NET PROTOCOL SUITE USER MANUAL

Software Version 6.21

Generated: March 7, 2024; 09:19

Teledyne LeCroy Protocol Solutions Group

Trademarks and Servicemarks

Teledyne LeCroy, CATC Trace, SierraNet M1288, SierraNet M648, SierraNet T328, SierraNet M328Q, SierraNet M328, SierraNet M408, SierraNet M168, SierraFC M164, SierraFC M8-4 and Net Protocol Suite are trademarks of Teledyne LeCroy.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

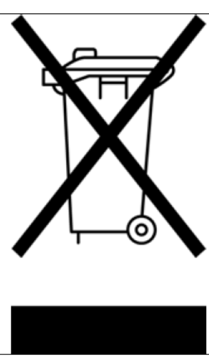
Intel and Pentium are registered trademarks of Intel Corporation.

All other trademarks and registered trademarks are property of their respective owners.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL INFORMATION, EXAMPLES AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE REPRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS ARE FULLY RESPONSIBLE FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN INFORMATION THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT Teledyne LeCroy FOR A COPY.

WEEE Program



This electronic product is subject to disposal and recycling regulations that vary by country and region. Many countries prohibit the disposal of waste electronic equipment in standard waste receptacles. For more information about proper disposal and recycling of your Teledyne LeCroy product, please visit teledynelecroy.com/recycle.

Teledyne LeCroy
teledynelecroy.com

Contents

Chapter 1

Introduction

This manual describes the installation and operation of the following Teledyne LeCroy devices:

- SierraNet M1288™ QSFP-DD 10/25/40/50/100/200/400/800G-L1/800* Gigabit Ethernet (*requires 2 SierraNet M1288 units and an M1288 Probe) and Gen7 Fibre Channel Analyzer platform (via the SFP112 connections)
- SierraNet M648™ SFP+ 10/25/40/50/100/200* Gigabit Ethernet (*via the QSPP-DD connections) and Gen6 Fibre Channel Analyzer platform
- SierraNet T328™ SFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer platform
- SierraNet M328Q™ QSFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer/Jammer platform
- SierraNet M328™ SFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer/Jammer platform
- SierraNet M408™ Fibre Channel and Ethernet Protocol Analyzer
- SierraNet M168™ Protocol Analyzer

1.1 Analyzer Deliverables

TABLE 1.1: Analyzer Deliverables

	Model						
Deliverable	**M1288**	**M648**	**T328**	**M328Q**	**M328**	**M408**	**M168**
Analyzer (with packing list)	✓	✓	✓	✓	✓	✓	✓
Quick Start Guide	✓	✓	✓	✓	✓	✓	✓
USB A-B 3.0 cable, 1 meter	N/A	✓	✓	✓	✓	✓	✓
USB A-B 2.0 cable, 1.8 meter	N/A	N/A	✓	N/A	✓	✓	✓
USB A-C 3.1 cable, 1m	✓	N/A	N/A	N/A	N/A	N/A	N/A
Ethernet cable, 10 feet	✓	✓	✓	✓	✓	✓	✓
2 QSFP-DD to QSFP-DD direct attach cables, 1 meter	✓	N/A	N/A	N/A	N/A	N/A	N/A
2 SFP+ to SFP+ direct attach cables, 1 meter	✓	ü	N/A	N/A	N/A	N/A	N/A
2 SFP to SFP direct attach cables, 0.5 meter	N/A	ü	N/A	N/A	N/A	N/A	N/A
Three-Prong AC power cable	✓	✓	✓	✓	✓	✓	✓
C13-C14 10A power cord, 2 meter	✓	✓	✓	✓	✓	✓	✓
DB9 (male) to DB9 (female) extension cable, 6 feet	✓	✓	✓	✓	✓	Available	Available
Rack Mount Installation Guide	Available	Available	Available	Available	Available	Available	Available

✓ = Included; N/A = Not Applicable

1.1.1 Unpacking the Analyzer

1. Inspect the received shipping container for any damage.
2. Unpack the container and account for each of the system components listed on the accompanying packing list.
3. Visually inspect each component for damage.

NOTE: In the event of damage, notify the shipper and Teledyne LeCroy. Retain all shipping materials for shipper's inspection.

1.2 Analyzer Features

TABLE 1.2: Analyzer Features

	Model						
Feature	**M1288**	**M648**	**T328**	**M328Q**	**M328**	**M408**	**M168**
QSFP-DD Port Pair (digitally retimed, 4 lanes only) (P1 and P2)	✓	N/A	N/A	N/A	N/A	N/A	N/A
QSFP-DD port pair (analyzer only) (P3 and P4)	✓	N/A	N/A	N/A	N/A	N/A	N/A
QSFP-DD Port Pair (P9 and P10)	N/A	✓	N/A	N/A	N/A	N/A	N/A
QSFP Port Pair (P9 and P10)	N/A	N/A	N/A	N/A	N/A	✓	N/A
QSFP Port Pair (A and B)	N/A	N/A	N/A	✓	N/A	N/A	N/A
SFP Port Pair 1 (P1 and P2)	N/A	✓	✓	N/A	✓	✓	✓
SFP Port Pair 2 (P3 and P4)	N/A	✓	✓	N/A	✓	✓	✓
SFP Port Pair 3 (P5 and P6)	N/A	✓	✓	N/A	✓	✓	✓
SFP Port Pair 4 (P7 and P8)	N/A	✓	✓	N/A	✓	✓	✓
SFP112 Port Pair 1 (P5 and P6)	✓	N/A	N/A	N/A	N/A	N/A	N/A
SFP112 Port Pair 2 (P7 and P8)	✓	N/A	N/A	N/A	N/A	N/A	N/A
Status and Configuration LCD Display	✓	✓	✓	✓	✓	✓	✓
Front Panel Configuration Buttons	✓	✓	✓	✓	✓	✓	✓
External Trigger (Input and Output)	✓	✓	✓	✓	✓	✓	✓
External Clock In (1588) through Ext Trigger In SMA	✓	N/A	N/A	N/A	N/A	N/A	N/A
Power Switch	✓	✓	✓	✓	✓	✓	✓
USB-C Port for Host Connectivity	✓	N/A	N/A	N/A	N/A	N/A	N/A
USB 3.0 Port for Host Connectivity	N/A	✓	✓	✓	✓	✓	✓

TABLE 1.2: Analyzer Features

	Model						
Feature	**M1288**	**M648**	**T328**	**M328Q**	**M328**	**M408**	**M168**
USB 2.0 Port for Host Connectivity	N/A	✓	✓	✓	✓	✓	✓
Rack Mountable	Available	Available	Available	Available	Available	Available	Available

✓ = Included; N/A = Not Applicable

1.3 SierraNet M1288 Analyzer

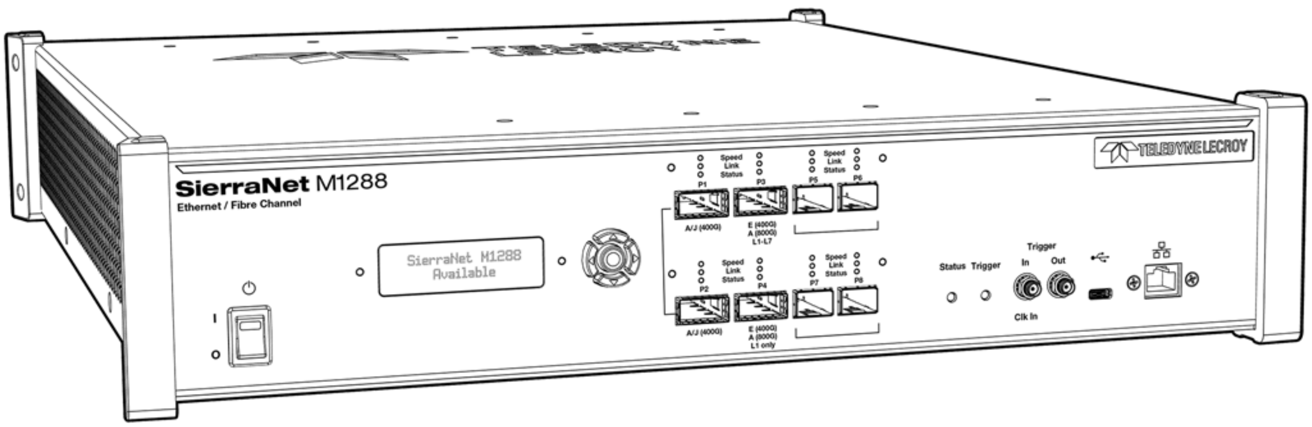


Figure 1.1: SierraNet M1288

The SierraNet M1288 analyzer is Teledyne LeCroy's QSFP-DD 10/25/40/50/100/200/400/800G-L1/800* Gigabit Ethernet (*requires 2 SierraNet M1288 units) and Gen7 Fibre Channel Analyzer platform (via the SFP112 connections). It has:

- two (2) Digitally Retimed QSFP-DD ports (P1, P2),
- two (2) Analysis-only ports (P3, P4, require the M1288 Probe, sold separately), and
- four (4) SFP112 ports.

Up to 256 GB of capture memory allows for capturing of extensive line-speed data. The SierraNet M1288 Probe employs Teledyne LeCroy's T.A.P.6 non-intrusive probing technology, which enables complete protocol capture, fast signal locking, and very little loss and jitter. The analyzer can be controlled either by using a one (1) Gigabit Ethernet connection to the local network, or a USB connection. The SierraNet M1288 provides the user with easy-to-understand control panel and LED indicators.

Major features of the M1288 include:

- triggering on back-to-back events,
- use of counters within trigger conditions, and

- ❑ multi-state (up to 24) triggering and filtering state machines with four transitions per state.

The Net Protocol Suite software for controlling the analyzer and displaying the captured data installs on the latest Microsoft® Windows® version.

See the ReadMe file for the latest information on host machine requirements.

1.3.1 M1288 Analyzer Front

The M1288 Analyzer has the following front features:

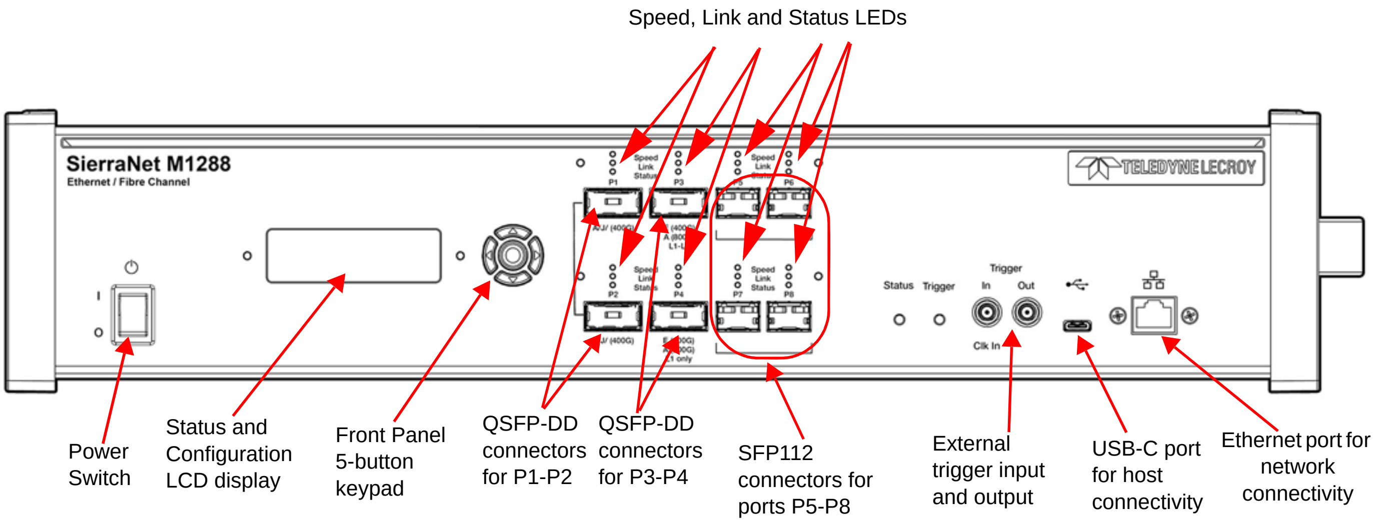


Figure 1.2: SierraNet M1288 Front Panel Features

1.3.1.1 M1288 LEDs

LED Indicators for ports P1- P2, P3-P4, P5-P6, P7-P8 for Speed, Link and Status:

TABLE 1.3: M1288 Front Panel LEDs

Speed LEDs		
	Ethernet	Fibre Channel
Yellow	🟡 Legacy GbE NRZ	🟡 Legacy FC NRZ
Green	🟢 50GbE/lane PAM4	🟢 64G FC PAM4
Blue	🔵 100GbE/lane PAM4	🔵 128G FC PAM4
Link Activity LEDs		
Green	🟢 Network activity Detected	
Yellow	🟡 Link up, no activity	
No Color	⚪ No link	
Status LEDs		
Yellow Blinking	🟡 Waiting for trigger	

TABLE 1.3: M1288 Front Panel LEDs

Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

1.3.2 M1288 Analyzer Back

On the back, the M1288 Analyzer has Power In and Sync Expansion Connectors.

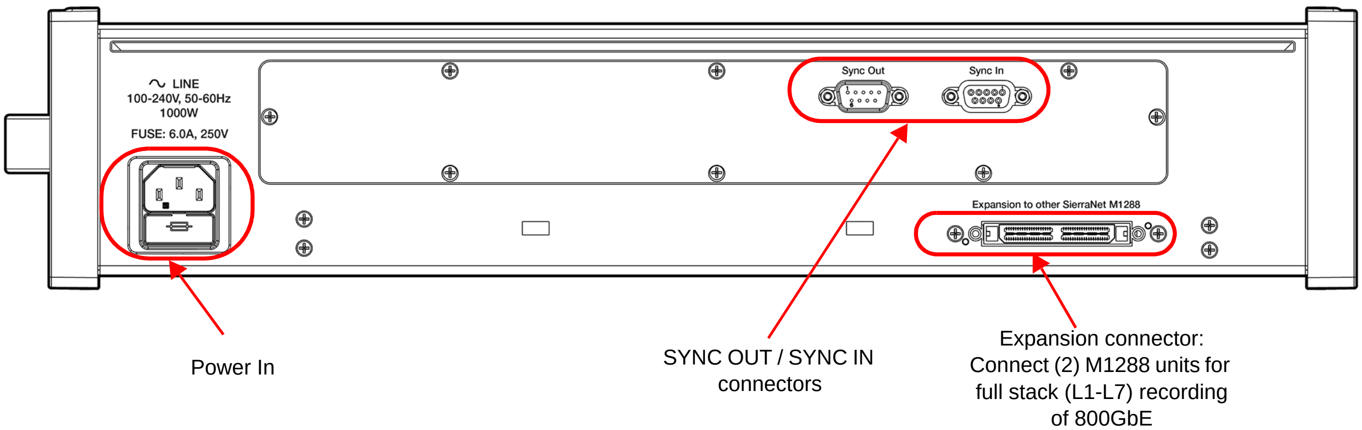


Figure 1.3: SierraNet M1288 Back Panel Features

1.4 M1288 Probe

The SierraNet M1288 Probe employs Teledyne LeCroy's T.A.P.6 non-intrusive probing technology, which enables complete protocol capture, fast signal locking, and very little loss and jitter. The M1288 Probe is used only with the M1288 Analyzer to capture data up to 800MB.

The M1288 Probe has two models available:

TABLE 1.4: M1288 Probe Models

Model	Description
HSF-M1288-QSFP	SNET M1288 QSFP-DD Probe
HSF-M1288-OSFP	SNET M1288 OSFP Probe

The OSFP connectors on the OSFP probe cables can be swapped in the field, by the customer, between a 'Fin' configuration and a 'Flat' configuration. .

NOTE: To learn more about toggling the cables of the SNET M1288 Probe, please refer to the guide "OSFP 800G Cable Shell Replacement.pdf", which can be found under the Documents folder once you install Net Protocol Suite software.

1.4.1 M1288 Probe Front Panel

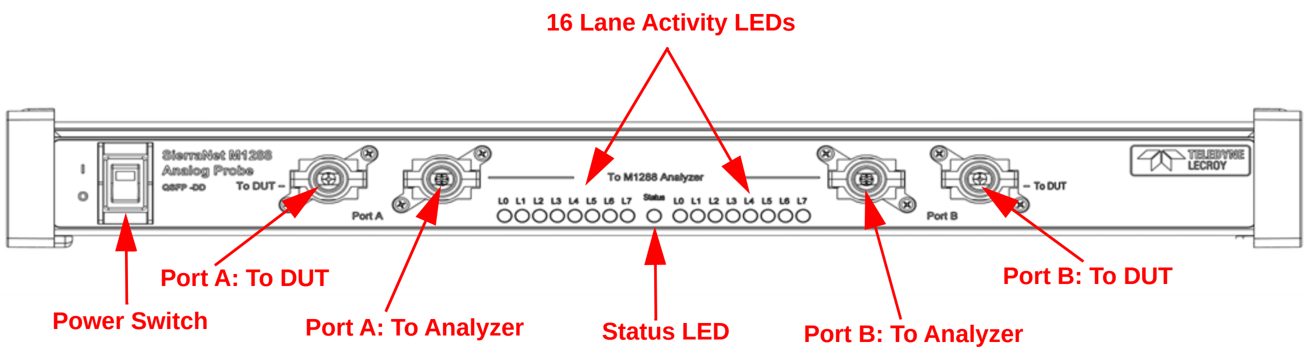


Figure 1.4: M1288 Probe Front Panel

The M1288 Probe has 4 connection cables:

- To DUT: The outer-most probe connection cables are labeled 'To-DUT'. These need to be connected to the Devices Under Test (DUT).
- To M1288 Analyzer: The inner-most probe connection cables are labeled as 'To M1288 Analyzer'. These need to be connected to ports P3 and P4 of the SierraNet M1288 Analyzer.

NOTE: The 'captive' Probe cables (the inner most cables) are the only cables that need to be connected to the SierraNet M1288 Analyzer. The analyzer uses sideband signals in the cables to control the Probe.

Additionally, the left pair of Probe connections is labeled as 'A', and the right pair of connections is labeled as 'B':

- DUT traffic on the 'A' side will be recorded by the Analyzer port connected to the 'A' side, and
- DUT traffic on the 'B' side will be recorded by the Analyzer port connected on the 'B' side.

See “M1288 Connections” on page 31 and Figures 2.5 and 2.6.

1.4.1.1 M1288 Probe LEDs

The M1288 has the following LEDs:

- Status: The middle LED displays the connectivity status between the probe and the M1288 analyzer:
  - Red - No(0) Analyzer cables connected to the M1288 Analyzer ports (P3/P4)
  - Blue - One(1) Analyzer cable is connected to one of the M1288 Analyzer ports (P3/P4)
  - Blinking Green - Both Analyzer cables are successfully connected to both M1288 Analyzer ports (P3/P4)
- Lane Activity: 16 Lane LEDs denote activity on the respective lane.

1.4.2 M1288 Probe Back Panel

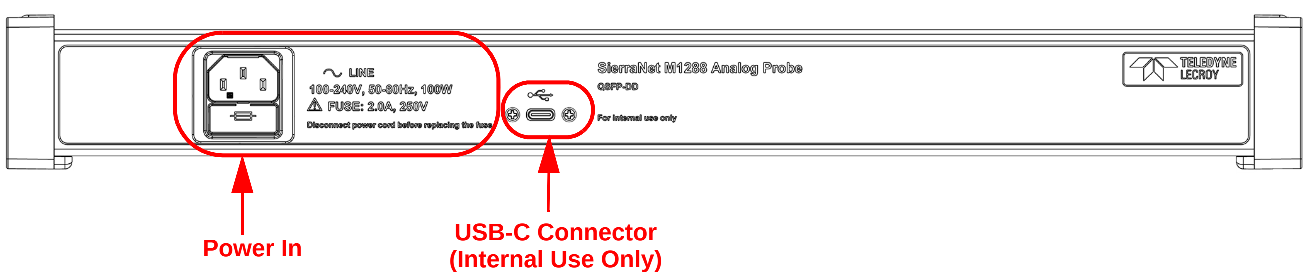


Figure 1.5: M1288 Probe Back Panel

On the back, the M1288 Probe has Power In and a single USB-C connector. .

NOTE: The USB-C connector is labeled 'For Internal use only' and customers should not use this connector.

1.5 SierraNet M648 Analyzer

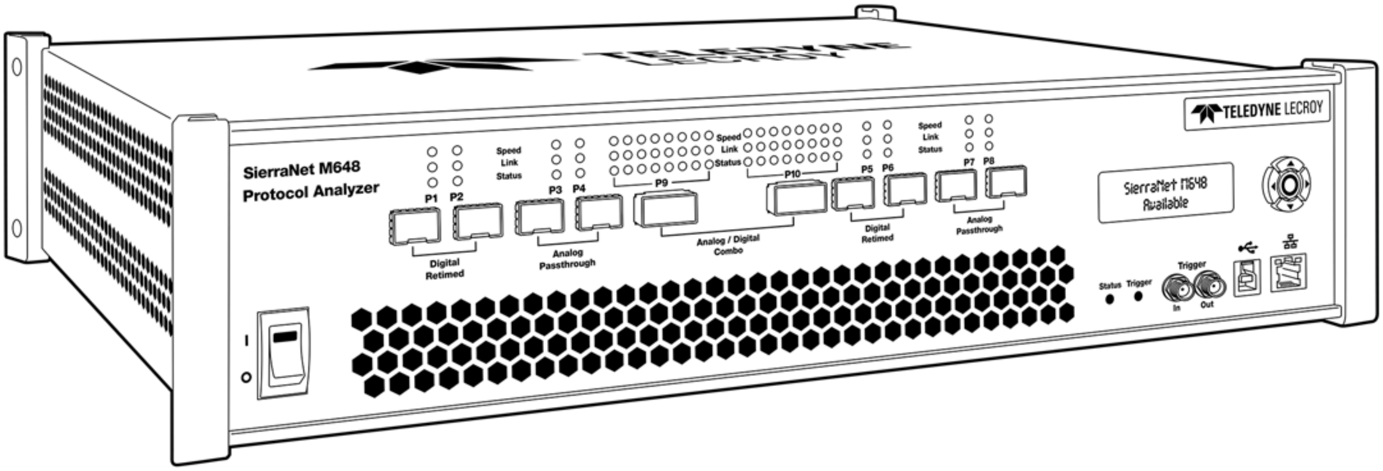


Figure 1.6: Teledyne LeCroy SierraNet M648 Protocol Analyzer

The SierraNet M648 analyzer is Teledyne LeCroy's SFP+ 10/25/40/50/100/200* Gigabit Ethernet (*via the QSFP-DD connections) and Gen6 Fibre Channel Analyzer platform. It has four (4) Analog Pass Through SFP-56 ports; four (4) Digitally Retimed SFP-56 ports and two (2) Analog Pass Through/Digitally Retimed QSFPDD-56 ports. Up to 64 GB of capture memory allows for capturing of extensive line-speed data. The SierraNet M648 employs Teledyne LeCroy's T.A.P.4 non-intrusive probing technology, which enables complete protocol capture, fast signal locking, and very little loss and jitter. The analyzer can be controlled either by using a one (1) Gigabit Ethernet connection to the local network, or a USB connection.

The SierraNet M648 provides the user with easy-to-understand control panel and LED indicators. Major features of the M648 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state and FlexPort, which allows concurrent Ethernet and FC analysis. The Net Protocol Suite software for controlling the analyzer and displaying the captured data installs on the latest Microsoft® Windows® version. See the *ReadMe* file for the latest information on host-machine requirements.

1.5.1 M648 Analyzer Front Panel

The M648 Analyzer has the following front panel features:

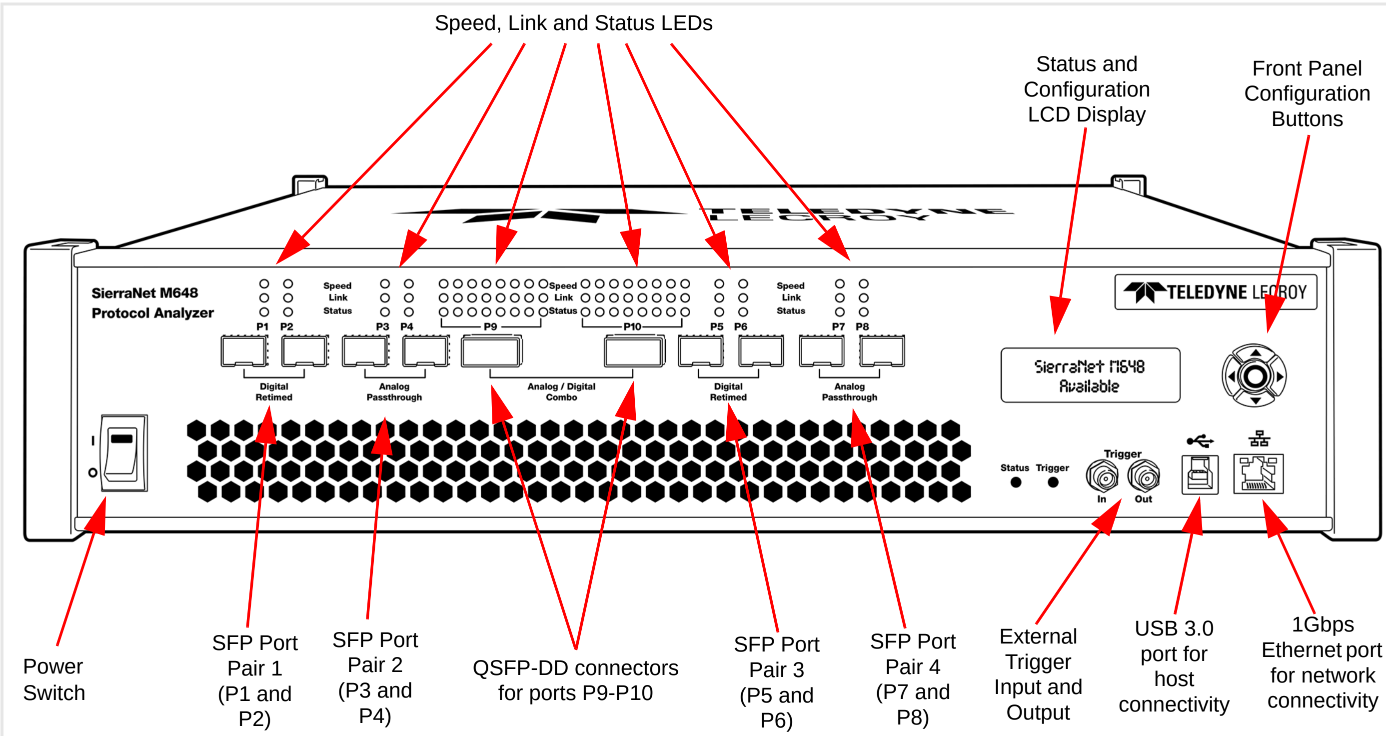


Figure 1.7: M648 Front Panel

1.5.1.1 M648 LEDs

LED indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6, P7 - P8 and P9 - P10) with the following functionality (see Figure 1.8, Table 1.5 and Table 1.6).

Speed LEDs (Mode Dependent)

	Ethernet	**Fibre Channel**
Yellow	Auto-Negotiation	16G FC
Green	10/40 GigE	32G FC
Blue	25/50/100 GigE	64G FC

Link Activity LEDs

Green	Network Activity Detected
Yellow	Link up, no activity
No Color	No link

Status LEDs

Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

1.5.1.2 M648 LED Port Configuration Verses Speed

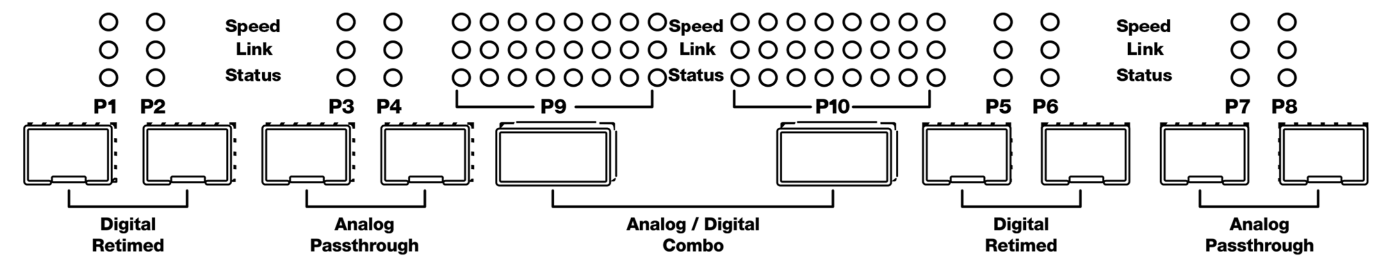


Figure 1.8: LEDs on the M648 Front Panel

TABLE 1.5: Port Configuration P1-P8 Speeds

Connector Type	Port Configuration	P1-P8 Speeds		
SFP	10/25G-NRZ	25G	10G	Auto-Negotiation
	50G-PAM4	50G		Auto-Negotiation
	32G-NRZ	32G	16G	
	64G-PAM4	64G	32G	16G

TABLE 1.6: Port Configuration P9-P10 Speeds

Connector Type	Port Configuration	P9 – P10 Speeds (Lanes 1 – 4)											
		L1			L2			L3			L4		
DD-QSFP	10/25G-NRZ	25G	10G	AN*									
	50G-NRZ	50G		AN*									
	100/40G-NRZ	100G	40G	AN*	100G	40G	AN*	100G	40G	AN*	100G	40G	AN*
	50G-PAM4	50G		AN*									
	100G-PAM4	100G		AN*	100G		AN*						
	200G-PAM4	200G		AN*	200G		AN*	200G		AN*	200G		AN*
	400G-L1	50G-LT*		AN*	50G-LT*		AN*	50G-LT*		AN*	50G-LT*		AN*
		P9 – P10 Speeds (Lanes 5 – 8)											
		L5			L6			L7			L8		
DD-QSFP	400G-L1	50G-LT*		AN*	50G-LT*		AN*	50G-LT*		AN*	50G-LT*		AN*

AN* = Auto-Negotiation; LT* = Link Training

1.5.2 M648 Analyzer Back Panel

On the back, the M648 Analyzer has Power In and Sync Expansion Connectors.

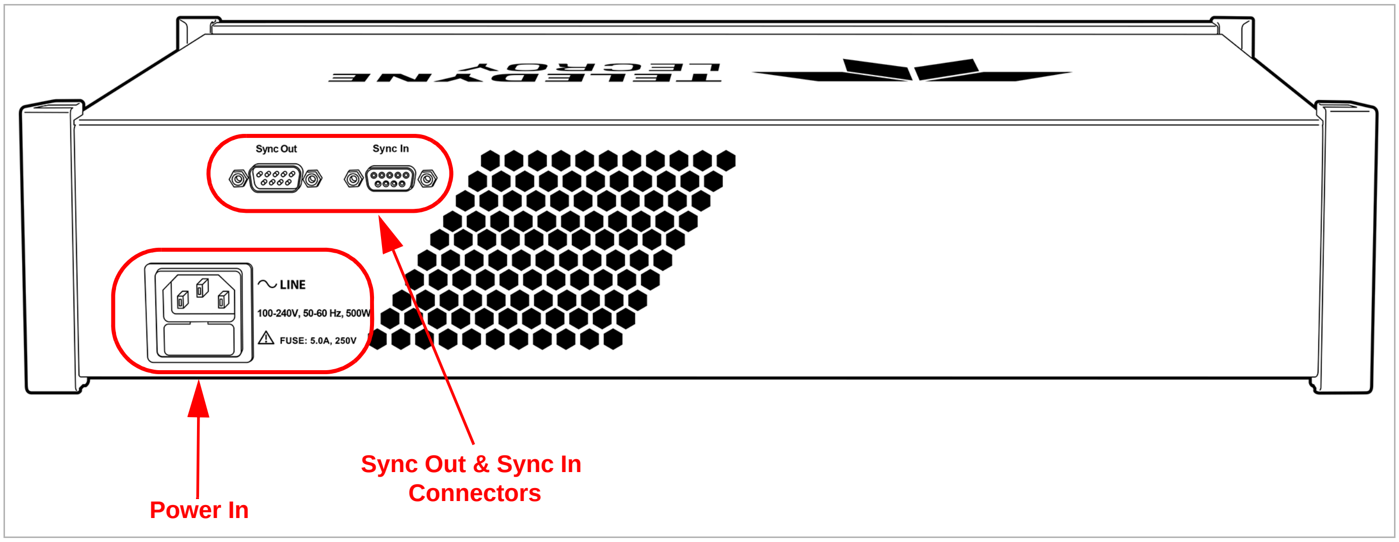


Figure 1.9: M648 Rear Panel

1.6 SierraNet T328 Analyzer

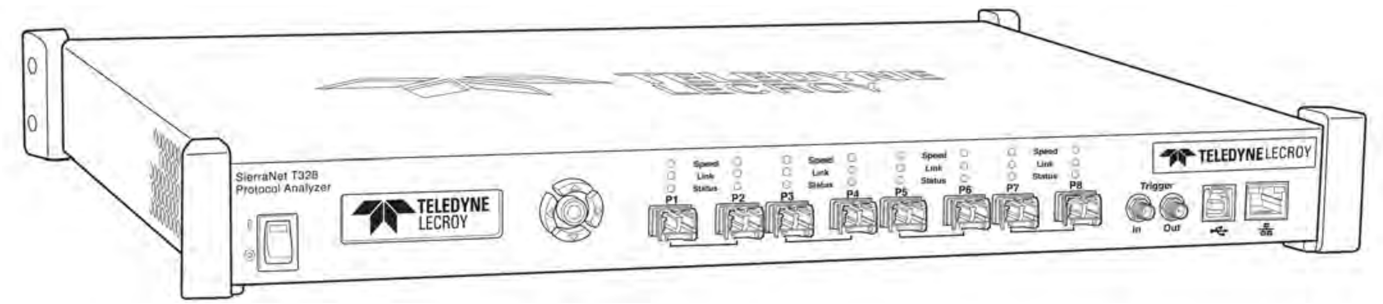


Figure 1.10: Teledyne LeCroy SierraNet T328 Protocol Analyzer

The SierraNet T328 analyzer is Teledyne LeCroy's SFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer platform. It has eight SFP+ ports. Up to 128 GB of capture memory allows for capturing extensive line-speed data. The SierraNet T328 employs Teledyne LeCroy's T.A.P.3 non-intrusive probing technology, which enables complete protocol capture, fast signal locking, and very little loss and jitter. The analyzer can be controlled with either a one (1) Gigabit Ethernet connection to the local network, or a USB connection.

The SierraNet T328 provides the user with easy-to-understand control panel and LED indicators. Major features of the T328 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state and FlexPort, which allows concurrent Ethernet and FC analysis. The Net Protocol Suite software for controlling the analyzer and displaying the captured data installs on the latest Microsoft® Windows® version. See the *ReadMe* file for the latest information on host-machine requirements.

1.6.1 T328 Analyzer Front Panel

The T328 Analyzer has the following front panel features:

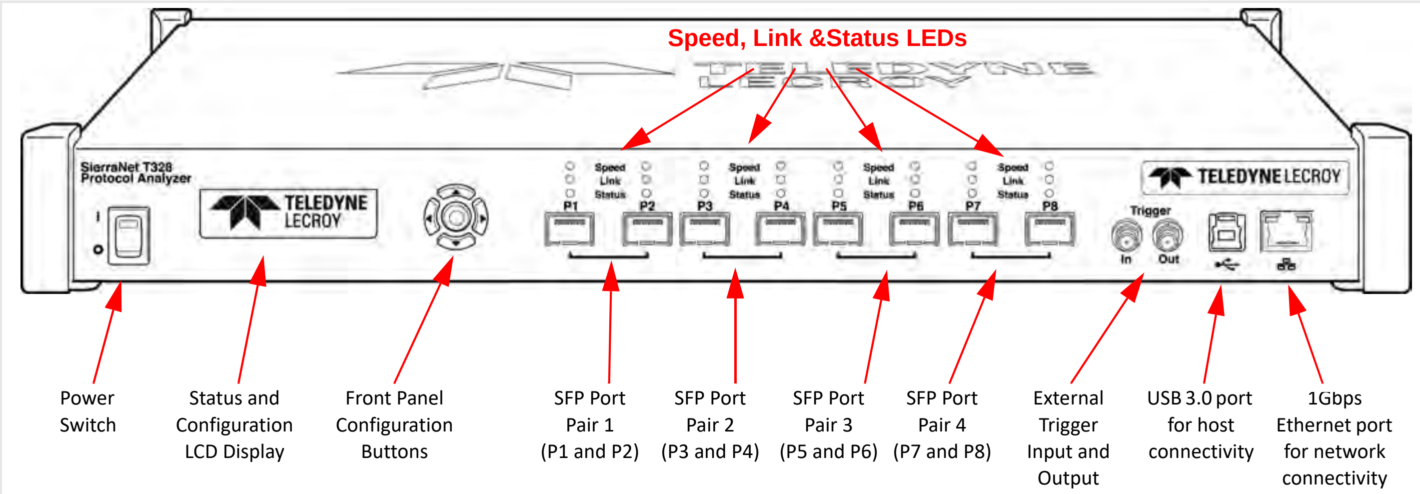


Figure 1.11: T328 Front Panel

1.6.1.1 T328 LEDs

LEDs indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6 and P7 - P8) with the following functionality (see Figure 1.12).

Speed LEDs

	Ethernet	Fibre Channel
Yellow	Reserved	8G FC
Green	10/40 GigE	16G FC
Blue	25/50/100 GigE	32G FC

Link Activity LEDs

Green	Network activity Detected
Yellow	Link up, no activity
No Color	No link

Status LEDs

Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

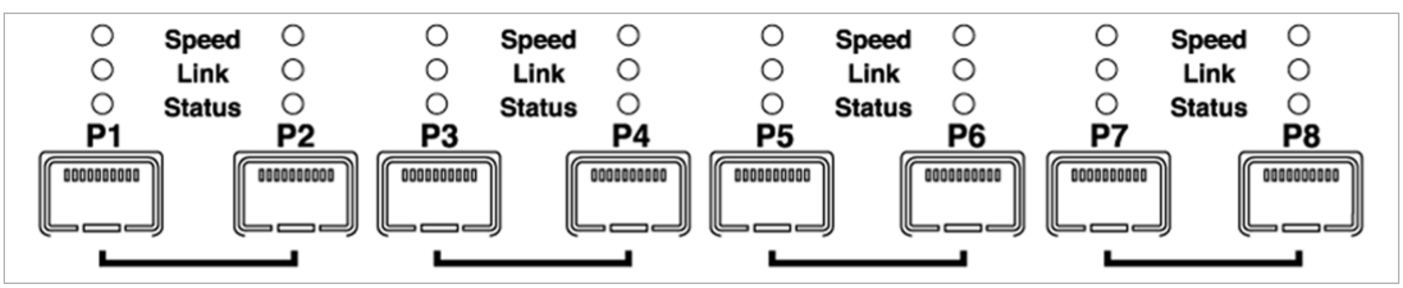


Figure 1.12: LEDs on the T328 Front Panel

1.6.2 T328 Analyzer Rear Panel

On the back, the T328 Analyzer has Power In and Sync Expansion Connectors.

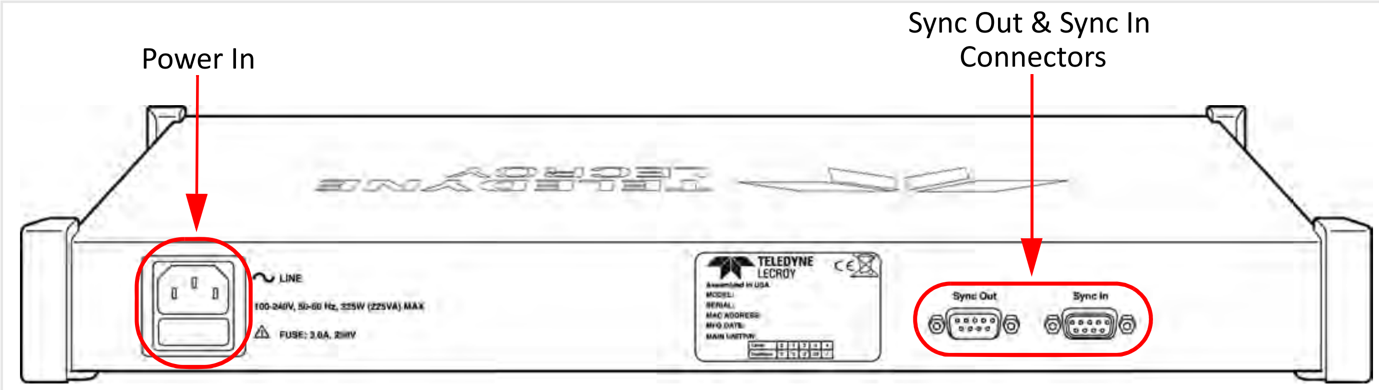


Figure 1.13: T328 Rear Panel

1.7 SierraNet M328Q Analyzer/Jammer

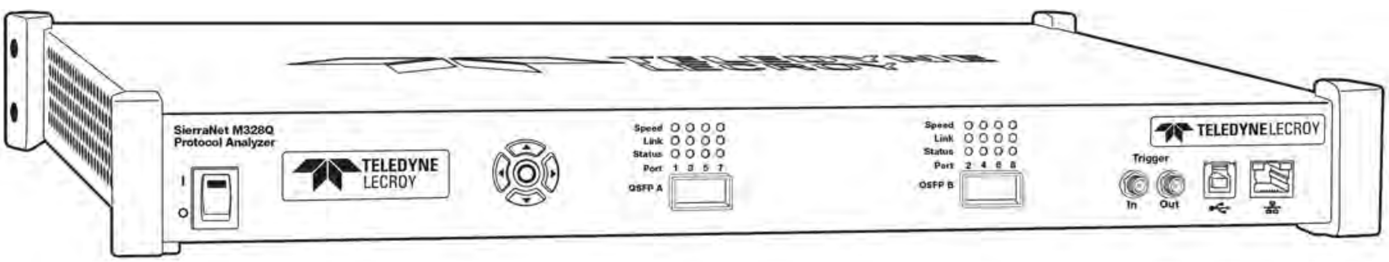


Figure 1.14: Teledyne LeCroy SierraNet M328Q Protocol Analyzer/Jammer

The SierraNet M328Q analyzer is Teledyne LeCroy's QSFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer/Jammer platform. It has two QSFP28 ports. Up to 128 GB of capture memory allows for capturing of extensive line-speed data. The analyzer can be controlled with either a one (1) Gigabit Ethernet connection to the local network, or a USB connection.

The SierraNet M328Q provides the user with easy-to-understand control panel and LED indicators. Major features of the M328Q include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state and FlexPort, which allows concurrent Ethernet and FC analysis.

The Net Protocol Suite™ software for controlling the analyzer and displaying the captured data installs on the latest Microsoft® Windows® version. See the *ReadMe* file for the latest information on host-machine requirements.

1.7.1 M328Q Analyzer Front Panel

The M328Q Analyzer/Jammer has the following front panel features:

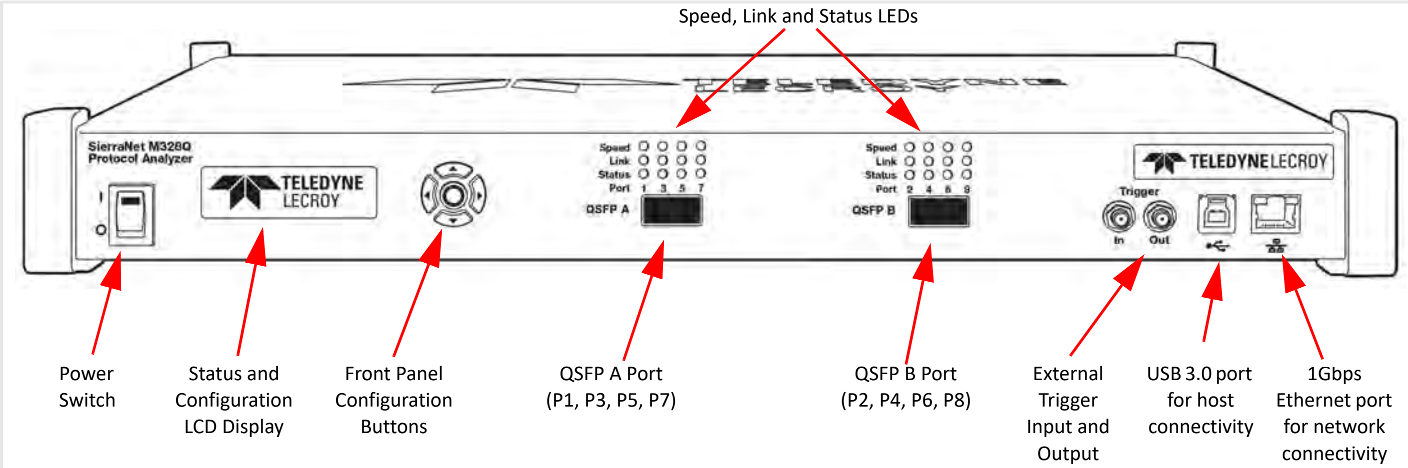


Figure 1.15: M328Q Front Panel

1.7.1.1 M328Q LEDs

LEDs indicators support each port link pair (A - B) with the following functionality (see Figure 1.16).

