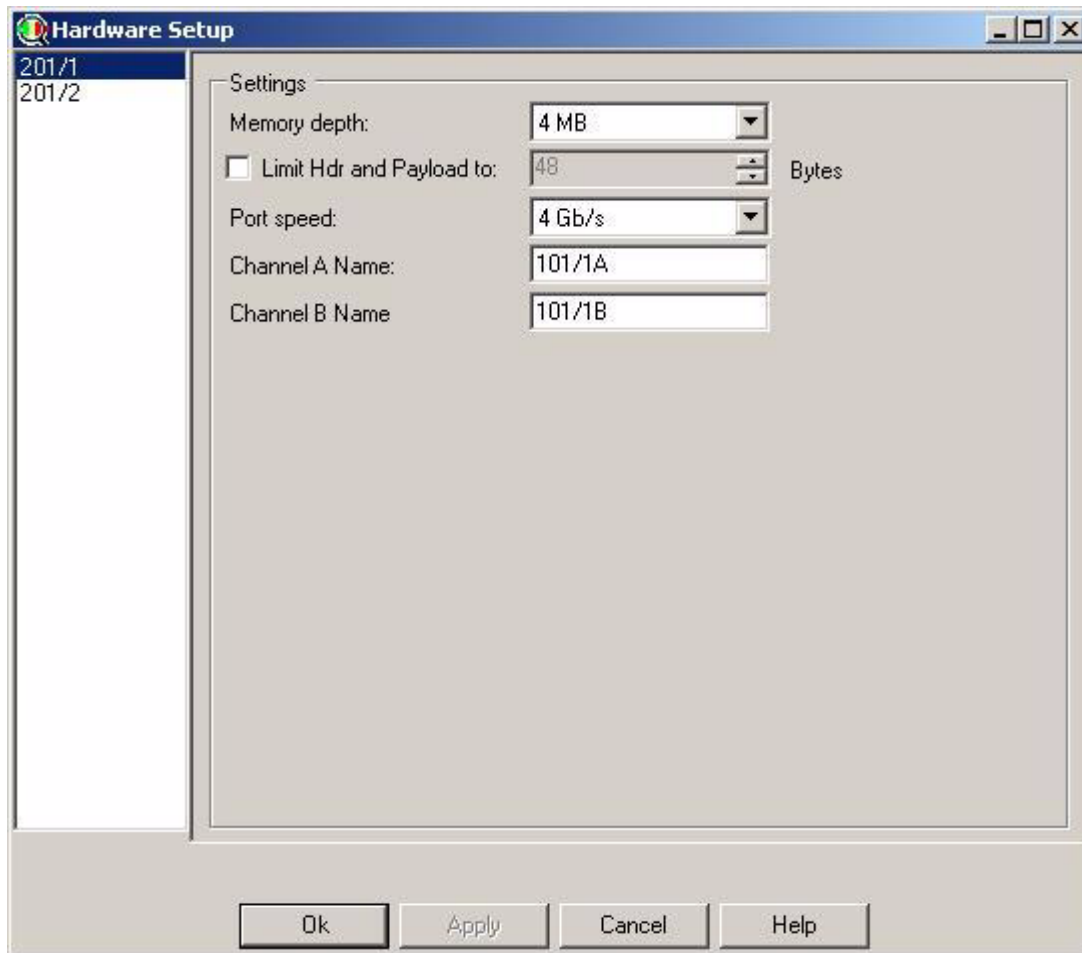
Figure 26 Hardware Setup dialog box for Fibre Channel

Table 21 briefly describes the components of the Hardware Setup dialog box for Fibre Channel.

Table 21 Components of the Fibre Channel dialog box

Component	Description
Port Selector	The **Port Selector** list displays a list of available ports for Fibre Channel. Select the port for which you intend to specify hardware settings.

Table 21   Components of the Fibre Channel dialog box

Component	Description
Memory depth	Click the **Memory depth** drop-down list to select the size of the trace memory, where all the captured data is stored. This drop-down list allows you to choose between 1 KB and 1 GB of trace memory size. The default trace memory size is 8 MB. You can increase the memory depth to save more number of records in the trace, however it may increase the *file save time* and *data upload time* considerably. Therefore, it is very important to carefully decide upon the memory depth requirements.
Limit Hdr and Payload to	Select the **Limit Hdr and Payload to** check box to allow the hardware to limit payload storage to a particular size (in bytes). Selecting this check box enables the adjacent text box. Here, type in the number of bytes to which you want to limit the payload. You can decide this value based on the importance of payload content. Limiting the payload storage will allow more ordered sets or frames to be stored
Port speed	Click the **Port speed** drop-down list to select an appropriate speed for the port. If you have multiple ports within a single module, then you can select one of the following combinations of port speed: • **1 Gb/s** and **2 Gb/s** • **2 Gb/s** and **4 Gb/s** Note that a port speed combination of 1 Gb/s and 4 Gb/s in the same module is not possible. For this, you need to use two separate modules in your application.
Channel A Name	Specifies the name of Channel A.
Channel B Name	Specifies the name of Channel B.
OK	Click **OK** to close the Hardware Setup dialog box after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in the Hardware Status dialog box.
Cancel	Click **Cancel** to close the Hardware Setup dialog box without saving any changes.
Help	Click **Help** to display online help.

Setting Up the Hardware for x16

Figure 27 displays the Hardware Setup dialog box for x16.
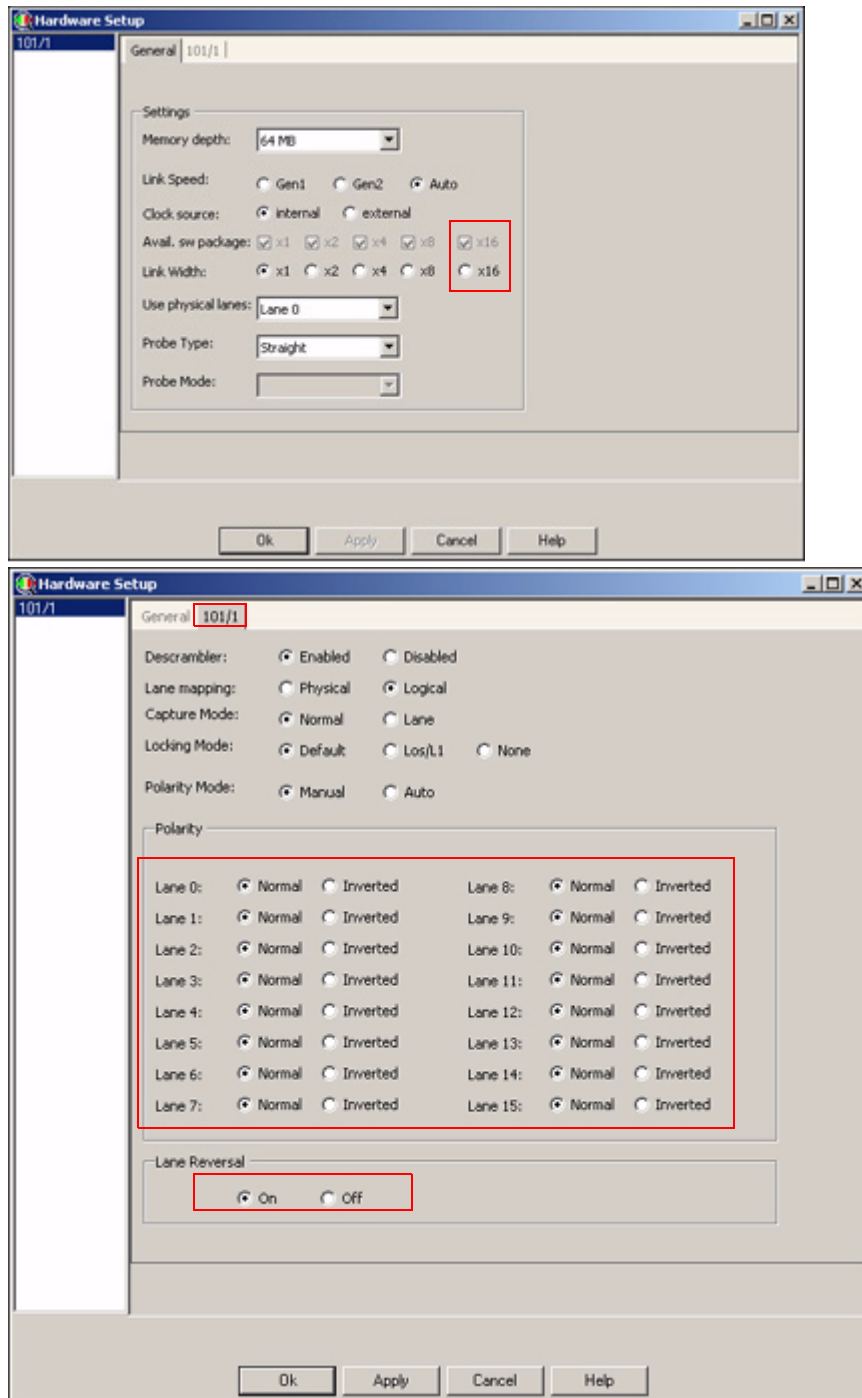
Figure 27 Hardware Setup dialog box for x16

The Hardware Setup dialog box for x16 is marginally different from the Hardware Setup dialog box for x8. These difference are highlighted in Figure 27. A brief description of these differences is given below:

- The General tab provides an additional option button to help you select the x16 link width. Select this link width only when it matches the negotiated link width of the transmitter and receiver.