Speed LEDs

	Ethernet	Fibre Channel
Yellow	Reserved	8G FC
Green	10/40 GigE	16G FC
Blue	25/50/100 GigE	32G FC

Link Activity LEDs

Green	Network activity Detected
Yellow	Link up, no activity
No Color	No link

Status LEDs

Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

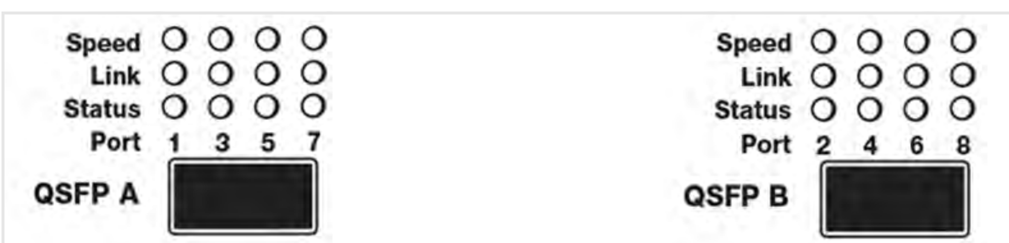


Figure 1.16: LEDs on the M328Q Front Panel

1.7.2 M328Q Analyzer Rear Panel

On the back, the M328Q Analyzer has Power In and Sync Expansion Connectors (Figure 1.8).

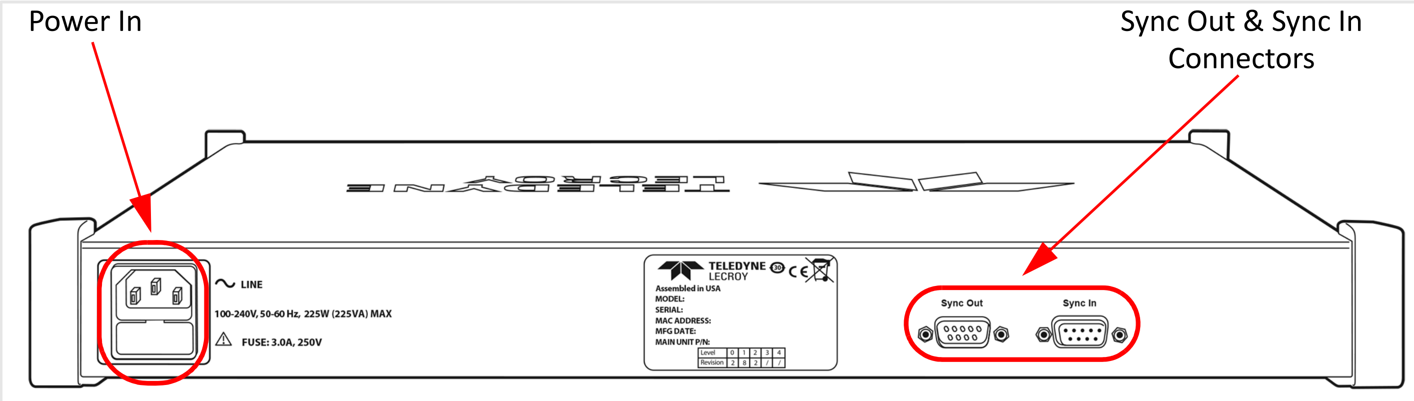


Figure 1.17: M328Q Analyzer Rear Panel

1.8 SierraNet M328 Analyzer/Jammer

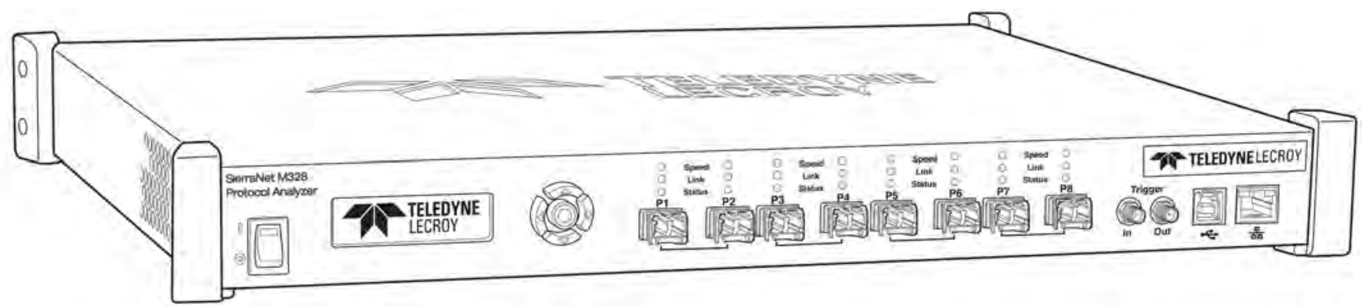


Figure 1.18: Teledyne LeCroy SierraNet M328 Protocol Analyzer/Jammer

The SierraNet M328 analyzer is Teledyne LeCroy's SFP+ 10/25/40/50/100 Gigabit Ethernet and Gen6 Fibre Channel Analyzer/Jammer platform. It has eight SFP+ ports. Up to 128 GB of capture memory allows for capturing of extensive line-speed data. The analyzer can be controlled with either a one (1) Gigabit Ethernet connection to the local network, or via a USB connection.

The SierraNet M328 provides the user with easy-to-understand control panel and LED indicators. Major features of the M328 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state and FlexPort, which allows concurrent Ethernet and FC analysis.

The Net Protocol Suite™ software for controlling the analyzer and displaying the captured data installs on the latest Microsoft® Windows® version. See the *ReadMe* file for the latest information on host-machine requirements.

1.8.1 M328 Analyzer Front Panel

The M328 Analyzer/Jammer has the following front panel features in Figure 1.19:

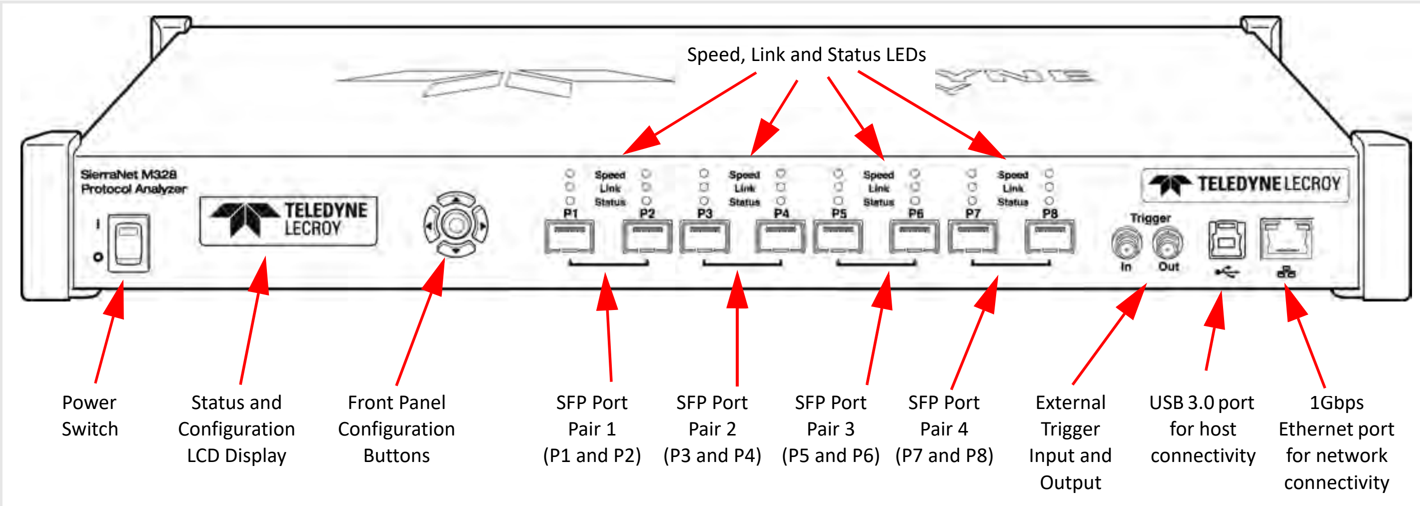


Figure 1.19: M328 Front Panel

1.8.1.1 M328 Analyzer LEDs

LEDs indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6 and P7 - P8) with the following functionality (see Figure 1.20).

Speed LEDs

	Ethernet	**Fibre Channel**
Yellow	Reserved	8G FC
Green	10/40 GigE	16G FC
Blue	25/50/100 GigE	32G FC

Link Activity LEDs

Green	Network activity Detected
Yellow	Link up, no activity
No Color	No link

Status LEDs

Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

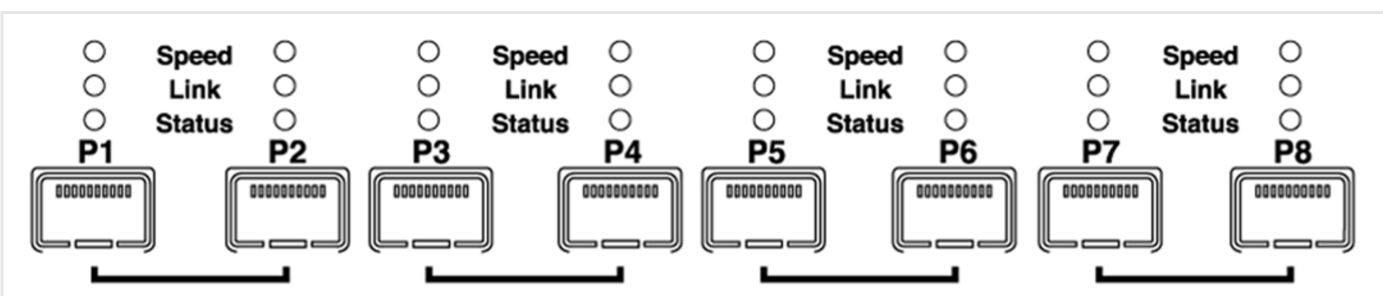


Figure 1.20: LEDs on the M328 Front Panel

1.8.2 M328 Analyzer Rear Panel

On the back, the M328 Analyzer has Power In and Sync Expansion Connectors.

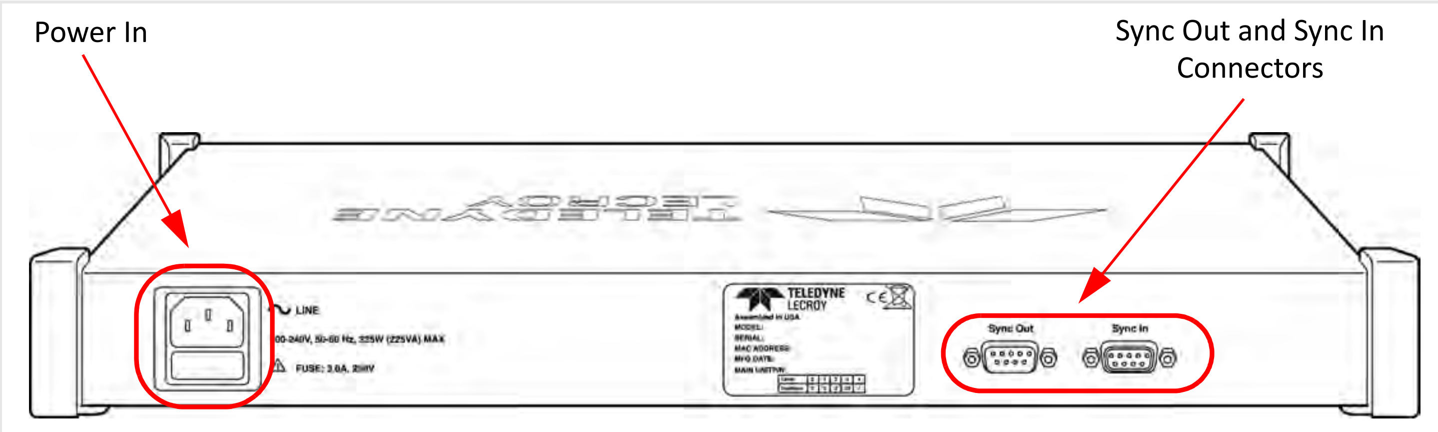


Figure 1.21: M328 Rear Panel

1.9 SierraNet M408 Analyzer

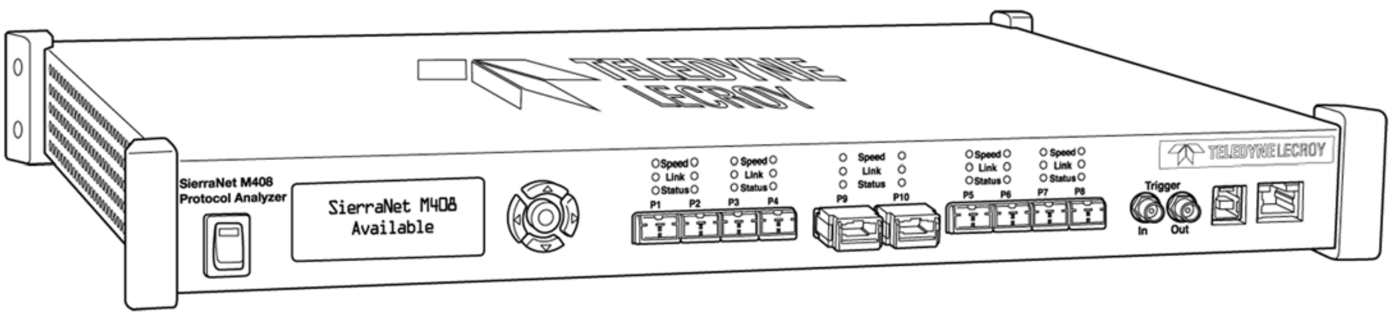


Figure 1.22: Teledyne LeCroy SierraNet M408 Protocol Analyzer

The SierraNet M408 analyzer is Teledyne LeCroy's 10 Gigabit Ethernet, 40 Gigabit Ethernet and 16 Gigabit Fibre Channel Analyzer and Jammer platform. The M408 has eight SFP+ 10GigE/16G FC and two QSFP 40GigE ports. The M408 is very portable and can also be rack mounted (1U form-factor). Up to 64 GB of capture memory allow extensive line-speed capturing.

Major features of the M408 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state. The analyzer supports "Super Jumbo" events up to 64K.

The M408 ports allow signals to pass through without re-timing, ensuring that the test platform is as transparent as possible.

The analyzer can be controlled with either a 1GbE connection to the local network, or a USB connection. The SierraNet M408 provides the user with an easy to understand control panel and LED indicators.

1.9.1 M408 Analyzer Front Panel

The M408 Analyzer has the basic features shown in Figure 1.23:

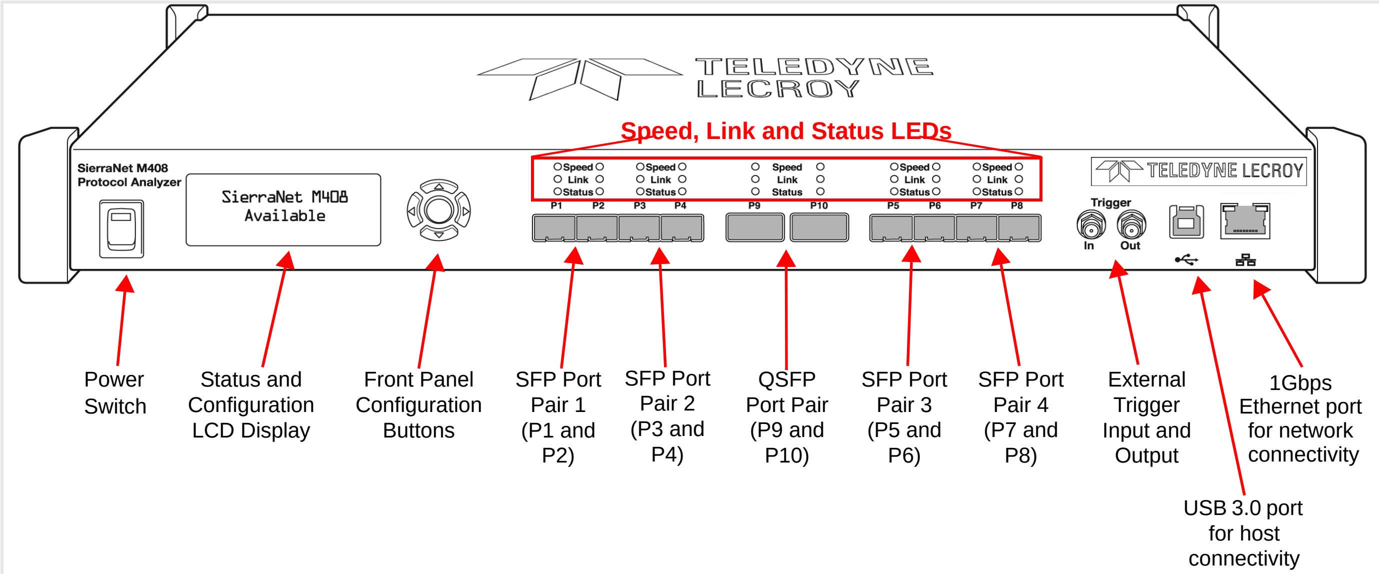


Figure 1.23: M408 Front Panel

1.9.1.1 M408 LEDs

LEDs indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6; P7 - P8 and P9 -10) with the following functionality (see Figure 1.24):

Speed LEDs

The LEDs for SPEED illuminate as follows:

	GBE	Fibre Channel
Yellow	Reserved	4G/2G/1G FC
Green	10 GigE	8G FC
Blue	40 GigE	16G FC

Link Activity LEDs

	GBE
Green	Network activity Detected
Yellow	Link up, no activity
No Color	No link

Status LEDs

Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

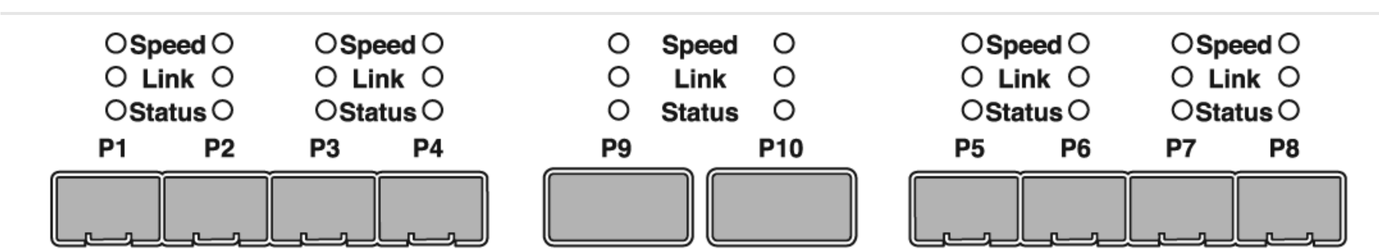
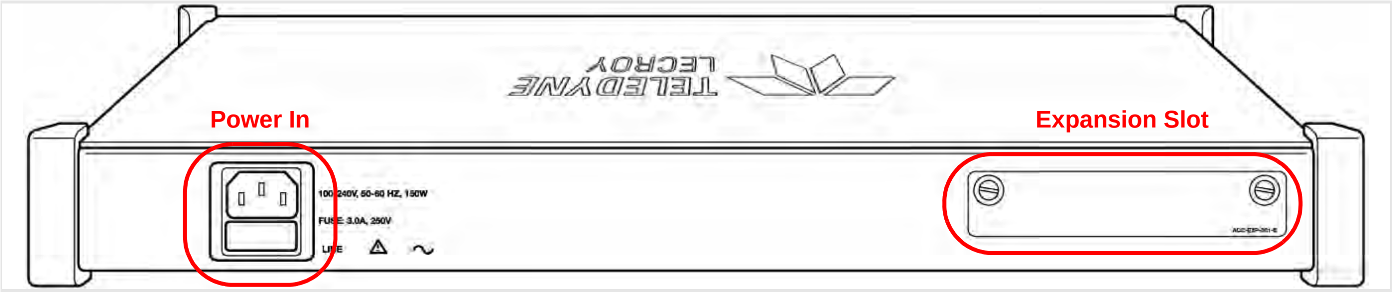


Figure 1.24: LEDs on the M408 Front Panel

1.9.2 M408 Analyzer Rear Panel

On the back, the M408 Analyzer has Power In and an Expansion Slot.



1.10 SierraNet M168 Protocol Analyzer

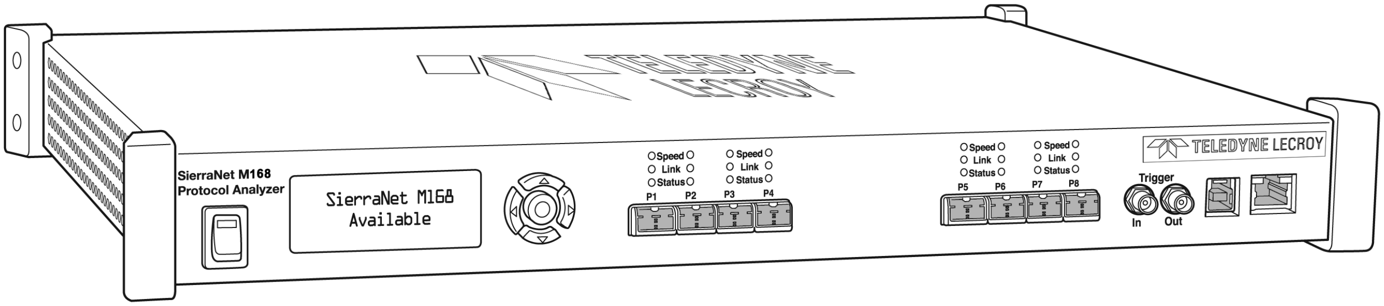


Figure 1.25: Teledyne LeCroy SierraNet M168 Protocol Analyzer

The SierraNet M168™analyzer is based on Teledyne LeCroy's 40 Gbps Analyzer platform. The M168 has eight SFP+ 10GigE/16G FC ports.

Major features of the M168 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state. The analyzer supports "Super Jumbo" events up to 64K. The M168 can also be used to capture and jam 40G Ethernet links using a dedicated "Octopus" cable (P/N 923694-00) and license (sold separately).

The M168 is very portable and can also be rack mounted (1U form-factor). Up to 64 GB of capture memory allow extensive line-speed capturing.

The M168 ports allow signals to pass through without re-timing, ensuring that the test platform is as transparent as possible.

The analyzer can be controlled with either a 1GbE connection to the local network, or a USB connection. The SierraNet M168™ provides the user with an easy to understand control panel and LED indicators.

1.10.1 M168 Analyzer Front Panel

The M168 Analyzer has the following front panel features shown in Figure 1.26:

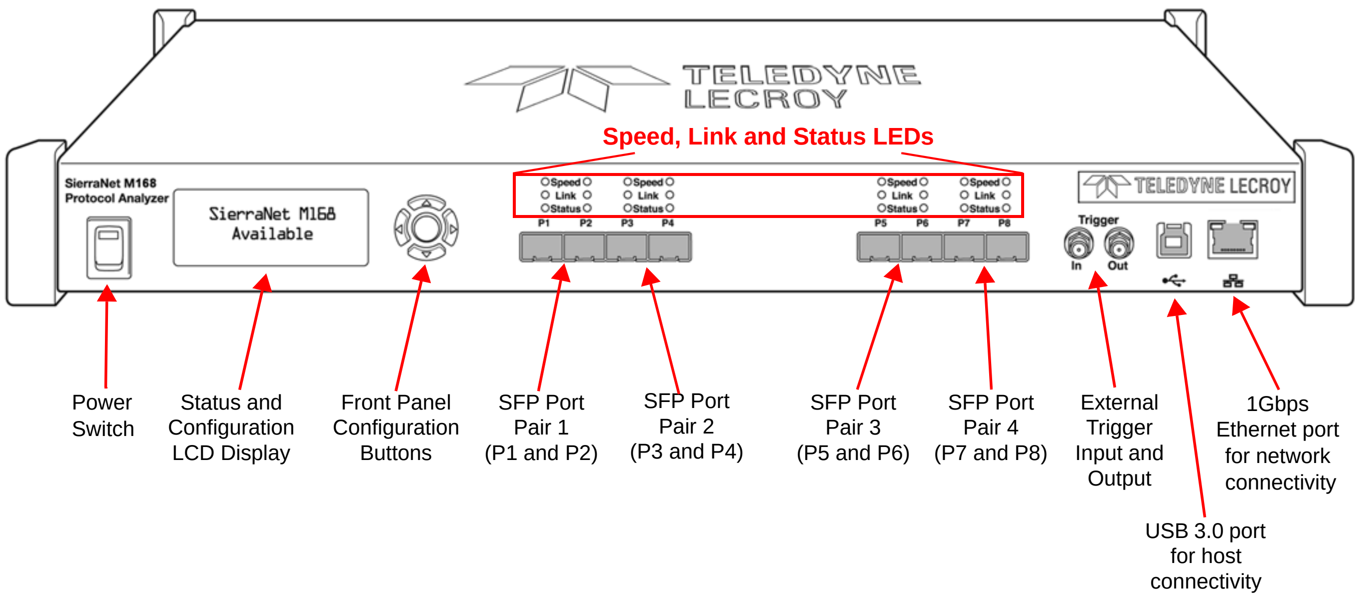


Figure 1.26: M168 Front Panel

1.10.2 M168 LEDs

LEDs indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6 and P7 - P8) with the following functionality (see Figure 1.27):

Speed LEDs

The LEDs for SPEED illuminate as follows:

	GBE	Fibre Channel
Yellow	Reserved	4G/2G/1G FC
Green	10 GigE	8G FC
Blue	N/A	16G FC

Link Activity LEDs	
Green	Network activity Detected
Yellow	Link up, no activity
No Color	No link
Status LEDs	
Yellow Blinking	Waiting for trigger
Yellow Solid	Triggered
Red	Error detected
No Color	No Activity

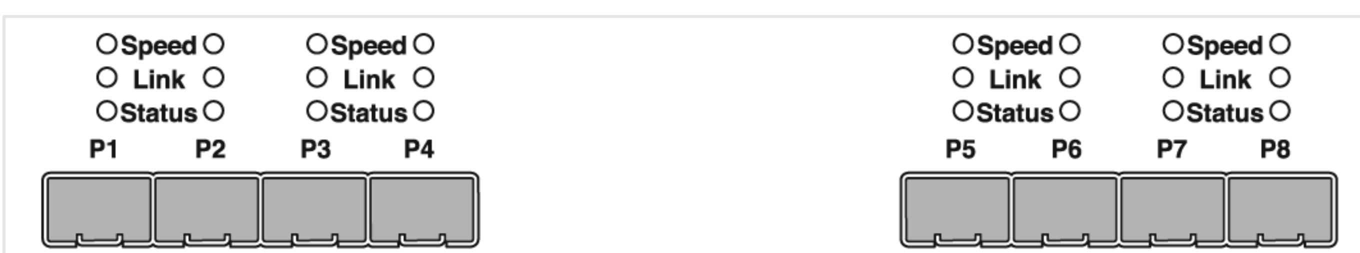


Figure 1.27: LEDs on the M168 Front Panel

1.10.3 M168 Rear Panel

On the back, the M168 Analyzer has Power In and an Expansion card slot (Figure 1.26).

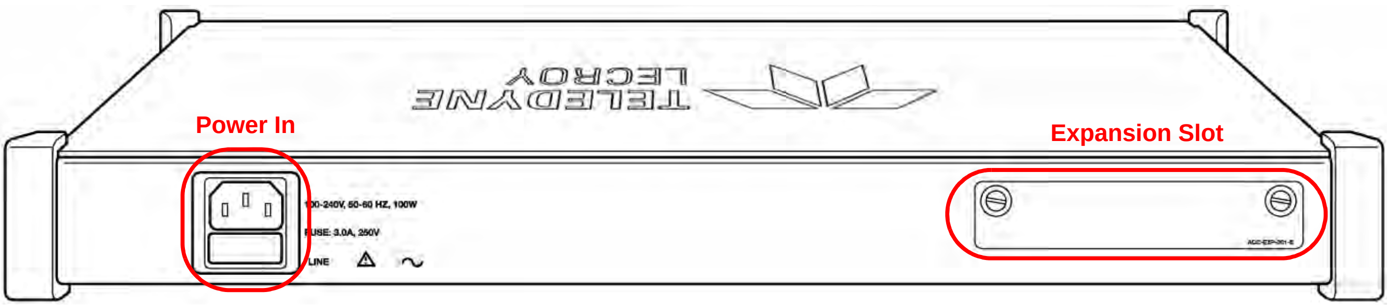


Figure 1.28: M168 Back Panel

1.11 Status and Config Display

The SierraNet Analyzer front LCD display indicates the configuration and status of the device. For example, during initialization, the LCD panel displays boot status messages. See Figure 1.29.

1.11.1 LCD Display and Button Functions for Analyzer Host Connection Setup

The host connection settings of the SierraNet can be configured from the unit itself. Five buttons are provided to navigate menus and input settings presented on the LCD display. When you first turn on the Analyzer, after initialization, the LCD displays **SierraNet M1288/M648/T328/M328Q/ M328/M408/M168 Available** with two arrows pointing up and down as shown in the illustration below.

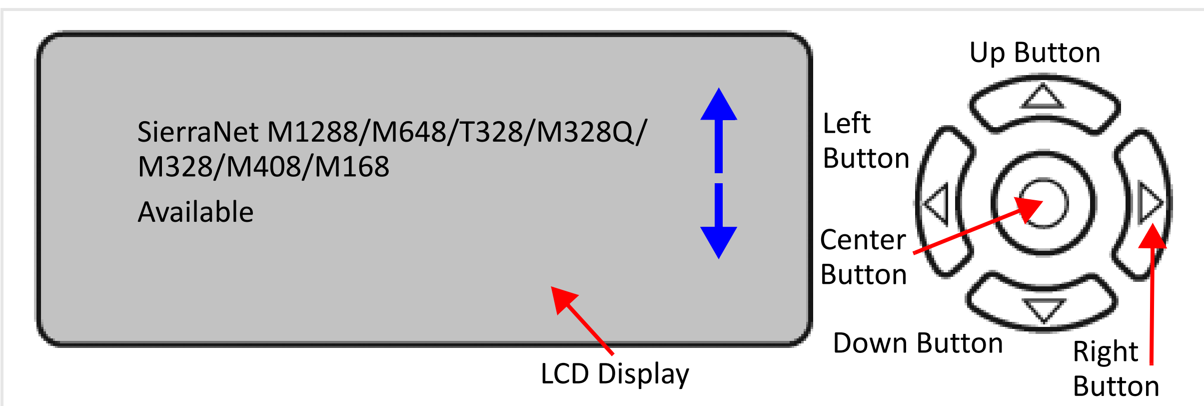


Figure 1.29: LCD Display and Button on the Front Panel

Press the **Up** △ and **Down** ▽ buttons to navigate through the following menu items:

- ❑ Display current Static or Dynamic IP Address
- ❑ SierraNet M1288/M648/T328/M328Q/M328/M408/M168 SN (serial number)
- ❑ Connection
- ❑ Unit Name
- ❑ Set IP Configuration
- ❑ IP Mode Dynamic, or
- ❑ IP Mode Static

The **Left** ◁ and **Right** ▷ buttons are used to change the configuration properties.

The LCD will display **Button Inactive In This Menu Item** if the button does not serve any purpose for that selection.

See sections 1.11.1.1 through 1.11.1.4 for instruction on setting the IP Configuration and Static on Dynamic IP using the buttons and the LCD display on the Analyzer.

1.11.1.1 Set IP Configuration

1. Power on the Analyzer with the **TELEDYNE** LECROY logo displayed (TELEDYNELECROY). The unit begins initialization (**Initializing......**).
2. Once the Analyzer has finished initializing, press **Down** ▽ button to scroll through the LCD Menu display:

   Main menu → IP Address → **Available** (Unit not in use by other user)
3. Press the **Down** ▽ button again to scroll through the other menus:
   - Main Menu → Product Name → **Serial Number**
   - Main Menu → IP Mode → **Dynamic**

     The display will show you the current IP Configuration mode of your product—Dynamic or Static. In this case, it is in Dynamic IP Address Mode.
   - Main Menu → **Set IP Configuration**

     From this menu you can change the IP Configuration from Dynamic to Static or from Static to Dynamic
   - Main menu → IP Address → **Available** (Unit not in use by other user)

NOTE: If Main Menu → IP Address → ENET Connected comes up when you are using the **Down** ▽ button to scroll through the menus, this means a user has already connected the unit to the network. You can bump the unit off the network by pressing the **Right** button and resetting the IP address as explained in 1.11.1.2, *Changing from Dynamic to Static IP Mode*, below.

1.11.1.2 Changing from Dynamic to Static IP Mode

If the Analyzer is in Dynamic IP Mode, perform the following steps to change it to Static IP Mode and manually set the IP Address:

To set a Static IP Address:

1. After initialization, press the **Down** ▽ button to ensure your unit is in Dynamic IP Mode.
2. Press the **Down** ▽ button until you see *Set IP Configuration*.
3. Press the **Center** ◎ button once to select **Set IP Configuration**. Set IP Mode → Static appears in the LCD display.

4. Press the **Center** ◎ button once to select *Set IP Mode Static*. The Static IP address appears in the LCD display (e.g., 188.168.040.036).

5. Press the **Center** ◎ button once to set the Static IP address.

   The first numeral of the IP address will have an up arrow ↑ below it.

6. Use the **Up** △ or **Down** ▽ button to change the IP Address.

7. Press the **Right** ▷ or ◁ **Left** button to move to the right or left to change each component of the static or dynamic IP address and change it using step 6.

8. Once the IP Address is selected, press the **Center** ◎ button to set the new Static IP Address.

9. The new **Static IP Address** will be displayed.

10. Press the **Up** △ button once. **Accept and Reboot** is displayed.

11. Press the **Center** ◎ button. **Center Button to Confirm Reboot** is displayed.

12. If you want the new Static IP Address to be stored and your unit to Reboot**,** press the **Center** ◎ button. **Rebooting ......** will be displayed.

    Press any other button and your changes will be canceled.

13. After **Rebooting** has completed, to check that you are in **Static IP Mode**, just scroll through the Main menu using the **Down** ▽ button.

1.11.1.3 Changing from Static to Dynamic IP Mode

If your unit is in Static IP Mode you can change it to Dynamic IP Mode, the IP Address will be set automatically by the network using DHCP.

To change from a Static IP address to a Dynamic IP address follow the steps below:

1. Ensure your unit is in Static IP Mode by scrolling through the Menus displayed on the LCD by pressing the down button. Main Menu → IP Mode → **Static.**

2. Press the **Down** ▽ button one more time and **Set IP Configuration** should be displayed.

3. Press the **Center** ◎ button once to select **Set IP Configuration**. **Set IP Mode → Dynamic** should be displayed.

4. Press the **Center** ◎ button once again to select **Set IP Mode Dynamic.**

5. **Accept and Reboot** should be displayed. Press the **Center** ◎ button once.

   Center Button to Confirm Reboot should be displayed.

6. If you want the new Dynamic IP Address to be stored and your unit to Reboot, press the **Center** ◎ button. **Rebooting ......** will be displayed.

   Press any other button to chancel your changes.

7. To check that you are in Dynamic IP Mode, just scroll through the Main Menu using the **Down** ▽ button.

NOTE: In case the device is often moved from one subnet to the other, it is recommended to set the IP Mode to Dynamic and to configure the DHCP server so that the device always receives the same (known) IP address. Many DHCP servers allow this type of static allocation based on the device MAC address.

1.11.1.4 Setting the Gateway and Subnet Mask

NOTE: Setting the Gateway and Subnet Mask require a detailed knowledge of your network.

1. Ensure that you are in Static IP Mode by following the steps in 1.11.1.1, *Set IP Configuration* and 1.11.1.2, *Changing from Dynamic to Static IP Mode* if necessary.
2. Press the **Down** ▽ button to get to the **Set IP Configuration** menu.
3. Press the **Center** ◎ button, then the **Down** ▽ button to get to the **Set IP Mode Static** menu.
4. Press the **Center** ◎ button once, then press the **Down** ▽ button to get to the **Subnet Mask** menu.
5. To set the **Subnet Mask**, Press the **Center** ◎ button. The first numeral of the **Subnet Mask** will have an up arrow ↑ below it.
6. Use the **Up** △ or **Down** ▽ button to change the **Subnet Mask**.
7. Press the **Right** ▷ or ◁ **Left** button to move to the right or left to change each component of the **Subnet Mask** and change it as described in Step 6.
8. Once the **Subnet Mask** is selected, press the **Center** ◎ button to set and display the new **Subnet Mask**.
9. The press the **Down** ▽ button to get to the **Gateway Address** menu.
10. To set the **Gateway Address**, press the **Center** ◎ button. The first numeral of the **Gateway Address** will have an up arrow ↑ below it.
11. Use the **Up** △ or **Down** ▽ button to change the **Gateway Address**.
12. Press the **Right** ▷ or ◁ **Left** button to move to the right or left to change each component of the **Gateway Address** and as described in Step 11.
13. Once the **Gateway Address** is selected, press the **Center** ◎ button to set and display the new **Gateway Address**.
14. Press the **Up** △ button to confirm the **Subnet Mask,** then press the **Up** △ button again to confirm the **Static IP Address.**

15. Press the **Up** △ button one more time to display **Accept and Reboot**.

16. Press the **Center** ◎ button once. The LCD display will read **Center Button to Confirm Reboot**.

17. If you want the new **Subnet Mask, Gateway Address**, and **Static IP Address** to be stored and your unit to Reboot, press the **Center** ◎ button. **Rebooting ......** will be displayed.

18. Press any other button and your changes will be canceled.

Chapter 2

S/W and H/W Installation and Setup

2.1 Software Installation and Setup

2.1.1 Installation of the Net Protocol Suite Software

The Net Protocol Suite software is supported on systems using a **Microsoft Windows**® -based host machine running **Windows Server** 2016, **Windows Server** 2019, Windows 10 and Windows 11 64-bit operating systems and serves as the interface for the Analyzer.

NOTE: For Windows Server 2016/2019 users, please reference Appendix H, *Windows Server 2016 / 2019 Installation*. This appendix provides detailed instructions on how to add the firewall exceptions to ensure the application finds the Analyzers over the Ethernet network.

2.1.2 Downloading the Net Protocol Suite software

You can download the latest version of the Net Protocol Suite software from the following site:

https://teledynelecroy.com/sw/netprotocolsuite/

NOTE: First-time user registration is required.

2.1.3 Command Line Installation

The default component installation includes the mandatory components:

- Net protocol Suite,
- Link Expert,
- CrossSync, and
- Documentation.

To install the Net software via command line (aka Silent Install), type the following:

```
<Installer directory in administrator mode> installer.exe in -c --am --al
```

2.1.3.1 Selective Component Installation

Selective component installation includes the mandatory components in *, The default component installation includes the mandatory components:* and the selected analyzer component(s):

To install via command line, type the following:

```
<Installer directory in administrator mode> installer.exe in
component.SierraNetM1288Support component.SierraNetM648Support.. in -c --am -
-al
```

2.1.3.2 Command Line Options

Command Line Installation Options:

Command	Function
`-c`	Create a local repository inside the installation directory
`--am`	Accept all message queries without user's input
`--al`	Accept all licenses without user's input
`pr`	Uninstall all packages and remove the program directory
`--da`	Automatically answer to message queries with their default values

NOTE: For a full list of commands, refer to:

https://doc.qt.io/qtinstallerframework/ifw-cli.html

2.1.3.3 Command Line Uninstall

To uninstall the Net software via command line, type the following:

```
<C:\Program Files\LeCroy\Net Protocol Suite in administrator mode>
maintenancetool.exe pr -c --da
```

2.1.4 Error Messages

If you get an error message during drivers installation for Windows, consult your system administrator. Your system may require only administrator-level users to copy driver files.

2.2 Hardware Setup

NOTE: Follow standard optical cable cleaning procedures every time a cable is unplugged and replugged into an optical module.

2.2.1 Connecting the SierraNet M1288 Analyzer

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

Connect to and from devices using cables suitable for your setup. The M1288 supports single and multi-mode fiber, active copper, and passive copper cabling. See *Chapter 1* *Introduction.*

1. Connect the Ethernet cable between the SierraNet M1288 Analyzer Ethernet Port and one of the following:
   - Ethernet Port on the host machine
   - Ethernet switch
   - Gigabit Ethernet interface

   You can also connect a USB cable from the USB port on the Analyzer to the host machine.
2. Connect the Analyzer to a 100V–240V, 50Hz–60Hz power outlet and turn on the Power switch. The host machine detects the Analyzer, loads the driver files, then the Analyzer undergoes the initialization as shown on the LCD display.
3. Connect your devices under test using either optical modules and fiber cables or appropriate copper cabling, suitable for your configuration.
4. Connect your devices under test to port pairs P1-P2, P3-P4, or P5-P8. See 2.2.1.1, *M1288 Connections*.

2.2.1.1 M1288 Connections

The SierraNet M1288 has 3 sets of connectors: P1-P2, P3-P4 and P5-P8. Each set has different characteristics and different capabilities.

Ports P1-P2

These ports are digitally re-timed, and are often called “the Jammer ports”, though they can also act as analyzer ports. These ports use QSFP-DD cages, but only lanes 0 through 3 are connected. Traffic going to P1 is digitally re-timed in the M1288 and sent back out on P2, and vice-versa. As only 4 lanes are connected, these ports can be used to analyze, Jam or exercise GbE traffic up to 400Gbps on a single SierraNet M1288 unit. See Figure 2.1.

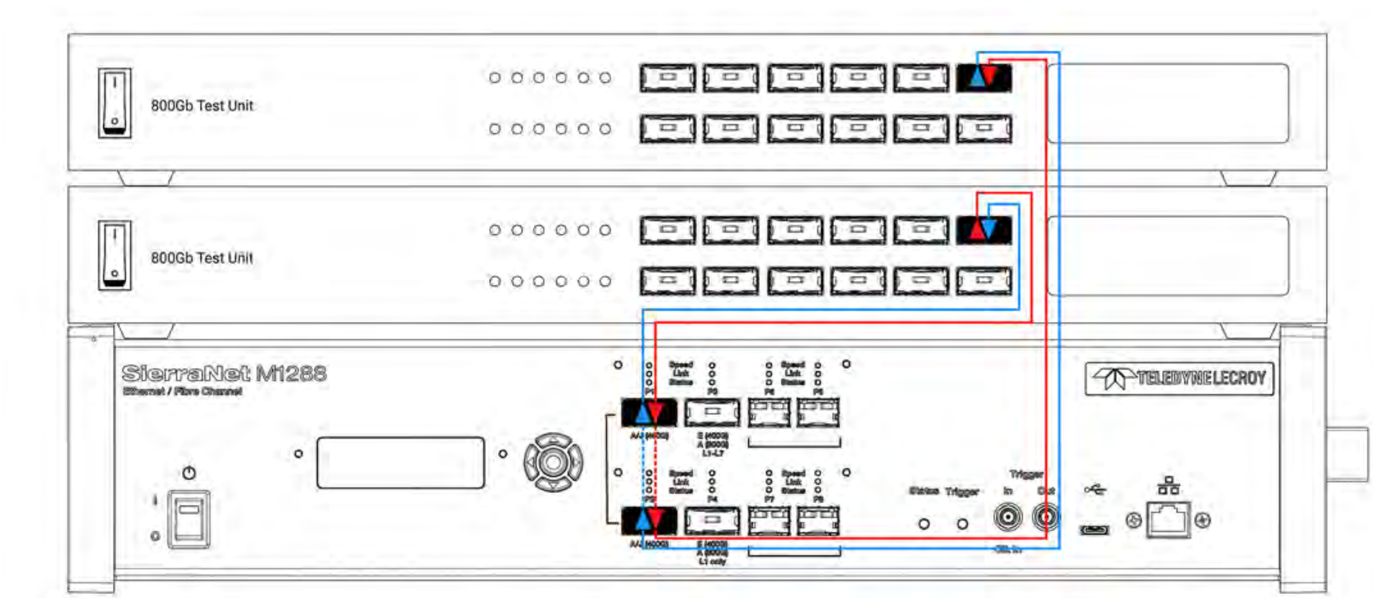


Figure 2.1: P1-P2 Connections

The benefit of using ports P1-P2 is that it is not necessary to use a M1288 Probe.

In the Sierra Net Protocol Suite software, the port configuration options for P1-P2 connections are shown in Figure 2.2, Figure 2.3, and Figure 2.4.