- The Probe Type drop-down list now provides the following options for different types of midbus probe:
  - Straight
  - Swizzled A
  - Swizzled B
  - N4223A Gen1 Probe

- The Polarity section now provides option buttons for all the 16 lanes, which are needed for the x16 link width. You can set the polarity of these lanes automatically during the initial link training or manually.

- The second tab still enables you to set the hardware settings for the underlying stream. However, it does not enable you to set the hardware settings for both Upstream and Downstream. This is because all the available 16 lanes are used for the single underlying stream.

  To simultaneously analyze both Upstream and Downstream using Protocol Analyzer for x16:
  - Add two separate ports, one for Upstream and the other for Downstream, in the Port Selection dialog box.
  - Specify separate hardware settings for these ports in the Hardware Setting dialog box.

About Capturing the Data

Once you have specified the desired hardware settings, you can start using Protocol Analyzer to capture the data.

Capturing the Data

To capture the data:

- Click **Capture > Start**.

  You can also start capturing the data by clicking the ▶ icon on the toolbar.

  Once the data of the size of trace memory is captured, Protocol Analyzer stops and the captured data is displayed in the Packet view.

  You can also stop Protocol Analyzer by clicking the **Capture > Stop** menu command or by clicking the ■ icon on the toolbar.

About Filtering and Finding the Records

In this section, you will learn about:

* Filtering the Records
* Finding the Records

Filtering the Records

When you capture the data, it is first stored in the trace memory. From there, it is displayed in the Packet view. There are situations when, instead of viewing the complete data, you want to view and analyze only a few specific records. For this, you want to display only the required portion of the data from the trace memory. To deal with this situation, Protocol Analyzer enables you to apply filters to the captured set of records.

A *filter* is a set of one or more conditions that you apply on the data stored in the trace memory of Protocol Analyzer. You do this to display a specific portion of data in the Packet view to analyze. For example, if you want to analyze only TLPs, then you can create a filter that displays only TLPs in the Packet view.

In Protocol Analyzer, you can create and apply filters using the Filter dialog box (Figure 28).

To access the Filter dialog box:

* Click **View > Filter > Custom**.

  The Filter dialog box appears (Figure 28).

Listing tab   Add/Remove Condition menu   Condition text box

Boolean Operation drop-down list

Channel drop-down list
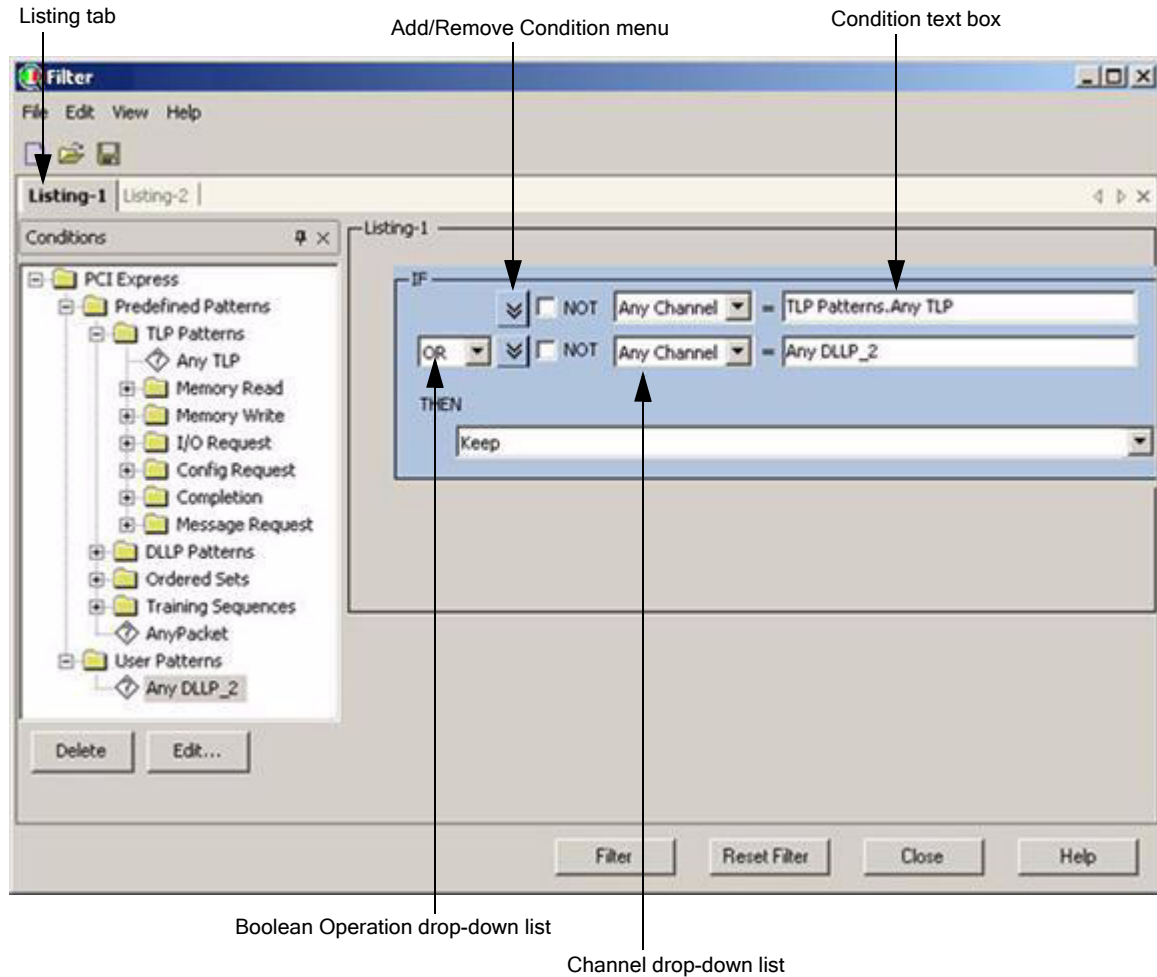
Figure 28   Filter dialog box

Table 22 briefly describes the components of the Filter dialog box.

Table 22   Components of the Filter dialog box

Component	Description
Listing	The **Listing** tab allows you to select and set different filters for different listings of the Packet view.

Table 22 Components of the Filter dialog box

Component	Description
Conditions	The **Conditions** list box displays a hierarchical list of predefined and user patterns. All patterns under the **Predefined Patterns** folder are predefined patterns. These patterns are protocol specific and are provided by Protocol Analyzer. All patterns under the **User Patterns** folder are user patterns. These patterns are created by copying the predefined patterns to this folder, and then modifying them to match your requirements.
IF	The **IF** section provides the following components to specify the filter criteria: • **Add/Remove Condition**: This menu enables you to add a new condition criteria to the IF section, or remove an existing condition criteria from the IF section. Note that you can remove conditions only when the IF section has more than one condition criteria. • **NOT**: This check box enables you to apply the logical NOT function to the pattern in the Condition text box. • **Channel**: This drop-down list provides options to specify which channel to include in the filter criteria. This drop-down list is displayed when you add a pattern in the Condition text box. This drop-down list is not displayed for the x16 link width. • **Condition**: This text box contains a pattern that you drag and drop from the Conditions list box. • **Boolean Operation**: This drop-down list provides options to apply the logical OR or AND functions to the filter criteria. This drop-down list is displayed for every new condition that you add using the Add/Remove Condition menu.
THEN	The **THEN** drop-down list provides options that you can choose as an action to be taken when the filter criteria is met. This drop-down list has the following options: • **Keep**: Selecting **Keep** displays all the packets, meeting the filter criteria, in the Packet view. • **Drop**: Selecting **Drop** removes all the packets, meeting the filter criteria, from the Packet view.
Copy	Click **Copy** to copy the selected predefined pattern in the User Pattern folder. You generally do this to further modify the copied pattern. The Copy command button is available only when you select a predefined pattern in the Conditions list box.

Table 22   Components of the Filter dialog box

Component	Description
Show	Click **Show** to display the Show Condition dialog box for the selected predefined pattern. This dialog box displays the contents of the selected predefined pattern and also allows you to edit it.
Delete	Click **Delete** to delete the selected user pattern. The Delete command button appears only when you select a user pattern.
Edit	Click **Edit** to display the Edit Condition dialog box for the selected user pattern. Here, you can make any modifications to the selected user pattern, as desired.
Filter	Click **Filter** to apply the filter criteria on the data displayed in the Packet view.
Reset Filter	Click **Reset Filter** to remove the applied filter criteria from the data displayed in the Packet view.
Close	Click **Close** to exit the Filter dialog box.
Help	Click **Help** to display the online help.

Finding the Records

Consider that you have captured and displayed all TLPs in the Packet view. Now, you want to look at the details of a particular type of TLP to analyze it. In this situation, you can search the desired data packet using the Find dialog box (Figure 29).