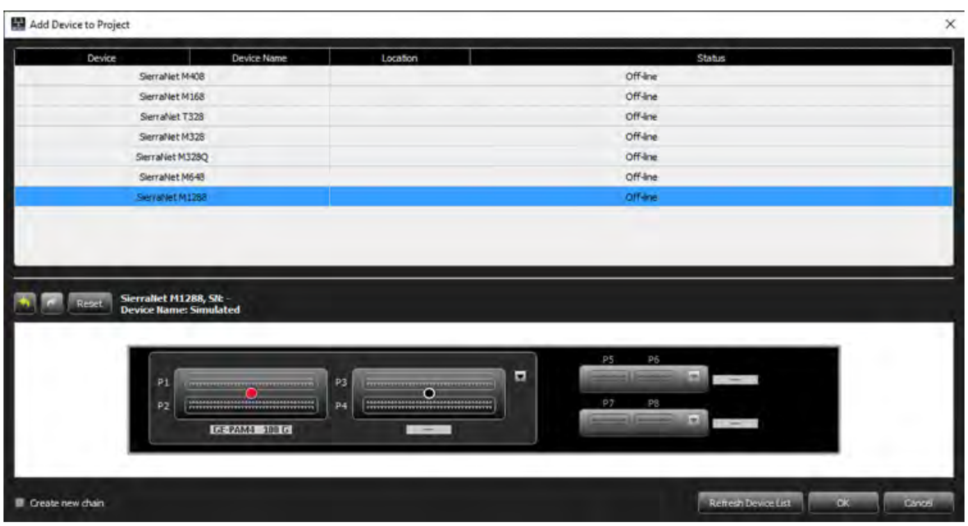


Figure 2.2: Net Protocol Suite GE-PAM4 100G Port Configuration

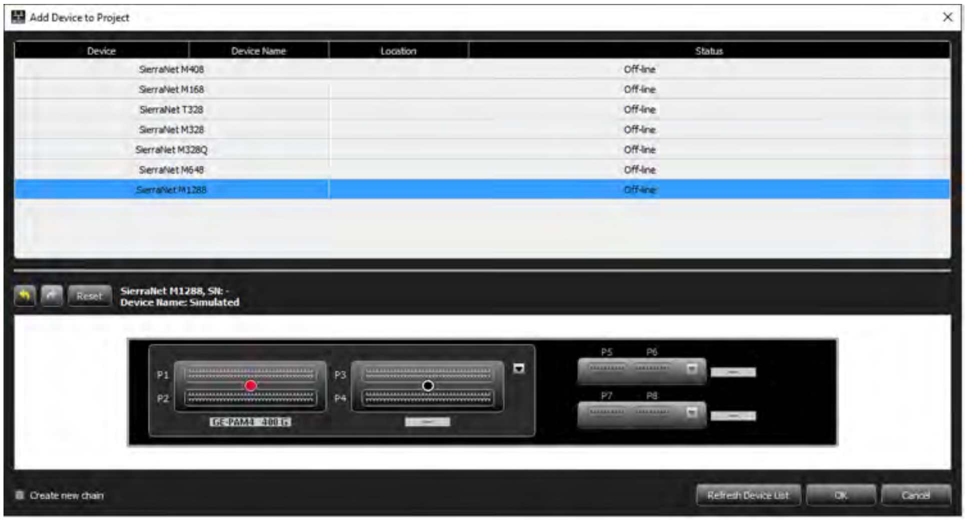


Figure 2.3: Net Protocol Suite GE-PAM4 400G Port Configuration

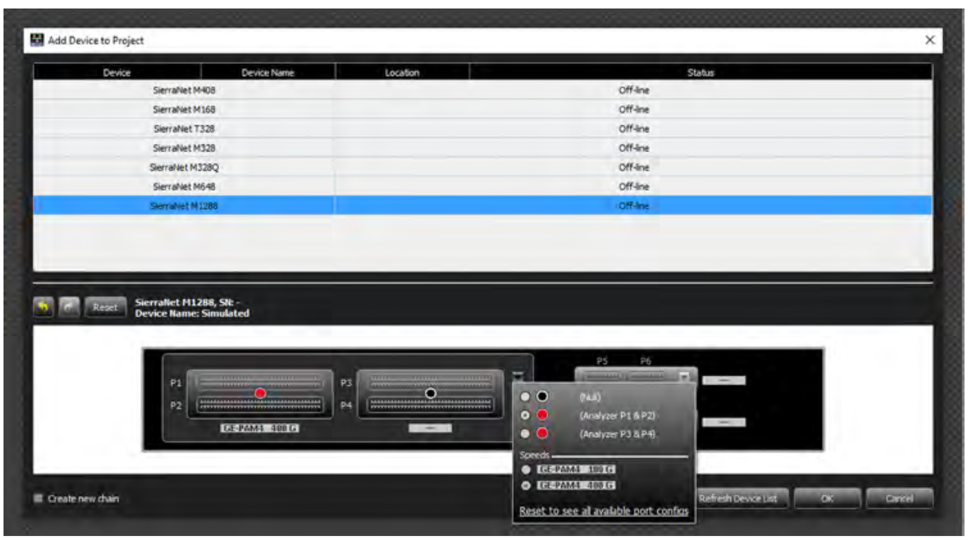


Figure 2.4: Net Protocol Suite GE-PAM4 100G and 400G Port Configurations

Ports P3-P4

These ports are purely analyzer ports, they only analyze the input traffic on them, and do not copy it over between them. Using these ports requires the use of the M1288 Probe unit (sold separately) . The M1288 Probe is used to 'close the loop' between the 2 DUTs by connecting traffic between the DUT ports and sending a copy to the P3-P4 ports. These ports use QSFP-DD cages, and all 8 lanes (0-7) are connected, allowing for up to 800Gbps traffic analysis:

1. For L1 analysis only in 800GbE (only Auto Negotiation (AN) and Link Training (LT)), these ports can be used on a single SierraNet M1288 unit and the M1288 Probe, as follows: See Figure 2.5.
2. For full stack (L1 through L7) analysis of 800GbE, these ports must be used on 2 stacked SierraNet M1288 units and one M1288 Probe. For this port configuration,

the 2 SierraNet M1288 units must be connected using the custom Expansion cable through the dedicated Expansion ports on the back panel. See Figure 2.6.

NOTE: This port configuration is not yet available in version 6.00.

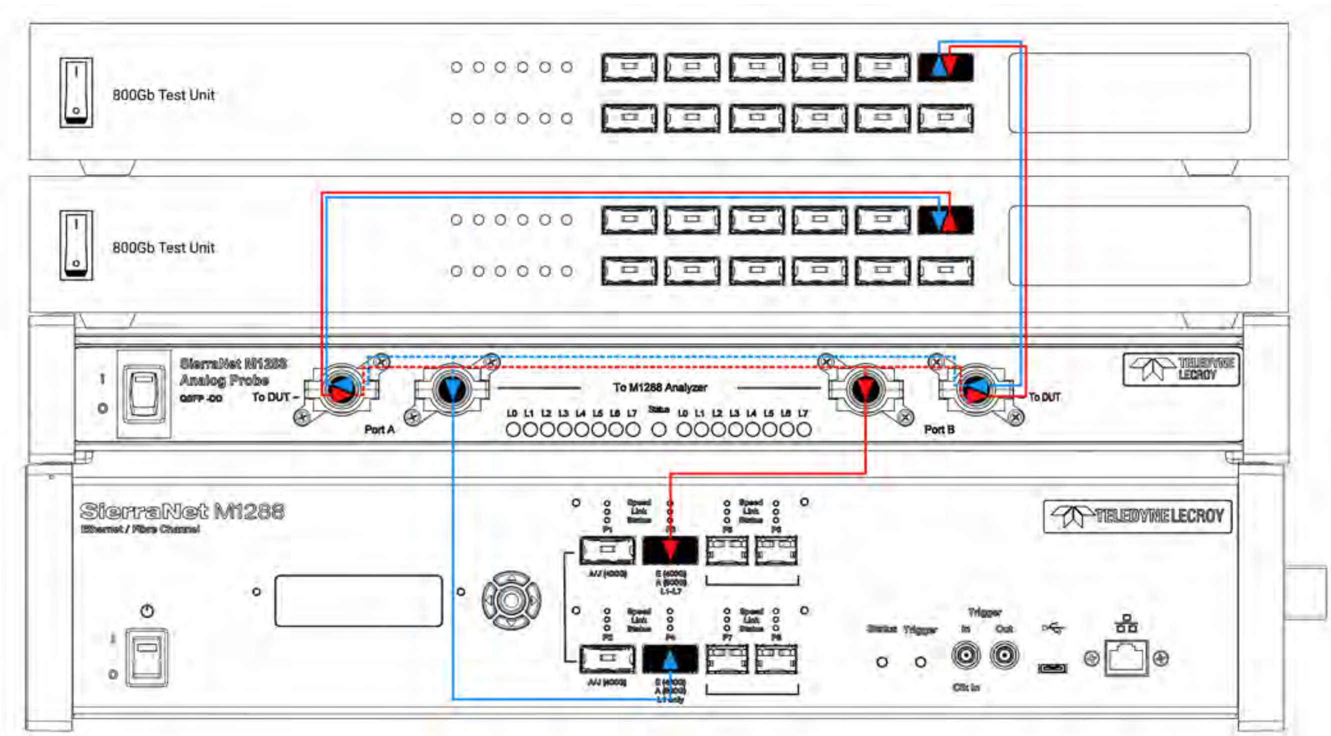


Figure 2.5: L1 Analysis through Ports P3-P4 Connections

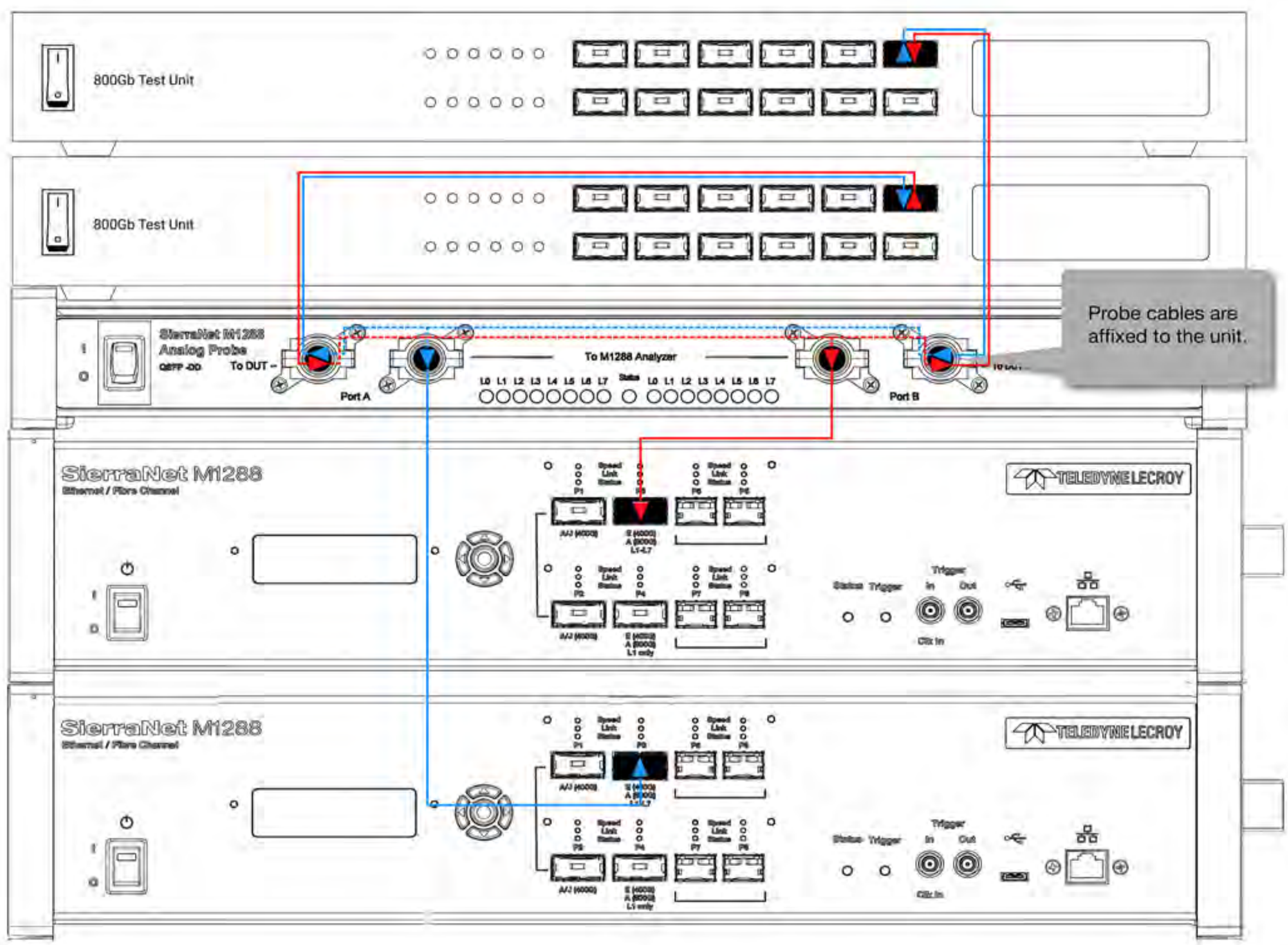


Figure 2.6: Full Stack 800 Gbe Connections

3. Once connected, the central Status light on the M1288 Analog probe will display the connection status:
   - RED: Both Analyzer QSFP cables are not connected
   - BLUE: One Analyzer QSFP cable is connected
   - Green, blinking: Both Analyzer QSFP cables are connected

In the Sierra Net Protocol Suite software, the port configuration options for P3-P4 connections are shown in Figure 2.7.

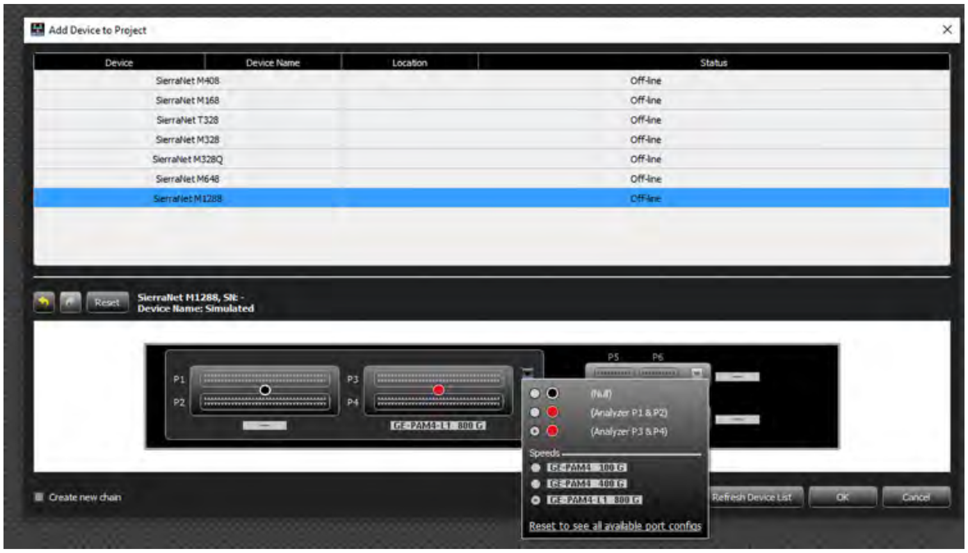


Figure 2.7: Net Protocol Suite GE-PAM4 100G, GE-PAM4 400G and GE-PAM4-L1 800G Port Configurations

Ports 5-8

These SFP112 ports are digitally retimed and used for 128GFC.

NOTE: This is not yet supported in version 6.00.

2.2.2 Connecting the SierraNet M648 Analyzer

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

---

1. Connect the Ethernet cable between the SierraNet M648 Analyzer Ethernet Port and one of the following:
   - Ethernet Port on the host machine
   - Ethernet switch
   - Gigabit Ethernet interface

   You can also connect a USB cable from the USB port on the Analyzer to the host machine.

2. Connect the Analyzer to a 100V–240V, 50Hz–60Hz power outlet and turn on the Power switch.

   Once the Analyzer is turned on, the host machine detects the Analyzer, loads the driver files, then the Analyzer undergoes the initialization as shown on the LCD display.

3. Connect your devices under test using either optical modules and fiber cables or appropriate copper cabling, suitable for your configuration.

4. Connect your devices under test to port pairs P1/P2, P3/P4, P5/P6, P7/P8 and/or P9/P10. See Figure 2.8.

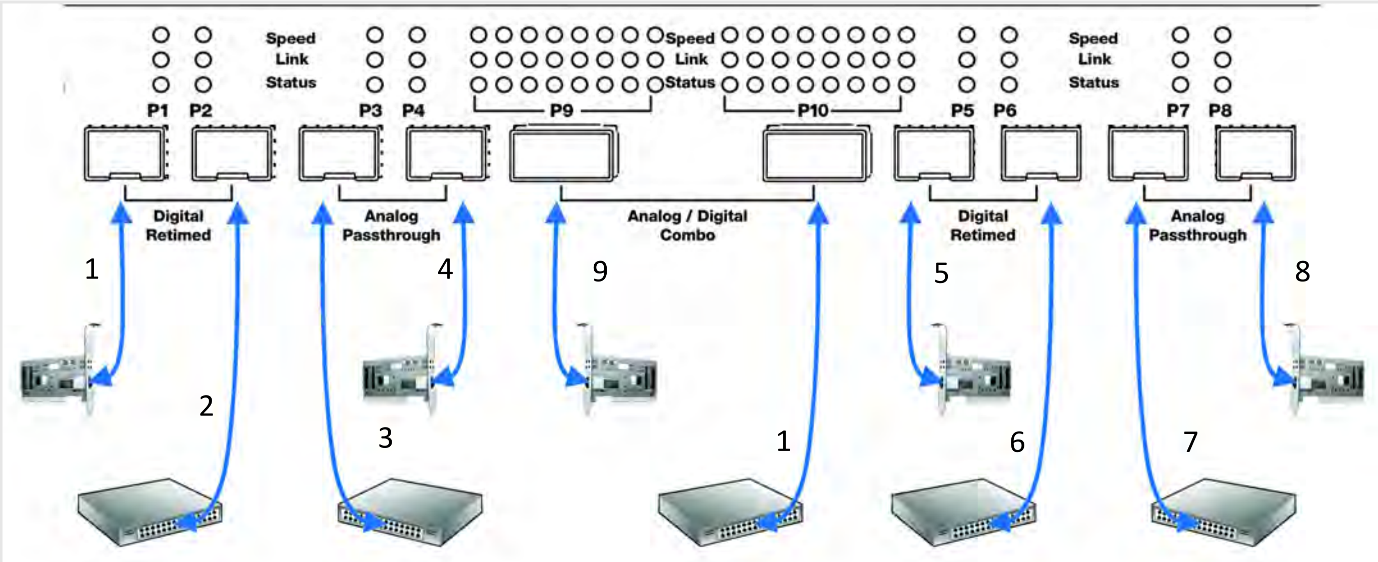


Figure 2.8: M648 Analyzer with SFP+ and QSFP-DD Connections

2.2.2.1 Cables to Use with M648 Analyzer

Connect to and from devices using optical modules and cables suitable for your setup. Single and multi-mode fiber, active copper, and passive copper cabling is supported. See figures Figure 2.9 and Figure 2.10.

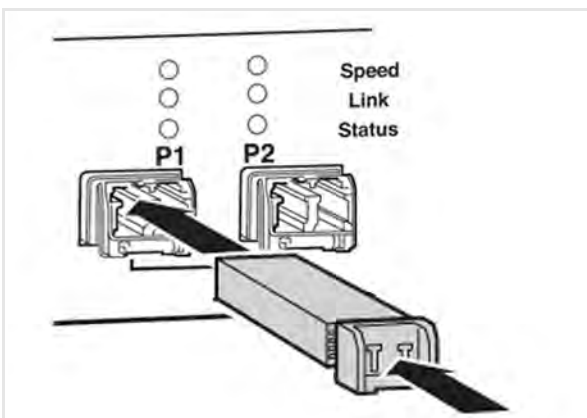


Figure 2.9: M648 Analyzer SFP+ Connections

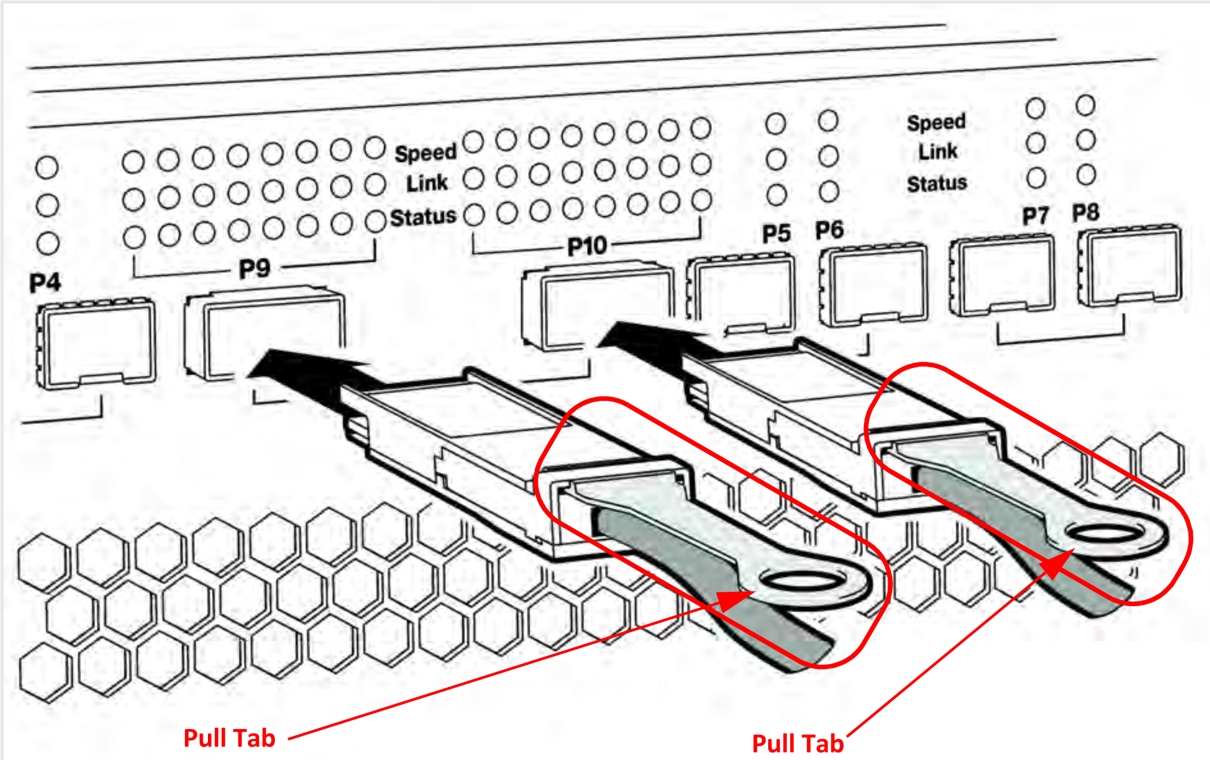


Figure 2.10: M648 Analyzer QSFP-DD Connections

2.2.2.2 400G L1 Analysis

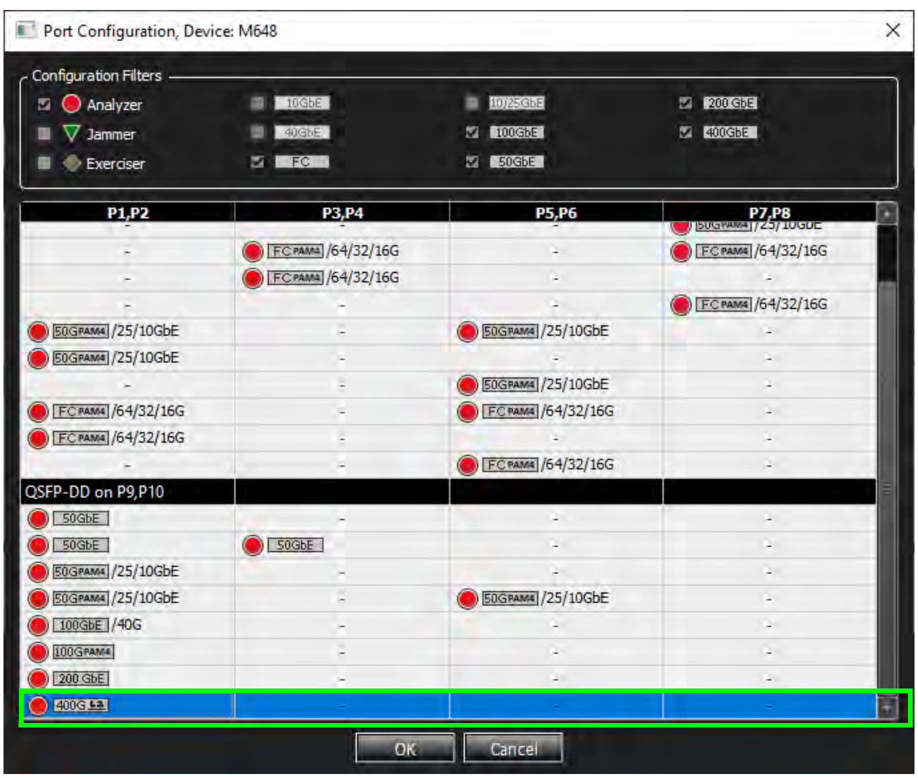


Figure 2.11: Port Configuration – M648 Analysis

400G L1 Analysis is unique in that:

- There is no L2 and up support.
- 400G L1 port configuration only records the Auto Negotiation (AN) and Link Training (LT) phases of the link bring-up. Full speed data cannot be recorded; this includes any L2 or higher traffic, but also the full PRBS phases of the link bring-up. This affects the Link LED, which works in reverse; that is, during Link bring-up, the LED will be lit, but once the link is up, the Link LED will go dark.
- PRBS can only be recorded on one lane.
- Unpacked mode and the requirement to select the specific lane for showing PRBS.
- You cannot record actual 400G traffic; you can only record the sections of the link bring up such as Speed Negotiation (SN) and Link Training (LT).

2.2.2.3 M648 Dual User Support

The Sierra M648 now supports two users to simultaneously connect to a single unit, with both working independently on a different set of SFP ports.

This is easier to explain by defining “Hemispheres”, as follows:

- Hemisphere 1: P1-P4
- Hemisphere 2: P5-P8

Each Hemisphere can be connected individually by a different user. A single user can still connect to both Hemispheres at once by reverting to the standard mode of operation.

NOTE: The QSFP-DD ports CANNOT be split/shared.

When the Dual User mode needs to be used, you can use either the Device Management dialog or by activating a unit on another project.

NOTE: In order to use the Dual User support, you must open the following TCP Ports on your network firewall: 5000 to 5003; 6000 to 6003.

Ask your IT department to add the above ports to your firewall exceptions.

Using the Device Management Dialog for Dual User Support

The first way you can use the Device Management dialog:

1. Select **Setup** → **Device Management**. The Device Management window opens.
   - Units that support Dual User show a separator under the Status column, and each Hemisphere will report its status.
   - Under the Available Ports column, the drop-down allows you to select the desired set of ports to use (see the figure below).

Figure 2.12: Port Selection

- When both Hemispheres are available, the options are:
  - ♦ SFP (P1-P8) – Use all SFP ports (single user only).
  - ♦ SFP (P1-P4) – Use only the first four SFP ports, allowing another to share the unit by only using the lower half of the ports.
  - ♦ SFP (P5-P8) – Use only the last four SFP ports, allowing another to share the unit by only using the upper half of the ports.
  - ♦ QSFP-DD – Use the QSFP-DD ports (single user only).

2. Choose the SFP (P1-P4) option above to connect to ports P1-P4 (Figure 2.13).

Figure 2.13: P1-P4 Connected

3. Select the desired Port Configuration for ports P1-P4 (Figure 2.14). See *Ethernet Configuration* for more information on Port Configurations.

At this point, another user can repeat the above process and connect to ports P5-P8 (Figure 2.14).

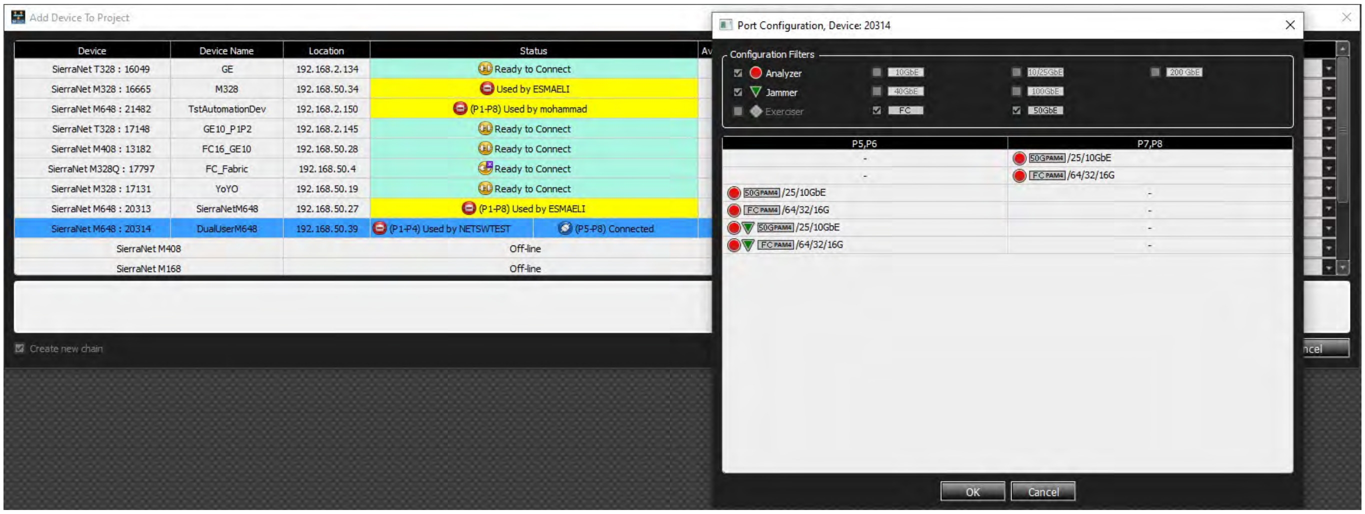


Figure 2.14: H2 Available Projects

The resulting state will look, to the first user, similar to Figure 2.15, below.

At this point, each user connected to the unit can work with their half of the unit as a separate, small Analyzer.

Figure 2.15: H1 and H2 Connected

Activating a Unit on an Existing Project for Dual User Support

Alternately, you can activate a unit on an existing project. To do this, right-click on the device and select a unit from the drop-down list as shown in Figure 2.16.

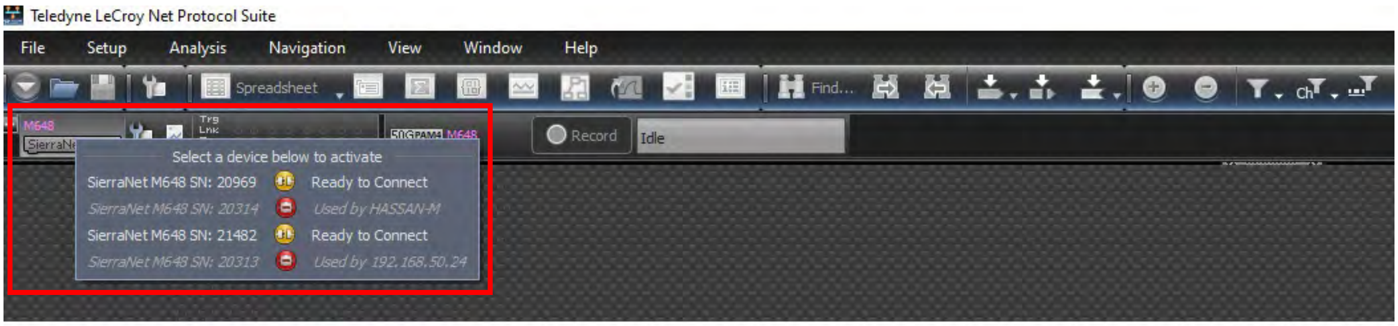


Figure 2.16: Activating a Unit in a Project

In the dual user mode, the above option is available to activate the unit, which follows the rules shown in Table 2.1, below.

TABLE 2.1: Dual User Mode Rules

Port Configuration in Project	Visible Units
0-A-0-A A-0-A-0 AJ-0-AJ-0 AJ-0-0-A AE-0-AE-0	Only units with all ports available will be listed in the menu.
0-A-0-0 A-0-0-0 AJ-0-0-0 AE-0-0-0	Only units with all ports available, and units with P1-P4 available will be listed in the menu. If all ports of a unit are available, then it will be listed as two items in the menu. This means that in this case you have two options, one is to activate all ports on the project, and the second is to activate only P1-P4 on the current project.
0-0-0-A	Only units with all ports available, and units with P5-P8 available will be listed in the menu. If all ports of a unit are available, then it will be listed as two items in the menu. This means that in this case you have two options, one is to activate all ports on the project, and the second is to activate only P5-P8 on the current project.

The following limitations are applicable:

- Global/shared resources, like external trigger in/out and cascading, may not function as expected if both users try to use them. For example:
  - If two users connect to the unit at the same time, and if User 1 sets the External Trigger Out and User 2 also does the same thing, then the output signal may not be what both users expect.
  - Also, if user 1 sets the External Trigger in the Jammer/Exerciser, and User 2 has an External Trigger In in their project, then the Analyzer will be triggered. So any shared hardware resource can be used only by one user.
  - Cascading (in general) and CrossSync (specifically) are not supported in Dual User mode.

- In Device Management, when a user connects to half of the unit, there are the following limitations:
  - Device update is disabled. It means the user can only update the device when connected to all ports.
  - IP settings is functional (enabled) only if the user is connected to all ports.

2.2.3 Connecting the SierraNet T328 Analyzer

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

1. Connect the Ethernet cable between the SierraNet T328 Analyzer Ethernet Port and one of the following:
   - Ethernet Port on the host machine
   - Ethernet switch
   - Gigabit Ethernet interface

   You can also connect a USB cable from the USB port on the Analyzer to the host machine.
2. Connect the Analyzer to a 100V–240V, 50Hz–60Hz power outlet and turn on the Power switch.

   Once the Analyzer is turned on, the host machine detects the Analyzer, loads the driver files, then the Analyzer undergoes the initialization as shown on the LCD display.
3. Connect your devices under test using either optical modules and fiber cables, or appropriate copper cabling suitable for your configuration.
4. Connect your devices under test to port pairs P1/P2, P3/P4, P5/P6 and/or P7/P8. See Figure 2.17.

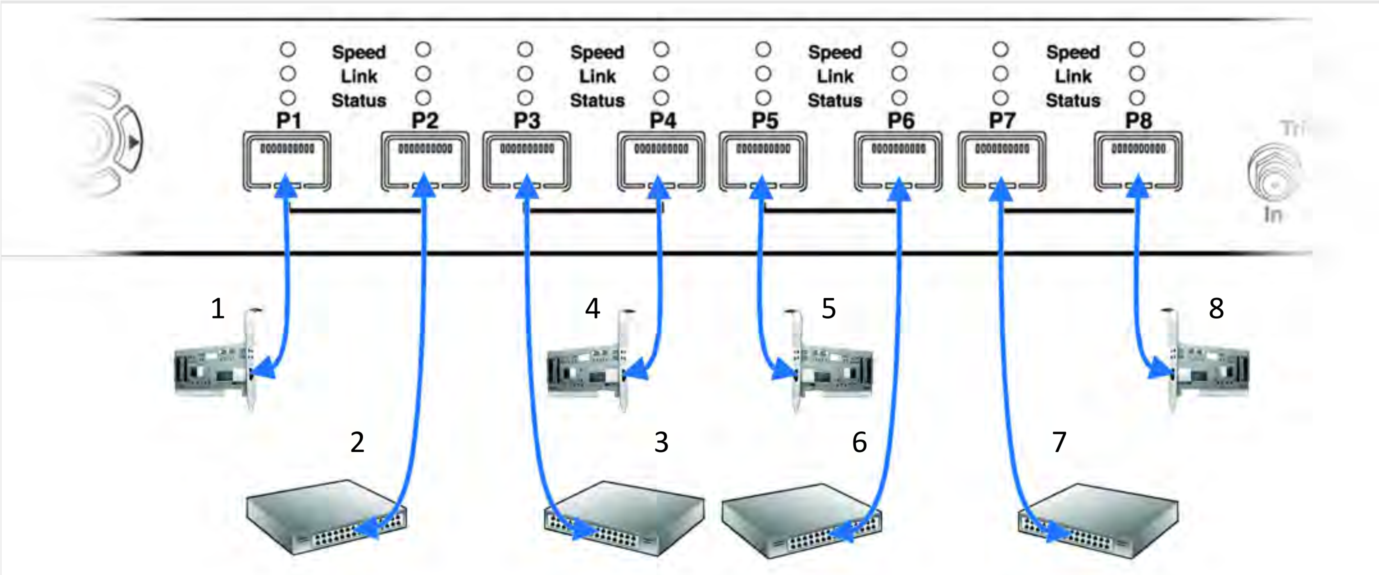


Figure 2.17: T328 Analyzer with SFP+ Connections

2.2.3.1 Cables to Use with T328 Analyzer

Connect to and from devices using optical modules and cables suitable for your setup. Single and multi-mode fiber, active copper, and passive copper cabling are supported.

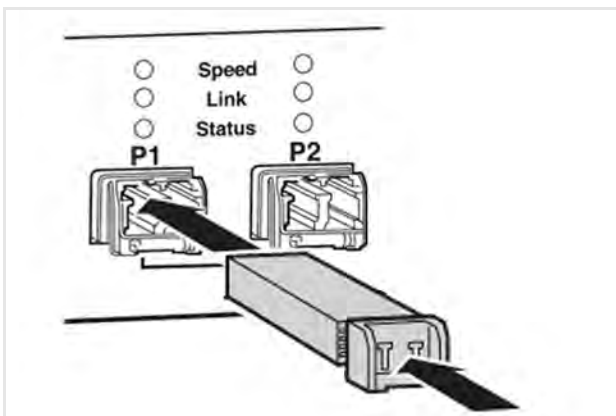


Figure 2.18: T328 Analyzer SFP+ Connections

2.2.4 Connecting the SierraNet M328Q Analyzer Overview

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

1. Connect the Ethernet cable between the SierraNet M328Q Analyzer Ethernet Port and one of the following:
   - Ethernet Port on the host machine
   - Ethernet switch
   - Gigabit Ethernet interface

You can also connect a USB cable from the USB port on the Analyzer to the host machine.

2. Connect the Analyzer to a 100V–240V, 50Hz–60Hz, power outlet and turn on the Power switch.

   Once the Analyzer is turned on, the host machine detects the Analyzer, loads the driver files, then the Analyzer undergoes the initialization as shown on the LCD display.

3. Connect the devices under test using either optical modules and fiber cables or appropriate copper cabling, suitable for the configuration.

4. Connect the devices under test to port pairs P1/P2, P3/P4, P5/P6 and/or P7/P8. See Figure 2.19.

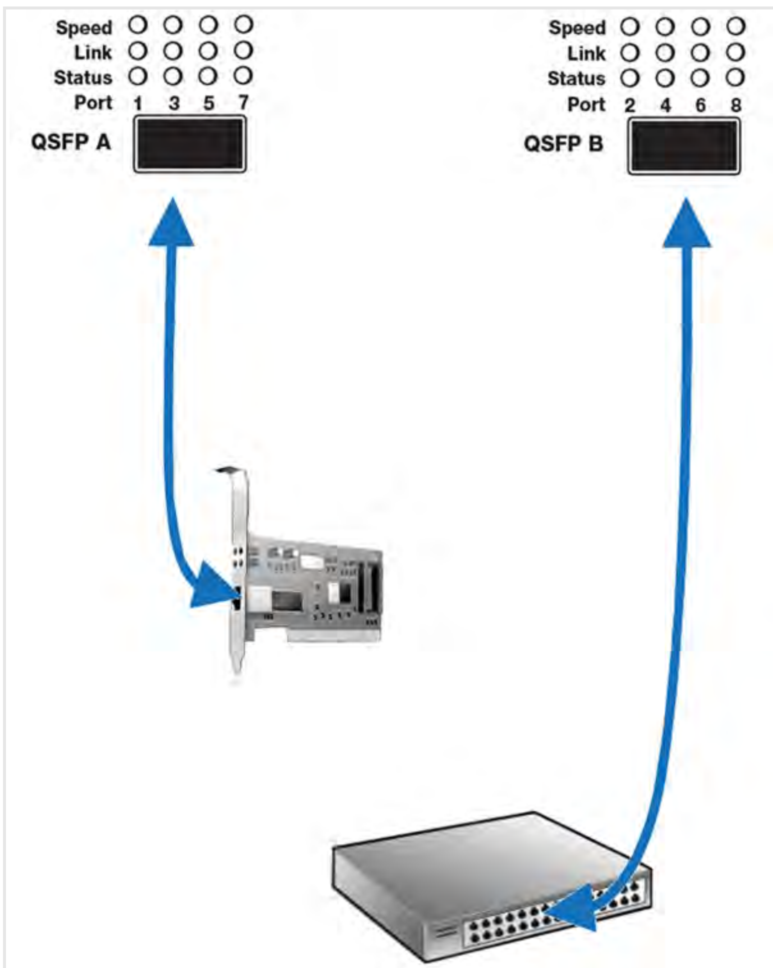


Figure 2.19: M328Q Analyzer with QSFP – 4XSFP Connections

2.2.4.1 Cables to Use with M328Q Analyzer

Connect to and from devices using optical modules and cables suitable for your setup. Single and multi-mode fiber, active copper, and passive copper cabling is supported. See Figure 2.20.

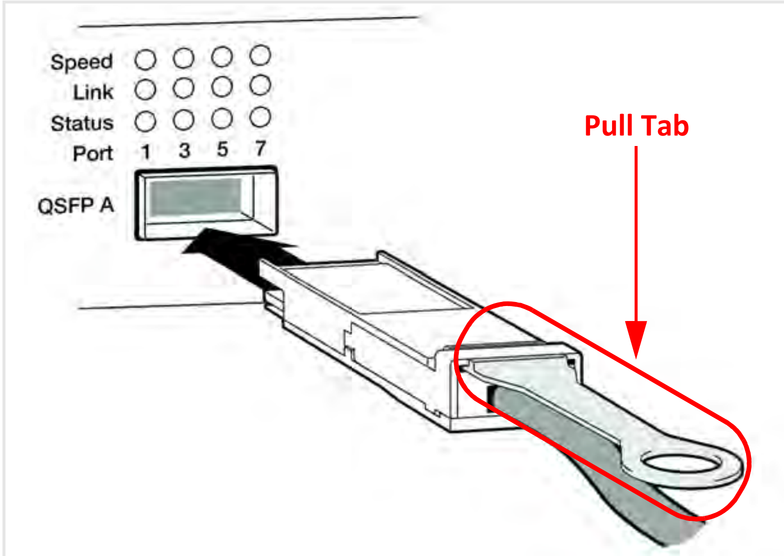


Figure 2.20: M328Q Analyzer QSFP+ Connections

NOTE: To avoid putting undue stress on the connector and cable, use the plastic pull tab to disconnect the cable from the Analyzer.

2.2.4.2 Analysis Configuration

For analysis only, the supported port configurations are shown below:

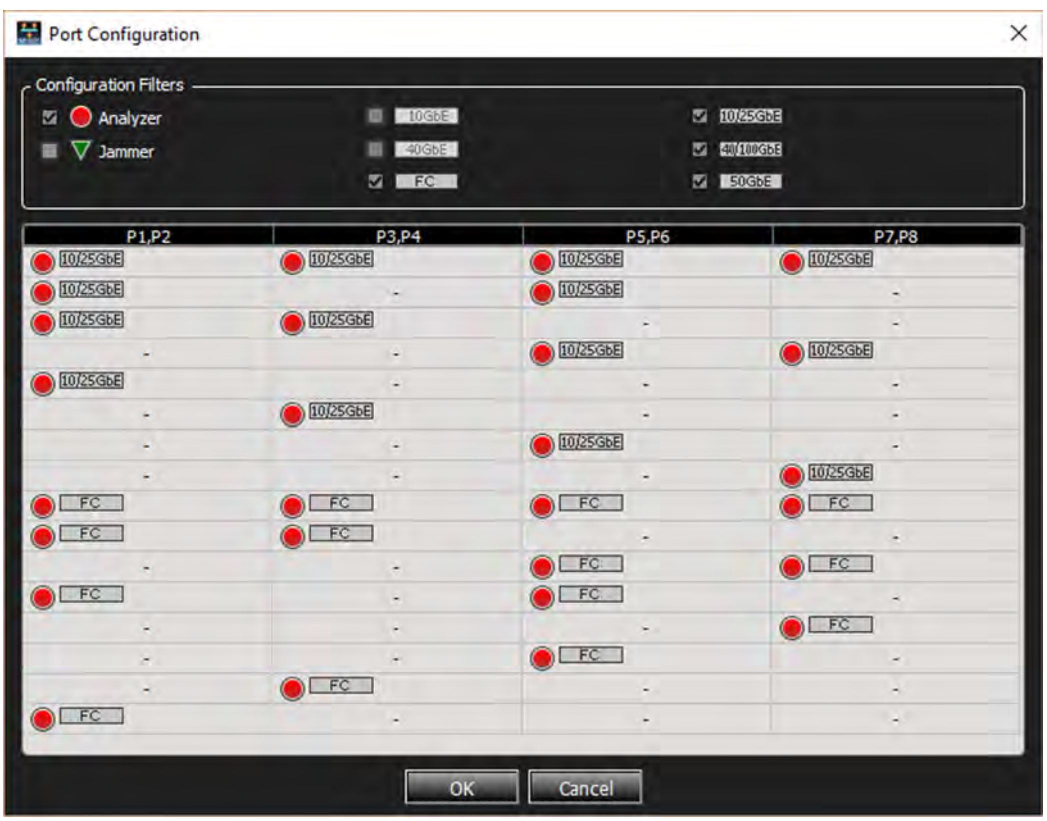


Figure 2.21: Port Configuration – M328Q Analysis

2.2.4.3 Analysis and Jamming

For analysis + jamming the supported jammer port configurations are shown below:

Figure 2.22: Port Configuration, M328Q Analysis + Jamming

- ❑ P1/P2 ports are used for connecting a DUT link. Before Jammer traffic can be assigned to P1/P2 in the trace and After Jammer traffic will be assigned to P3/P4 in the trace. The physical P3/P4 ports on the unit are not used, though their LEDs will reflect the After Jammer link state.
- ❑ P5/P6 ports are used for connecting another DUT link. Before Jammer traffic will be assigned to P5/P6 in the trace, and After Jammer traffic will be assigned to P7/P8 in the trace. The physical P7/P8 ports on the unit are not used, though their LEDs will reflect the After Jammer link state.

2.2.5 Connecting the SierraNet M328 Analyzer

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

1. Connect the Ethernet cable between the SierraNet M328 Analyzer and one of the following:
   - Ethernet Port on the host machine
   - Ethernet switch
   - Gigabit Ethernet interface

   You can also connect a USB cable from the USB port on the Analyzer to the host machine.
2. Connect the Analyzer to a 100V–240V, 50Hz–60Hz, power outlet and turn on the Power switch.

   Once the Analyzer is turned on, the host machine detects the Analyzer, loads the driver files, then the Analyzer undergoes the initialization as shown on the LCD display.
3. Connect your devices under test using either optical modules and fiber cables or appropriate copper cabling, suitable for your configuration.
4. Connect your devices under test to port pairs P1/P2, P3/P4, P5/P6 and/or P7/P8. See Figure 2.23.

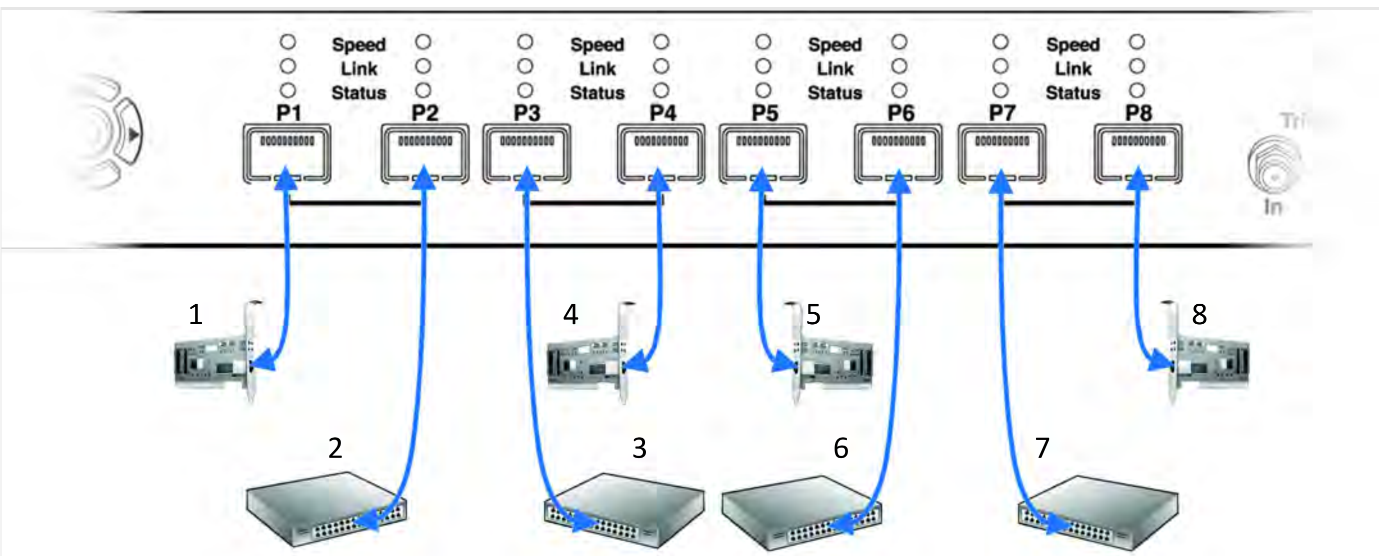


Figure 2.23: M328 Analyzer with SFP+ Connections

2.2.5.1 Cables to Use with M328 Analyzer

Connect to and from devices using optical modules and cables suitable for your setup. Single and multi-mode fiber, active copper, and passive copper cabling is supported.

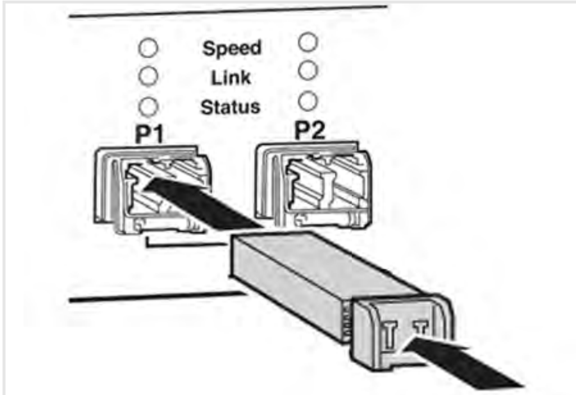


Figure 2.24: M328 Analyzer SFP+ Connections

2.2.5.2 Analysis Configuration

For analysis only, the supported port configurations are A_0_A_0, A_0_0_0 and 0_0_A_0. These are shown in Figure 2.25:

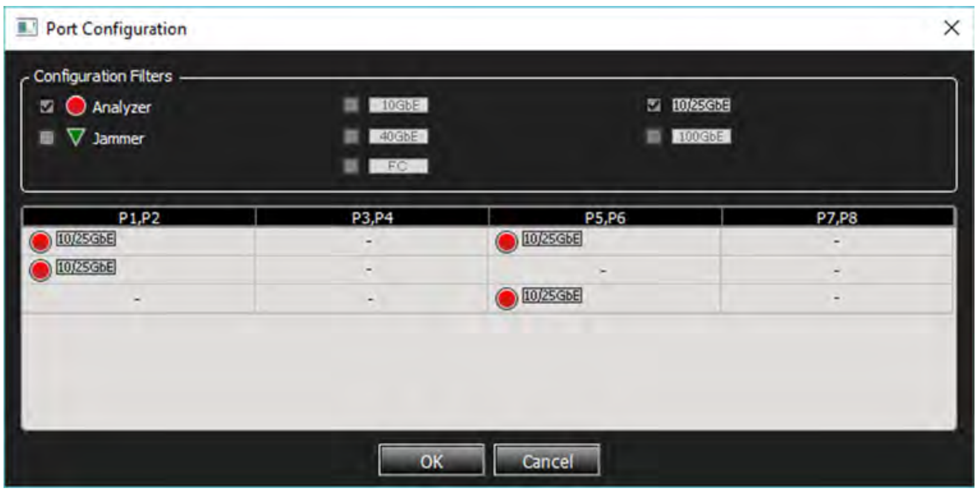


Figure 2.25: Port Configuration, Analysis

2.2.5.3 Analysis and Jamming

For analysis + jamming the supported jammer port configurations are AJA_0_AJA_0, AJA_0_0_0 and 0_0_AJA_0. This is implemented as follows (Figure 2.26):

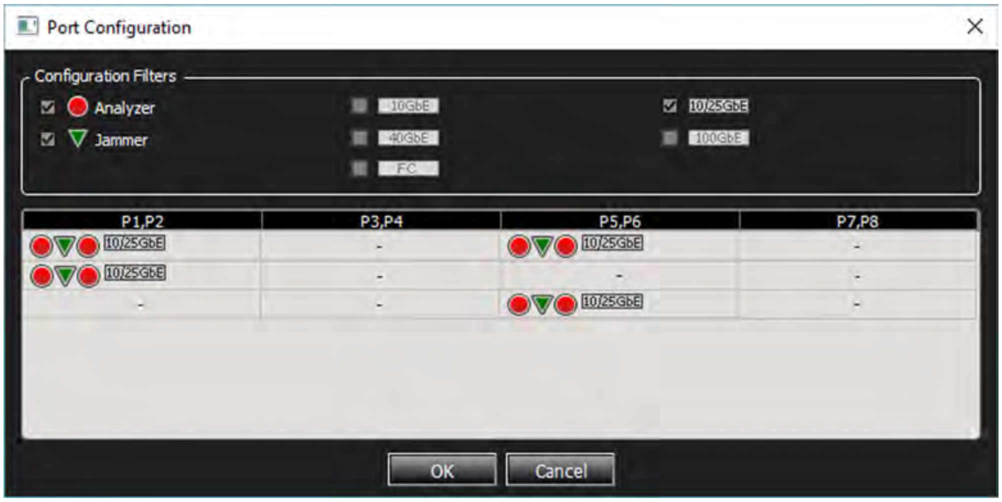


Figure 2.26: Port Configuration, Analysis + Jamming

- P1/P2 ports are used for connecting a DUT link. Before-Jammer traffic is assigned to P1/P2 in the trace and After-Jammer traffic is assigned to P3/P4 in the trace. The physical P3/P4 ports on the unit are not used, though their LEDs will reflect the After-Jammer link state.
- P5/P6 ports are used for connecting another DUT link. Before-Jammer traffic is assigned to P5/P6 in the trace, and After-Jammer traffic is assigned to P7/P8 in the trace. The physical P7/P8 ports on the unit are not used, though their LEDs will reflect the After-Jammer link state.

2.2.6 Connecting the SierraNet M408/M168 Analyzer

NOTE: You must install the software before connecting the Analyzer to the host machine for the first time.

To set up the Analyzer:

1. Connect the Analyzer to a 100V–240V, 50Hz–60Hz power outlet and turn on the Power switch.

   At power on, the Analyzer will go through initialization as shown on the LCD display.

2. Connect the USB cable between the SierraNet M408/M168 USB port and a USB port on the Host PC.

   The host PC operating system detects the Analyzer and configures the drivers automatically. (See 2.5.2, *Connecting via Ethernet* for Ethernet connectivity.)

3. Connect the Analyzer as shown in the following figure, which shows connections between Port-pairs P1-P2 to Device 1 and Device 2; P3-P4 to Device 3 and Device 4; and so on.

4. Bi-Directional data traffic flows through the Analyzer to/from Device 1 through Port 1 and to/from Device 2 through Port 2. Bi-Directional data traffic flows similarly between Devices/Ports 3 & 4, 5 & 6 and 7 & 8.

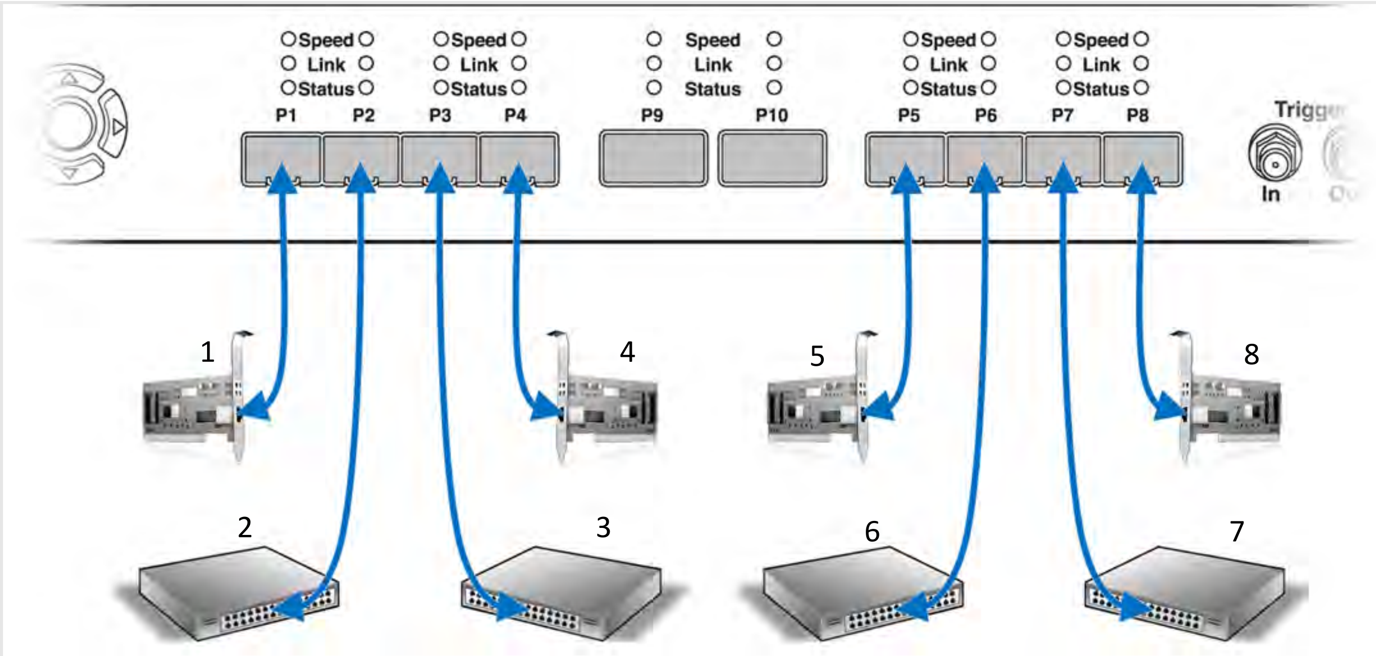


Figure 2.27: Analyzer M408/M168 SFP+ Connections

5. **M408 only** — For QSFP connections, Bi-Directional data traffic flows through the Analyzer to/from Device 9 through Port 9, and to/from Device 10 through Port 10.

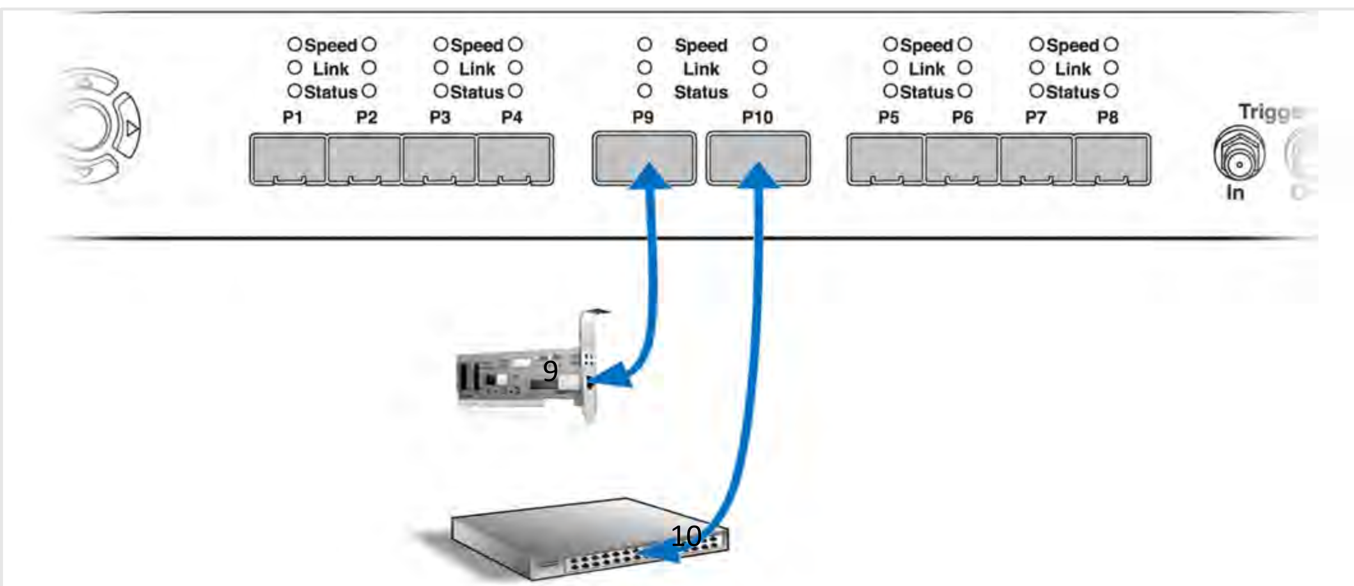


Figure 2.28: Analyzer QSFP Connections

NOTE: The P9/P10 ports are only available on the SierraNet M408.

2.2.6.1 Cables to Use with M408/M168 Analyzer

Connect to and from devices using SFP+/QSFP and a cable suitable for your setup. Single and multi-mode fiber, active copper, and passive copper cabling is supported.

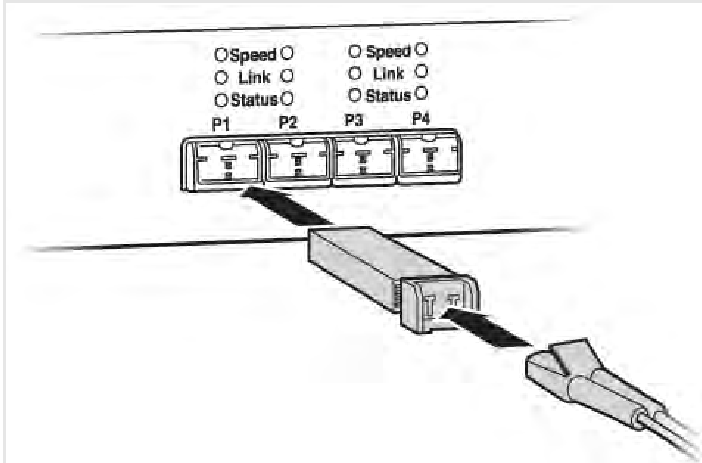


Figure 2.29: Analyzer Connections

For passive copper Ethernet cabling, the M408/M168 has been calibrated to work optimally with the following cables:

- 40 GigE cables (M408 only) — Molex 74757-1101 (1 meter, 30 awg QSFP)
- 10 GigE cables — Molex 74752-2101 (1 meter 28 awg SFP)

2.3 Expandability: SierraNet M1288, M648, T328, M328Q, and M328

You can expand the capacity of the Analyzer by daisy-chaining multiple SierraNet M1288, SierraNet M648, SierraNet T328, SierraNet M328Q and SierraNet M328 Analyzers or connect to other Teledyne LeCroy protocol Analyzers with the CATC SYNC Expansion Cards. The sync ports are built into the SierraNet M1288, SierraNet M648, SierraNet T328, the SierraNet M328Q and the SierraNet328; however, other Analyzers must have CATC SYNC Expansion Cards installed (see below for installation and extraction instructions). See a typical example of 2.4.3, *Daisy-Chaining with CATC SYNC Expansion Cards*.

2.4 Expandability: SierraNet M408 and SierraNet M168

You can expand the capacity of the Analyzer by daisy-chaining multiple SierraNet M408 and SierraNet M168 Analyzers or connect to other Teledyne LeCroy protocol Analyzers with the CATC SYNC Expansion Cards (ACC-EXP-002-X).

You can remove expansion cards with two simple tools.

2.4.1 Installation of Expansion Cards

You can install expansion cards using a Standard (flat head) 3/16" screwdriver.

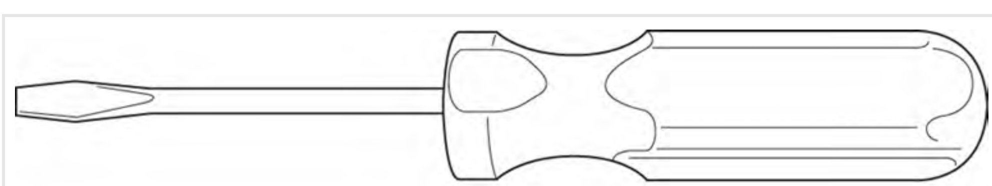


Figure 2.30: Screwdriver needed to Install the CATC SYNC Expansion Cards

1. Find the blank panel on the rear of the Analyzer (Figure 2.31).

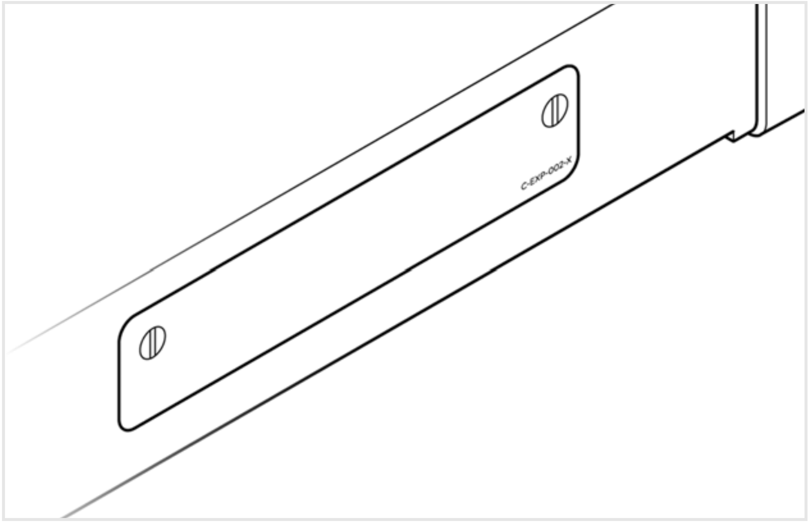


Figure 2.31: Rear of Analyzer: Blank Panel

2. Using a flat-head screw driver (Figure 2.30), loosen the two retaining screws.

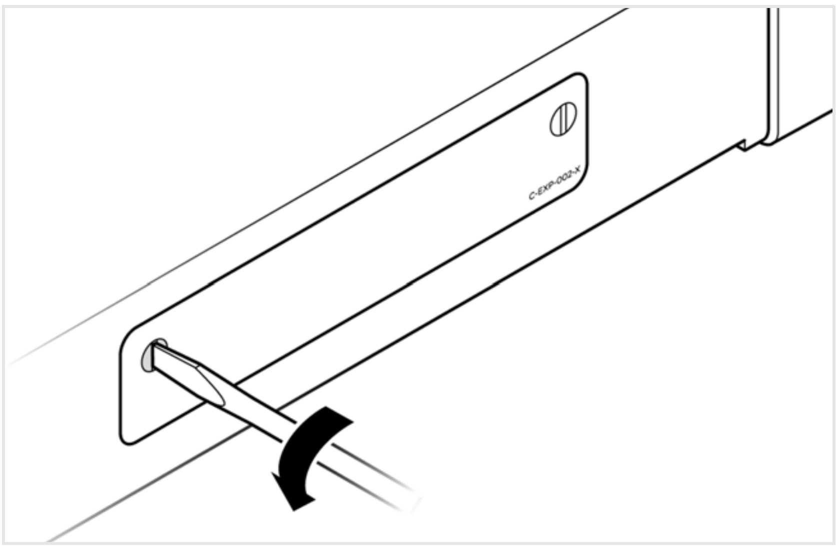


Figure 2.32: Loosen Retaining Screws from Blank Panel

3. Remove the retaining screws and blank panel, exposing the inside of the Analyzer.

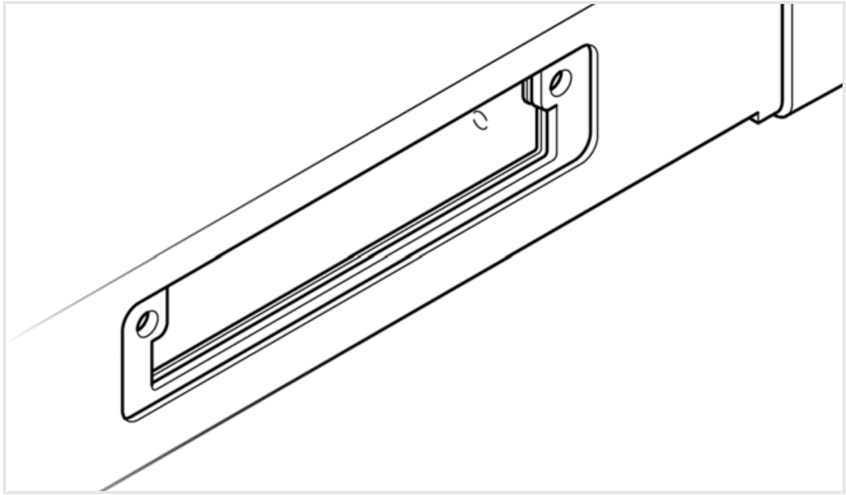


Figure 2.33: Rear of Analyzer with Blank Plate Removed

4. Insert the CATC card into the rear of the Analyzer. Gently push on the back panel of the card until you feel the card seat with the internal connector.

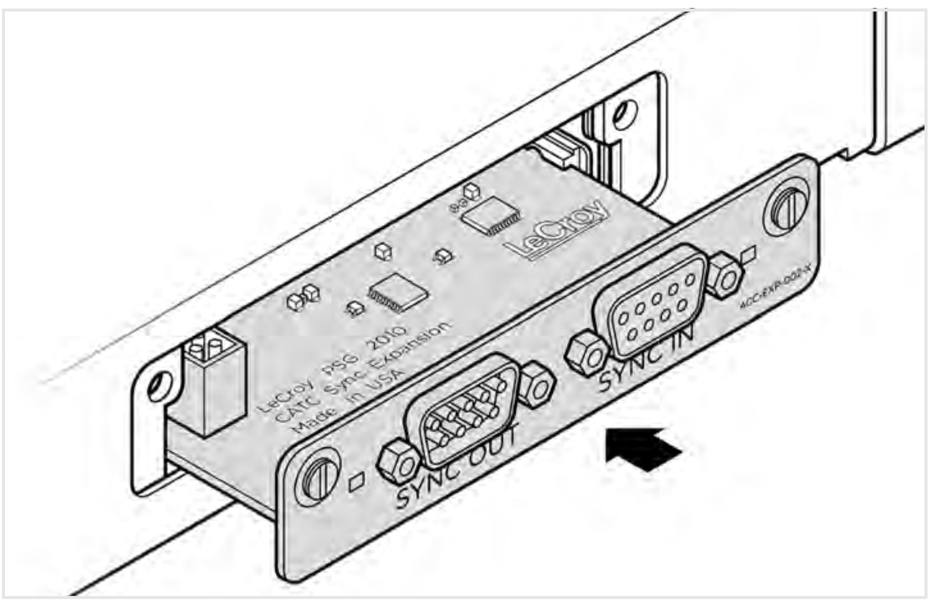


Figure 2.34: CATC Card Being Inserted into Rear of Analyzer

5. After the card is seated, tighten the retaining screws.

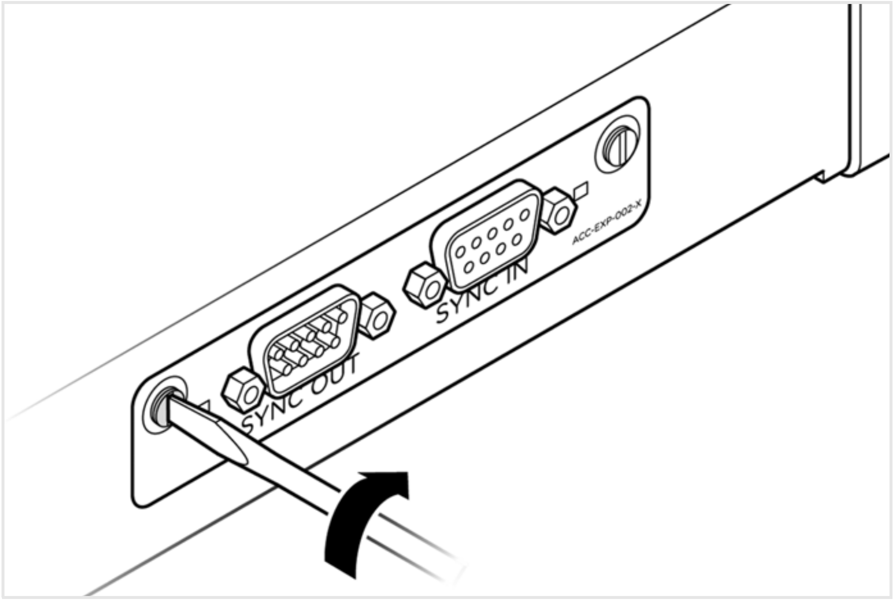


Figure 2.35: Tighten the Retaining Screws on the CATC Card

6. The CATC card can now be connected to other CATC cards in other Analyzers. As described in the next section (2.4.3, *Daisy-Chaining with CATC SYNC Expansion Cards*).

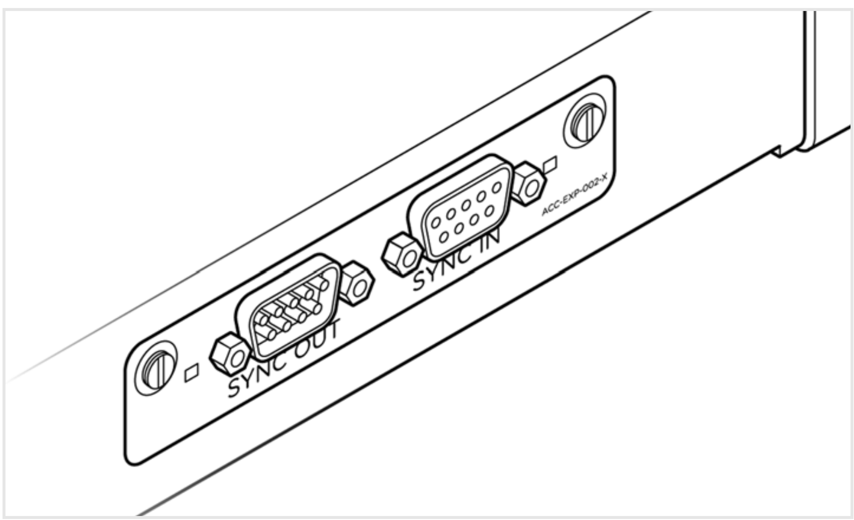


Figure 2.36: Analyzer with CATC Card Installed

2.4.2 Removal of Expansion Cards

You can remove expansion cards using two tools:

- Standard (flat blade) 3/16" screwdriver
- Teledyne LeCroy Extraction Tool (part number 230-0160-00)

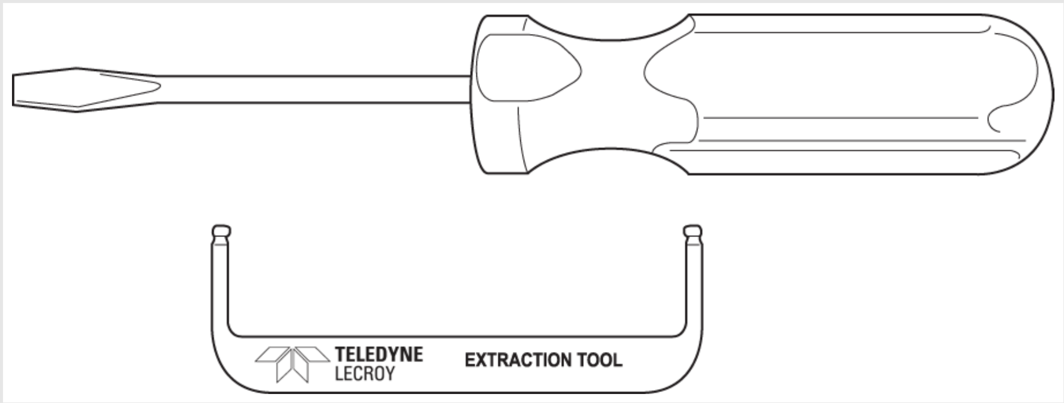


Figure 2.37: Tools needed to Remove the Expansion Cards

To remove an expansion card, follow these steps:

1. Unplug the system from power and turn the system so the expansion port is facing you.

NOTE: There are two retaining screws and the holes for the extraction tool that are located on the panel of the expansion card. See figures Figure 2.38 and Figure 2.39.

2. Using the screwdriver, loosen both retaining screws by rotating them counter-clockwise approximately two full turns, until feeling slight resistance. **Do not force the retaining screws** after two turns.

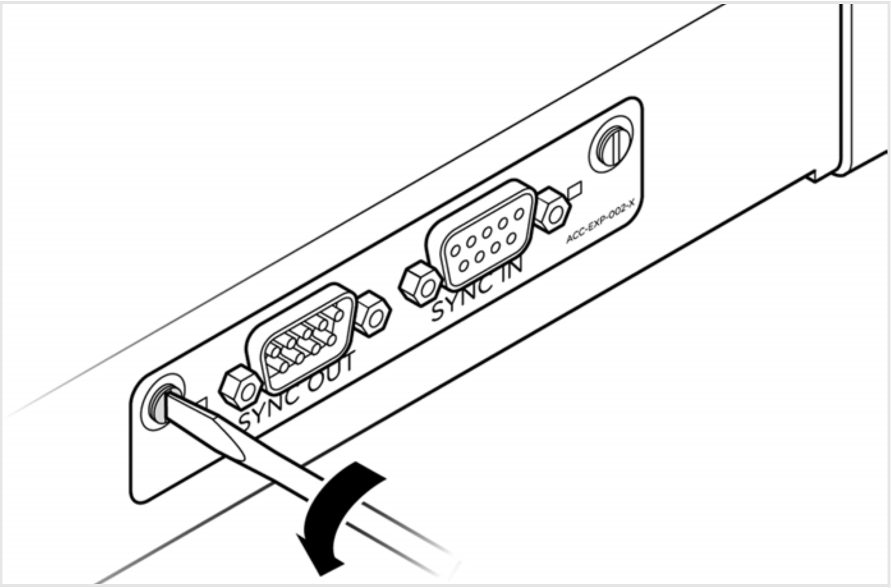


Figure 2.38: Loosen Retaining Screws on CATC Card

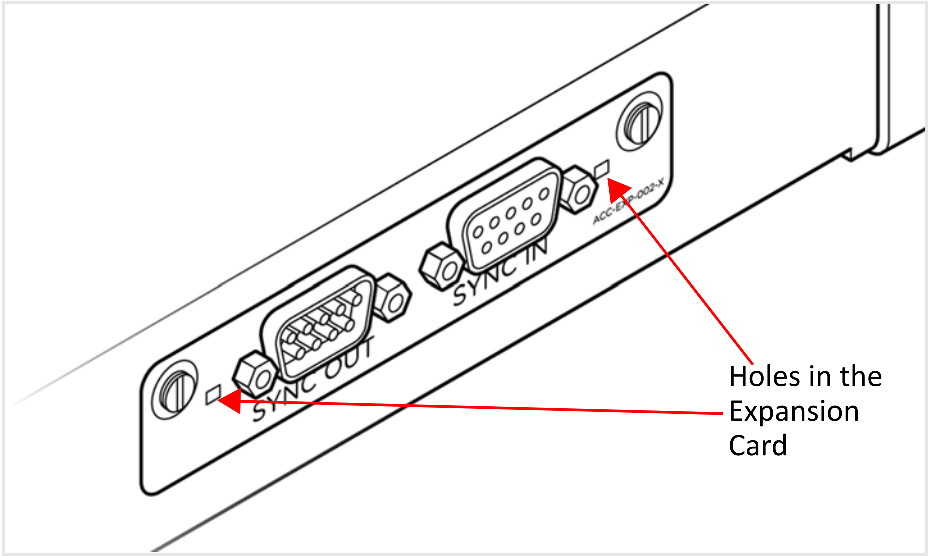


Figure 2.39: Holes in the Expansion Card Panel

3. Insert the extraction-tool prongs into the holes in the expansion card panel.

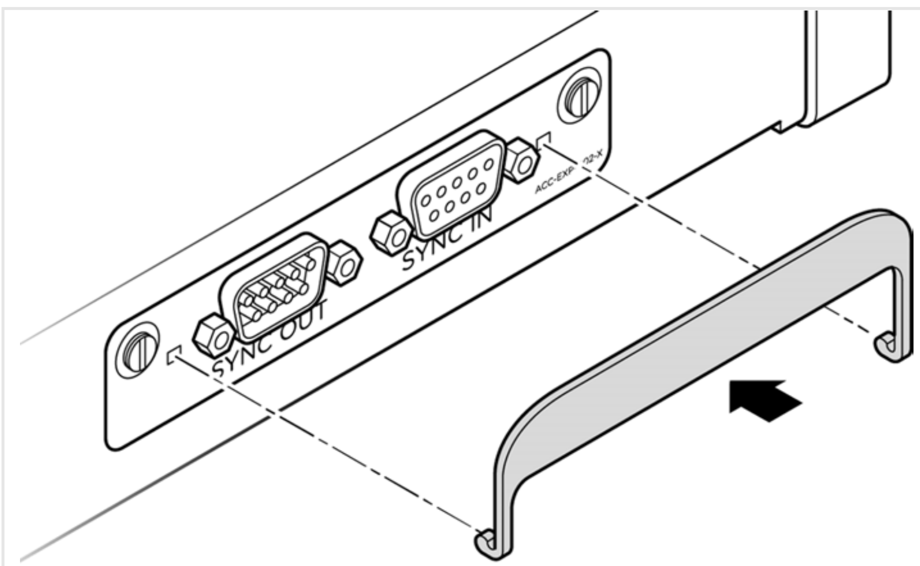


Figure 2.40: Insert Extraction Tool

NOTE: If the prongs do not slip easily into the holes, use a small nail file or similar device to remove paint from the prongs.

---

4. Rotate the extraction tool to a horizontal position to lock the prongs into place and make a handle.

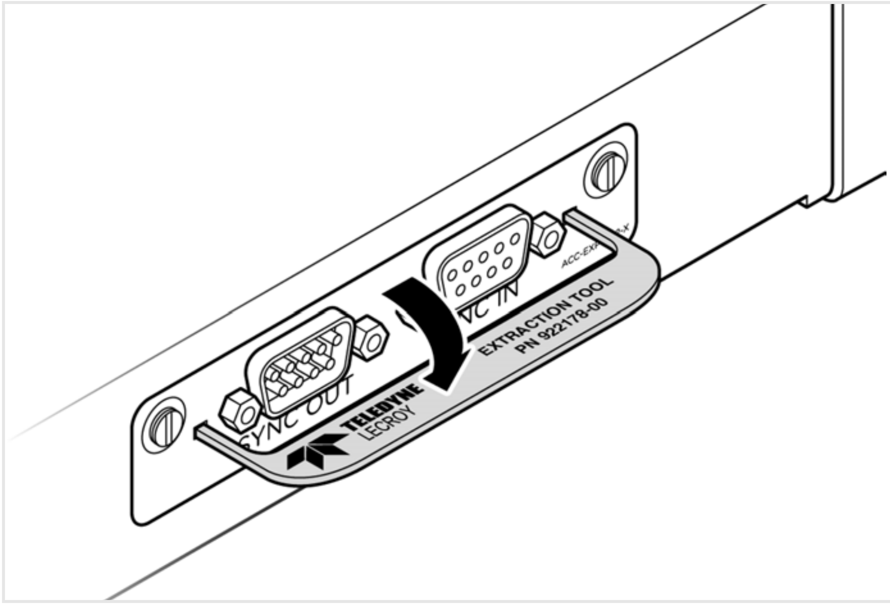


Figure 2.41: Insertion of Handle/Tool into Expansion Card Panel

5. Using the extraction tool as a handle, gently wriggle the expansion card forward, about 1/8" (Figure 2.42).

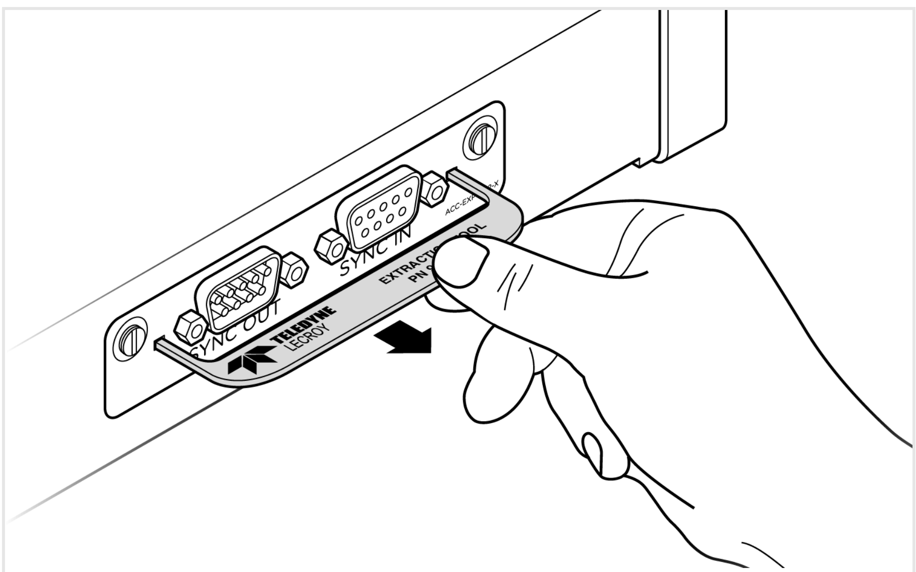


Figure 2.42: Use of Extraction Tool to Remove Card

6. Repeat step 5 approximately three times, until the card is free from the retaining screws and you can remove the card from the system.
7. Replace the CATC Expansion Card with a blank panel and tighten the retaining screws. See Figure 2.43.

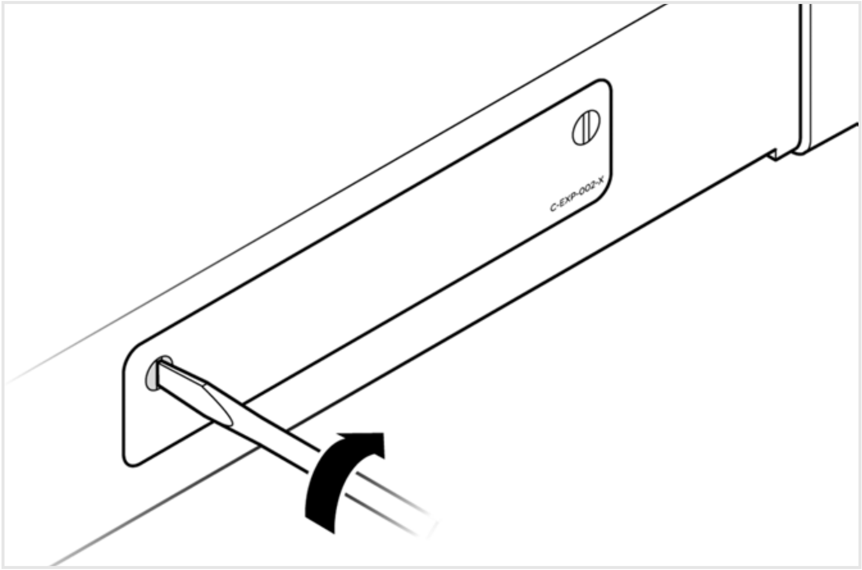


Figure 2.43: Replace Retaining Screws in Blank Panel and Tighten

2.4.3 Daisy-Chaining with CATC SYNC Expansion Cards

You may daisy-chain up to eight Analyzer units for higher port count by connecting the units through the optional CATC SYNC Expansion Card on the Analyzer back.

Daisy-chained Analyzer units will have their time-stamping, recording, and triggering functions synchronized to +/- 100ns. You can daisy-chain any combination of the following Analyzers:

- SierraNet M1288
- SierraNet M648
- SierraNet T328
- SierraNet M328Q
- SierraNet M328
- SierraNet M408
- SierraNet M168

Perform the following steps to connect the CATC Sync ports between two or more Analyzers:

1. Make sure to stop any recordings in progress.

NOTE: You may plug/unplug the sync cable while the Analyzer unit is powered on.

2. Connect the female end of the sync cable to the SYNC OUT port of one Analyzer.
3. Connect the male end of the sync cable to the SYNC IN port of the other Analyzer (Figure 2.44).
4. Repeat steps 2-3 to connect additional units (up to eight total) as needed.

WARNING: DO NOT create a closed loop from the last unit back to the first unit.