In Protocol Analyzer, the Find dialog box enables you to specify single or multiple conditions to find the required data packet in the Packet view.

To access the Find dialog box:

• Click **Edit > Find**.

The Find dialog box appears (Figure 29).

Figure 29   Find dialog box

Table 23 briefly describes the components of the Find dialog box.

Table 23   Components of the Find dialog box

Component	Description
Listing	The **Listing** tab allows you to select and set different search criteria for different listings of the Packet view.
Conditions	The **Conditions** list box displays a hierarchical list of predefined and user patterns. All patterns under the TLP Patterns, DLLP Patterns, Ordered Sets, Training Sequences folders are predefined patterns. These patterns are protocol specific. All patterns under the User Patterns folder are user patterns. These patterns are created by copying the predefined patterns to this folder, and then modifying them to match your requirements.
Copy	Click **Copy** to copy the selected predefined pattern in the User Pattern folder. You generally do this to further modify the copied pattern. The Copy command button is available only when you select a predefined pattern in the Conditions list box.
Show	Click **Show** to display the Show Condition dialog box for the selected predefined pattern. This dialog box displays the contents of the selected predefined pattern and also allows you to edit it.

Table 23   Components of the Find dialog box

Component	Description
Delete	Click **Delete** to delete the selected user pattern. The Delete command button appears only when you select a user pattern.
Edit	Click **Edit** to open the Edit Condition dialog box. This dialog box displays various parameters for editing and customizing the selected user pattern. The Edit command button appears only when you select a user pattern.
Port Selection	The **Port Selection** list box displays a check box list of ports connected with the current instance of Protocol Analyzer.
Enter Search Condition(s)	The **Enter Search Condition(s)** section provides the following components to specify the search criteria: • **Add/Remove Condition**: This menu enables you to add a new condition criteria to the Enter Search Condition(s) section, or remove an existing condition criteria from the Enter Search Condition(s) section. Note that you can remove conditions only when the IF section has more than one condition criteria. • **NOT**: This check box enables you to apply the logical NOT function to the pattern in the Condition text box. • **Channel**: This drop-down list provides options to specify which channel to include in the filter criteria. This drop-down list is displayed when you add a pattern in the Condition text box. • **Condition**: This text box contains a pattern that you drag and drop from the Conditions list box. • **Boolean Operation**: This drop-down list provides options to apply the logical OR or AND functions to the filter criteria. This drop-down list is displayed for every new condition that you add using the Add/Remove Condition menu.
Find next	Click **Find next** to find the next occurrence of the data packet that matches the search criteria.
Find prev	Click **Find prev** to find the previous occurrence of the data packet that matches the search criteria.
Close	Click **Close** to exit the Find dialog box.
Help	Click **Help** to display the online help.

Important Points About Find and Filters

Remember the following points while specifying the filter and search criteria:

- The NOT check box is not available if you have already selected an individual channel in the Channel Selector drop-down list.

- The Drop option of the THEN drop-down list is not available if you have already selected an individual channel in the Channel Selector drop-down list.

- You cannot select an individual channel in the Channel Selector drop-down list if you have already specified the NOT or Drop pattern.

- You cannot load a saved search or filter, which has the NOT or Drop pattern, if you have already selected an individual channel in the Channel Selector drop-down list.

- You cannot edit training sequences and ordered sets.

- Selecting an individual channel in the Channel Selector drop-down list disables all the filter icons on the toolbar of the main Protocol Analyzer window.

- You can add maximum of eight patterns in each filter and search criteria.

- If you are using the Gen2 hardware, then you can add maximum of four patterns.

Filter Examples

This section provides examples of creating and using filters for different requirements.

In this section, you will learn:

- Creating a Simple Filter
- Creating Filters for different ports
- Using Predefined Filters

Creating a Simple Filter

Consider that you want to create a filter to keep only TLPs and DLLPs. You want to filter out all remaining data packets from the Packet View.

Using the pattern condition mentioned above, you will learn how to create and apply a filter.

To create and apply filter

1 Click **View > Filter > Custom**.

The Filter dialog box appears.

You can also open the Filter dialog box by clicking [EDIT] icon on the toolbar.

2 Select the desired listing for which you want to add a filter.

3 In Condition list box, expand **PCI Express > Predefined Patterns > TLP Patterns**.

4 Drag **Any TLP** from the Conditions list box and drop it in the Condition text box.

5 Click the **Add AND/OR condition below** menu command from the Add/Remove Condition menu.

This adds a new condition criteria.

You can add a maximum of eight AND/OR pattern conditions while creating a filter.

6 Select **OR** from the Boolean Operation drop-down list.

7 Expand **DLLP Patterns** in the Conditions list box.

8 Drag **Any DLLP** from the Conditions list box and drop in the newly added Condition text box.

9 Select **Keep** from the THEN drop-down list.

This creates the filter that will display the captured TLPs and DLLPs in the Packet view.

10 Click **Filter**.

This filters the data in the Packet view.

11 Click **Close**.

This completes your activity for creating a simple filter. You can now run Protocol Analyzer to use this filter. You can also choose to save this filter for later needs by clicking **File > Save as** from the filter dialog box.

NOTE	To enable or disable filters for a current listing you can click **View > Filter > Reset Filter.** You can also click ⊠ (to disable filters) or ▽ (to enable filters) on the toolbar.

Creating Filters for different ports

Consider that you have captured trace for two ports and you want to create a separate filter for each port. You want to create filters for the following conditions:

- For the first port, you want to filter and display the records for TLP memory read condition on the Upstream channel.

- For the second port, you want to filter out and drop the records for TLP memory write condition on the downstream channel. The packet view must display all records except the ones for memory write on downstream channel.

Using the pattern condition requirement mentioned above, you will learn how to create and apply filter for it.

To create and apply filters for different ports

1 Create two listings, one for each port. Lets say for Port 101 and 102.

To add a listing right click *Listing* tab and select *Duplicate* option.

2 Select Listing2 from **Listings** tab.

3 Expand Channel Selector from the Toolbar as shown in Figure 30 and select port 102.

The packet view for listing 2 will display records only for port 102.

Channel Selector

Figure 30   Channel Selector

4 Select Listing1 from the Listings tab.

5 Expand Port/ Channel Selector from the Toolbar and select port 101 from the list.

The packet view for listing 1 displays records only for port 101.

6 Click **View > Filter > Custom**.

The Filter dialog box appears.

7 In Condition list box, expand **PCI Express > Predefined Patterns > TLP Patterns > Memory Read**.

8 Drag **Any Memory Read** from the Conditions list box and drop it in the Condition text box. This adds a new condition criteria.

9 Select Upstream from the Channel selector drop list.

10 Select **Keep** from the THEN drop-down list.

This creates the filter that will display the Memory read TLPs in the Packet view for Upstream channel, port 101.

11 Click **Filter**.

12 Click **Close**.

13 Similarly to create a memory write filter for port 102, select Listing 2 and open the Filter dialog box.

14 In Condition list box, expand **PCI Express > Predefined Patterns > TLP Patterns > Memory Write**.

15 Drag **Any Memory write** from the Conditions list box and drop it in the Condition text box. This adds a new condition criteria.

16 Select Downstream from the Channel selector drop list.

17 Select **Drop** from the THEN drop-down list.

18 This creates the filter that will filter out and drop all the Memory write TLPs in the Packet view for Downstream channel, port 102 and display all the remaining records.

19 Click **Filter**.

20 Click **Close**.

This completes your activity for creating filter for multiple ports. You can also choose to save this filter for later needs.

NOTE	Though you can save the filter conditions created, you cannot save the filtered trace.

Using Predefined Filters

Consider that you want to filter out all *Skip Ordered sets* from the packet view. Or you want to filter out all *Ordered sets* along with all *Update Flowcontrol packets* and *Training Sequences*.

Using the pattern condition requirement mentioned above, you will learn how to use Predefined Filters provided by Analyzer GUI for PCI express protocol.

You can use Predefined Filters only when *All ports* option is selected in the Port/ Channel selector list, from the Toolbar. In case you de-select any port or channel, then the pre-defined filters option will no longer remain valid.

To apply predefined filters

1 Select the listing that you want to work on.

2 Expand Port/ Channel Selector from the Toolbar and select *All ports*.

3 Click on the *Filter all Skip Ordered sets* icon from the Toolbar as shown in Figure 31.

.

Filter all Update Flowcontrol packets,
Ordered sets and Training sequences

Filter all Skip Ordered sets
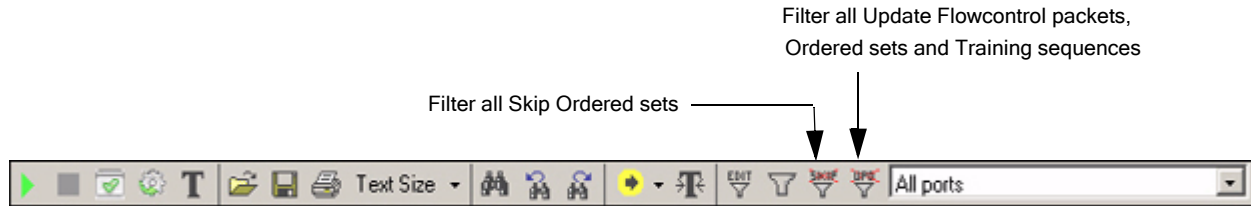
Figure 31   Filter Icons

All skip order sets get filtered out. The packet view displays all the remaining records for the chosen port/channel.