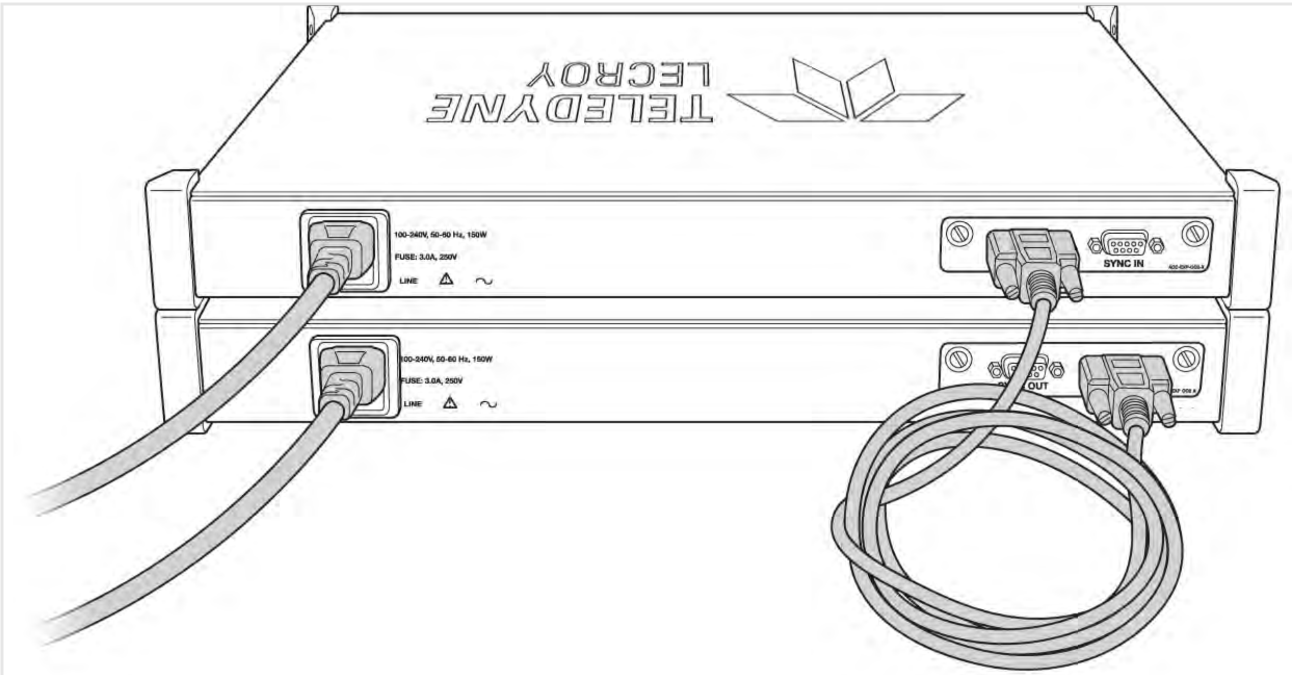


Figure 2.44: An Example of Connecting Two SierraNet M408 Analyzers

2.5 Using the Net Protocol Suite Software

The Net Protocol Suite software application has the following capabilities:

- Hardware Configuration (see 2.5.1, *Device Management*).
- Defining a New Project (see Chapter 3, *Analyzer Startup – New Project*).
- Protocol Analysis (see Chapter 4, *Recording Configuration with Real Time Traffic*).
- Display Manipulation (see Chapter 5, *Trace File Analysis*).
- Error Injection and Traffic Modification (see Chapter 6, *InFusion*).
- Running the Analyzer in Batch Mode (see Chapter 7, *Infusion Batch Test Scenarios*).

IMPORTANT! Power up all units before starting the software.

2.5.1 Device Management

To launch the software, perform the following steps:

1. Double-click the **Net Protocol Suite** Icon in the Program Manager Window.

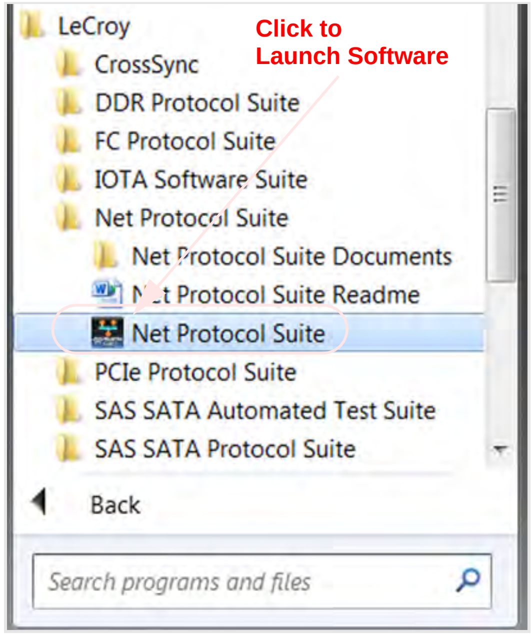


Figure 2.45: Net Protocol Suite Software

This brings up the main Toolbar for the Net Suite Protocol Software (Figure 2.46).

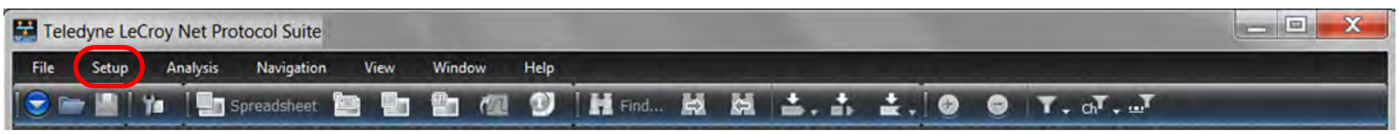


Figure 2.46: Main Toolbar for Net Suite Protocol

2. Click **Setup** → **Device Management** (Figure 2.47). The Device Management dialog window opens (see Figure 2.48).

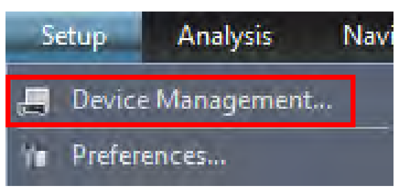


Figure 2.47: Connecting to Device(s).

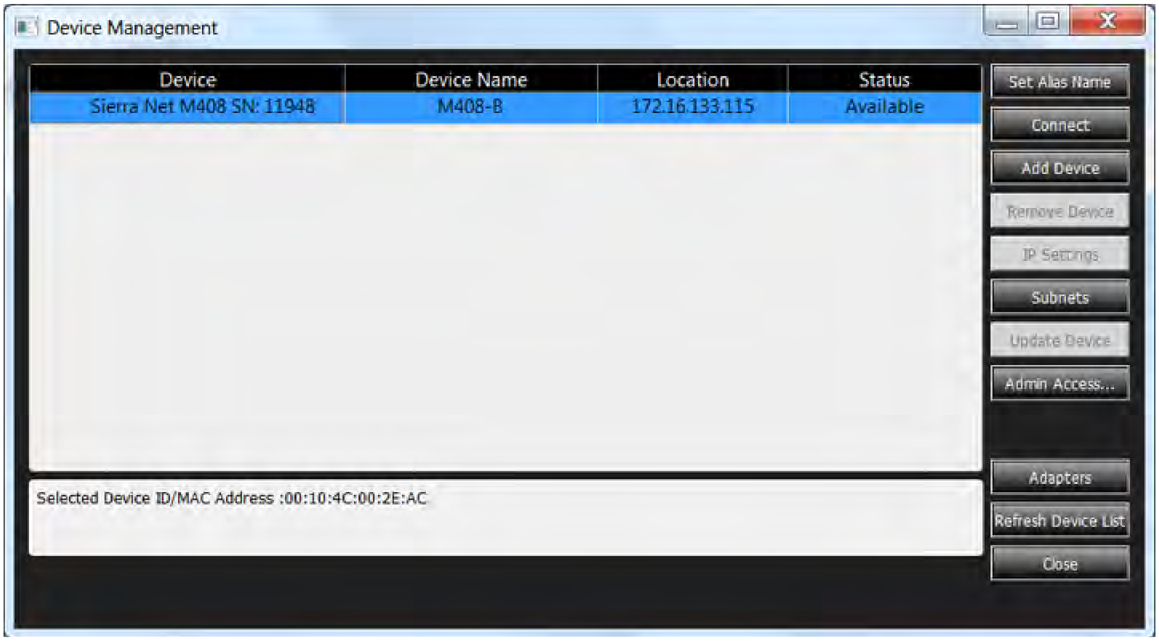


Figure 2.48: Device Management Dialog Window

- **Device:** Analyzer Model Number and Serial Number
- **Device Name**: Analyzer Model Number
- **Location**: IP Address of Analyzer
- **Status**: Ready, Ready to Connect (Available), Connected (connected to your machine), Used By (Being used by someone else – Unavailable)

TABLE 2.2: Analyzer Status

Analyzer Status	Symbol	Description
Available		Device is present and no one else is connected to it or is using it.
Connected		You are connected to the Device.
Activated		You are connected to the device and have assigned it to an open Project.
Used by [hostname]		Another user, on the computer identified by [hostname], is connected to the device.
Unknown		Connection state is unknown; for example, a device that was previously added manually, but may not be present currently.

2.5.1.1 Status of Analyzer

The status of the Analyzer can be found through the Device Management dialog window or by right-clicking on the Analyzer Model Number in the Main Menu.

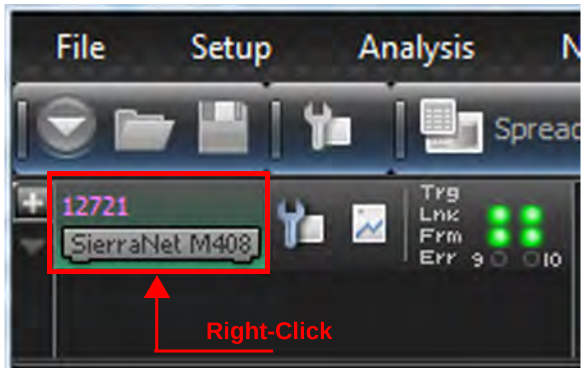


Figure 2.49: Analyzer Status

Some examples of various Status modes are shown in figures Figure 2.49 through Figure 2.52:

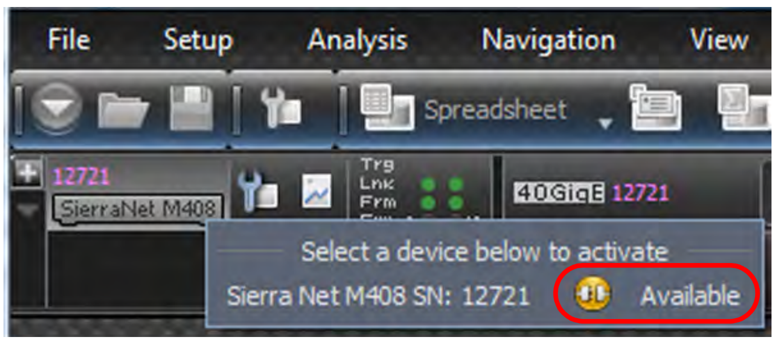


Figure 2.50: Analyzer Status – Available

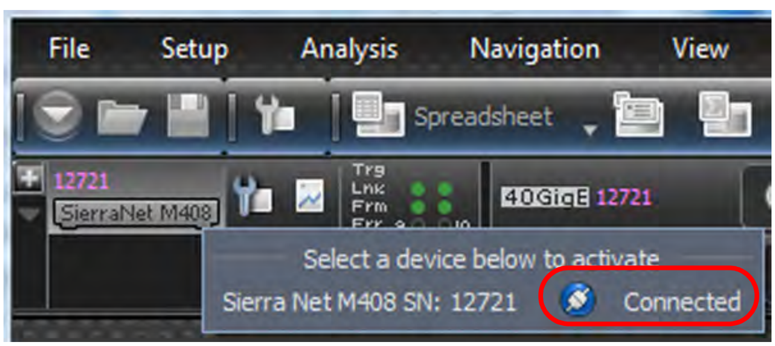


Figure 2.51: Analyzer Status – Connected

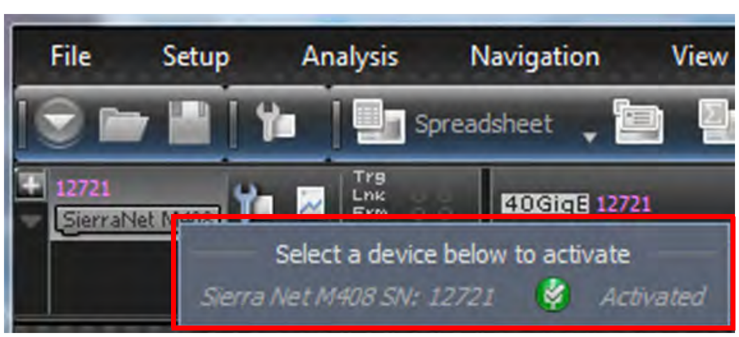


Figure 2.52: Analyzer Status – Ready to be Activated

2.5.1.2 Set Alias Name

Address Alias allows you to assign a meaningful name to each address to assist in interpreting the results displayed in the trace view. To assign address names in an open trace view:

1. Select **Setup** → **Device Management** → **Set Device Alias Name** (Figure 2.53).

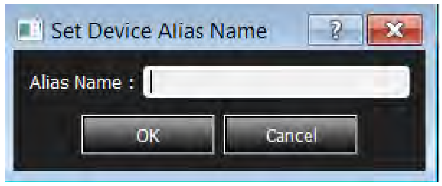


Figure 2.53: Assign Alias Name

2. Assign a meaningful name to each address in use, then click **OK**. The assigned names replace the address in the Trace View, Search, Filter, and Statistical Report.

   If you elect to save the captured trace file, the assigned address names are saved together with the result; therefore, when you open the trace file later, the assigned names are retained.

3. To set these address aliases for trace files that will be captured later, you can set them as Default. New traces will be opened by these default address aliases.

2.5.1.3 Connect/Disconnect

Click **Connect** to connect or click **Disconnect** to disconnect a device.

2.5.1.4 Add Device...

Click **Add Device** to add a device with a static IP address.

Figure 2.54: Add device

NOTE: When entering addresses, you must include the leading zeros. Use 003.010.195.006 as entering 3.10.195.6 will not work. This is also applicable for Figure 2.76.

Find

Click the **Find** button to test if the device at the specified IP address can be located.

Force Add/Connect Attempt

Use this option if the **Find** function fails; however, you must be sure the address is correct to attempt the connection. This setting is stored in the device list database and is applied when attempting to connect to the device.

2.5.1.5 Remove Device

Click **Remove Device** to remove a previously added device.

2.5.1.6 IP Settings

Click **IP Setting** to reset a device IP settings. The following IP Setting dialog box appears (see Figure 2.55).

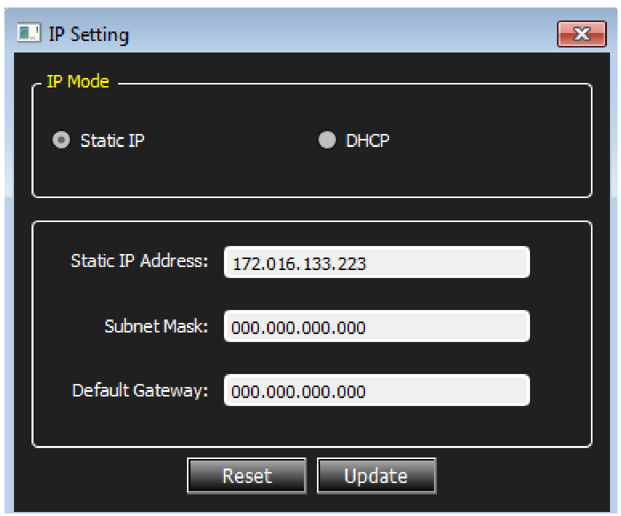


Figure 2.55: IP Setting Dialog Box

2.5.1.7 Subnets

Refer to 2.5.2.4, *Ethernet Connectivity Through a Different Subnet*.

2.5.1.8 Update Device

Click **Update** to update a device (see 2.5.4, *Update Device*).

2.5.1.9 Admin Access

1. Click **Admin Access...** The Administration dialog window appears (Figure 2.56).

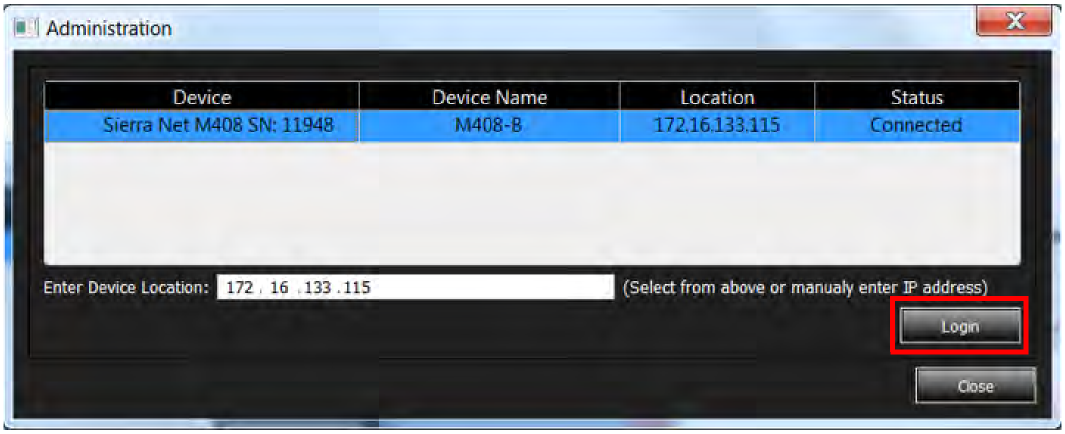


Figure 2.56: Administration Dialog Window

2. Click **Login**. The Administration Functions dialog box appears (Figure 2.57), which allows you to take control of the Analyzer from its current user.

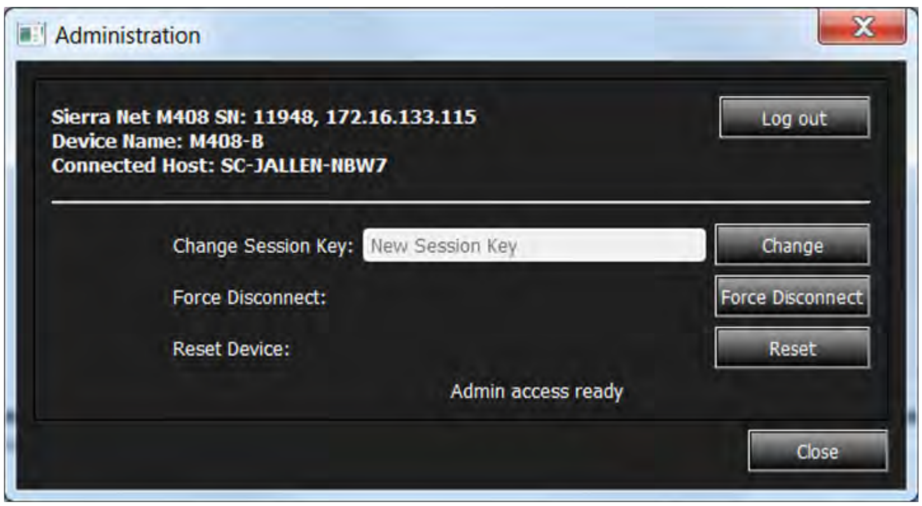


Figure 2.57: Administration Functions

The Administration dialog box displays the Model, Serial Number, and IP address of the Analyzer to which you are connected. The Device Name and the name of the Connected Host (your computer) are also displayed.

Functions available in the Administration dialog box include:

- **Log out**—Takes you back to the Admin Access dialog (Figure 2.56)
- **Change**—Change the Session Key (*Change Session Key*)
- **Force Disconnect**—Disconnect the Current User from the Analyzer (*Force Disconnect*)
- **Reset**—Reset the Analyzer (*Reset Device*)
- **Close**—Close the Admin Access dialog and return to the Device Management dialog

Change Session Key

Enter a new session key in the Change Session Key field and click **Change**. You can chose a combination of letters and numbers.

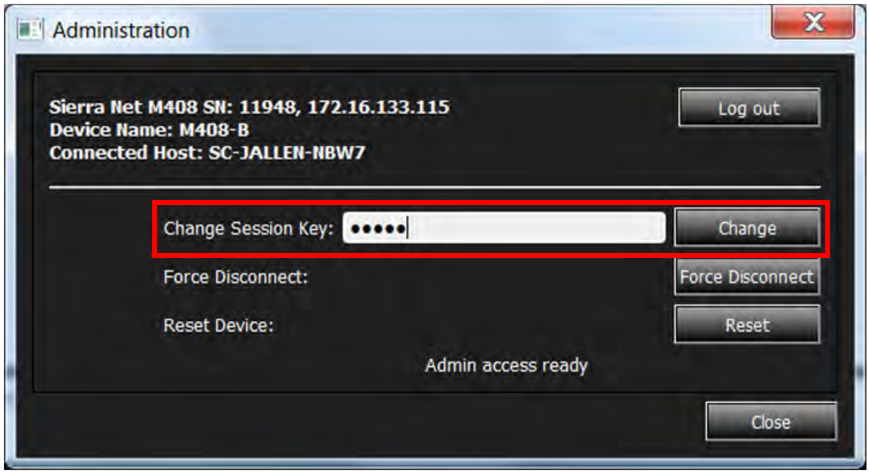


Figure 2.58: Change Session Key

If successful, the following confirmation pops up (Figure 2.59).

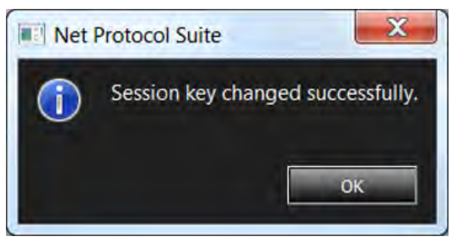


Figure 2.59: Confirmation of Successful Session Key Change

See 3.2.1.1, *Resume Session* for more details about continuing to record a session while not physically connected to the Analyzer.

Force Disconnect

Click the **Force Disconnect** button to force the current user off of the Analyzer.

- A pop-up box appears confirming you were successful (Figure 2.60).
- A confirmation pop-up box also appears if you successfully disconnected (Figure 2.61).

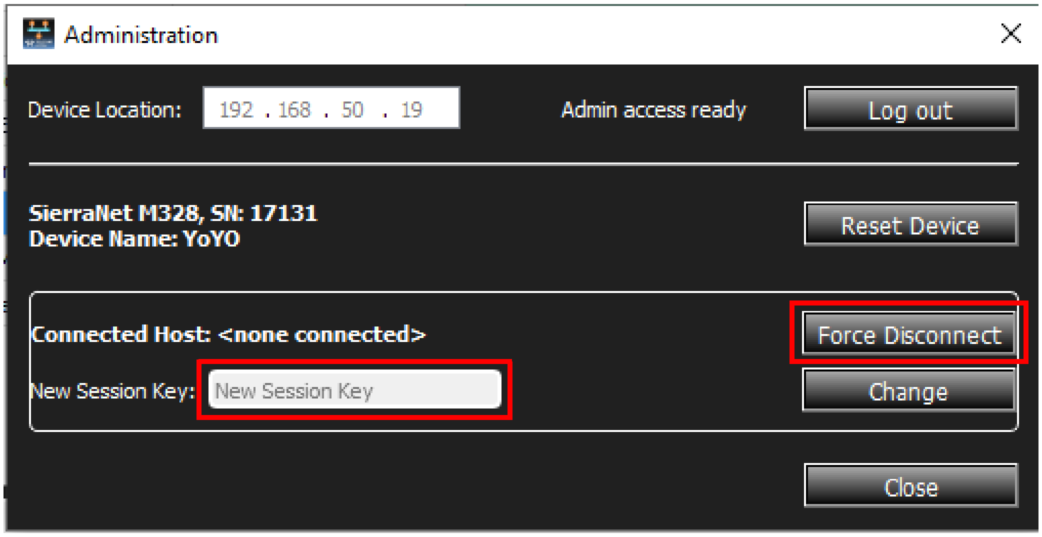


Figure 2.60: Administration Dialog Box – Forced Disconnect Successful

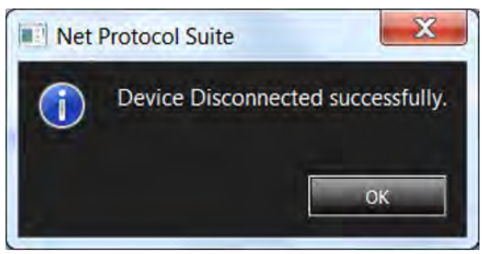


Figure 2.61: Device Disconnected Successfully Confirmation

The Device Management window will reflect the new status of the Analyzer (that it is now Available for someone else to use). See Figure 2.62.

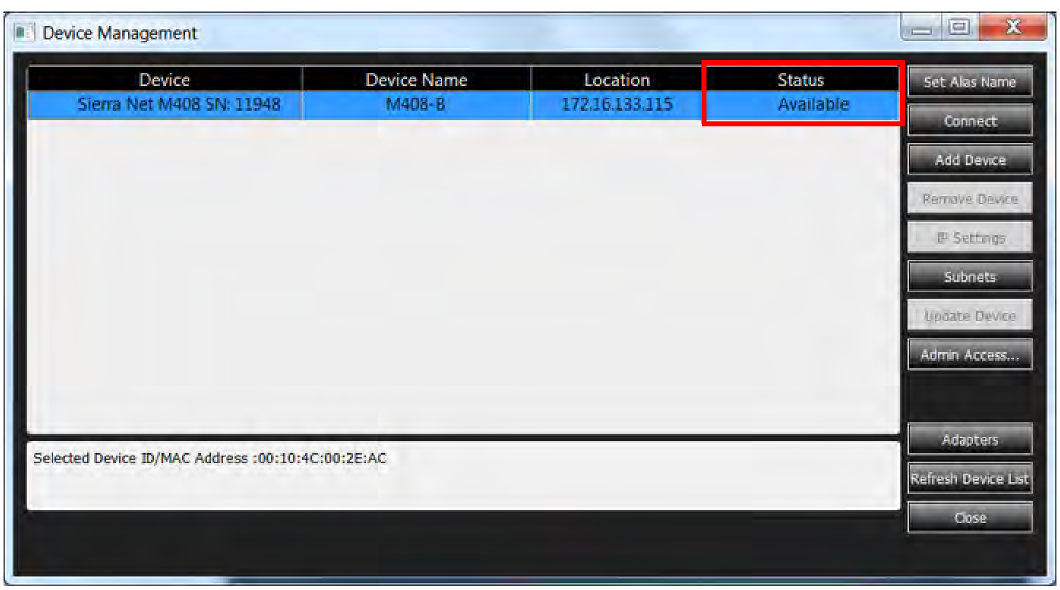


Figure 2.62: Device Status After Forced Disconnect

Reset Device

Click the **Reset Device** button to reset the device. Initially, you will see the following Administration window. See Figure 2.63.

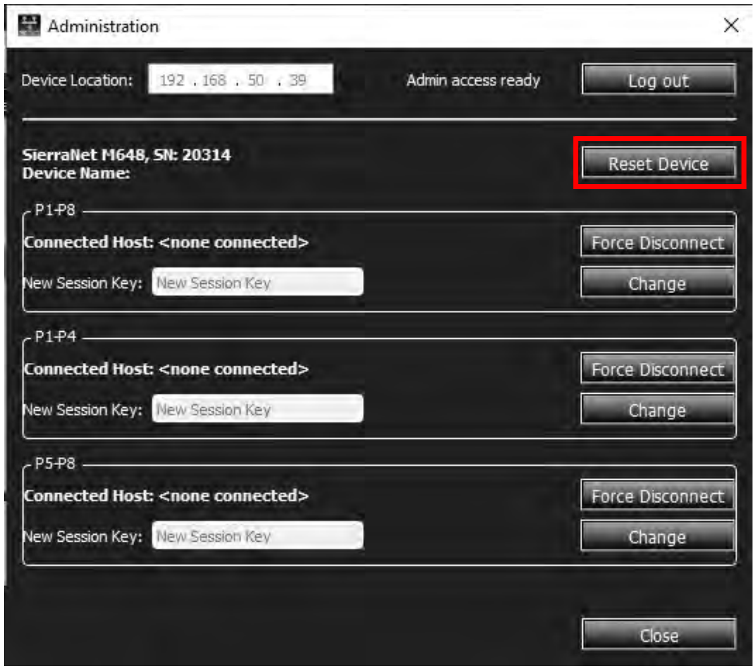


Figure 2.63: Administration Window – Reset Process

Once the Reset cycle is complete, a pop-up box appears with a confirmation message (Figure 2.64).

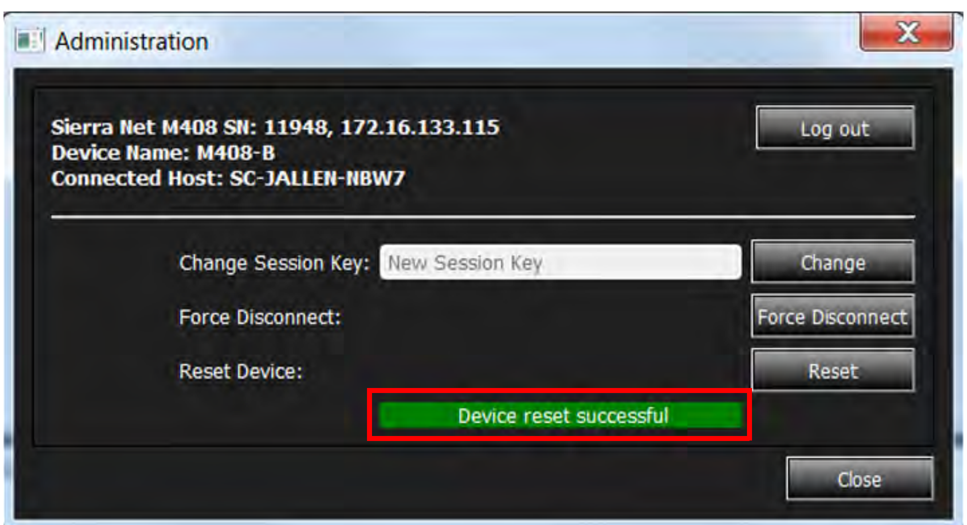


Figure 2.64: Device Reset Successful

Close

The **Close** button simply closes the Administration dialog box and returns you to the Device Management window.

2.5.1.10 Adapters

Click **Adapters** to select the network adapter to use for connecting to Ethernet-connected devices. The Select Adapter dialog window appears (Figure 2.65).

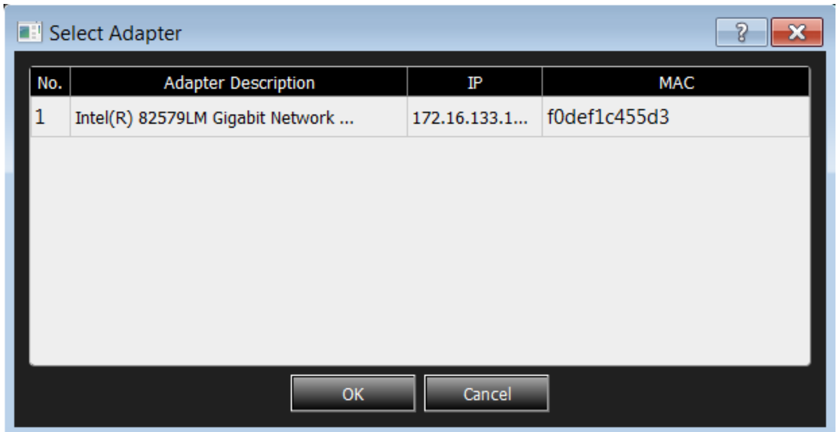


Figure 2.65: Select Adapter Dialog Window

NOTE: Some PCs have multiple adapters for connecting to different networks; therefore, be sure to choose the one to which your desired device is connected.

2.5.1.11 Refresh Device List

1. From the Device Management window, click **Refresh Device List**.
2. To connect to a device, select a device that is Ready to Connect and click the **Connect** button on the right.

   The Connection Properties pop-up box appears (see the following screen capture).

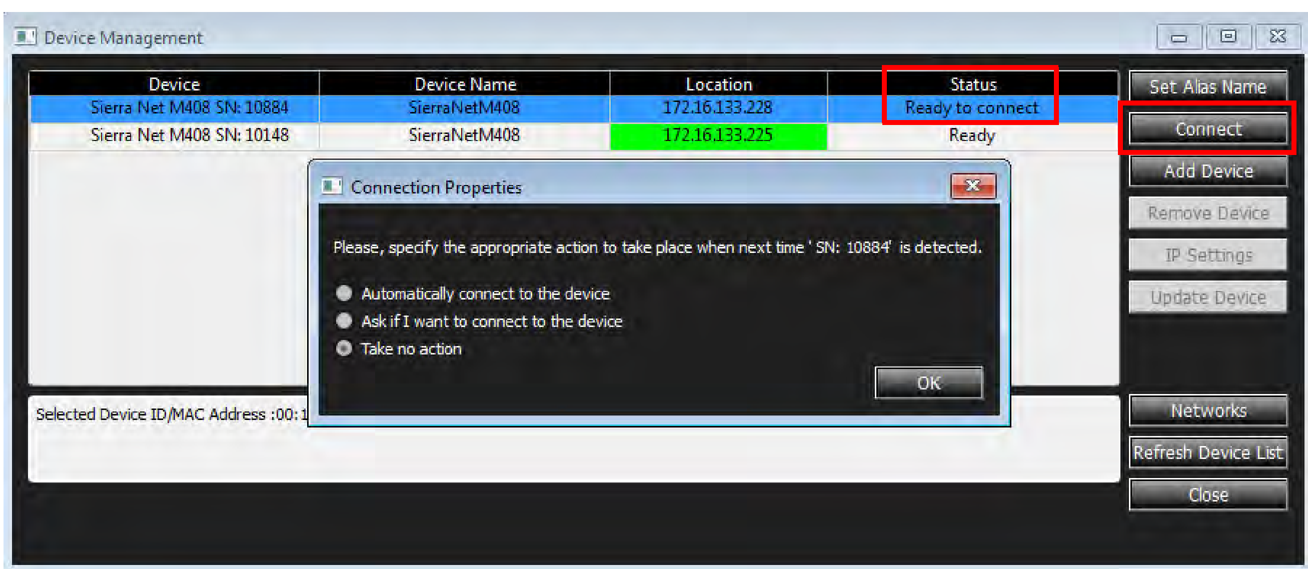


Figure 2.66: Connection Properties Dialog

3. Specify an action from the following:
   - Automatically connect to the device
   - Ask if I want to connect to the device
   - Take no action

   If you select **Automatically connect to the device**, the next time the application opens, the device will be automatically connected.

   In the Device Management window, daisy-chained units are displayed in the *Device* column with a **[** (square bracket) symbol. The sequence of units is shown in the *Order* column. See Figure 2.67.

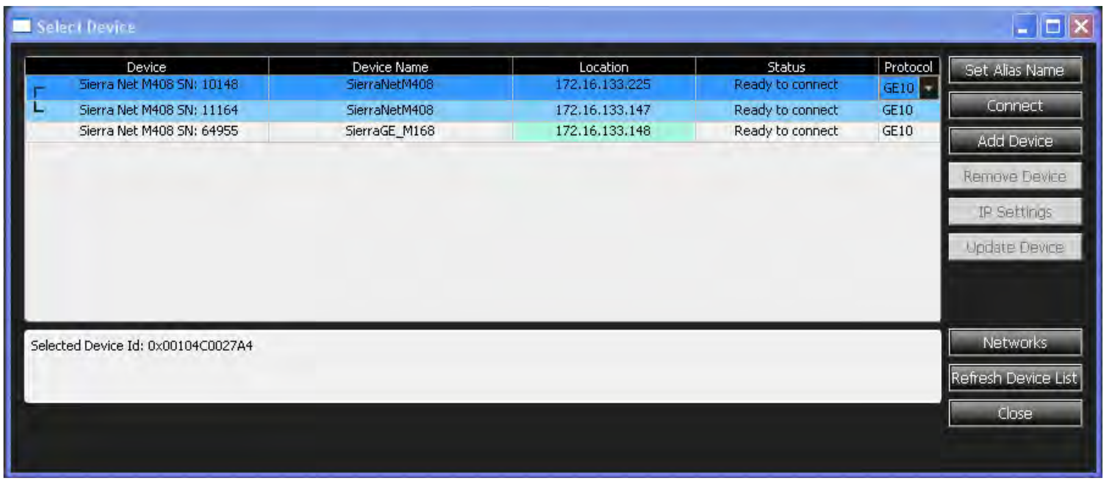


Figure 2.67: Device Management – Unit 1 & Unit 2 Daisy-Chained Together

NOTE: When using the CATC Sync cards, the order is automatically detected.

2.5.2 Connecting via Ethernet

The Ethernet connection can have any of these configurations:

- Analyzer connected to the host computer (machine running the application software), using a switch, Gigabit Ethernet interface, or similar device.
- Analyzer connected directly to the host computer using an Ethernet crossover cable. To connect via USB refer to 2.5.3, *Connecting Via USB*.

2.5.2.1 Connecting to a Network

When connected to a network, the Analyzer can communicate with the DHCP server to obtain its IP address configuration. The client needs to send a request to the DHCP server to obtain an IP. The server sends only one reply, but does not necessarily send the available IP address.

The SierraNet products use the following ports:

- TCP Ports: 3999 – 4003
- UDP Ports: 4033 – 4035

NOTE: To use the Dual User support, you must open the following TCP Ports on your network firewall: 5000 to 5003; 6000 to 6003.

Ask your IT department to add the above ports to your firewall exceptions.

2.5.2.2 Connecting using a Switch, or Similar Device

If the Analyzer and the host PC on which the application is running are on the same Ethernet subnet, the application automatically detects the SierraNet M408 Analyzer. If the Analyzer and the host PC are located on different subnets, then the IP address of the Analyzer needs to be configured manually in the application.

To add the IP address to the Select Device dialog, use the **Add Device** button (refer to 2.5.1.4, *Add Device...*). See Figure 2.55 to set the IP address.

2.5.2.3 Connect Analyzer Directly to Host Machine with Crossover Ethernet Cable

SierraNet M408 Systems are designed to connect to host PCs using a network connection, which allows the user to control the SierraNet M408 System from a local or remote host system. When connected to the host machine using a crossover Ethernet cable, the Analyzer must be given a static IP address such that it will reside on the same subnet as the Ethernet interface of the host computer. See Figure 2.55 to set the IP address.

2.5.2.4 Ethernet Connectivity Through a Different Subnet

The default discovery mechanism relies on broadcast messaging, which typically does not traverse between different subnets. Thus, alternate mechanisms are required to discover devices on different subnets. This section describes two methods: *Automatic Subnet Scanning* (below) and adding a device manually (refer to 2.5.2.6, *Connecting Manually*).

Automatic Subnet Scanning

The software can be configured to automatically discover devices on other subnets. This section describes how to add subnets so that the software will scan them for available devices. To do this, you must specify which subnets you would like the software to scan.

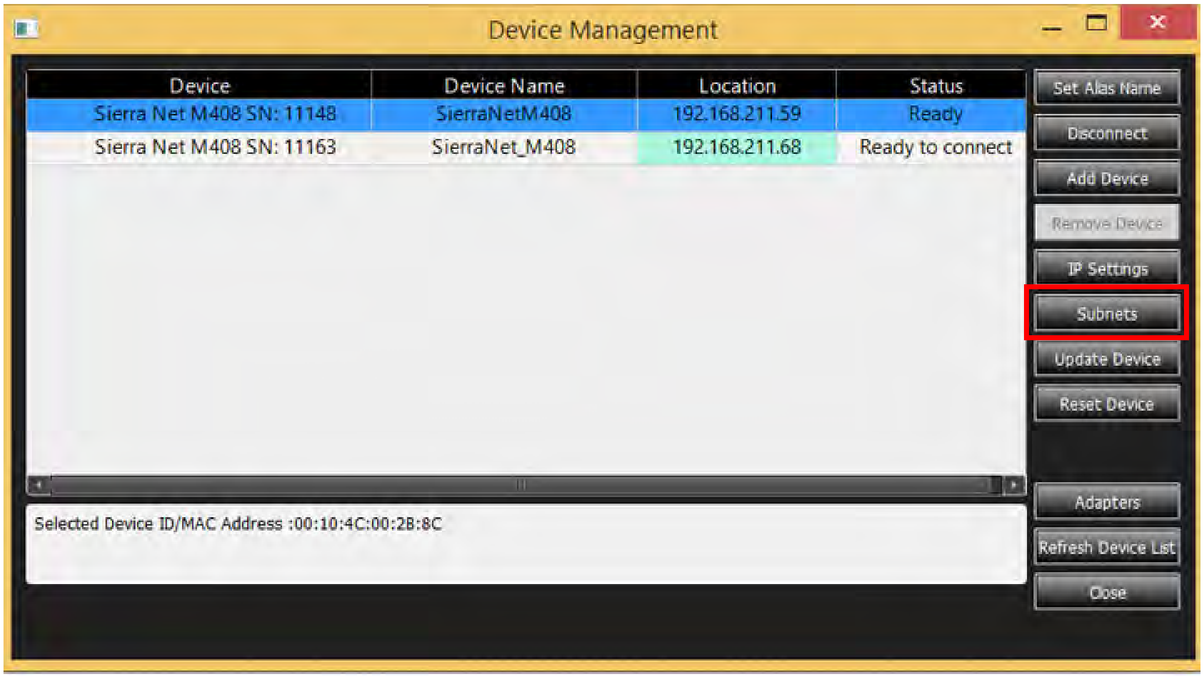


Figure 2.68: Device Management Window

Manage Additional Subnets

1. From the Main Toolbar (Figure 2.46), select **Setup** → **Device Management**. The Device Management window opens (Figure 2.68).
2. Click the **Subnets** button.
   - The *Manage Additional Subnets* window appears (Figure 2.69), which shows the existing subnets and allows you to add or remove them.

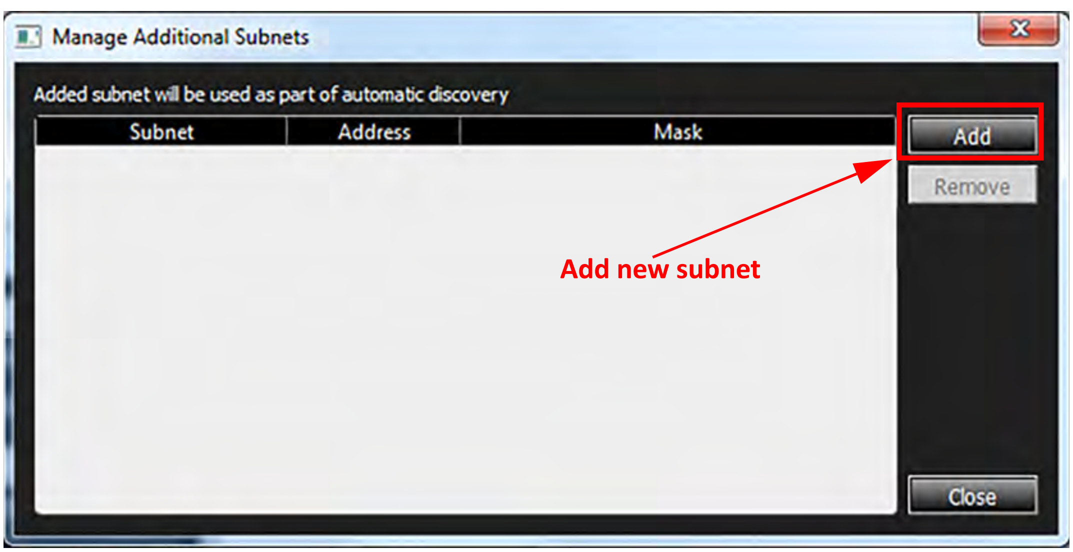


Figure 2.69: Manage Additional Subnets Dialog

   - Subnets in this list will be saved (e.g., to the Windows registry).

3. Click the **Add** button to add another subnet.

4. Add a Meaningful Name to the Subnet:

   a. Type the new name into the subnet Name field (Figure 2.70).

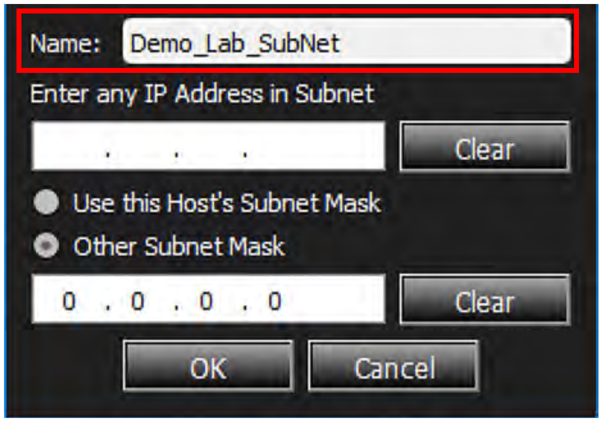


Figure 2.70: Adding a Meaningful Name to a Subnet

   b. Enter an IP Address for the Subnet (Figure 2.71).