4 To Filter out all Update Flowcontrol packets, Ordered sets and Training sequences, first select the listing that you want to work on and then click on *Filter out all Update Flowcontrol packets, Ordered sets and Training sequences* icon from the toolbar as shown in Figure 31 above.

All *Update Flowcontrol packets, Ordered sets and Training sequences* get filtered out. The packet view displays all the remaining records for the chosen port/channel.

This completes your activity for using predefined filters. You can now run Protocol Analyzer to use these filters.

| NOTE | In contrast to PCI express, Fibre Channel provides only one predefined filter. It is used to filter or show *Ordered sets*. You can access it by clicking OS icon on the toolbar. |

Find Example

This section provides example of Finding records from the packet view.

Creating a Find condition

Consider that you want to find a particular type of memory read TLP in the packet view. You want to filter out all remaining data packets from the Packet View.

Using the pattern condition mentioned above, you will learn how to create a find condition and use it to find the desired data packet.

To find a data packet

1 Click **Edit > Find**.

   The Find dialog box appears (Figure 29).

   You can also open the Find dialog box by clicking [icon] icon on the toolbar.

2 Select the appropriate listing from the Listing tab.

3 From the Conditions list box, click to expand **PCI Express > Predefined Patterns > TLP Patterns > Memory Read** folders.

4 Drag **Any Memory Read** from the Conditions list box and drop it in the Condition text box.

5 Click **Find next**.

   This highlights the first data packet in the Packet view, which matches the search criteria.

6 To see the next record you can click **Find Next** on the Find dialog box, or you can also click [icon] on the toolbar.

   To see the previous record you can click **Find Prev**, or you can also click [icon] on the toolbar.

7 Repeat Step 6 until you find the required data packet.

8 Click **Close** to exit the Find dialog box.

   This completes your activity for finding records. You can now run Protocol Analyzer to find records.

5

Triggers

This chapter introduces you to the concept of triggers in Protocol Analyzer, and provides information on general trigger conditions and editing trigger conditions. This chapter also provides various use cases for creating triggers.

Agilent Technologies

Triggers

When you run Protocol Analyzer, it by default captures all types of packets it encounters, and saves them in the trace memory. There may be a situation when you do not want to capture all the packets in the trace memory. Rather, you want to perform one or more specific actions only when Protocol Analyzer encounters a particular type of packets. To deal with this situation, Protocol Analyzer enables you to create triggers.

A *trigger* is a combined set of conditions and their associated actions. A *trigger condition* specifies Protocol Analyzer about the type of data it should locate in the traffic. A *trigger action* instructs Protocol Analyzer about the action to be taken when the trigger condition is met.

In Protocol Analyzer, you can create triggers using the Trigger Setup window (Figure 32).

The Trigger Setup window also enables you to work on different protocols in a single session. For this, it provides a tabbed view where a separate tab is defined for each protocol. For example, if you are using PCIe and FC ports in a single session, then the Trigger Setup window provides separate tabs on these protocols. You can invoke these tabs to create and apply triggers on the respective protocols.

In this section, you will learn about:

• Accessing the Trigger Setup Window

• Understanding General Trigger Conditions

• Editing Trigger Conditions

Accessing the Trigger Setup Window

To access the Trigger Setup window:

• Click **Capture > Trigger Setup**.

The Trigger Setup window appears (Figure 32).

Add/Remove ELSE IF menu

Add/Remove State menu

Add/Remove Action menu

Action drop-down list

State section
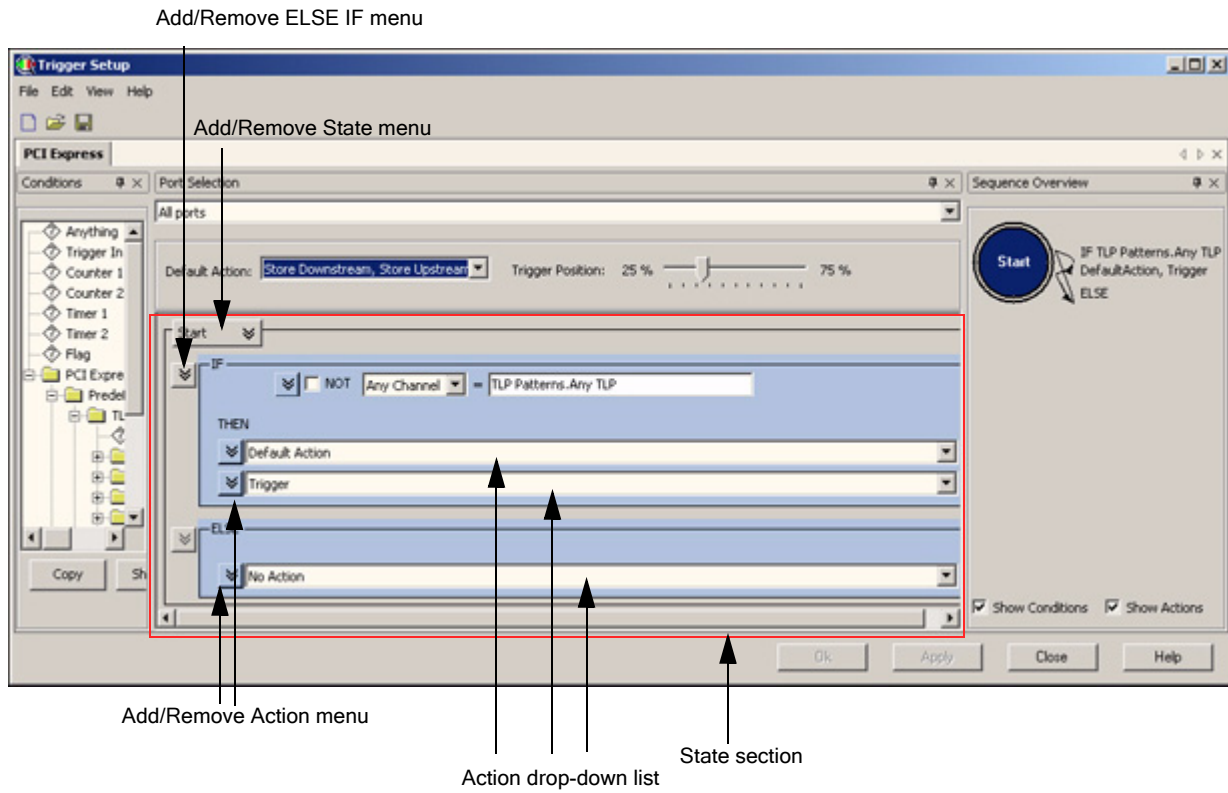
Figure 32   Trigger Setup window

Table 24 briefly describes the components of the Trigger Setup window.

Table 24   Components of the Trigger Setup window

Component	Description
Menu bar	Provides the following menus: • **File**: Provides the New, Open, and Save As menu commands to create a new trigger configuration (*.trg) file, open an existing trigger configuration file, and save the current trigger configuration in a file. • **Edit**: Provides the Edit Condition, Show Condition, Copy Condition, and Delete Condition menu commands. You can use these menu commands to edit, display, copy, and delete the selected condition. • **View**: Provides the Sequence Overview, Conditions, and Port Selection menu commands. You can use these menu commands to display or hide the Sequence Overview, Conditions, and Port Selection panes. The View menu also provides the Default Window Arrangement menu command that you use to resort to the default arrangement of the Trigger Setup window. • **Help**: Provides the Help menu command that you can click to display the online help.
Toolbar	Provides icons for the New, Open, and Save As menu commands.
Conditions	The **Conditions** pane provides components to select one or more predefined and/or user patterns to specify the trigger criteria.
Port Selection	The **Port Selection** drop-down list displays a check box list of ports connected with the current instance of Protocol Analyzer.

Table 24 Components of the Trigger Setup window (continued)

Component	Description
Default Action	The **Default Action** drop-down list provides options to specify the default action to be taken for the corresponding IF, ELSE IF, and/or ELSE condition. This drop-down list provides different options for the PCIe and FC protocols, and for the x16 link width. For the PCIe protocol, it provides the following options: • **No Action**: Select this option to not take any action. • **Store Downstream**: Select this option to store downstream packets. • **Store Upstream**: Select this option to store the upstream packets. • **Store Downstream, Store Upstream**: Select this option to store both the upstream and downstream packets. For the FC protocol, it provides the following options: • **No Action**: Select this option to not take any action. • **Store Channel A**: Select this option to store packets flowing through Channel A. • **Store Channel B**: Select this option to store packets flowing through Channel B. • **Store Channel A, Store Channel B**: Select this option to store packets flowing through Channel A and B. If you have selected to analyze the traffic flowing through the x16 link width, then irrespective of the underlying protocol, this drop-down list provides the following options: • **No Action**: Select this option to not take any action. • **Store**: Select this option to store packets flowing through the underlying stream.
Trigger Position	The **Trigger Position** scroll bar enables you to specify what range of data you want to capture in the trace memory. For example, assume that trace memory size is 8 MB. Now, you want that 25%, i.e. 2 MB, of the trace memory should get filled with the data that occurred immediately before the point where trigger condition is met, and rest of the trace memory should get filled with the data that occurred after the trigger condition is met. To do this, move the Trigger Position scroll bar to the point where its left-side is measured as 25% and its right-side is measured as 75%.
State	The **State** section provides components to specify the trigger criteria.