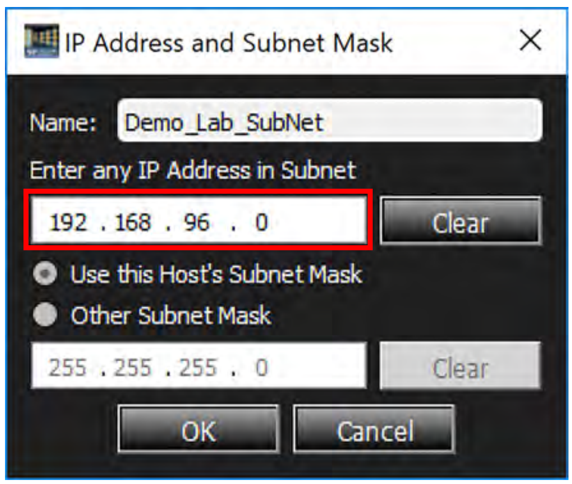


Figure 2.71: Adding a Subnet with Host Mask

By default, the Host subnet mask is used since it is very likely that, in enterprise environments, different subnets will still have the same mask. However, the option to provide another subnet mask is provided. See Figure 2.72.

NOTE: A subnet is identified by a network IP address and a subnet mask, so both parameters must be specified.

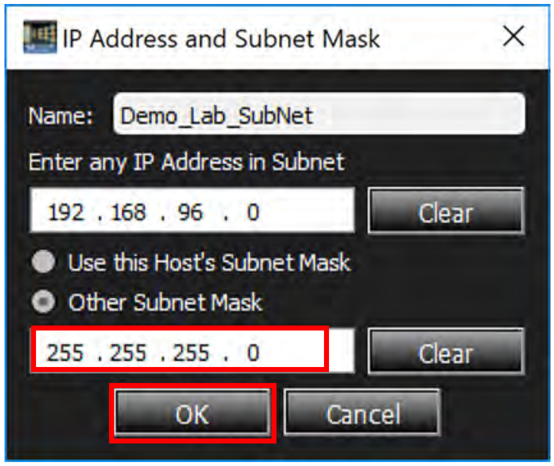


Figure 2.72: Adding a Subnet with a Different Mask

The software will validate the subnet to ensure it is not the same as the Host subnet.

3. Click **OK** to add the new Subnet to the network (Figure 2.73).

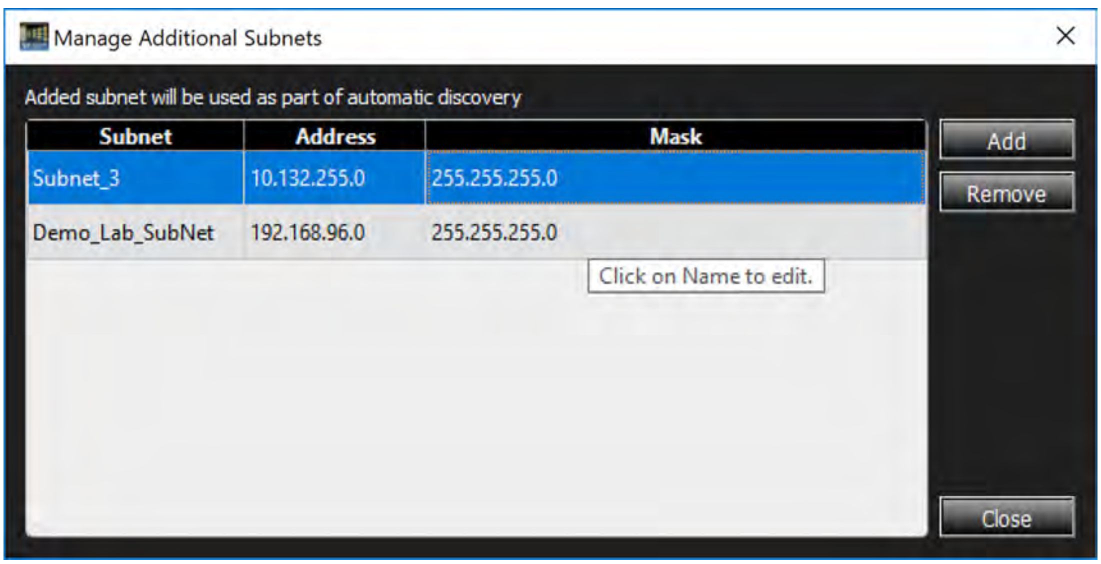


Figure 2.73: New Subnet Added to Network

2.5.2.5 Change the Name of a Subnet

1. From the Main Toolbar (Figure 2.46), select **Setup** → **Device Management**. The Device Management window opens (Figure 2.68).
2. Click the **Subnets** button to open the Manage Additional Subnets window.
3. To change the name of the Subnet, select the Subnet and type a new name.
4. To change the Address and Mask of the Subnet, select the Subnet you want to change, then do the following:

   a. Click **Remove**.

   b. Click **Add** and enter the new Name, Address, and Mask (Figure 2.74).

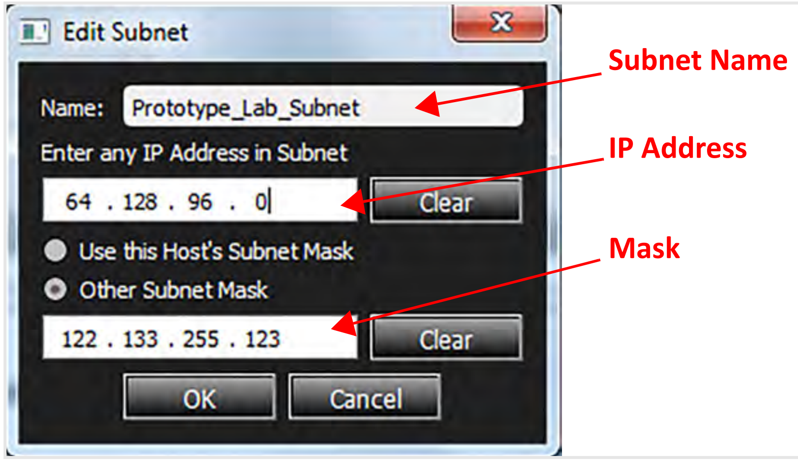


Figure 2.74: Update Subnet

c. Once you have completed the changes, click **OK**. An example of the changes can be seen in Figure 2.75.

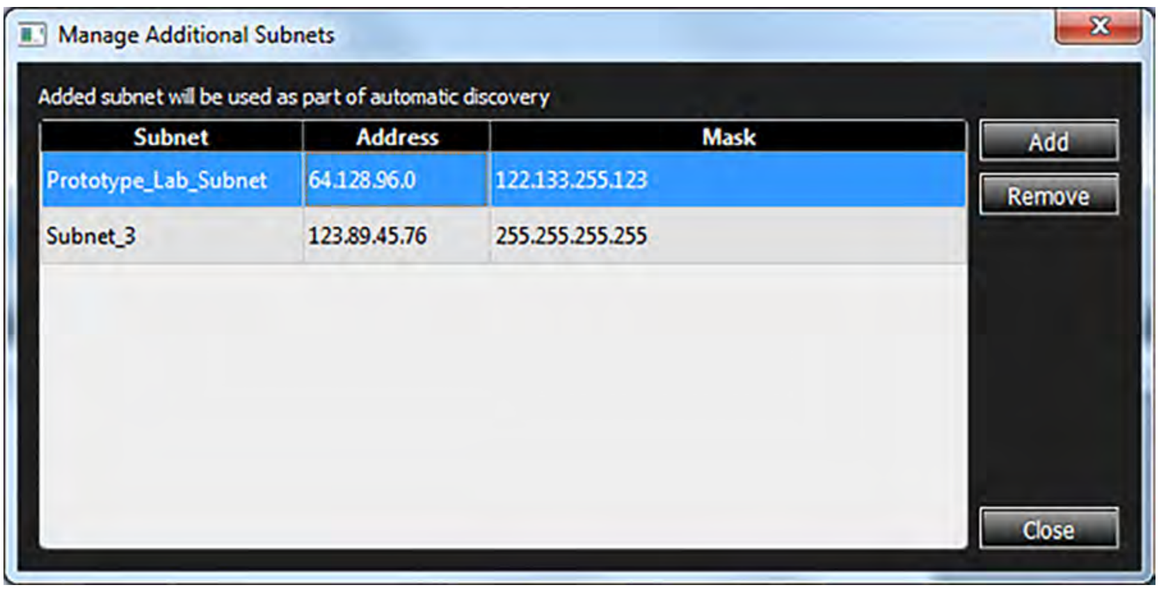


Figure 2.75: Updated Subnet Information

2.5.2.6 Connecting Manually

If the device cannot be discovered through Automatic Discovery, you can find it directly if you know its IP address. In this case, the SierraNet M408 IP address must be added manually. To do this, perform the following steps:

1. From the Main Toolbar (Figure 2.46), select **Setup → Device Management → Add Device**. The Add Device With Static IP dialog window appears.
2. Enter the IP address of the device you need to add.

Figure 2.76: Add New Device with Static IP Address

3. Click **OK**.

   Once the IP address is added, the application will then send a connection request to that IP address to connect to the SierraNet M408 System.

Set Up the IP

This section describes how the SierraNet M408 System is connected (see 2.5.1.6, *IP Settings*).

Ethernet Configuration

There are two ways to configure the SierraNet M408 for network connectivity:

- **DHCP** automatically assigns an IP address. DHCP is the default.
- **Static IP** prompts you to enter a specific IP address.

The SierraNet M408 can be configured from the unit itself using the five buttons and the LCD display on the front panel of the Analyzer. For additional information, see 1.11.1, *LCD Display and Button Functions for Analyzer Host Connection Setup*.

Dynamic Configurations

Dynamic configuration uses DHCP (Dynamic Host Configuration Protocol).

Under DHCP, SierraNet M408 will issue a broadcast to any DHCP Server requesting configuration. If a DHCP server is present on the network, it will assign an IP address, Subnet Mask, and a default GATEWAY (a router port IP address) to the SierraNet M408. The Gateway port will be used by SierraNet M408 to forward events to IP addresses that do not reside within the same subnet.

When using the dynamic configuration, the front panel display will only update the IP address.

The subnet mask and gateway address will remain at the last values programmed.

(000.000.000.000 by default, or whatever was last programmed in the static configuration). While in dynamic mode, these parameters will have been programmed within the IP STACK inside the SierraNet M408, but are not displayed in the LCD.

To change from DHCP to Static IP, select **Setup** → **All Connected Devices** → **IP Settings** from the menu bar.

NOTE: If you are connected to the device using Ethernet, changing the IP Address will cause the connection to drop. You will need to reconnect using the new IP Address.

If the gateway is not configured properly, you must manually change the setting with the front panel configuration buttons.

The IP Setting dialog box appears. For IP Mode, two radio buttons are available: **Static IP** and **DHCP**. DHCP is the default (see Figure 2.77).

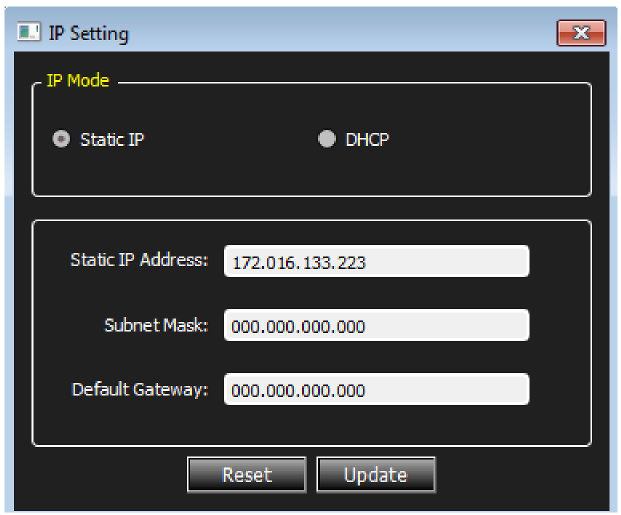


Figure 2.77: Static IP Setup Dialog Box

Static Configurations

Within static configurations, SierraNet M408 must be manually programmed with an IP address, Subnet Mask, and a default Gateway.

Once SierraNet M408 has been programmed with the static network configuration, it will broadcast a UDP message on its own subnet stating that is on line and available for connection.

NOTE: This broadcast is only on the subnet that includes the SierraNet M408 System.

When the application is started on the host machine, it will broadcast a UDP message on its own subnet asking all SierraNet M408s available to identify themselves.

NOTE: This broadcast is only on the host machine subnet.

If the host machine and the SierraNet M408 System reside on the same subnet, they will see each others' broadcasts and the application will automatically populate the Select Device list.

To change to a Static IP:

1. In the IP Setting dialog box, click the **Static IP** radio button.
2. Enter the **Static IP Address**.
3. Enter the **Subnet Mask**.
4. Click **Update**. A pop-up box with a Warning Message appears.
5. Click **Yes**. If the change is successful, a confirmation pop-up message appears.
6. Click **OK**. The message closes and the device resets.
7. To return to DHCP, in the IP setup dialog, click the **DHCP** radio button, then click **Update**. The Warning pop-up box appears.

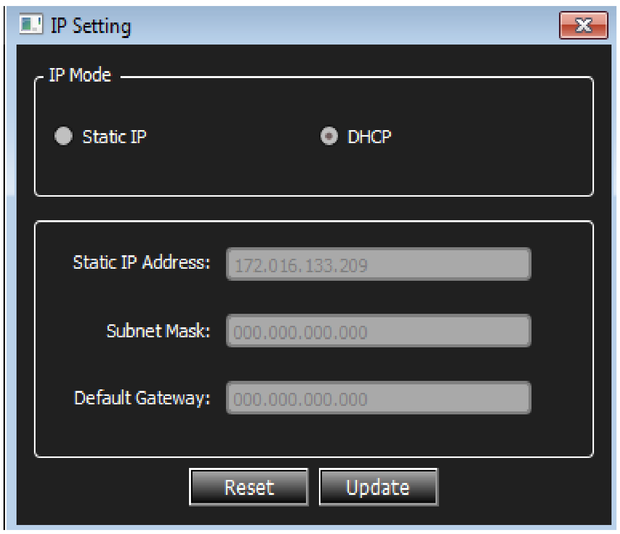


Figure 2.78: Dynamic IP Setup Success Message

8. To continue with changing back to DHCP, click **Yes**.
9. When the Success confirmation appears, click **OK**.

NOTE: You can also click **Reset**.

2.5.3 Connecting Via USB

To set up the Analyzer using a USB for the first time, do the following:

1. Install the software. See 2.1, *Software Installation and Setup*.
2. Connect the Analyzer to power.
3. Connect the USB cable.
4. Power on the Analyzer.
5. Follow the Windows device installation prompts, if any, to complete the driver installation.

WARNING: Do not change from USB to Ethernet, or back, without power cycling the Analyzer.

To connect the Analyzer to a host system via Ethernet, refer to 2.5.2, *Connecting via Ethernet*.

2.5.4 Update Device

For any Analyzer to be connected to the network and to work correctly, there are a variety of components that must match the correct version supported by the revision of the Net Protocol Suite software.

This section describes how to update the device. It uses the SierraNet M408 model as an example. Other SierraNet models will have different components; however, the procedure will be similar. The Update Device dialog allows you to update the following components of the Analyzer:

- Firmware
- Net10G Analyzer x2
- Net10G Infusion
- Net40G Analyzer x2
- Net FC Analyzer x2
- Net FC Infusion
- Net 10G_FC Analyzer x2
- Net FC_10G Analyzer x2
- Net 10G_FC Infusion
- NetFC_10G Infusion
- IOHub BusEngine

See Figure 2.79 below.

Figure 2.79: Components That Need to be Updated

In this example, we have intentionally loaded each component to be a “down-rev” version that will need to be updated so that the current revision of the Net Protocol Suite Software will work correctly.

1. Click the **Update Device** button (Figure 2.79). This produces the Update Device dialog window that shows which components need to be updated. See Figure 2.80.

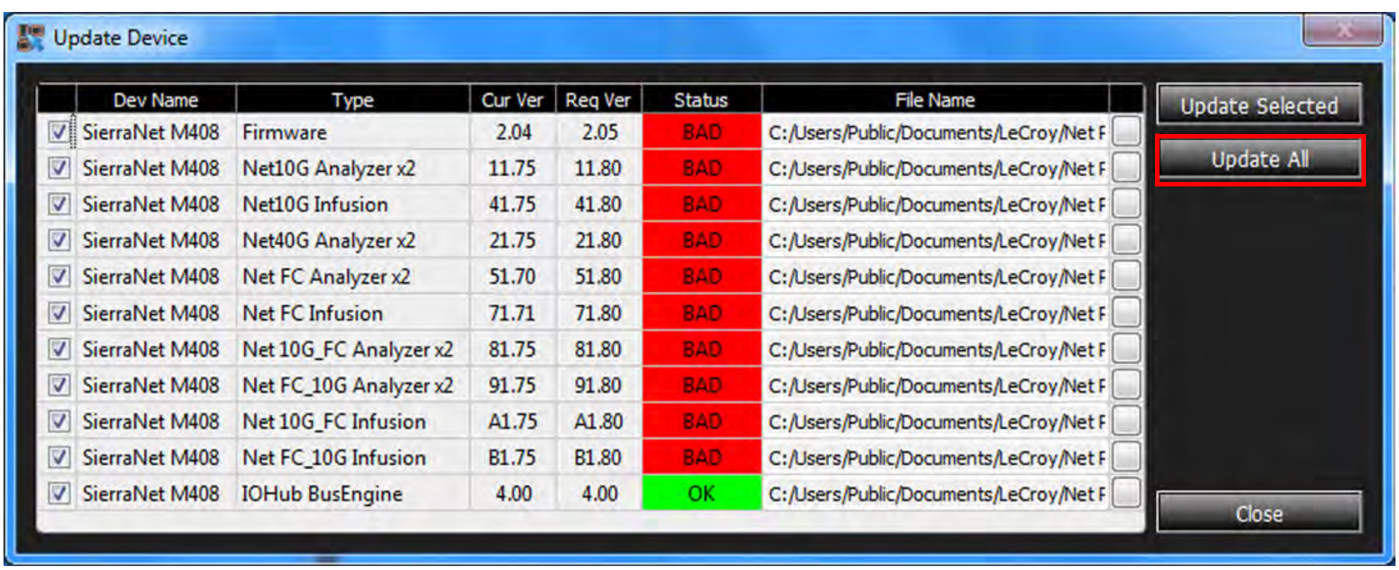


Figure 2.80: Components that need to be Updated

In this case, “Update All” is selected since “down-rev” versions were loaded.

2. Click the **Update All** button. Each component will be updated to the Required Version (Figure 2.81).

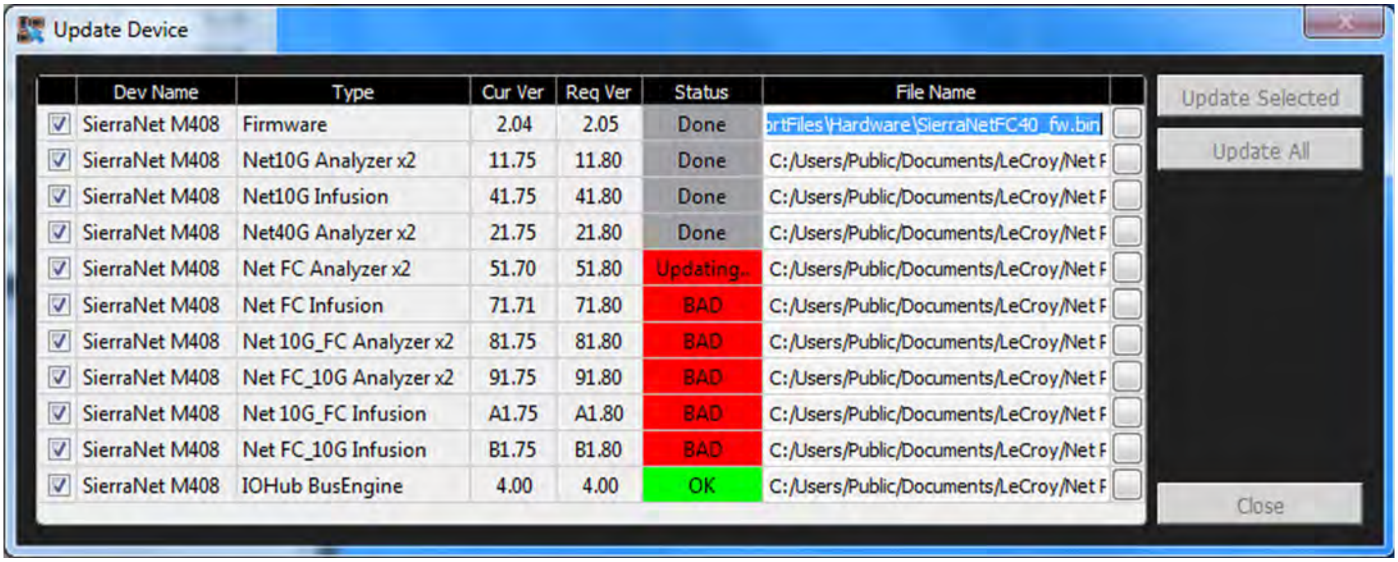


Figure 2.81: Components Being Updated

NOTE: You can click the ellipsis (...) at the end of a file path and name to display an Open dialog, in which you can browse for files.

When the system is updating the last component, the screen should resemble Figure 2.82.

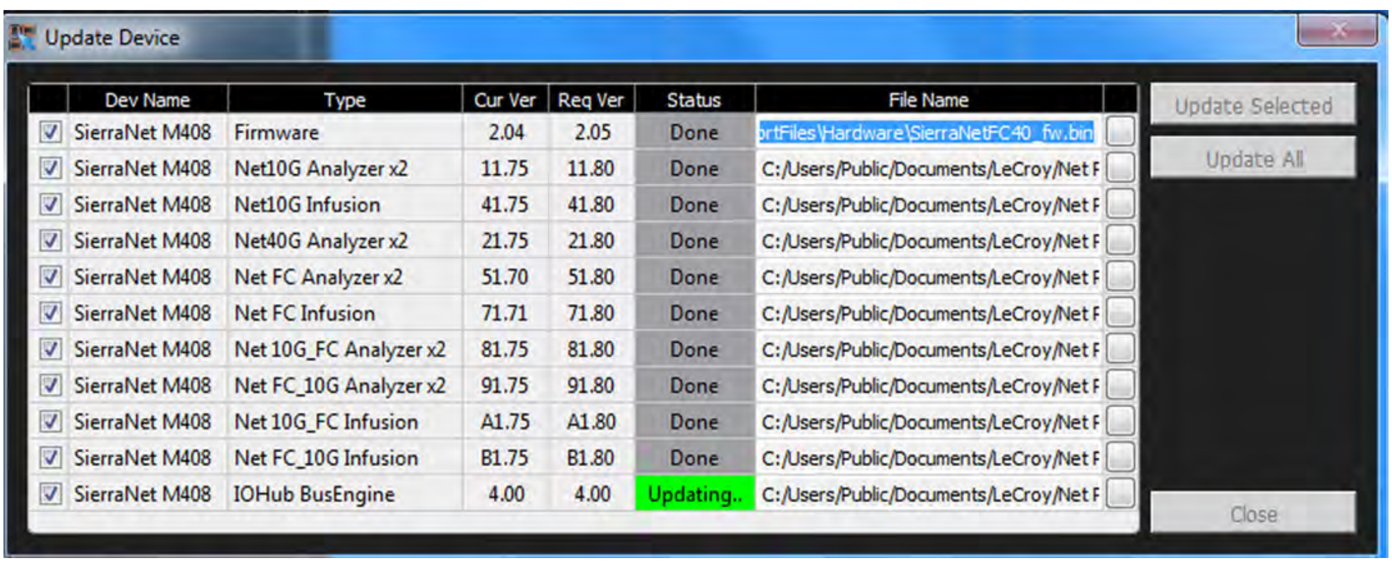


Figure 2.82: Last Component Being Updated

Once the update process is complete, the Analyzer may need to be power-cycled.

3. Be sure to follow the on-screen prompts to complete the update process successfully. See Figure 2.83.

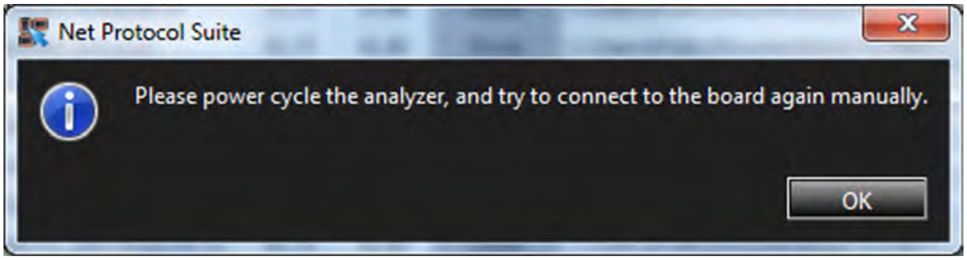


Figure 2.83: System Requesting Power Cycle

4. After power cycling, return to the Device Management dialog window. The Analyzer should be “Available”. See Figure 2.84.

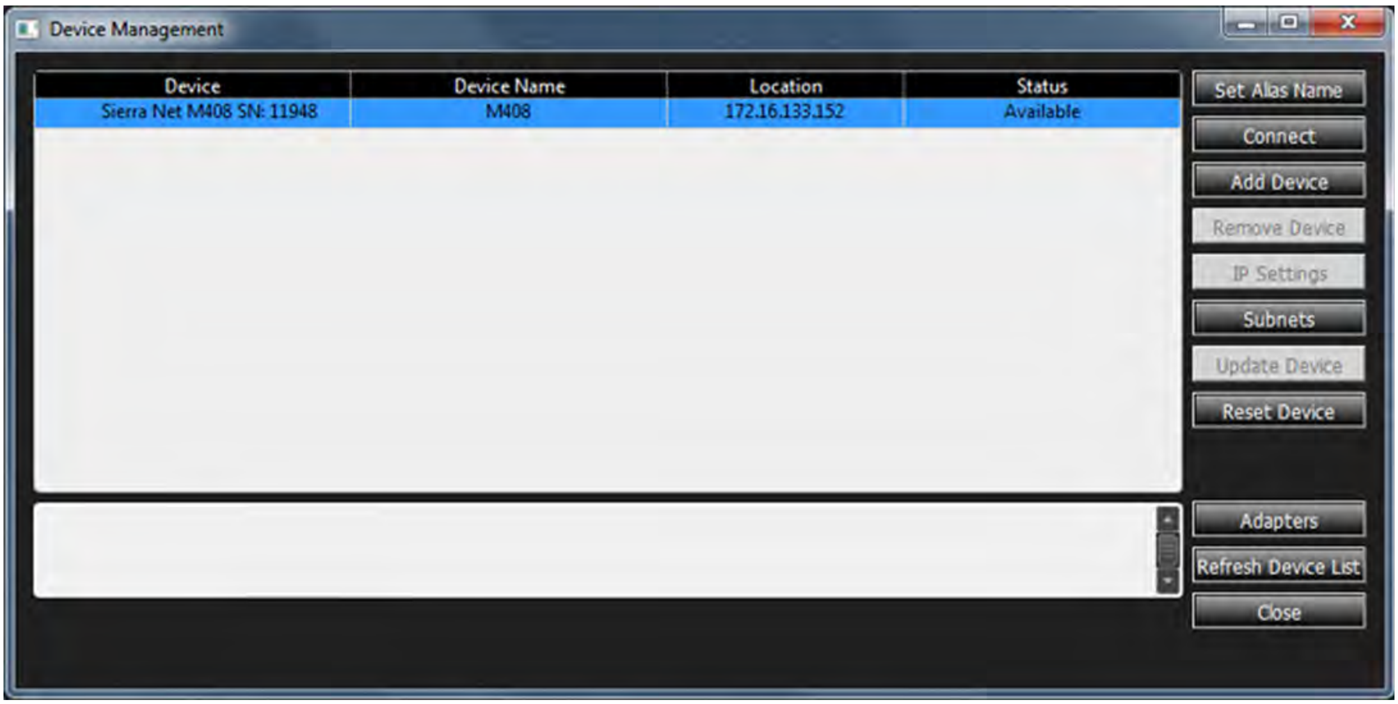


Figure 2.84: Analyzer Updated and Ready to be Connected

Once the components are updated, the system may prompt you to Connect (Figure 2.85).

5. Click **Yes** to connect the Analyzer.

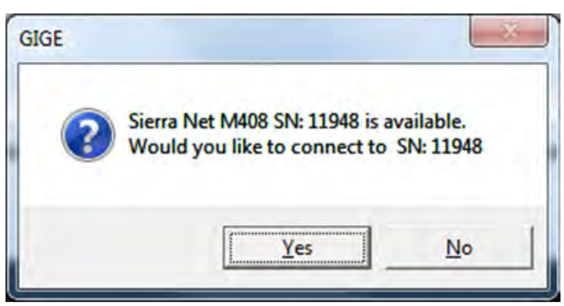


Figure 2.85: Ready to Connect Analyzer Dialog

6. Once the Analyzer is connected, you can proceed with a New Project. See Figure 2.86 and *Analyzer Startup – New Project*.

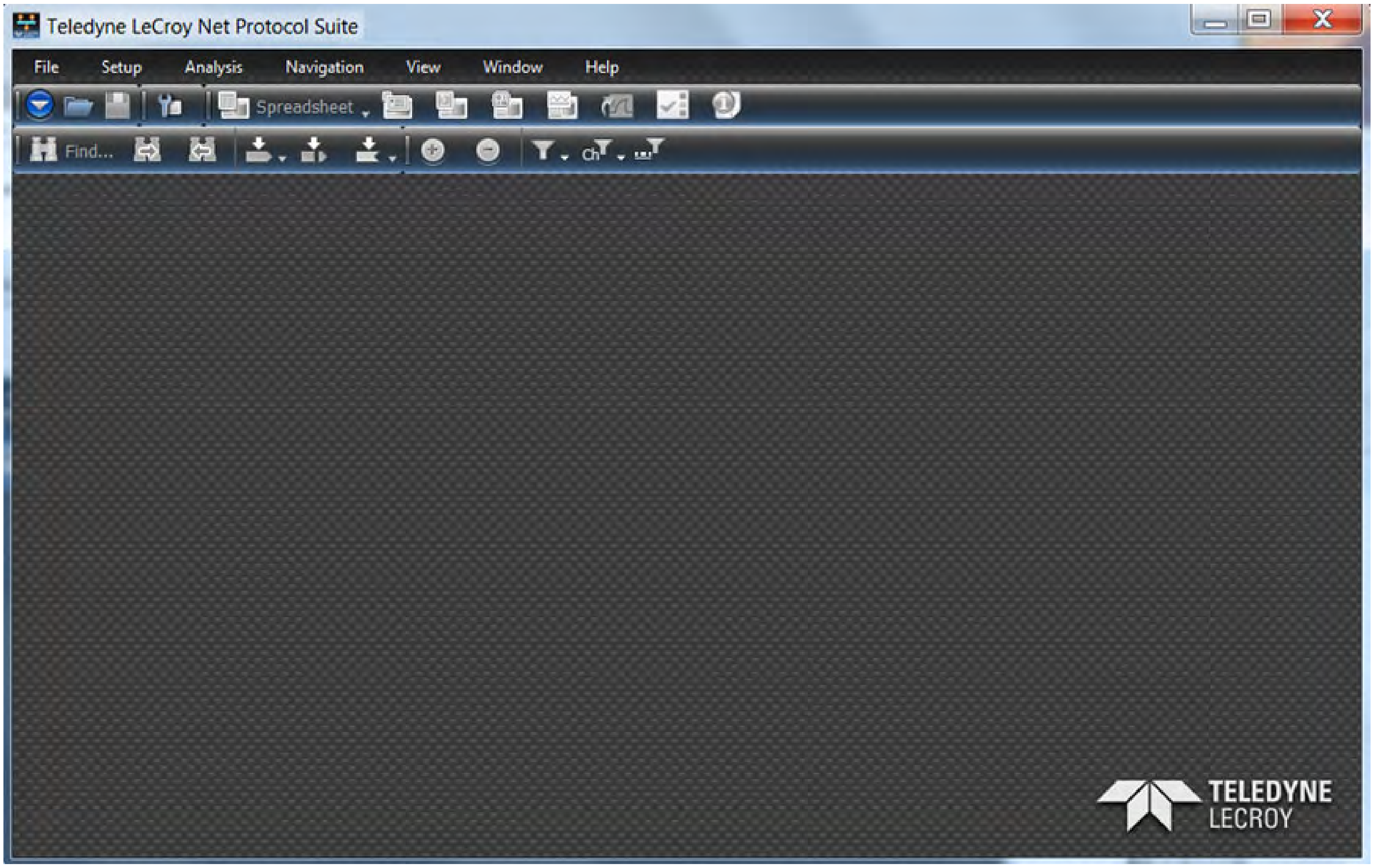


Figure 2.86: Net Protocol Suite Main Menu

Chapter 3

Analyzer Startup – New Project

3.1 Creating a New Project

You can create a new project either from the Application Menu Bar (see Figure 3.1) or you can click the **Hide Menu bar** icon to bring up the Application Tool Bars. Either action allows you to select **File** → **New Project** (see Figure 3.1 or Figure 3.2). Clicking on **New Project** will display the **Add Device to Project** dialog (see Figure 3.3).

NOTE: Click **Alt** to toggle between showing/hiding the Application menu bar. If all toolbars and icons have been hidden, clicking **Alt** will bring up the Application menu bar.

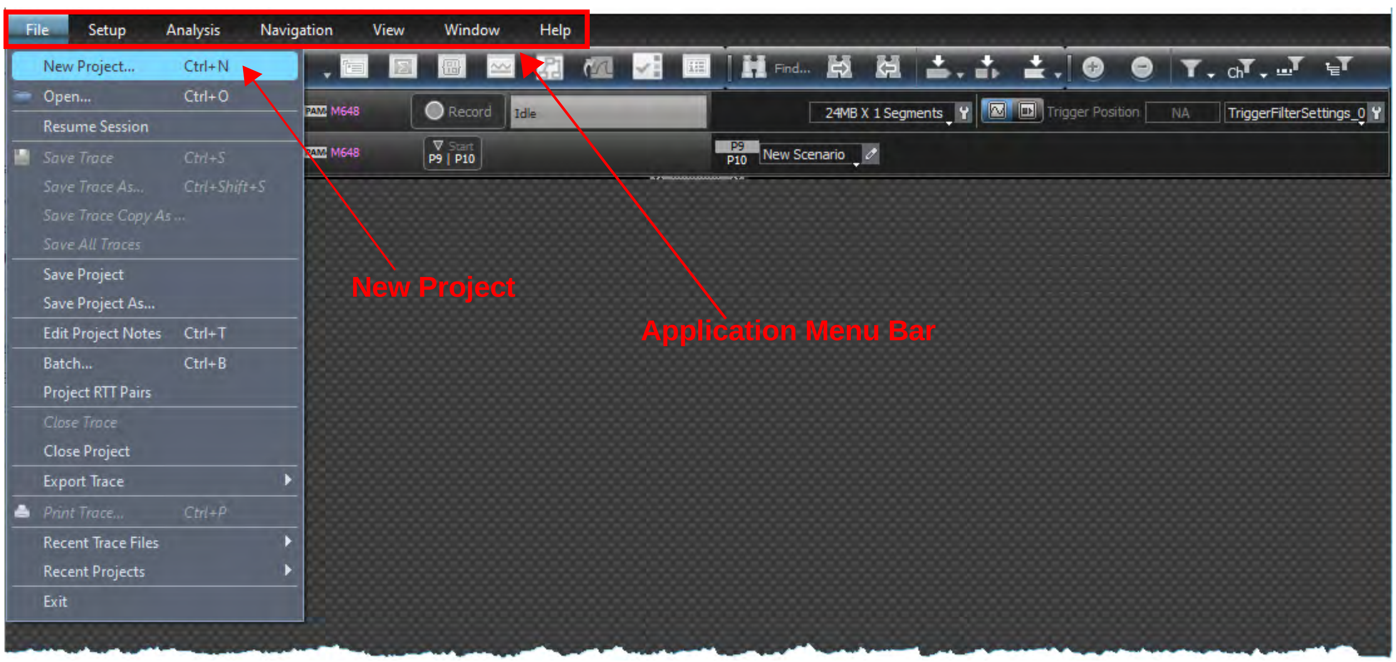


Figure 3.1: Starting a New Project from the Application Menu Bar

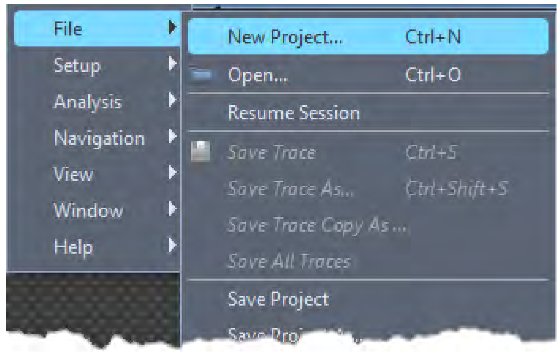


Figure 3.2: Start a New Project

3.1.1 Add a Device to a Project

To add a device to a project, do the following:

1. If you have not already done so, launch *Teledyne LeCroy Net Protocol Suite*.
2. Select **File → New Project**. The **Add Device to Project** dialog window opens (Figure 3.3).

NOTE: You can click **Refresh Device List** to display all devices on the on the local Ethernet subnet and devices connected with USB cable. This may take a few seconds.

All analyzers on the network and their status, by color, are displayed (Figure 3.3). The colors in the *Status* column have the following meanings:

- **Red**: Device is not updated (firmware or one of bus engines is not updated).
- **Light Blue**: Ready to connect.
- **Yellow**: Device is manually added, but it is not connected; OR the device is locked.
- **Green**: Connected.

3. Select a device with "Ready to connect" status (light blue). The ports available to the selected device appear in the bottom pane of the dialog window.

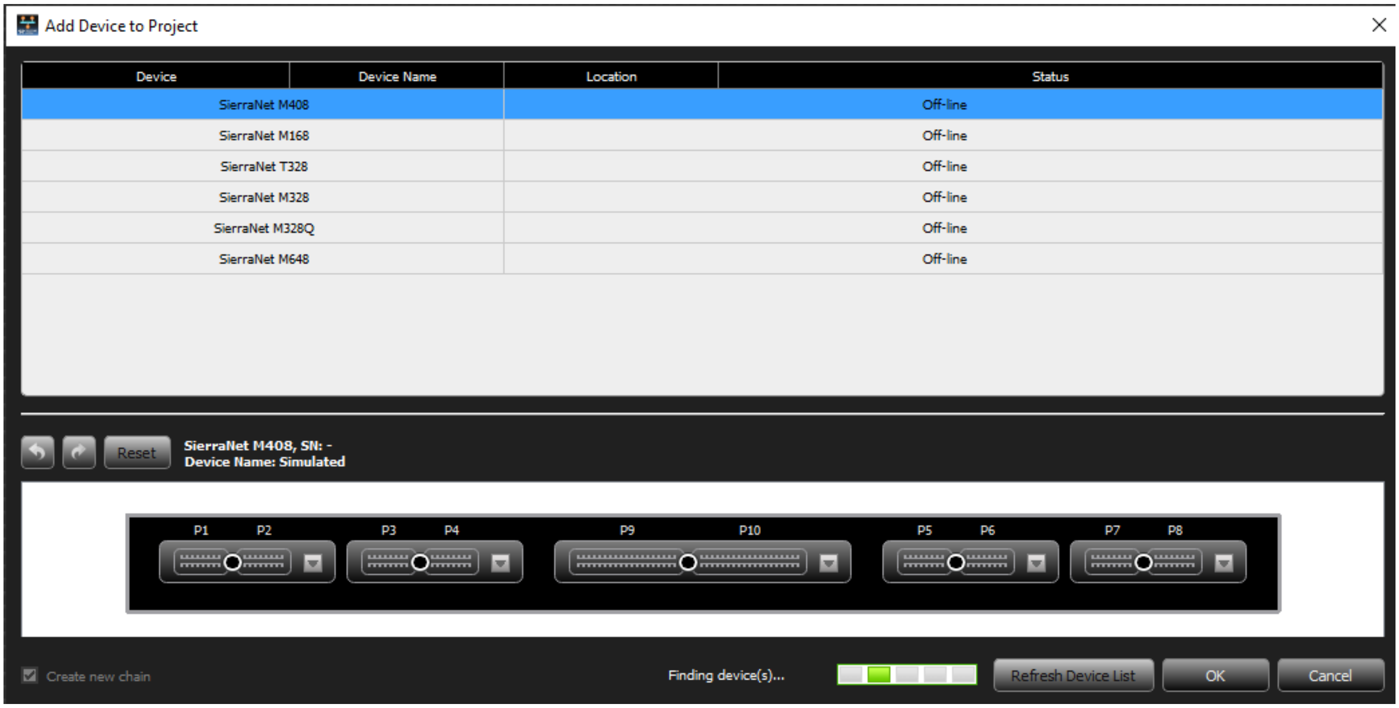


Figure 3.3: Add Device to Project

3.1.2 Port Configuration

1. Click the down arrow of the port group you need to configure and select the appropriate Function.

   - You can select a Function from the Analyzer, Jammer or Exerciser, as well as the protocols and speeds you want to work with, by selecting the port pair combinations.
   - Depending on the protocol and speeds you selected, additional ports and Functions may or may not be available.
   - Unavailable Ports are grayed out; unavailable Functions are not shown.
   - Null Ports are black. A link will not be established and traffic will not flow through the Port.

   See examples for Configuration options in Figure 3.4, and resulting Port Configurations in Figure 3.5.

NOTE: The device must be configured before it can be added to a project.