Table 24   Components of the Trigger Setup window (continued)

Component	Description
Sequence Overview	The **Sequence Overview** section displays the trigger conditions and the actions to be taken when the trigger conditions are met, in the form of the IF - ELSE IF - ELSE programming construct. This section has the following components: • **Show Conditions**: Select **Show Conditions** check box to display the trigger conditions. • **Show Actions**: Select **Show Actions** check box to display actions to be taken when trigger conditions are met.
OK	Click **OK** to close the Trigger Setup window after saving the changes made in it.
Apply	Click **Apply** to assign the changes made in the Trigger Setup window to the hardware.
Close	Click **Close** to exit the Trigger Setup window without saving any changes.
Help	Click **Help** to display online help.

Table 25 briefly describes the components of the Conditions pane.

Table 25   Components of the Conditions pane

Component	Description
Conditions	The **Conditions** list box displays a hierarchical list of predefined and user patterns. This list box displays a list of predefined patterns belonging to the currently selected protocol.
Copy	Click **Copy** to copy the selected predefined pattern in the User Patterns folder.
Show	Click **Show** to display the Show Condition dialog box for the selected predefined pattern. This dialog box displays the contents of the selected predefined pattern, and also allows you to edit it.
Delete	Click **Delete** to delete the selected user pattern.
Edit	Click **Edit** to display the Edit Condition dialog box for the selected user pattern. Here, you can make any modifications to the selected user pattern, as desired.

Table 26 briefly describes the components of the State section.

Table 26   Components of the State section

Component	Description
Add/Remove State	The **Add/Remove State** menu enables you to add a new state or remove an existing state. Note that you can remove a state only when there are more than one state in the current trigger configuration file.
Add/Remove ELSE IF	The **Add/Remove ELSE IF** menu enables you to add a new or remove an existing ELSE IF section. This section is same as the IF section.

IF	The **IF** section provides the following components to enable you to specify the trigger conditions:
	• **Add/Remove Condition**: This menu enables you to add a new condition criteria to the IF section, or remove an existing condition criteria from the IF section. Note that you can remove conditions only when the IF section has more than one condition criteria.
	• **NOT**: This check box enables you to apply the logical NOT function to the pattern in the Condition text box.
	• **Condition**: This text box contains a pattern that you drag and drop from the Conditions list box.
	• **Channel**: This drop-down list provides options to specify which channel to include in the trigger criteria. This drop-down list is displayed when you add a pattern in the Condition text box.
	• **Count**: This text box specifies the number of times the pattern, specified in the Condition text box, should occur to satisfy the trigger condition. This text box is displayed only when you are using FC and the specified pattern is not *Anything*.
	• **Occurrence**: This drop-down list provides two options:
	  • **Consecutively**: This option indicates that the pattern, in the Condition text box, should *occur consequently* the number of times specified in the Count text box to satisfy the trigger condition.
	  • **Eventually**: This option indicates that the pattern, in the Condition text box, should *occur in any order* the number of times specified in the Count text box to satisfy the trigger condition.
	• **Boolean Operation**: This drop-down list provides options to apply the logical OR or AND functions to the trigger criteria. This drop-down list is displayed for every new condition that you add using the Add/Remove Condition menu.

**Table 26** Components of the State section (continued)

Component	Description
THEN	The **THEN** sub-section, inside the IF section, has Action and GOTO drop-down lists, and Add/Remove Action menu. The Action drop-down list provides a list of actions to be taken when the trigger condition is met. The Add/Remove Action menu provides options to add a new or remove an existing Action drop-down list from this sub-section.
ELSE	The **ELSE** section has Action drop-down list and Add/Remove Action menu. The Action drop-down list provides a list of actions to be taken when the corresponding IF and ELSE IF conditions of the ELSE section are not met. The Add/Remove Action menu provides options to add a new or remove an existing Action drop-down list to or from the ELSE section.
GOTO	The **GOTO** drop-down list provides a list of states, e.g. Start, State2, and so on. By selecting a particular state, you specify where to jump once the action has been taken. The GOTO drop-down list is displayed in the THEN sub-section and in the ELSE section, below the Action drop-down list. Also, the GOTO drop-down list is displayed only when a trigger has more than one state.

Table 26 Components of the State section (continued)

Component	Description
Action	The **Action** drop-down list provides options to specify the action to be taken when the IF/ELSE IF condition is met or when it is not met. This drop-down list is given in the THEN sub-section and in the ELSE section, and provides the following options: • **No Action**: Select this option to not take any action. • **Default Action**: Select this option to apply the action selected in the Default Action drop-down list. • **Trigger**: Select this option to trigger Protocol Analyzer. • **External Trigger Out**: Select this option for sending out the *Trigger pulse* to a different device. Use this action in conjunction with the *Trigger In* condition. • **Store**: Select this option to store packets flowing through the underlying stream. This option is displayed only when you have selected the x16 link width. • **Store Upstream**: Select this option to store packets flowing through *upstream*. This option is displayed for PCIe, and only when the underlying link width is x8 or below. • **Store Downstream**: Select this action to store packets flowing through *downstream*. This option is displayed for PCIe, and only when the underlying link width is x8 or below. • **Store Channel A**: Select this action to store packets flowing through Channel A. This option is displayed for FC, and only when the underlying link width is x8 or below. • **Store Channel B**: Select this action to store packets flowing through Channel B. This option is displayed for FC, and only when the underlying link width is x8 or below. • **Reset Counter 1**: Select this option to reset Counter 1 to zero. • **Increment Counter 1**: Select this option to increment Counter 1 by one. • **Decrement Counter 1**: Select this option to decrement Counter 1 by one. • **Reset Counter 2**: Select this option to reset Counter 2 to zero. • **Increment Counter 2**: Select this option to increment Counter 2 by one. • **Decrement Counter 2**: Select this option to decrement Counter 2 by one. • **Start Timer 1**: Select this option to start Timer 1. This option is displayed only for PCIe. • **Enable Timer 1**: Select this option to start Timer 1. This option is displayed only for FC. • **Reset Timer 1**: Select this option to reset Timer 1 to zero. • **Start Timer 2**: Select this option to start Timer 2. This option is displayed only for PCIe. • **Enable Timer 2**: Select this option to start Timer 2. This option is displayed only for FC. • **Reset Timer 2**: Select this option to reset Timer 2 to zero. • **Set Flag**: Select this option to set the Flag condition.

Understanding General Trigger Conditions

In the Trigger Setup window, the Conditions list box provides certain conditions that do not depend on the availability of a particular type protocol. Such trigger conditions are called as *general trigger conditions*. These conditions are available irrespective of the protocol you use. It is because of this reason, these conditions are given at the top of the Conditions list box (Figure 33).
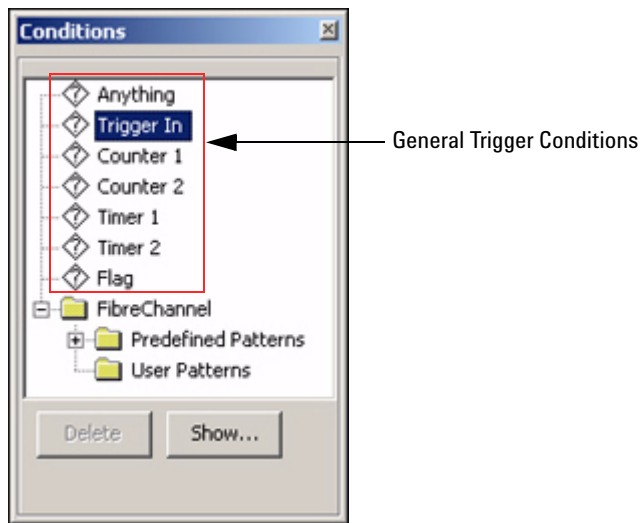
Figure 33   General Trigger Conditions

Protocol Analyzer provides the following general trigger conditions:

• **Anything**: The **Anything** condition is met when Protocol Analyzer encounters any type of packet in the trace. Use this condition when you want to trigger Protocol Analyzer on any type of packet it encounters in the trace.

• **Trigger In**: The **Trigger In** condition is met when it encounters the *Trigger pulse* send by a different device. For example, you want to trigger Protocol Analyzer only when it receives a Trigger pulse from an external device. In this situation, connect Protocol Analyzer with that external device using the *trigger cable*, and trigger Protocol Analyzer only when there is a Trigger pulse.

Use this condition in conjunction with the *External Trigger Out* action, which sends the Trigger pulse.

> **NOTE**   Using the Trigger In condition requires a physical connection between Protocol Analyzer and the device sending the Trigger pulse. For this connectivity, Agilent provides the trigger cable. Insert the one end of this cable in the *Synchronization Connector* (*Sync*) of the I/O module and the other end in the device sending the Trigger pulse.