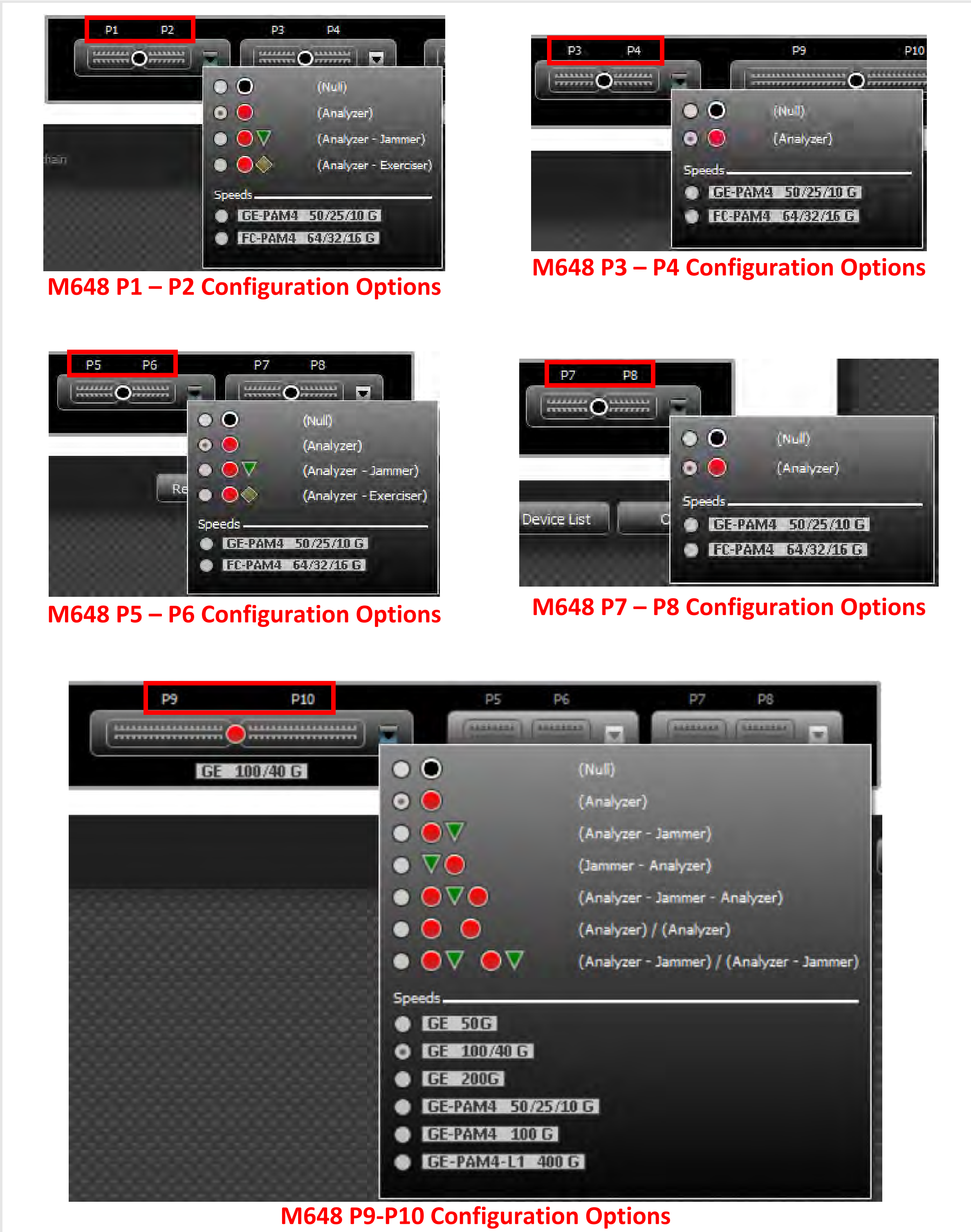


Figure 3.4: Configuration Options for SierraNet M648

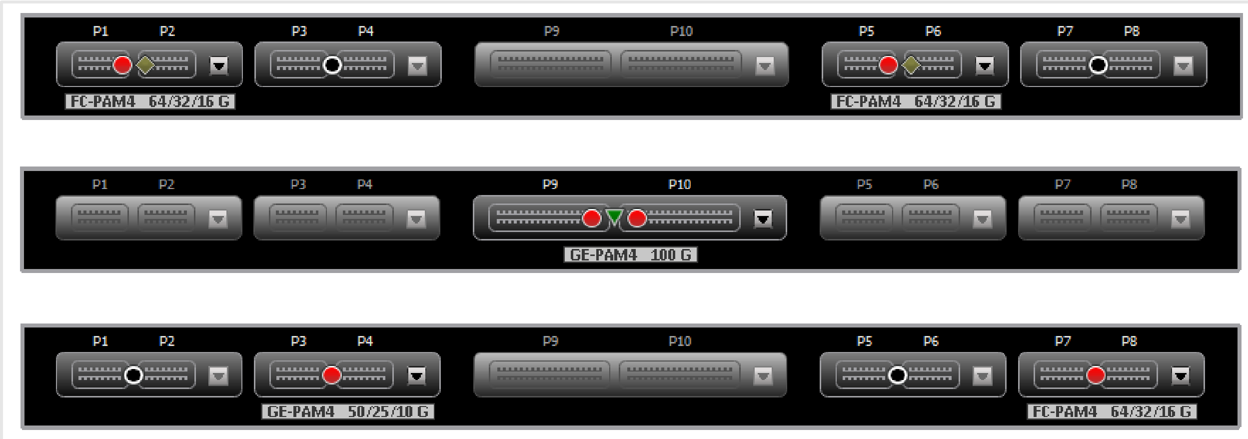


Figure 3.5: Example SierraNet M648 Port Configurations

3.2 Menu Bar Options

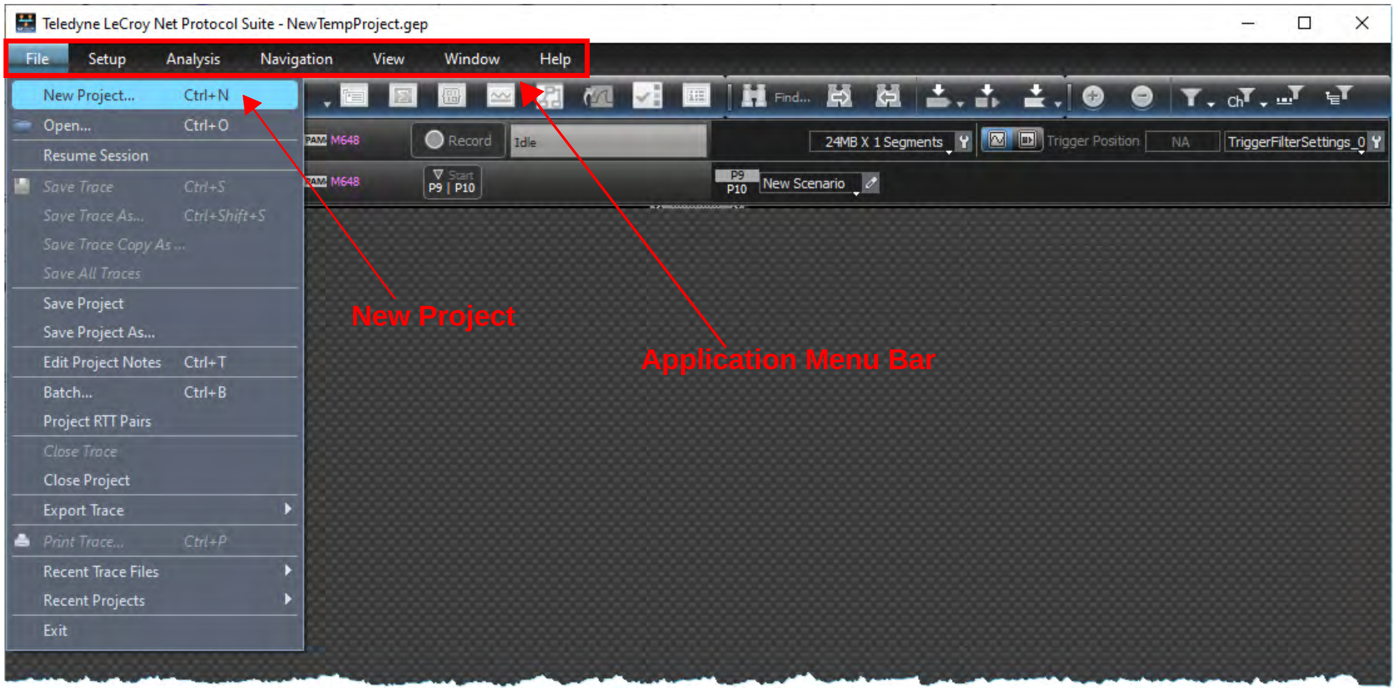


Figure 3.6: Starting a New Project from the Application Menu Bar

The following menu Bar options are displayed in the main window:

- File (see 3.2.1, *File*)
- Setup (see 3.2.2, *Setup*)
- Analysis (see 3.2.3, *Analysis*)
- Navigation (see 3.2.4, *Navigation*)
- View (see 3.2.5, *View*)
- Window (see 3.2.6, *Window*)
- Help (see 3.2.7, *Help*)

3.2.1 File

The File menu has the standard menu options as shown Figure 3.7.

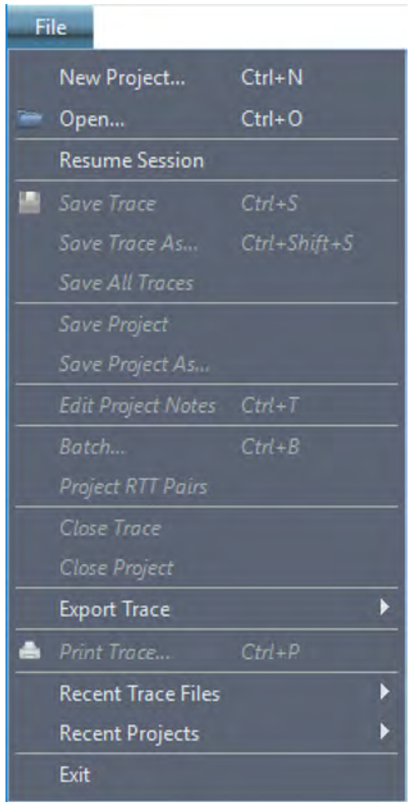


Figure 3.7: File Menu Options

The File Menu Options are defined in Table 3.1, below.

Table 3.1: File Menu Options

Menu Option	Description
New Project	Click to open a new project.
Open	Click to open an existing trace or trace files.*
Resume Session	Click to Resume an Existing Session. (See 3.2.1.1, *Resume Session*).*
Save Trace	Click to save an existing trace or trace files.*
Save Trace As	Click to save an existing trace or trace files with a different name or directory. (See 3.2.1.2, *Save Trace As*).*
Save All Traces	Click to Save All Trace files.*
Save Project	Click to save the current project.*
Save Project as	Click to save the current project with a different name or directory. (See 3.2.1.4, *Save Project As*).*
Edit Project Notes	Click to open a Text window to save notes about a Project as a device to remember what the primary purpose was or what the status of the Project was at a certain point in time. (See 3.2.1.5, *Project Notes*).*
Batch	Click to run batch scenarios. (See Chapter 7, *Infusion Batch Test Scenarios*). Available only after a project is open.*
Project RTT Pairs	See 3.2.1.6, *Project RTT Pairs* for details.

Table 3.1: File Menu Options (Continued)

Menu Option	Description
Close Trace	Click to close current Trace. (See 3.2.1.7, *Close Trace*.)*
Close Project	Click to close current Project. (See 3.2.1.9, *Close Project*.)*
Export Trace	◆ Export file to Excel ◆ Export to Text... ◆ Export and Open with Wireshark (See 3.2.1.10, *Export and Open with Wireshark*.)* ◆ Export to Exerciser Script (See 8.5, *Export to Exerciser Script*.)
Print Trace	Click to print current Trace.*
Recent Trace Files	Lists recent trace files to open.*
Recent Projects	Lists recent projects to open.*
Exit	Click to exit the application (see 3.2.1.11, *Exit the Application*).

* The functions of Opening, Saving or Closing a Project or Trace assumes that you have already connected to an analyzer and recorded a Trace (see Chapter 4, *Recording Configuration with Real Time Traffic*). You can use these functions with Projects and Traces that ship with the analyzer as Examples to learn how to use the analyzer.

3.2.1.1 Resume Session

Use *Resume Session* when you want the analyzer to continue recording data traffic. At a later point in time, you may want to re-start the application, which is still recording data. To do this, select **Resume Session**. See Figure 3.8.

Resuming a Session assumes the following:

- ❑ That you have already connected to an analyzer and started a Recording (4.1.5, *Recording Settings Pane*)
- ❑ That you have Closed the Project (3.2.1.9, *Close Project*)
- ❑ Or that you have Exited the Application (3.2.1.11, *Exit the Application*)

To Resume a Session:

1. Select **File** → **Resume Session**.

   - You will first be prompted for the analyzer you were using during your session. See Figure 3.9.

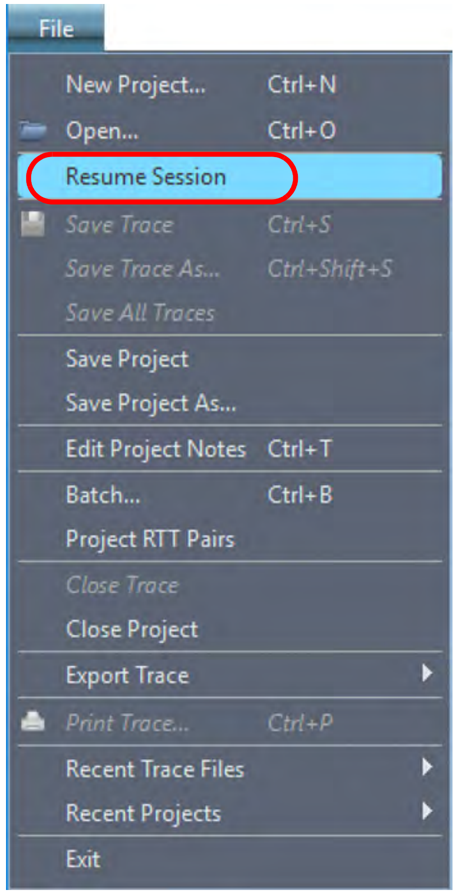


Figure 3.8: File, Resume Session

- If you changed host machines to open the application, you will be prompted for the Session Key that you entered when you Closed the Project or Exited the Application. See Figure 3.9.
- If you select **Resume** while you are still working on the same host machine, the application will remember the Session Key, so you will not be prompted to enter it.

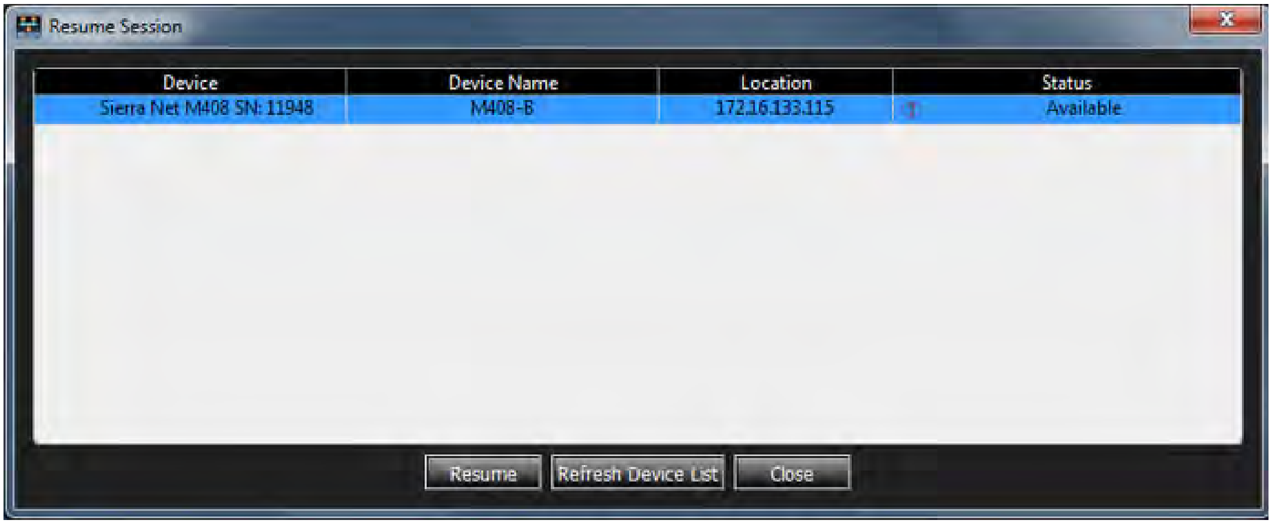


Figure 3.9: Analyzer Used During Previous Recording

2. Enter the Session Key, if needed. The Session Key is stored in Preferences (see 3.2.2.2, *Preferences*).

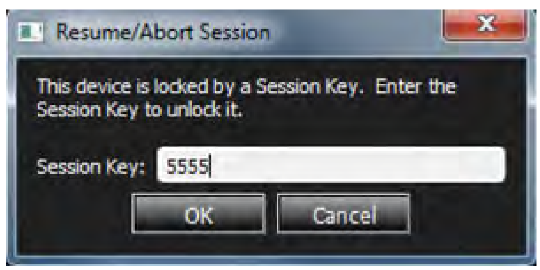


Figure 3.10: Prompt for Session Number

3. Click **OK** to continue your recording session. The following prompt appears (Figure 3.11).

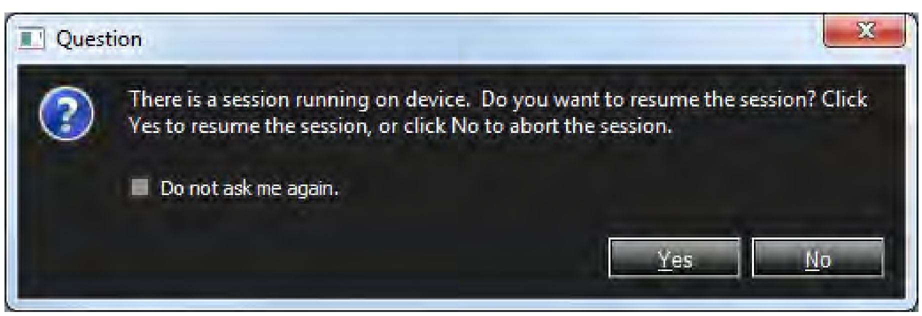


Figure 3.11: Prompt to Resume the Session or Not

4. Click **Yes**. The Session you had been Recording pops up. See Figure 3.12 for an example. By default the Project is labeled *RecoveryProject*.

Figure 3.12: Example of Existing Session

Once the Session has Resumed, you can continue recording without losing any data traffic.

3.2.1.2 Save Trace As

This function has several capabilities:

- ❑ Saving a Trace to a File
- ❑ Saving All events
- ❑ Saving part of a Trace between two Markers
- ❑ Saving Displayed Events

See figures 3.13, 3.14, and 3.15.

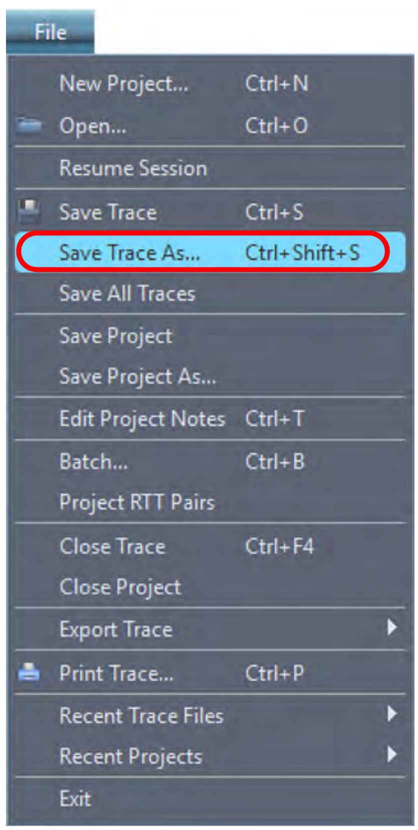


Figure 3.13: Save Trace As Option

To save a Trace as one of the available options, do the following:

1. Click **Save Trace As**. The following window appears:

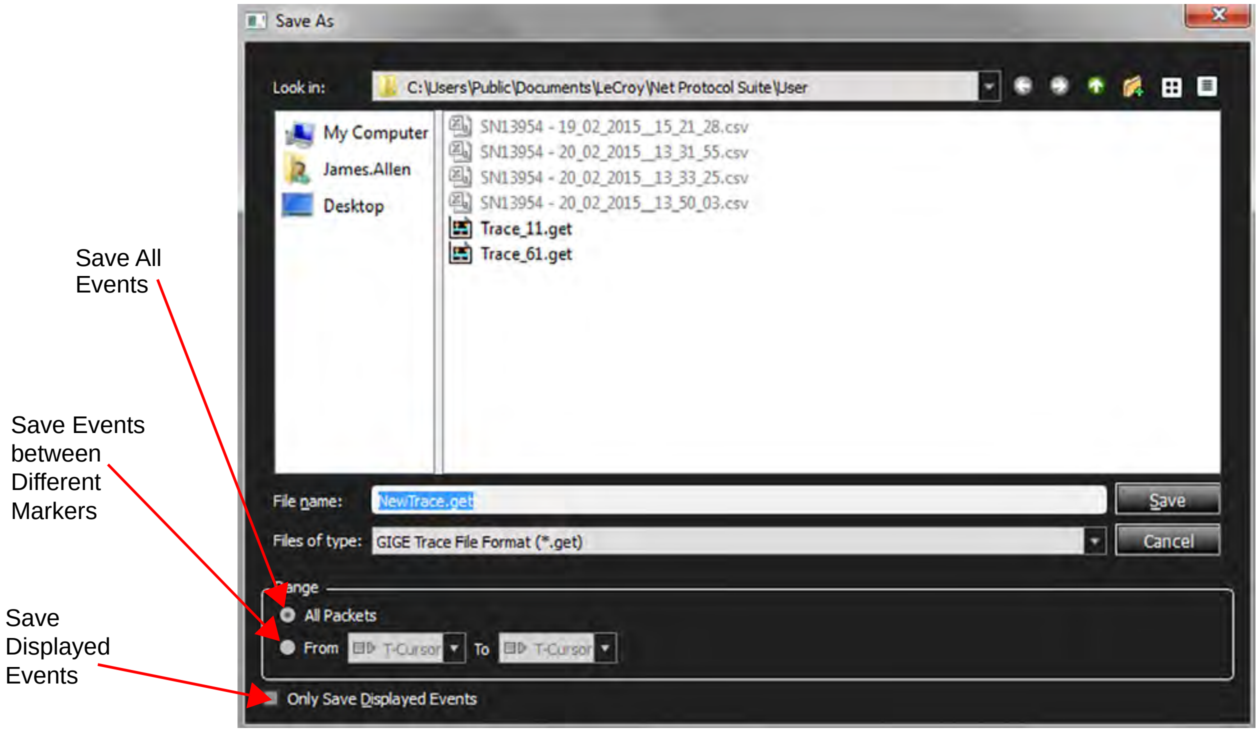


Figure 3.14: Save Trace As Window

2. Select the option you need, then select the range between Markers. For more information, see 5.2.1.7, *Markers*.

3. Click **Save**.

3.2.1.3 Save Events Between Markers

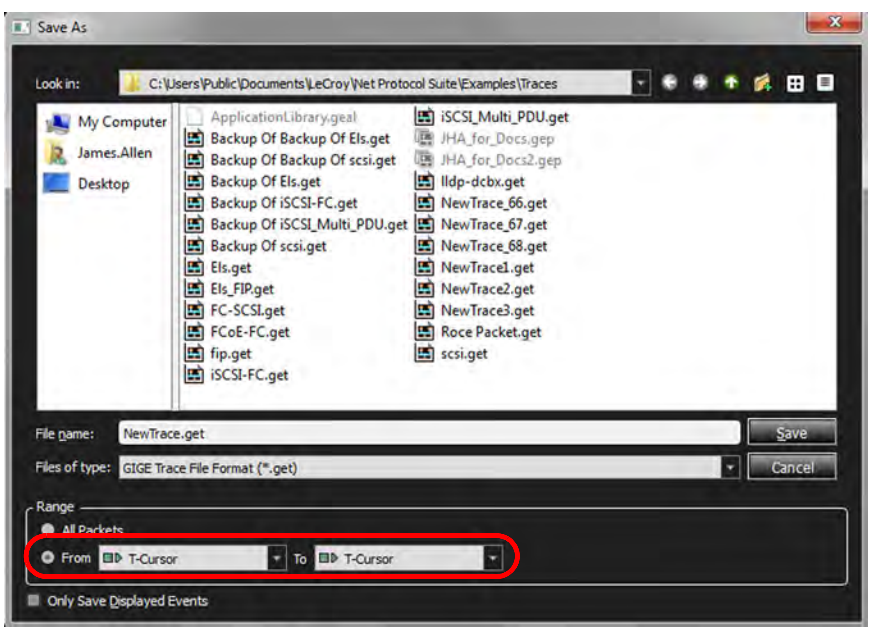


Figure 3.15: Save Markers in a Range

1. Click the arrows in the **From** and **To** boxes to select Markers (see 5.2.1.7, *Markers* for definition and generation of Markers).

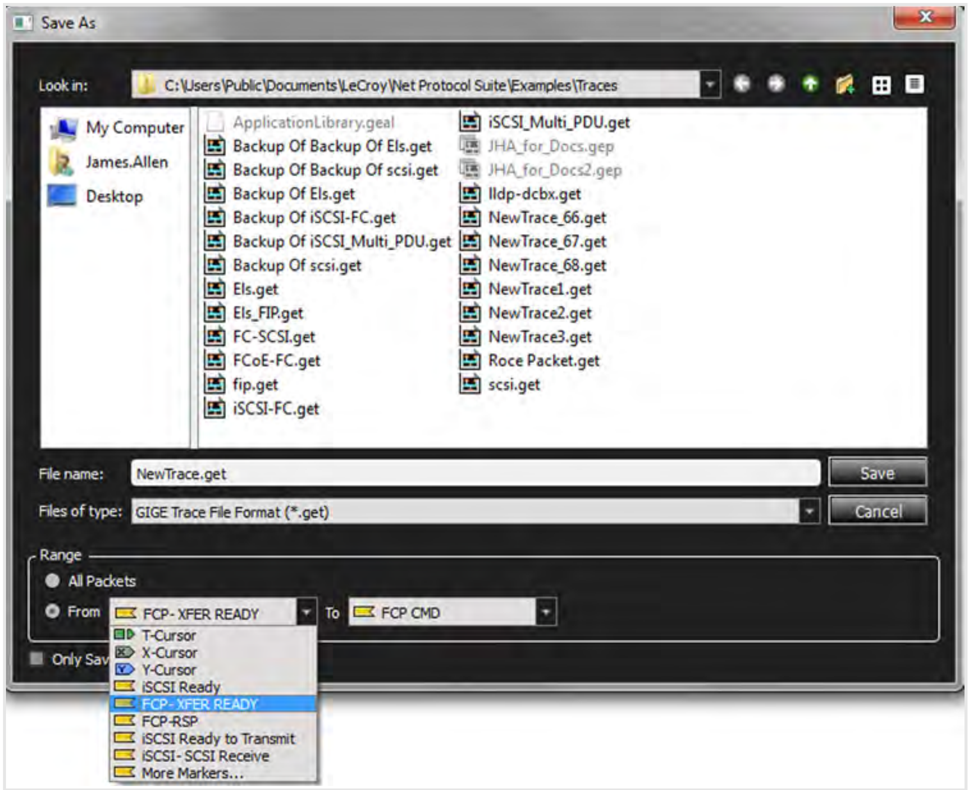


Figure 3.16: Choosing Markers

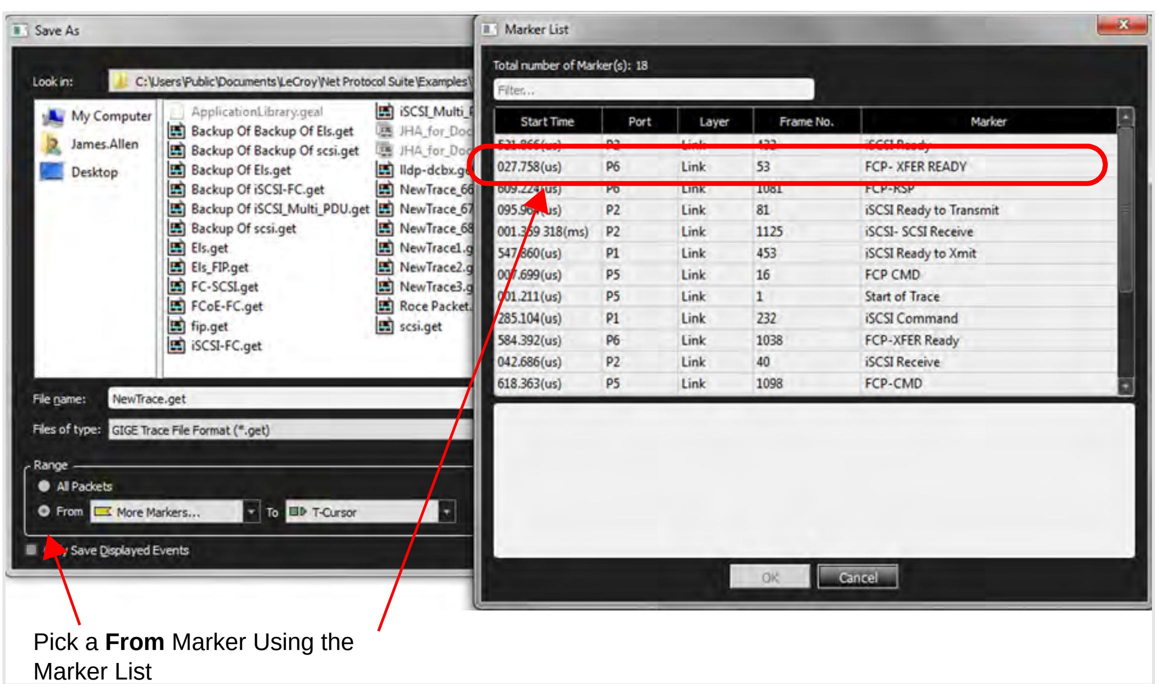


Figure 3.17: Selecting From and To Markers

2. After selecting **From** and **To** markers, **Save** the partial Trace. See Figure 3.18.

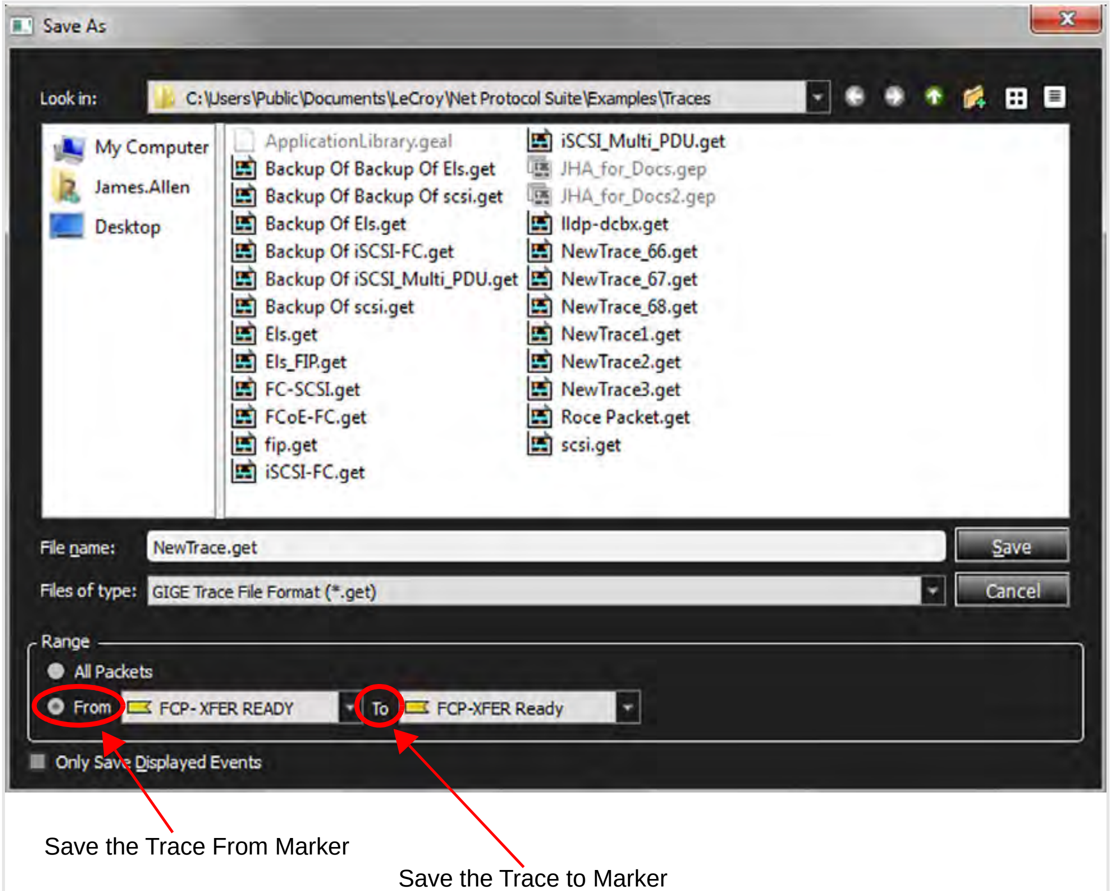


Figure 3.18: Save Partial Trace

3.2.1.4 Save Project As

Click on **Save Project As** to save a project with a different name. See Figure 3.19.

A window appears where you can save the Project in a specific location and with a specific name. See Figure 3.20.

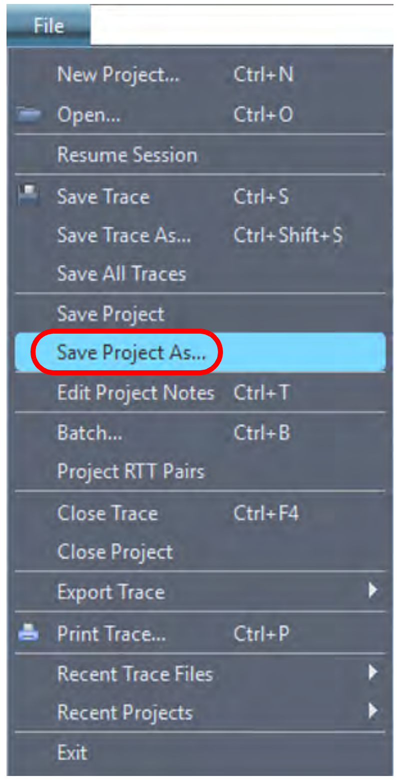


Figure 3.19: Save Project As

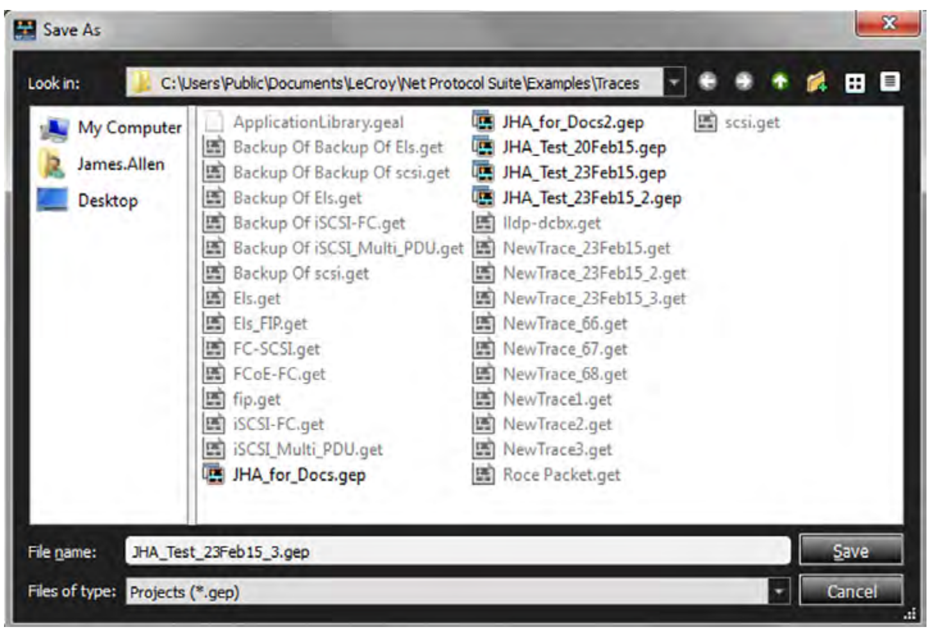


Figure 3.20: Save Project As with File Name and Path

3.2.1.5 Project Notes

To add notes to a Project, do the following:

1. Select **File → Edit Project Notes**. A Text Window where you can added notes to the Project. See figures 3.21 and 3.22.

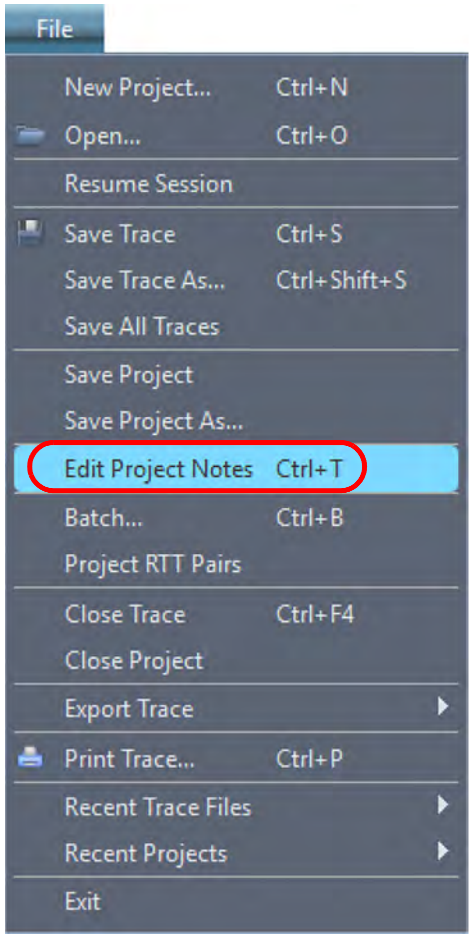


Figure 3.21: Edit Project Notes Button

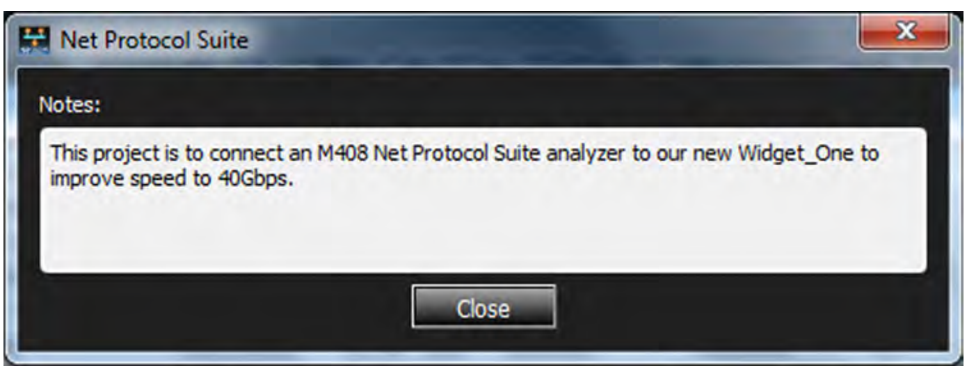


Figure 3.22: Project Notes

2. Enter the project note. When you are finished, click **Close**.
3. To continue adding notes, repeat steps 1 and 2.

3.2.1.6 Project RTT Pairs

"Project RTT Pairs" allows you to choose which ports pairs will be used to calculate the round trip time. See figures 3.24, 3.25, and 3.26.

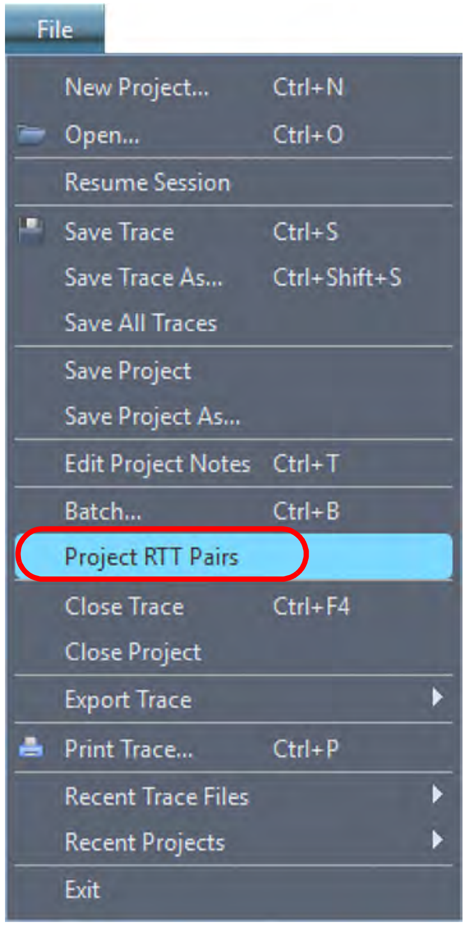


Figure 3.23: Project RTT Pairs

Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

For a given project these assignments will remain in effect as long as you are in that project.

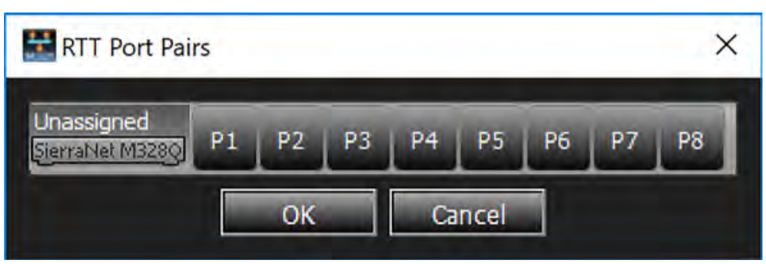


Figure 3.24: Choosing Project RTT Pairs: None Chosen

In the following diagram adjacent ports have been “paired” for RTT analysis:

- Port1 and Port2
- Port3 and Port4
- Port5 and Port6
- Port7 and Port8

Figure 3.25: Choosing Project RTT Pairs, Adjacent Port Pairs Selected

However, depending on the topology of your system, you can select any port to be "paired" with any other port for RTT analysis. An example diagram is shown in Figure 3.26.

- Port1 is paired with Port 5
- Port2 is paired with Port 6
- Port3 is paired with Port7
- Port4 is paired with Port8

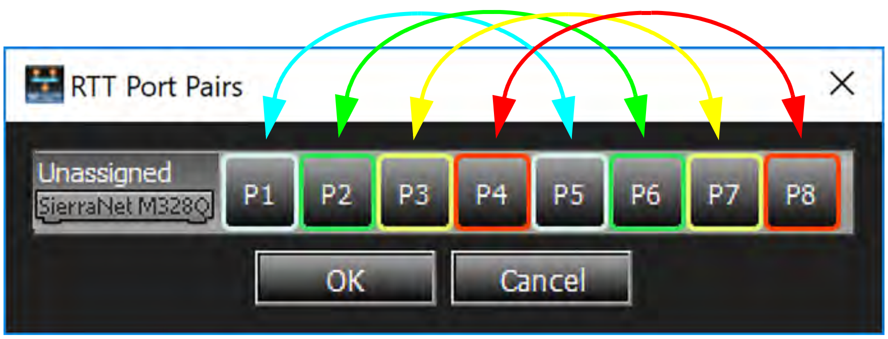


Figure 3.26: Choosing Project RTT Pairs: Mixed Port Pairs

For a more detailed description of how to use the RTT function see 5.4.1, *RTT for TCP*.

3.2.1.7 Close Trace

To close a Trace, perform the following steps:

1. Select **File → Close Trace** (Figure 3.27). The warning dialog box appears (Figure 3.28).
2. Choose whether to **Save**, **Discard**, or **Cancel**.

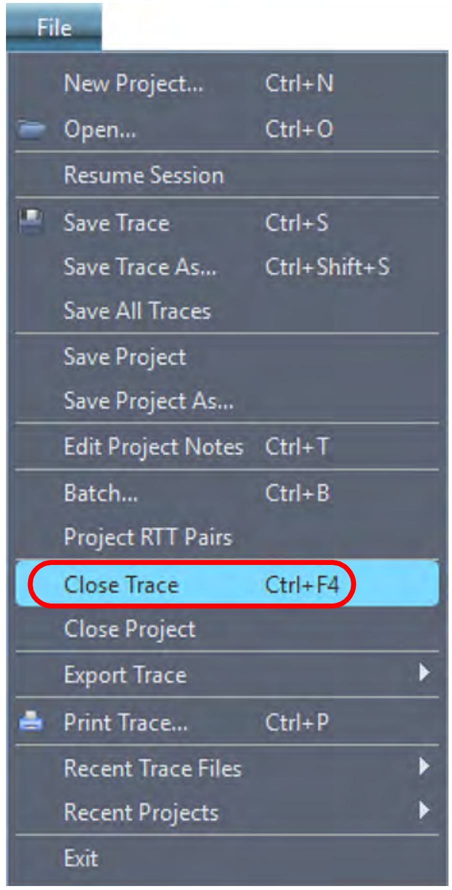


Figure 3.27: Close Trace

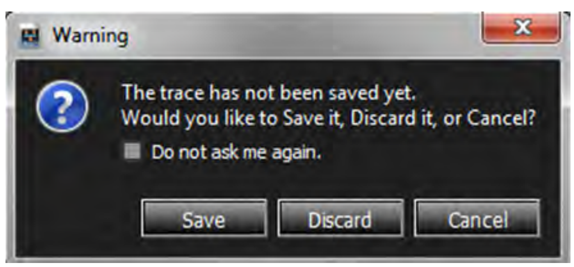


Figure 3.28: Close Trace Warning Prompt

3.2.1.8 Discard Trace – Upload Manager

If you choose to discard the Trace, but haven't closed the Project, you can still retrieve part or all of the Trace with Upload Manager. See Figure 3.29.

Figure 3.29: Upload Manager

1. Click on the text icon in the *Idle* window. The Upload Manager dialog box appears (Figure 3.30).

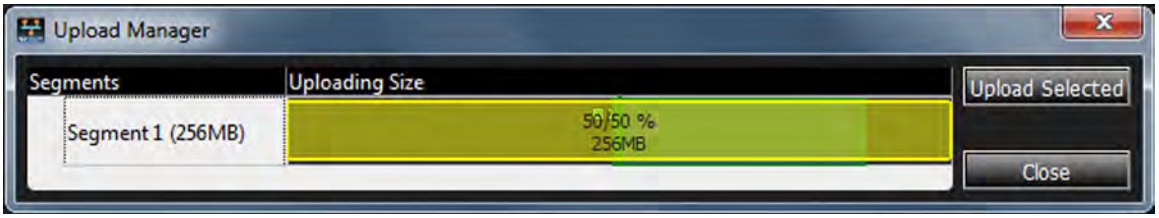


Figure 3.30: Upload Manager Dialog

2. To upload the entire Trace (in this case 256MB) or shrink the size of the Trace, place the cursor over the beginning or ending of the Trace and pull the edges toward the trigger point. See figures 3.31 and 3.32.