- **Counter**: The *counter* condition is met when the counter value equals or exceeds the specified count limit.

  You can directly type this limit in the *Count Limit* text box, or you can use the *Input Assistance* dialog box. Both of these components are displayed adjacent to the Condition text box, but only when you drag and drop a counter condition in it.

  Protocol Analyzer provides two counter conditions: *Counter 1* and *Counter 2*. In both cases, counter starts only after their respective start action, Start Counter 1 or Start Counter 2, has occurred.

- **Timer**: The *timer* condition is met when the timer value equals or exceeds the time limit, specified in nanoseconds.

  You can directly type this limit in the *Time Limit* text box, or you can use the *Input Assistance* dialog box. Both of these components are displayed adjacent to the Condition text box, but only when you drag and drop a timer condition in it. The maximum value that you specify in the Time Limit cannot exceed the value equivalent to 16 seconds.

  Protocol Analyzer provides two timer conditions: *Timer 1* and *Timer 2*. In both cases, timer starts only after their respective start action, (Start Timer 1 and Start Timer 2) or (Enable Timer 1 and Enable Timer 2), has occurred.

> **NOTE**   Start Timer 1 and Start Timer 2 actions are displayed only for PCIe. On the other hand, Enable Timer 1 and Enable Timer 2 actions are displayed only for FC.

• **Flag**: The **Flag** condition is met when it encounters the response sent by the Set Flag action from a different device.

For example, there are two modules: 101/1 and 101/2. You want to trigger 101/2 only when 101/1 triggers. In this situation, set flag whenever 101/1 triggers, and trigger 101/2 only when the flag is set.

Editing Trigger Conditions

There may be a situation when you want to include a predefined pattern in the trigger criteria. However, you want to make some modification to it before including it in the trigger criteria. To do this, copy the desired predefined pattern in the User Patterns folder, and then use the Edit Condition dialog box (Figure 34) to make the desired modifications.

To access the Edit Condition dialog box:

1 Select the desired user pattern in the Conditions pane.

2 Click **Edit**.

The Edit Condition dialog box displays (Figure 34).
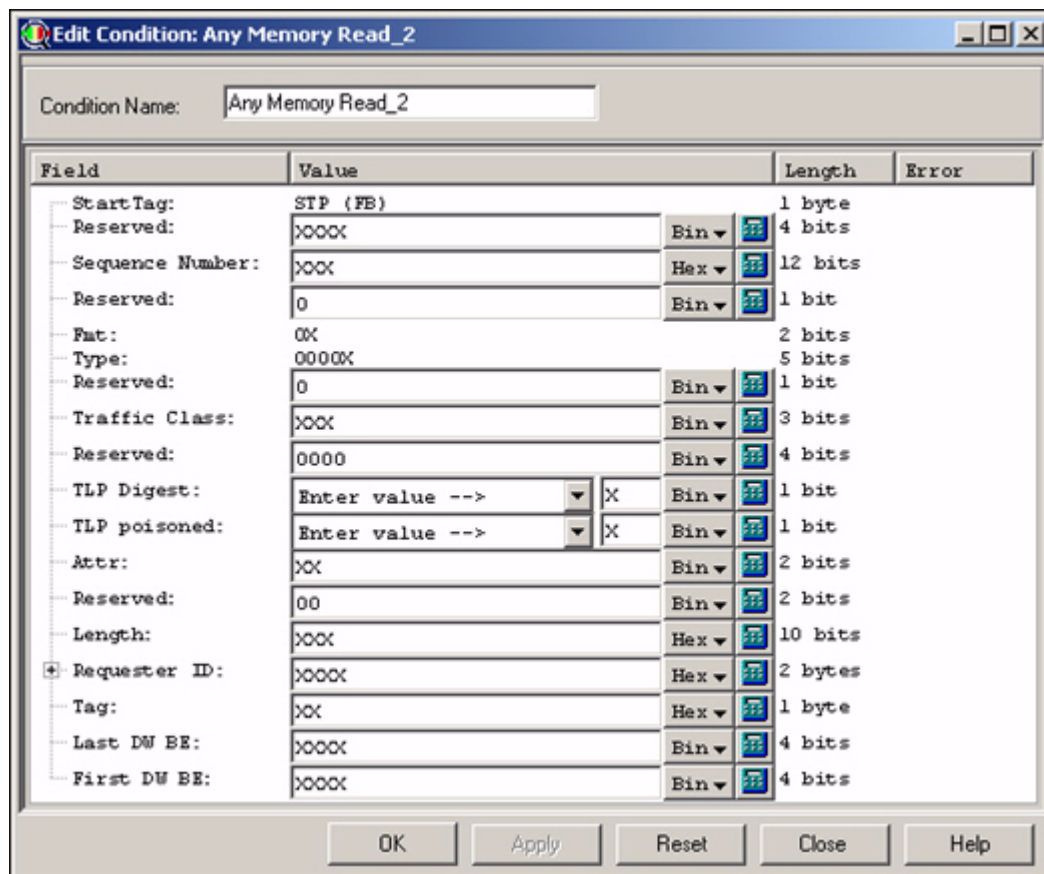
Figure 34   Edit Condition dialog box

Table 27 briefly describes the components of the Edit Condition dialog box.

Table 27   Components of the Edit Condition dialog box

Component	Description
Condition Name	The **Condition Name** text box displays the name of the user pattern to be edited.
Field	The **Field** column contains the names of the fields of a data packet. The number of fields displayed in this column may differ for different data packets.

Table 27 Components of the Edit Condition dialog box

Component	Description
Value	The **Value** column contains an input component for each data field. You can specify the desired inputs in these components to edit the selected data packet. This column also contains a drop-down list and a calculator for input assistance. The drop-down list enables you to specify your inputs in hexadecimal, binary, or decimal format. Clicking the calculator for input assistance displays the Input Assistant dialog box. Here, you can perform boolean operations over the hexadecimal, binary, and decimal values, and use the resulting value as the new value for the corresponding data packet field.
Length	The **Length** column displays the maximum length of a field in bits, bytes, or DWords.
OK	Click **OK** to close the Edit Condition dialog box and save the changes made to the user pattern.
Apply	Click **Apply** to assign the new settings to the user pattern.
Reset	Click **Reset** to ignore the changes made to the user pattern in the Edit Condition dialog box.
Close	Click **Close** to close the Edit Condition dialog box.
Help	Click **Help** to display the online help.

Important Points About Triggers

While creating a trigger, remember the following points:

- You can add maximum of eight states in a trigger.
- You can add any number of IF ELSE IF conditions.
- In case if you are using the Gen1 hardware, then:
  - You can add maximum of eight patterns in a trigger.
  - You can add maximum of one Training Sequence and Ordered Set pattern term.
- In case if you are using the Gen2 hardware, then:
  - You can add maximum of six patterns in a trigger. Out of this, you can add:
    - Maximum of two *Ordered Sets* or *Training Sequences.*
    - Maximum of four *TLPs*, *DLLPs*, or any other type of patterns.
  - You can add maximum of four *system triggers*, where using a system trigger reduces the number of remaining patterns by one.
- Using a Training Sequence and Ordered Set pattern term reduces the number of remaining patterns by one.
- Using *Flag* as a condition reduces the number of available pattern terms by one.
- You can add either *Counter 1* or *Timer 1* as a condition in a trigger.
- You can add either *Counter 2* or *Timer 2* as a condition in a trigger.
- You can add either *Counter 1* or *Timer 1* with *Trigger In* as a condition in a trigger.
- In case of a multiport trigger, if the trigger condition is met on one port, then that triggered port notifies the other port to trigger. This is true even when the trigger condition for both ports is different.
- In case you have applied different triggers to different ports, then selecting multiple ports at a time overwrites the trigger criteria of the selected ports by the trigger criteria of the port at the top of the hierarchy. For example, 101/1 and 102/1 have separate triggers. Now, selecting both ports simultaneously in the Port Selection drop-down list overwrites the trigger criteria of 102/1 by 101/1.

Trigger Examples

This section provides examples of creating triggers for different requirements.

In this section, you will learn:

- Creating a Simple Trigger
- Creating a Trigger on Protocol Error
- Creating a Trigger using the Counter Condition
- Creating a Trigger for x16

Creating a Simple Trigger

Consider that you want to create a trigger to capture all types of TLP memory read packets whose length is 4 DW. You also want that the trigger should:

- Store both upstream and downstream packets (by default).
- Capture 20% of pre-triggered trace and 80% of post-triggered trace.
- Not take any action when the trigger condition is not met.

Using the trigger condition requirement mentioned above, you will learn:

- To Edit a Trigger Condition
- To Create a Trigger

To Edit a Trigger Condition

1 Select **PCI Express > Predefined Patterns > TLP Patterns > Memory Read > Any Memory Read** in the Conditions pane.

2 Click **Copy**.

This copies the Any Memory Read option to the User Patterns folder with a new name, e.g. Any Memory Read_2.

3 Select **Any Memory Read_2** in the User Patterns folder.

4 Click **Edit**.

The Edit Condition dialog box for Any Memory Read_2 appears.

5 Type **004** in the text box for the **Length** field.

Figure 35 shows how you can do this in the Edit Condition dialog box.
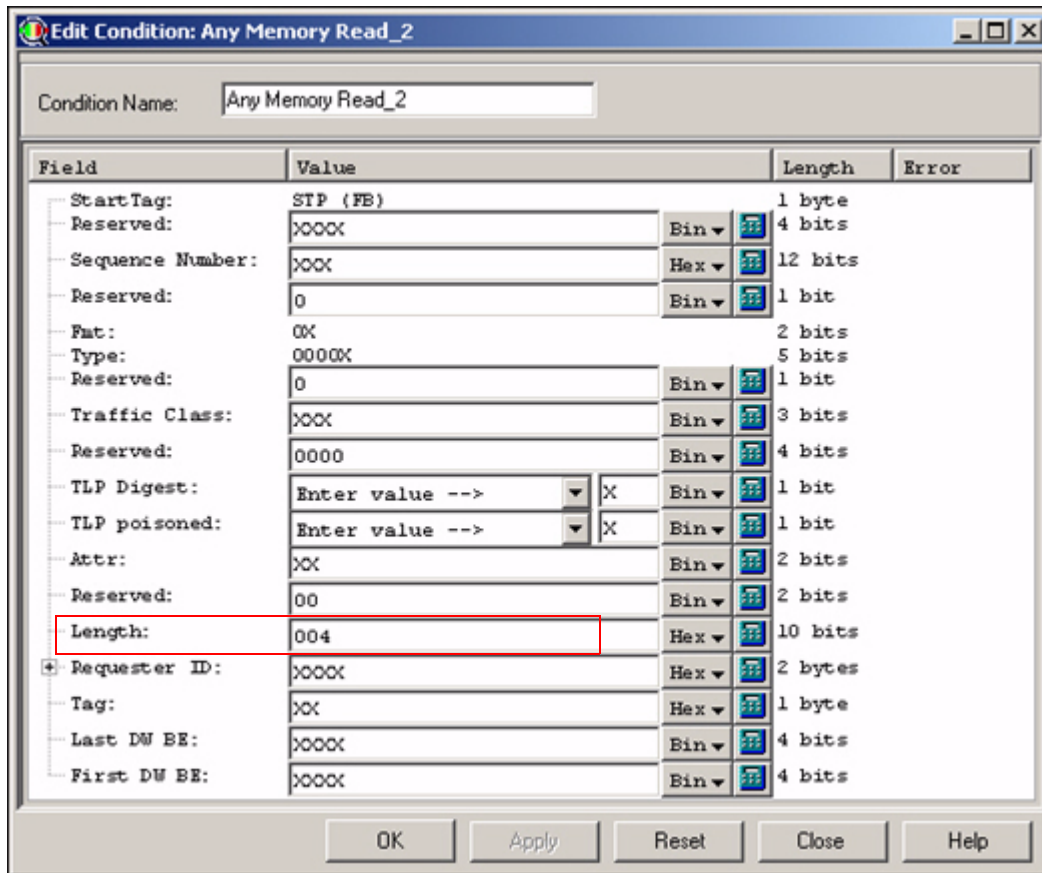
Figure 35   Edit Condition dialog box for Any Memory Read_2

6 Click **Apply**.

7 Click **OK**.

To Create a Trigger

1 Click **File > New** in the Trigger Setup window.

2 Select **Store Downstream, Store Upstream** from the Default Action drop-down list.

3 Move the Trigger Position scroll bar to the point, where its left and right sides are measured as 20% and 80%, respectively.

4 Expand the **User Patterns** folder in the Conditions list box.

5 Drag **Any Memory Read_2** from the Conditions list box and drop it in the Condition text box.

6 Select **Default Action** from the first Action drop-down list in the THEN sub-section.

7 Select **Trigger** from the second Action drop-down list in the THEN sub-section.

8 Select **No Action** from the Action drop-down list in the ELSE section.

9 Select **Show Conditions** and **Show Actions** check boxes in the Sequence Overview section.

This displays the trigger condition and the actions to be taken when the trigger condition is met, in the form of the IF ELSE programming construct.

10 Click **Apply**.

11 Click **OK**.

This completes your trigger creation activity. You can now run Protocol Analyzer to use this trigger. You can also choose to save this trigger in a trigger configuration file for later needs.

Creating a Trigger on Protocol Error

Consider that you want to create a trigger to capture a particular type of protocol error, such as *disparity error*. You also want that the trigger should:

- Store both upstream and downstream packets (by default).
- Store only the packets with disparity errors.
- Not take any action when the condition is not met.

The following procedure provides step-by-step instructions to create a trigger with above mentioned requirements.

To create a trigger on a protocol error - disparity error

1 Click **File > New** in the Trigger Setup window.

2 Select **Store Downstream, Store Upstream** from the Default Action drop-down list.

3 Expand the **PCI Express** folder in the Conditions list box.

4 Double-click **Protocol Error**.

The *Protocol Errors* dialog box appears (Figure 36). This dialog box lists all those protocol errors, which Protocol Analyzer supports for the underlying protocol.
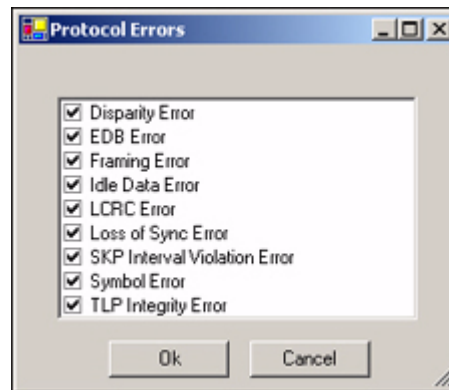
Figure 36   Protocol Errors dialog box

5 Clear all check boxes except the one for **Disparity Error**.

6 Drag **Protocol Error** from the Conditions list box and drop it in the Condition text box.

7 Select **Default Action** from the first Action drop-down list in the THEN sub-section.

8 Select **Trigger** from the second Action drop-down list in the THEN sub-section.

9 Select **No Action** from the Action drop-down list in the ELSE section.

10 Select **Show Conditions** and **Show Actions** check boxes in the Sequence Overview section.

This displays the trigger condition and the actions to be taken when the trigger condition is met, in the form of the IF ELSE programming construct.

11 Click **Apply**.

12 Click **OK**.

This completes your trigger creation activity. You can now run Protocol Analyzer to use this trigger.

NOTE	The list of protocol errors that appears in the Protocol Errors dialog box depends on the underlying protocol. For example, this dialog box displays only *Disparity Error* and *Symbol Error* if you are using the PCIe Gen2 hardware. Similarly, this dialog box displays a different set of protocol errors for FC.

Creating a Trigger using the Counter Condition

There may be a situation when you want to trigger Protocol Analyzer after encountering a particular type of packet, such as *Any Memory Read*, for a specified number of times, such as *10*. You also want that the trigger should:

- Store both upstream and downstream packets (by default).
- Reset the counter after the trigger condition is met.
- Not take any action when the condition is not met.

The following procedure provides step-by-step instructions to create a trigger with above mentioned requirements.

To create a trigger using a counter

1 Click **File > New** in the Trigger Setup window.

2 Select **Store Downstream, Store Upstream** from the Default Action drop-down list.

3 Reset the counter on encountering anything.

   To specify this, do the following:

   a Drag **Anything** from the Conditions list box and drop it in the Condition text box.

   b Select **Reset Counter 1** from the first Action drop-down list in the THEN sub-section.

   This ensures that counter's value is zero before it is used for further processing.

4 Add a new state, *State 2*.

   To a new state, do the following:

   a Click **Start > Add New State**. The Add State dialog box appears.

   b Type in **State 2** in the Enter State Name text box.

   c Click **OK**.

   This adds a new state, State 2.

5 Select **State 2** from the GOTO drop-down list in the first state (Start) section.

This ensures that the control moves to the State 2 section after resetting the counter.

Figure 37 displays the Start section.
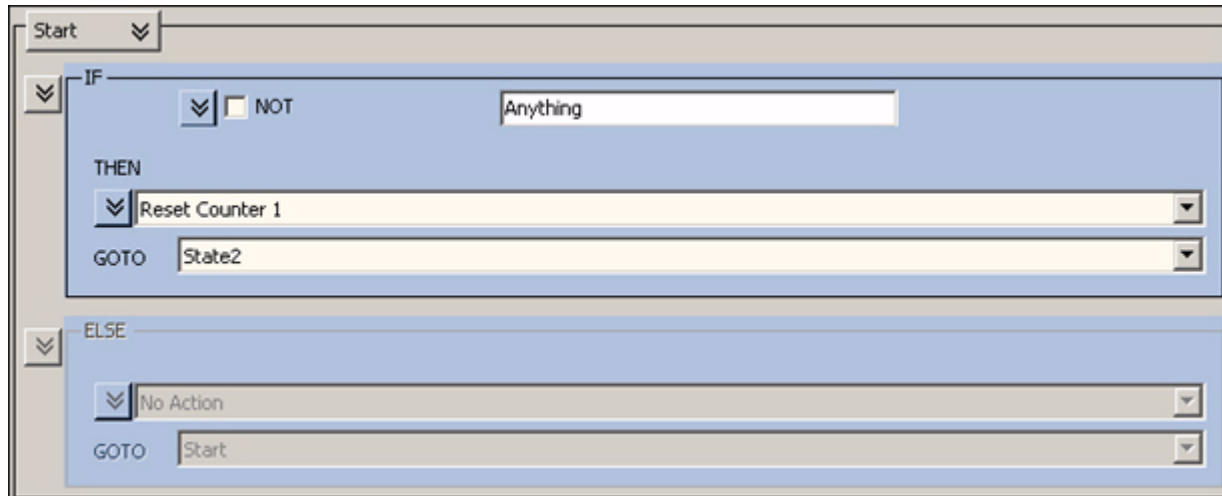
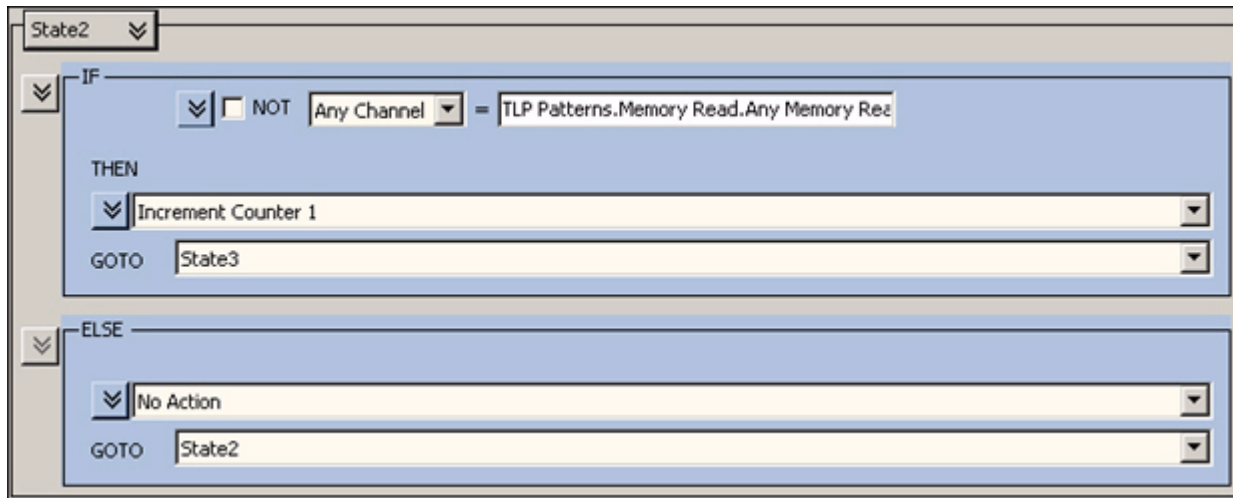**Figure 37**   Trigger using Counter - Start section

6 Specify to increment the counter every time there is a Any Memory Read packet.

To specify this, do the following:

a Expand the **PCI Express > TLP Patterns > Memory Read** folder in the Conditions list box.

b Drag **Any Memory Read** from the Conditions list box and drop it in the Condition text box of State 2.

c Select **Increment Counter 1** from the Action drop-down list in the THEN sub-section of State 2.

7 Add a new state, *State 3*.

To add a new state, follow the instructions given in Step 4.

8 Select **State 3** from the GOTO drop-down list of State 2.

This ensures that the control moves to the State 3 section after incrementing the counter.

Figure 38 displays the State 2 section.

Figure 38   Trigger using Counter - State 2 section

9 Verify the counter value and take appropriate action if the trigger condition is met.

To specify this, do the following:

a Drag **Counter 1** from the Conditions list box and drop it in the Condition text box of State 3.

b Type **10** in the corresponding Count Limit text box.

c Select **Default Action** from the Action drop-down list in the THEN sub-section of State 3.

d Select **Trigger** from the second Action drop-down list in the THEN sub-section of State 3.

e Select **Start** from the GOTO drop-down list of State 3.

10 Specify appropriate actions to handle the situation when the condition in all three states is not true.

To specify this, do the following:

a Select **No Action** from the Action drop-down list given in the ELSE section of State 2 and State 3.

b Select **State 2** from the GOTO drop-down list given in the ELSE section of the State 2 section.

c Select **State 2** from the GOTO drop-down list given in the ELSE section of the State 3 section.

Figure 39 displays the State 3 section.
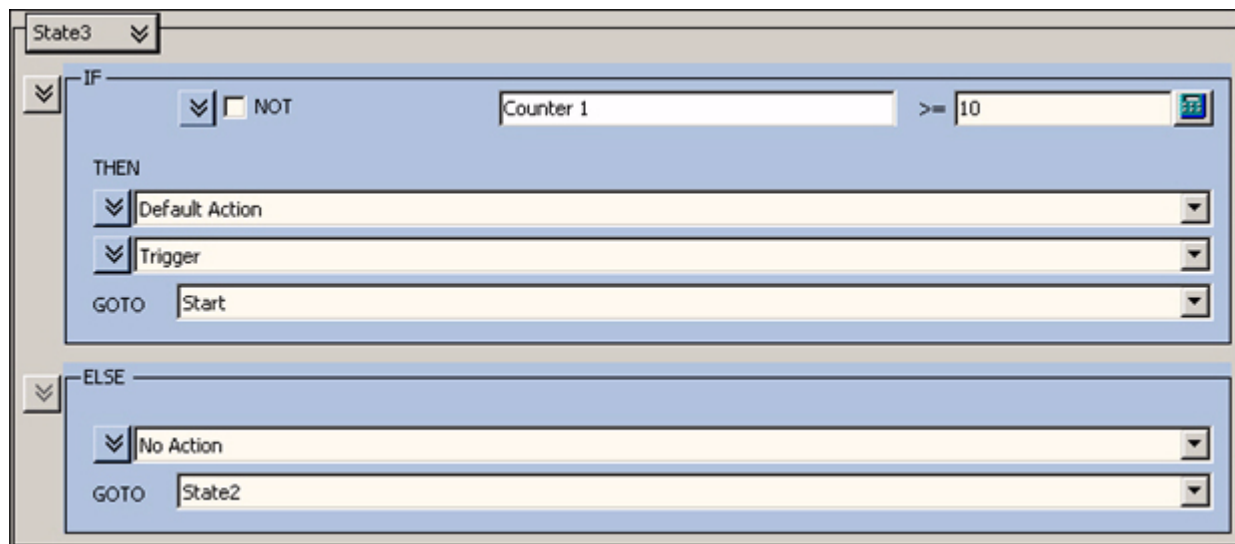
Figure 39   Trigger using Counter - State 3 section

11 Click **Apply**.

12 Click **OK**.

This completes your trigger creation activity. You can now run Protocol Analyzer to use this trigger.

Creating a Trigger for x16

Consider that you are using two ports, 101/1 and 102/1, on x16. Now, you want to specify separate trigger criteria for these ports. For port 101/1, you want to trigger Protocol Analyzer whenever there is a *DLLP NAK* packet. For port 102/1, you want to trigger Protocol Analyzer whenever there is a *Any Memory Read* packet. You also want that for both ports, the trigger should:

- Store packets as its default action.
- Not take any action when the condition is not met.

The following procedure provides step-by-step instructions to create a trigger with above mentioned requirements.

To meet the trigger condition requirement mentioned above, you need:

- To Specify a Trigger Criterion for Port 101/1
- To Specify a Trigger Criterion for Port 102/1

To Specify a Trigger Criterion for Port 101/1

1 Click **File > New** in the Trigger Setup window.

2 Clear the **102/1** check box in the Port Selection drop-down list.

   By default, all ports in the Port Selection drop-down list are selected. Clearing the check box for 102/1 ensures that the new trigger settings will apply to 101/1 only.

3 Select **Store** from the Default Action drop-down list.

4 Expand the **PCI Express > Predefined Patterns > DLLP Patterns** folder in the Conditions list box.

5 Drag **DLLP NAK** from the Conditions list box and drop it in the Condition text box.

6 Select **Default Action** from the first Action drop-down list in the THEN sub-section.

7 Select **Trigger** from the second Action drop-down list in the THEN sub-section.

8 Select **No Action** from the Action drop-down list in the ELSE section.

9   Click **Apply**.

This completes the trigger criterion for 101/1.

Now, follow the given below steps to specify the trigger criterion for 102/1.

To Specify a Trigger Criterion for Port 102/1

1   Clear the **101/1** check box in the Port Selection drop-down list.

2   Select the **102/1** check box in the Port Selection drop-down list.

This ensures that the new trigger settings will apply to 102/1 only.

3   Select **Store** from the Default Action drop-down list.

4   Expand the **PCI Express > Predefined Patterns > TLLP Patterns** folder in the Conditions list box.

5   Drag **Any Memory Read** from the Conditions list box, and drop it in the Condition text box.

6   Select **Default Action** from the first Action drop-down list in the THEN sub-section.

7   Select **Trigger** from the second Action drop-down list in the THEN sub-section.

8   Select **No Action** from the Action drop-down list in the ELSE section.

9   Click **Apply**.

This completes the trigger criterion for 102/1.

10 Click **OK**.

This completes your trigger creation activity. You can now run Protocol Analyzer to use this trigger.

Index

V

View menu, 26

Agilent Technologies