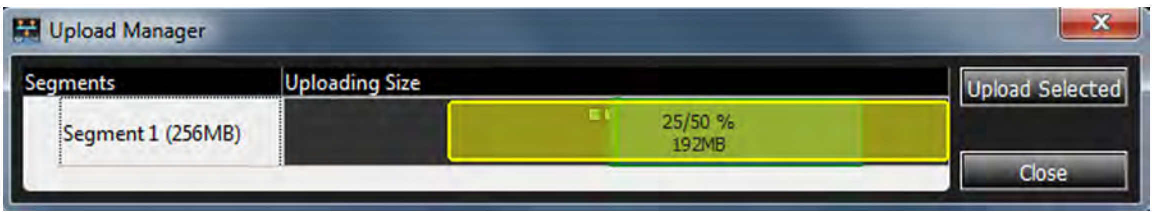


Figure 3.31: Upload Manager Dialog: Moving the Beginning of the Trace

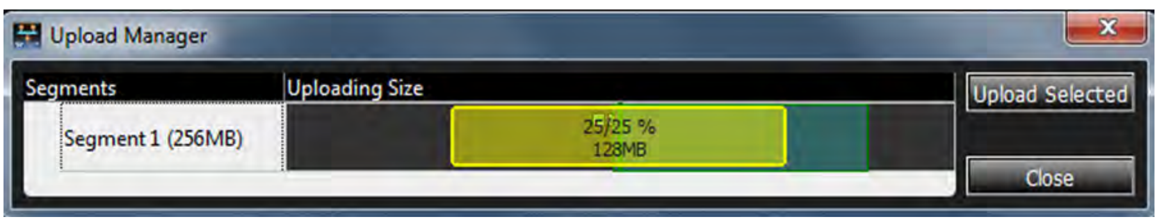


Figure 3.32: Upload Manager Dialog: Moving the Ending of the Trace

3. You can continue making the Trace smaller, so that it is concentrated around the trigger point (see Figure 3.33), or you can slide the section of the Trace you want to recover from the beginning to the end of the Trace. See Figure 3.34.

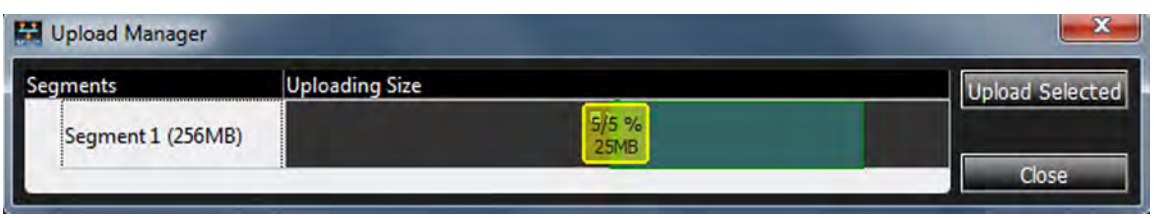


Figure 3.33: Shrinking the Trace Around the Trigger Point

Figure 3.34: Upload a Section of the Trace

4. Click the **Upload Selected** button. The section of the original Trace you outlined is uploaded. See Figure 3.35.

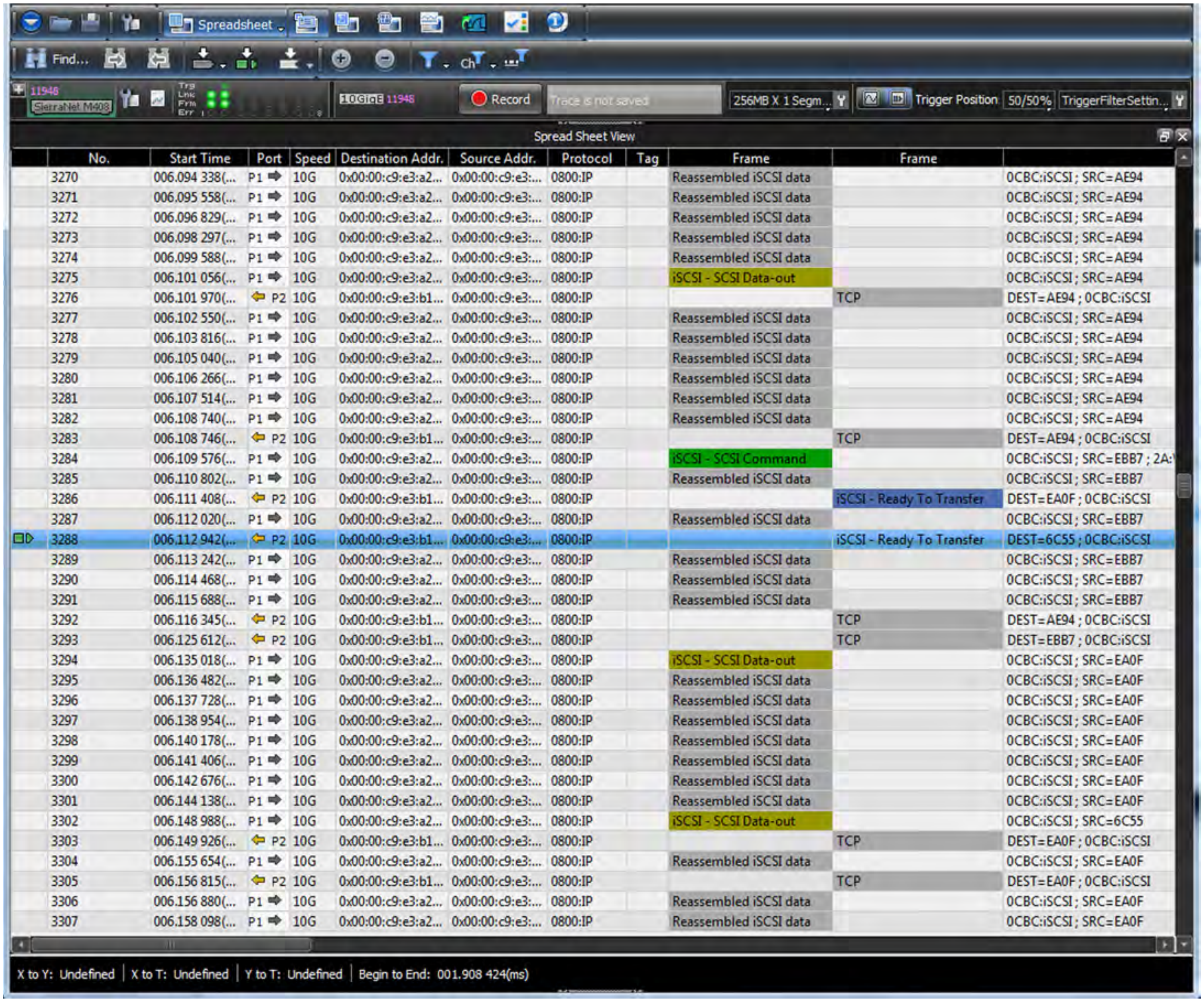


Figure 3.35: Uploaded Trace

3.2.1.9 Close Project

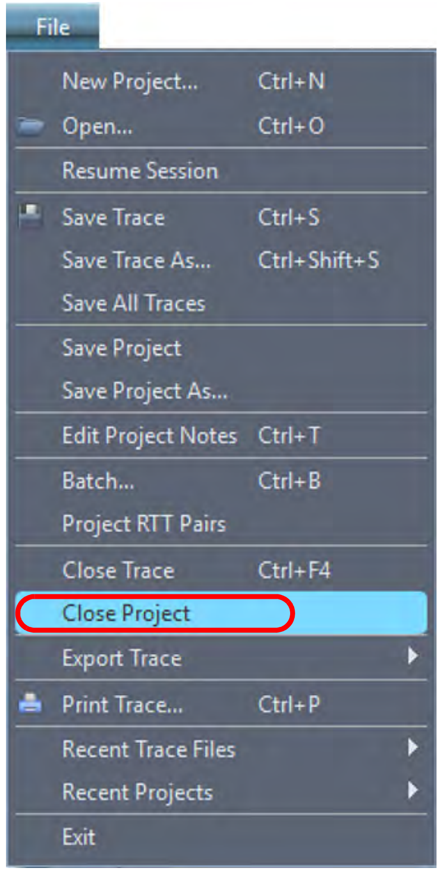


Figure 3.36: Close Project

If you decide to Close the Project, one of three different events will occur:

- No Changes to the Project have Occurred since it was last Saved.

  If you haven't made any changes to the Project since it was last Saved, the Project will simply close and the Application will remain Open.

- Not Recording Data Traffic.
  - If you are not actively recording data traffic, but have modified the Project, the following warning message will pop up:

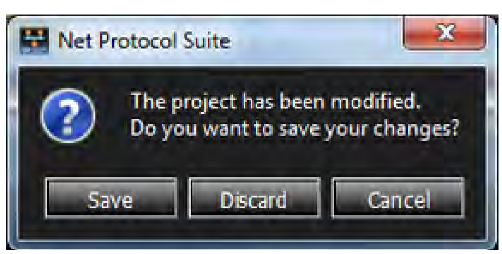


Figure 3.37: Close Project (but not Record Data)

  - You can then decide to **Save** or **Discard** any changes you've made to the Project. In either case the Application remains Open.

- Actively Recording Data Traffic
  - If you are Recording Data Traffic, the *Abort/Pause Session* dialog pops up.
  - At this point you can decide to either:
    - Close the Project but continue Recording Data Traffic and return to the Session in the future. See Figure 3.38.

      OR
    - Close the Project, Abort the Recording of Data Traffic entirely, and lose any Data Traffic that has not already been saved. See Figure 3.39.

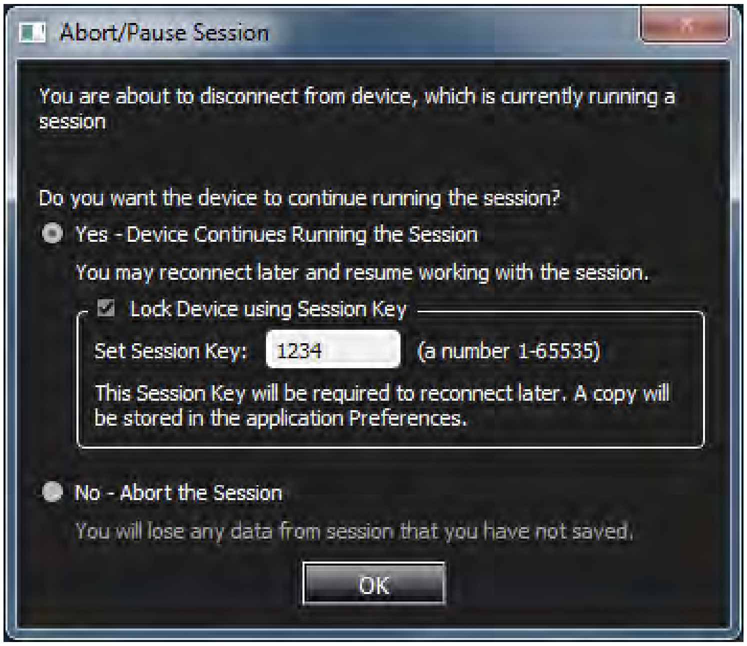


Figure 3.38: Continue the Recording Session

- If you click **Yes** in the context of "Close Project", the project closes, but data traffic will continue to be recorded. The Application continues to be Open and the Project can be Recovered. See 3.2.1.1, *Resume Session*.

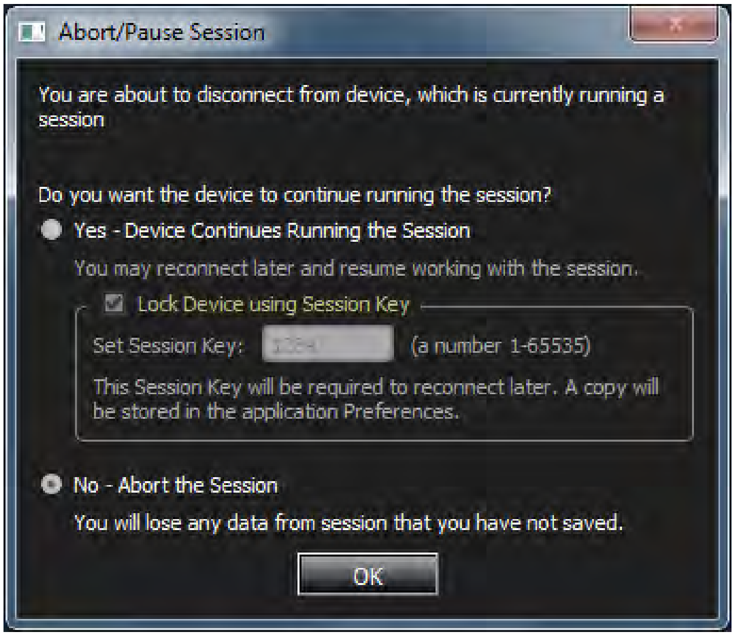


Figure 3.39: Abort the Recording Session

- If you click **No** in the context of "Close Project", the project is closed and any data traffic not already saved will be lost. The Application continues to be Open, but the Project cannot be Recovered.

3.2.1.10 Export and Open with Wireshark

To Export and Open with Wireshark, do one of the following:

- ❑ Select **File** → **Export** → **Export and Open with Wireshark**

  OR

- ❑ Click the **Export to Wireshark** icon (Figure 3.40).

The *Export to Wireshark* window appears (Figure 3.41).

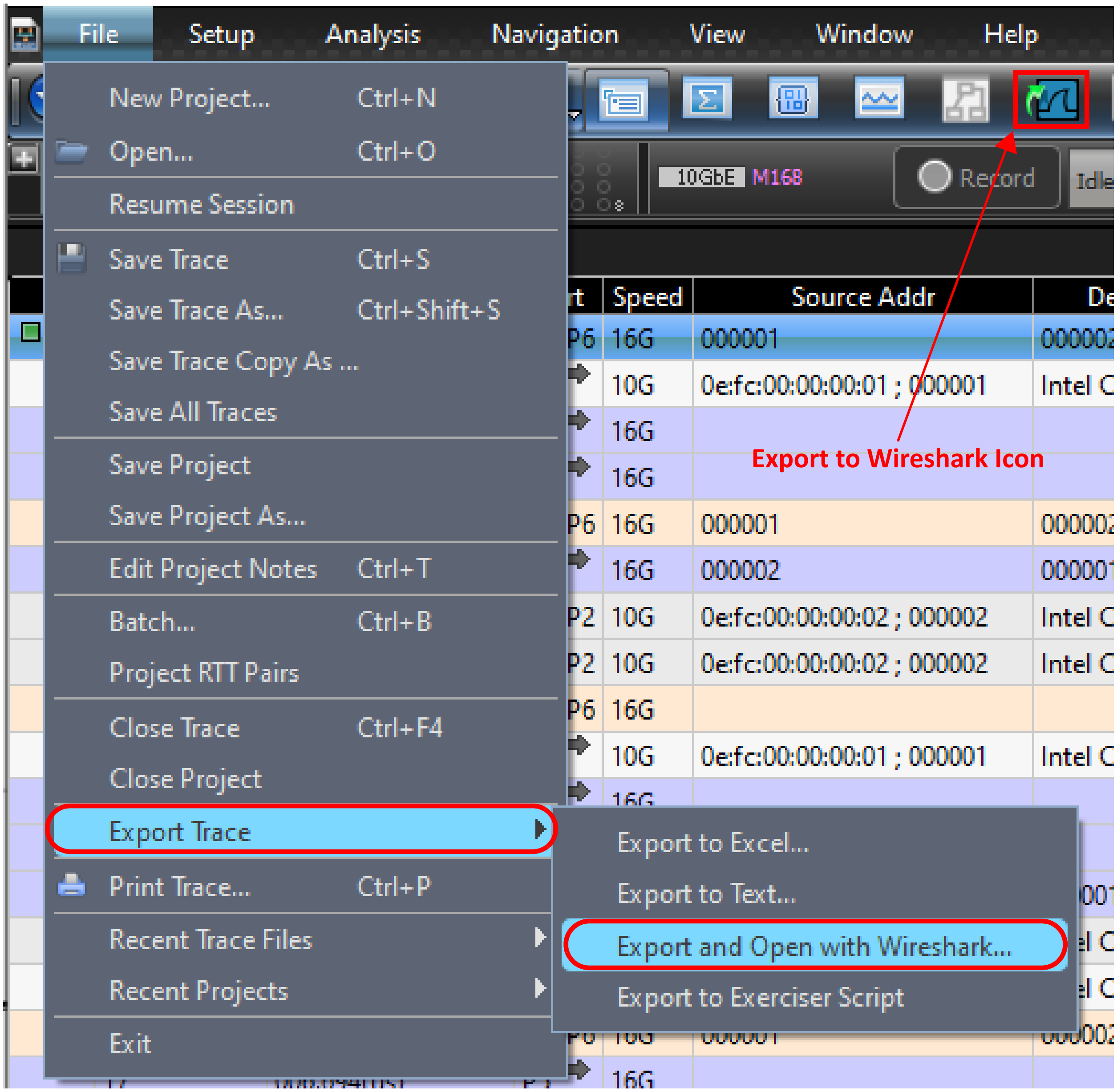


Figure 3.40: Export and Open with Wireshark

- The Export to Wireshark window (see Figure 3.41) has an option to choose between Ethernet and FC export. This option is only available if the trace contains both protocols. Only the selected protocol frames will be exported
- To get both types exported, the you must perform the export twice, choosing a different protocol each time.

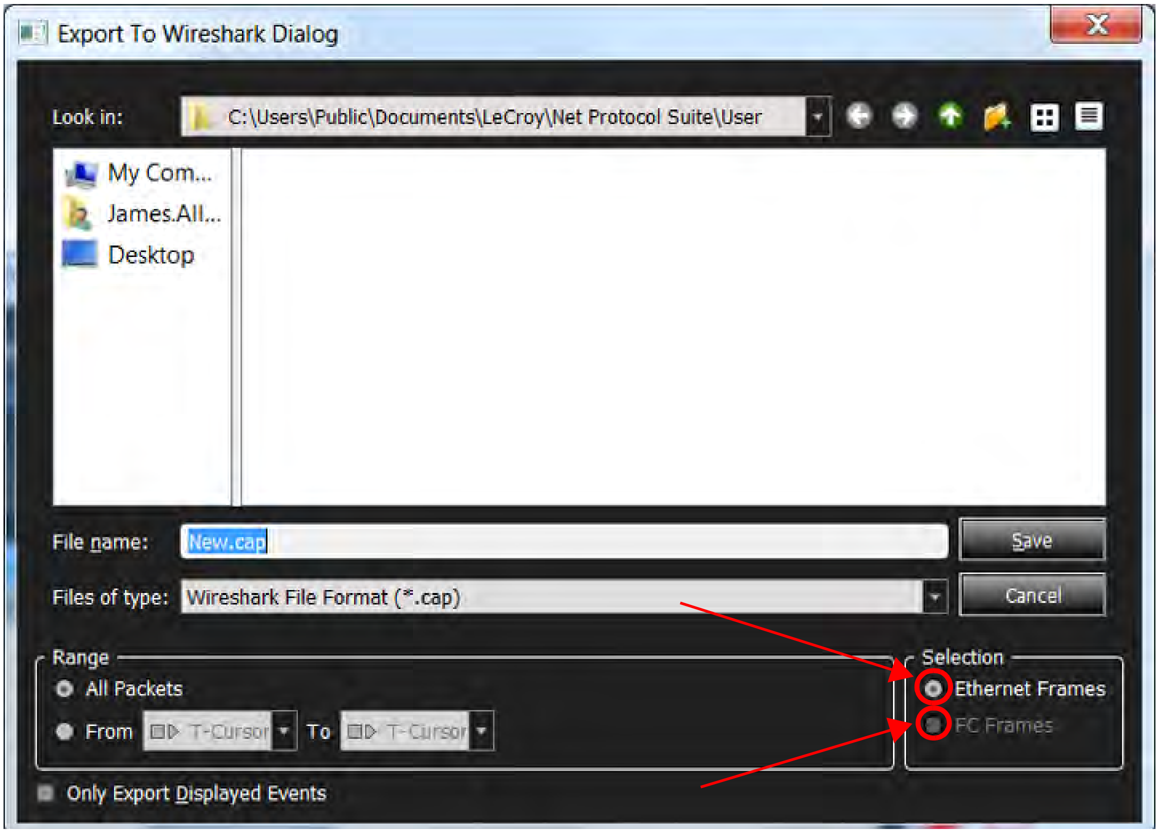


Figure 3.41: Export to Wireshark Window

3.2.1.11 Exit the Application

If you decide to Exit the Application, you can do this one of two ways (Figure 3.42):

- Selecting **File** → **Exit**

  OR

- Clicking the **X** in the upper right corner of the Main Menu

Several different sequences can occur, depending on what had been Opened (Project or Trace) and whether you want to continue recording or not. A few of those sequences are described in more detail below.

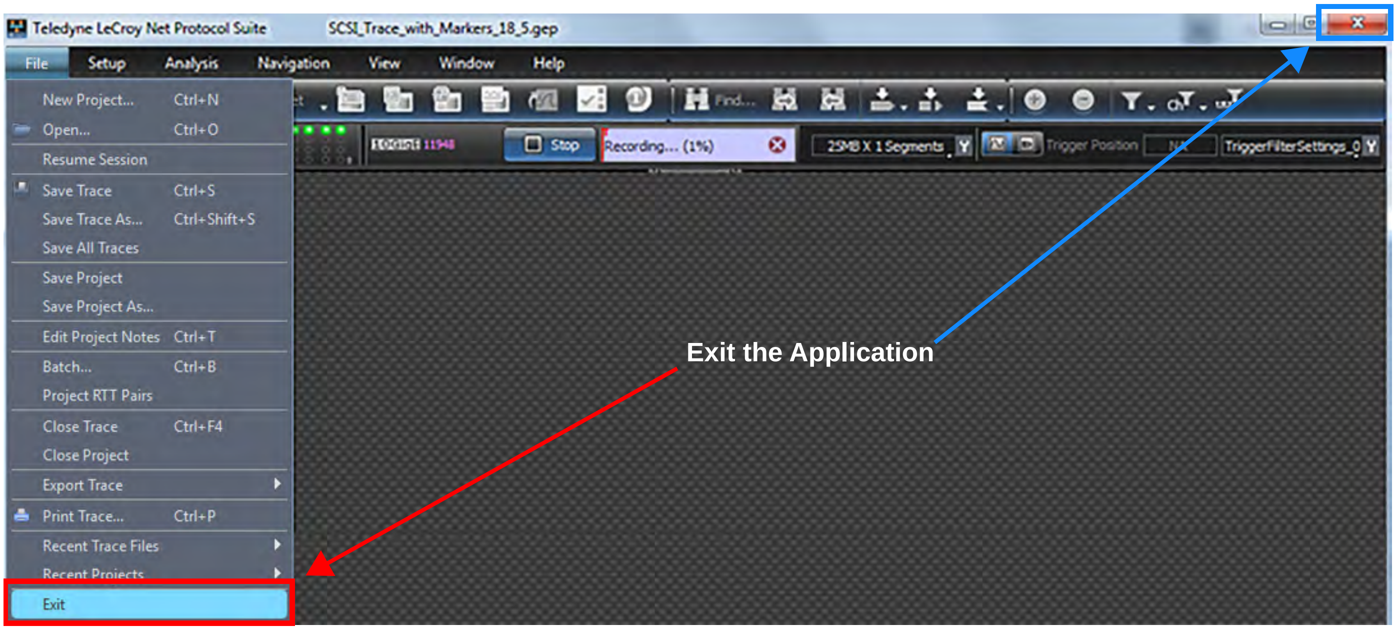


Figure 3.42: Exiting the Application

Not Recording Data Traffic

- ❑ If the Project has not been modified and Exit the Application, the Application will simply close.
- ❑ If the Project has been modified and you want to Exit the Application, the following message dialog will pop up:

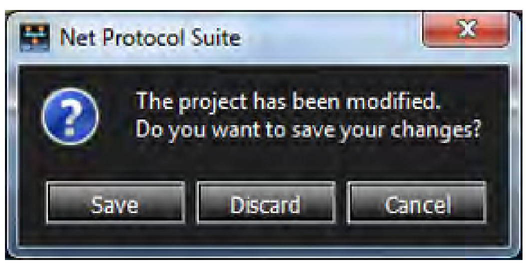


Figure 3.43: Exit the Application (not Record Data)

- ❑ You can decide to Save or Discard any changes made the Project. Once you make your selection, the Application will Exit.

Actively Recording Data Traffic

The process below illustrates Exiting the Application while still recording data traffic.

1. Select **File** → **Exit** or click the **x** in the upper right corner of the Main Menu (Figure 3.42). The the Abort/Pause Session dialog box appears.
2. At this point you can decide to either:
   - Exit the Application, continue Recording Data Traffic, and return to the Session in the future (Figure 3.44).

     OR

- Exit the Application, Abort the Recording of Data Traffic entirely, and lose any Data Traffic that has not already been saved (Figure 3.45).

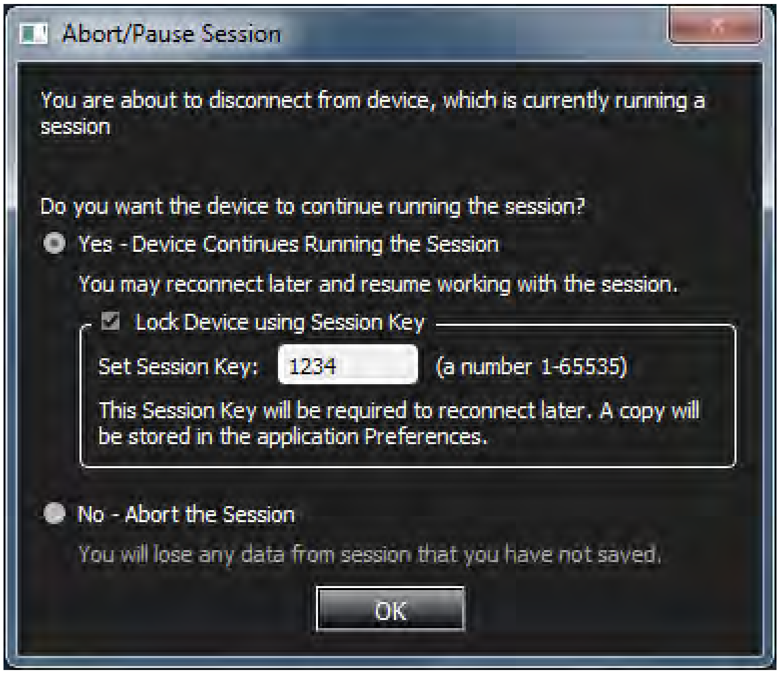


Figure 3.44: Continue the Recording Session

- Click **Yes**. The Application Exits, but data traffic will continue to be recorded and the Project can be Recovered. See 3.2.1.1, *Resume Session*.

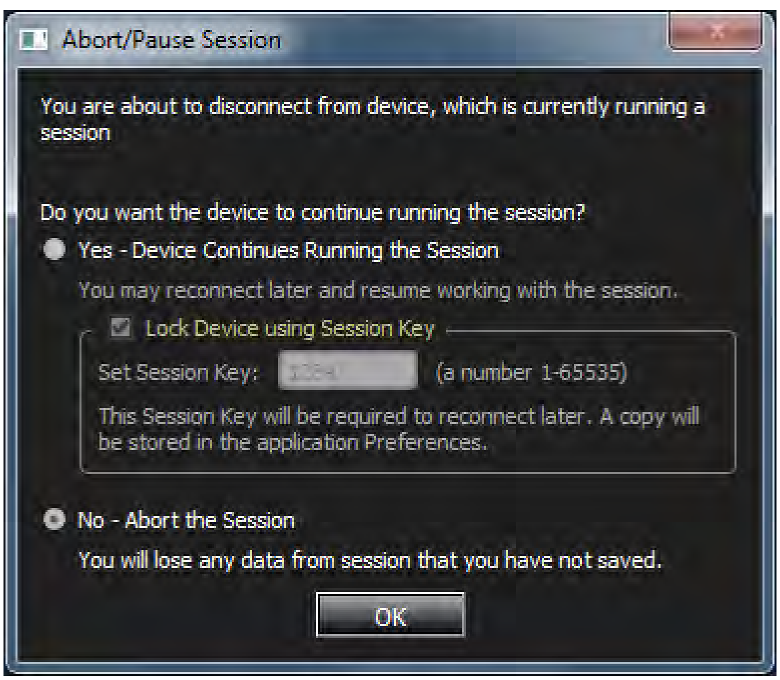


Figure 3.45: Abort the Recording Session

- Click **No**. The Application Exits and any data traffic not already saved will be lost. The Application closes and the Project cannot be Recovered.

3.2.2 Setup

The Setup menu has the following options to setup and configure the device:

- Device Management
- Preferences
- Launch CrossSync Control Panel

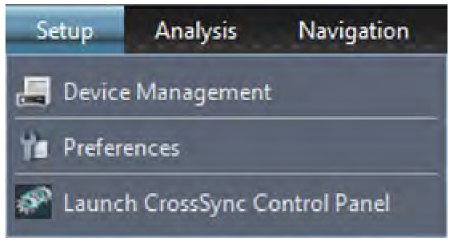


Figure 3.46: Setup Menu

3.2.2.1 Device Management

Click **Device Management** to display the Device Management dialog. Refer to 2.5.1, *Device Management* for more information.

3.2.2.2 Preferences

The Preferences option allows you to set the software and display settings.

Click on **Setup → Preferences** or click  icon to display the Preferences dialog (see figures 3.47 and 3.48).

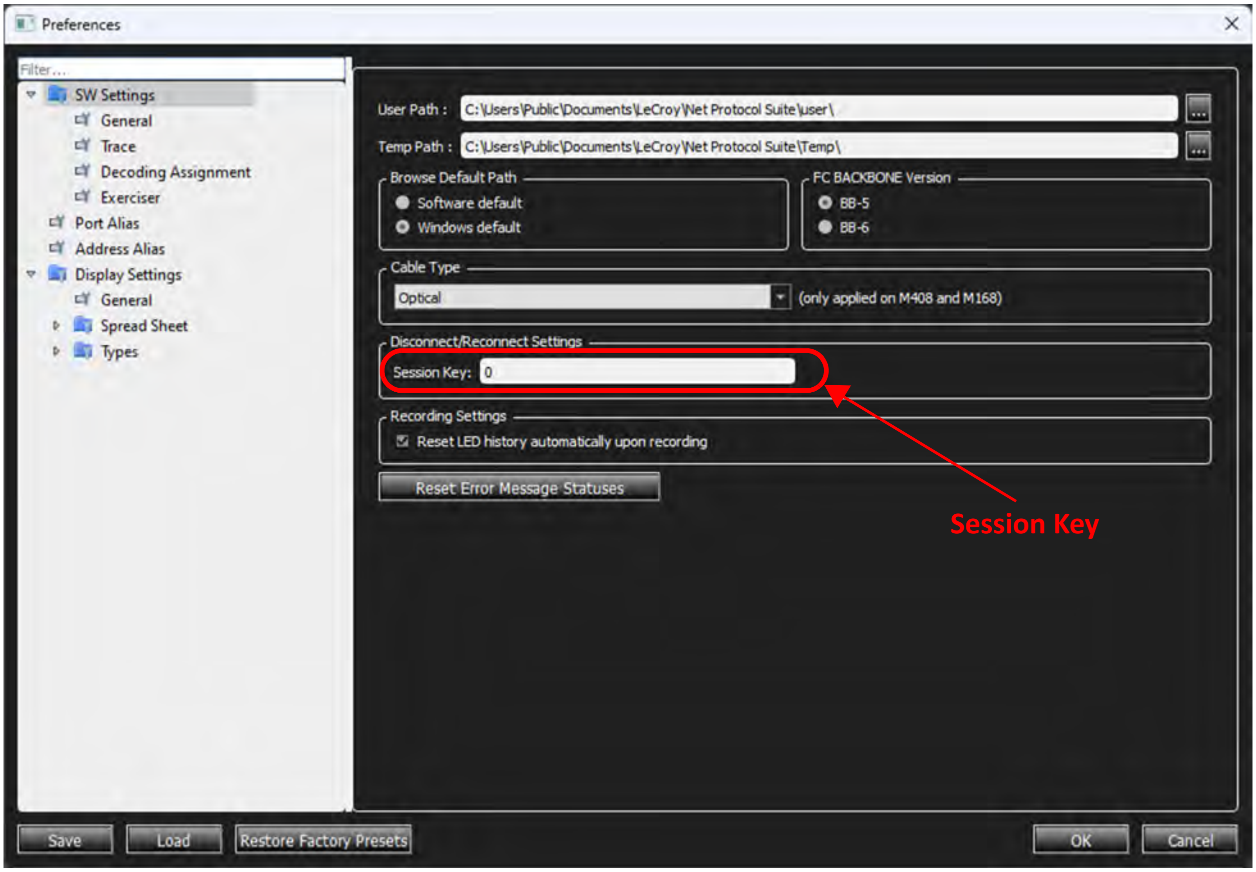


Figure 3.47: Preferences Showing Session Key

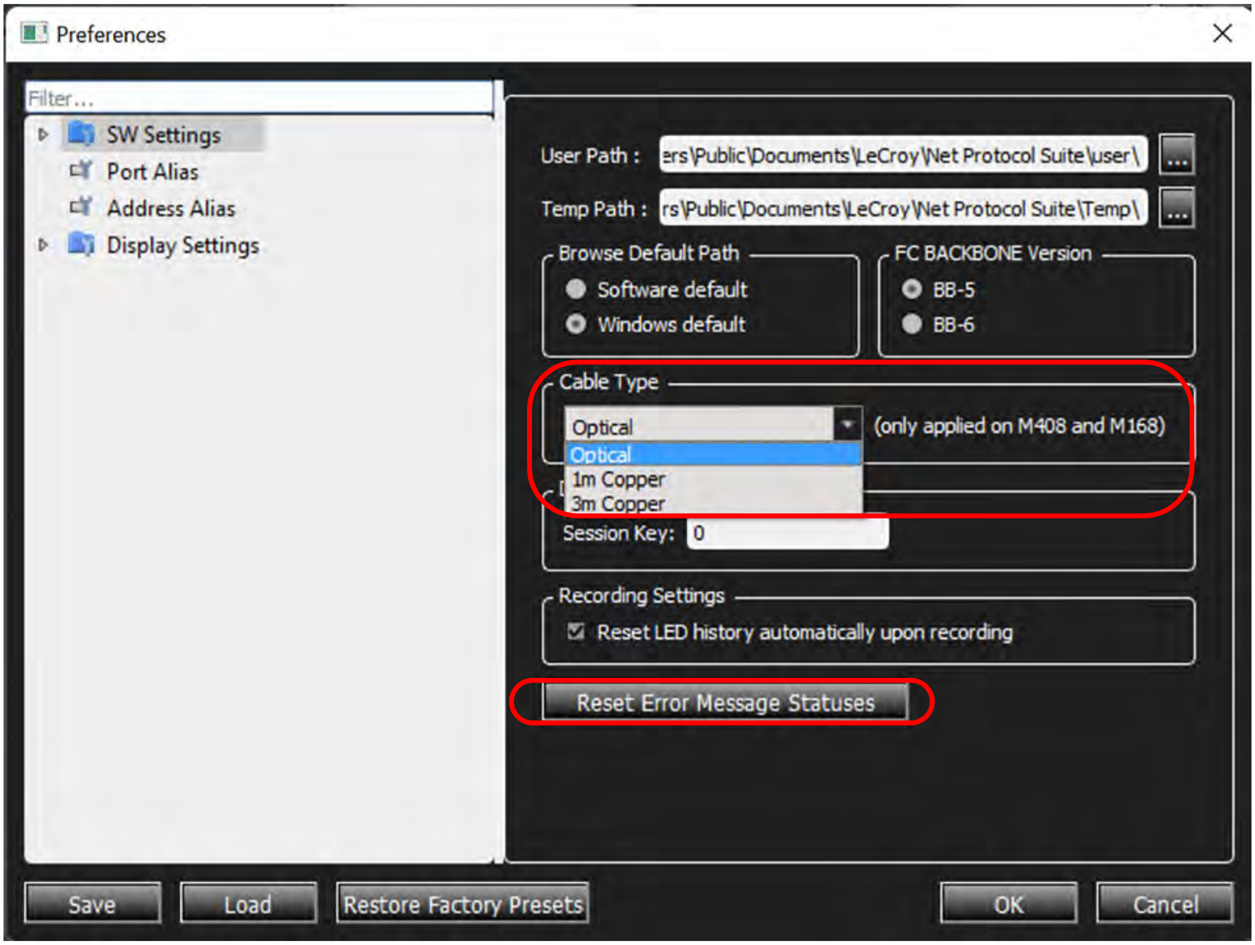


Figure 3.48: Preferences – Cable Type and Reset Error Message Statuses

The following can be configured in Preferences:

- Software Settings
  - General
  - Trace
  - Decoding Assignment
- Port Alias
- Address Alias
- Display settings
- User Path
- Temp Path
- Browse Default Path
  - Software default
  - **Windows**® default
- FC Backbone Version
  - BB-5
  - BB-6

- ❑ Cable Type
  - ■ Optical
  - ■ 1 Meter Copper
  - ■ 3 Meter Copper
- ❑ Recording Settings

  Reset the LED history automatically upon recording (set by default)
- ❑ Reset Error Message Statuses

  Reset message window pops up when successful (Figure 3.49)

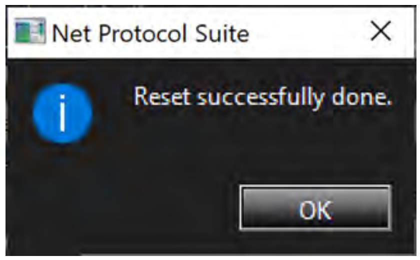


Figure 3.49: Successful Reset Prompt

3.2.2.3 Software Settings

Software Settings allow you to define template files for new Analyzer projects, to specify how trace files appear when opened, and to set Spec Assignment.

General Settings

In General Settings you can select the User Path and Temp path by clicking the ... icon, or you can browse to one of the default paths that are Software default and **Windows** default.

- ❑ Select BB-5 or BB-6 for the FC BACKBONE Version.
- ❑ Select Cable Type from the drop-down list. See Figure 3.50.

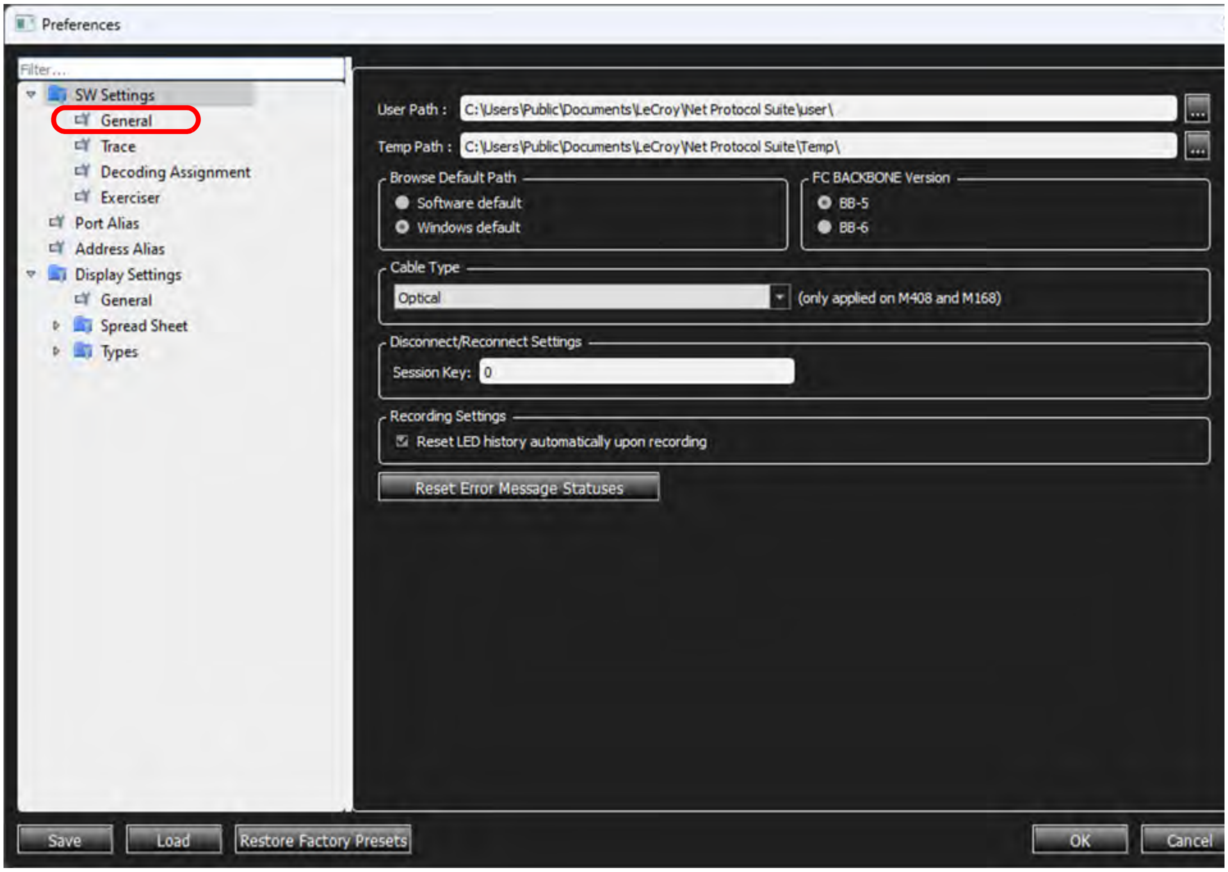


Figure 3.50: Software Settings General Options

Trace View

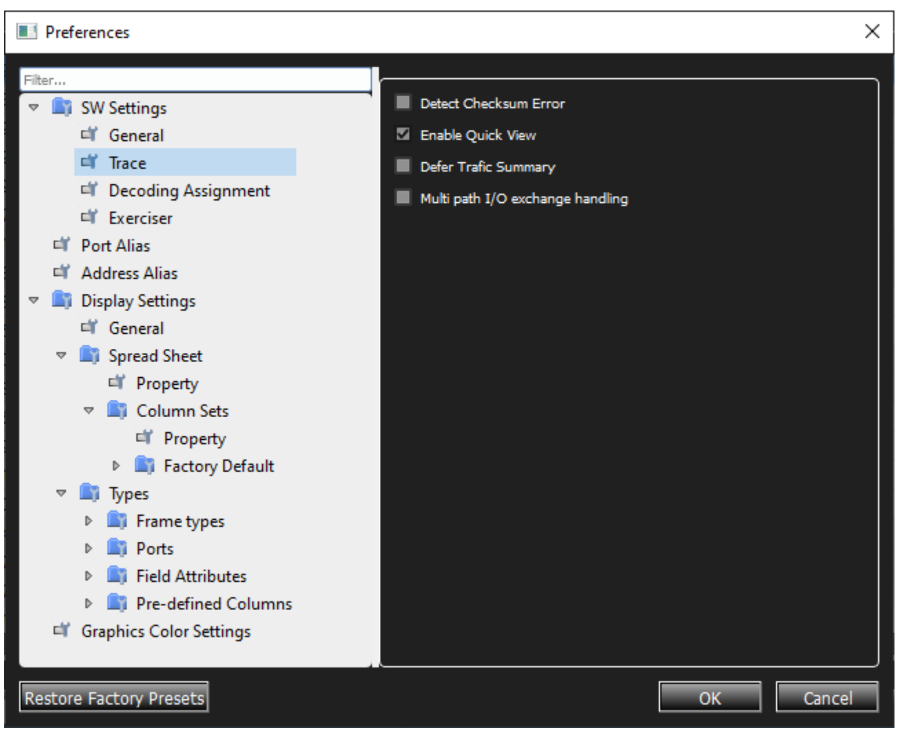


Figure 3.51: Trace View Dialog Box

By default, the Software Settings enable **Quick View**. Quick View allows full access to the whole trace more quickly, especially when using a Gigabit Ethernet connection. However, the trace is NOT written to the host machine hard drive. To save the trace, you must manually select **Save** or **Save As**.

- If you select **Save**, the application saves the entire trace to a default file name. The trace remains open and its name is updated to reflect the saved location.
- If you select **Save As**, the application saves the trace to the specified location, and opens that trace from the new location. The original Quick View mode trace remains open as well.
- If you de-select (disable) **Quick View** in the Software Settings, the trace loads more slowly, but is automatically saved to the host machine hard drive. When Quick View is **Enabled**, the Viewer displays successive parts of trace data as they upload. As soon as a trace part uploads, it is available in all trace views.
- If you only need quick successive traces, and do not need to save them, keep the default setting to enable Quick View.
- If you need to save all captured traces, de-selecting **Quick View** loads the traces faster, especially for larger traces and slower connections.
- To refresh the viewer display with more uploaded data, scroll to the end of the trace, using scroll bars, page down, arrow down, or CTRL-End. Newly uploaded data then appears there.

NOTE: High-level decoding and statistics are available only after the whole trace has uploaded.

- After the trace finishes uploading, the software automatically switches to full trace view.
- To go to the beginning of an uploaded trace, press CTRL Home, or CTRL End to go to the end of an uploaded trace.

Decoding Assignments

In the **Preferences** dialog you can see the default decoders available. These settings enable you to customize which protocol decoders are applied to new traces or when displaying previously captured traces. You can add different port numbers or SCSI spec assignments. There is also a **Decoding Script Path** you can use to load a custom decoding script. Any changes you make will become the default decoding assignments for all traces. The final section allows you to add a custom script to different Protocols and traffic types. See Figure 3.52.

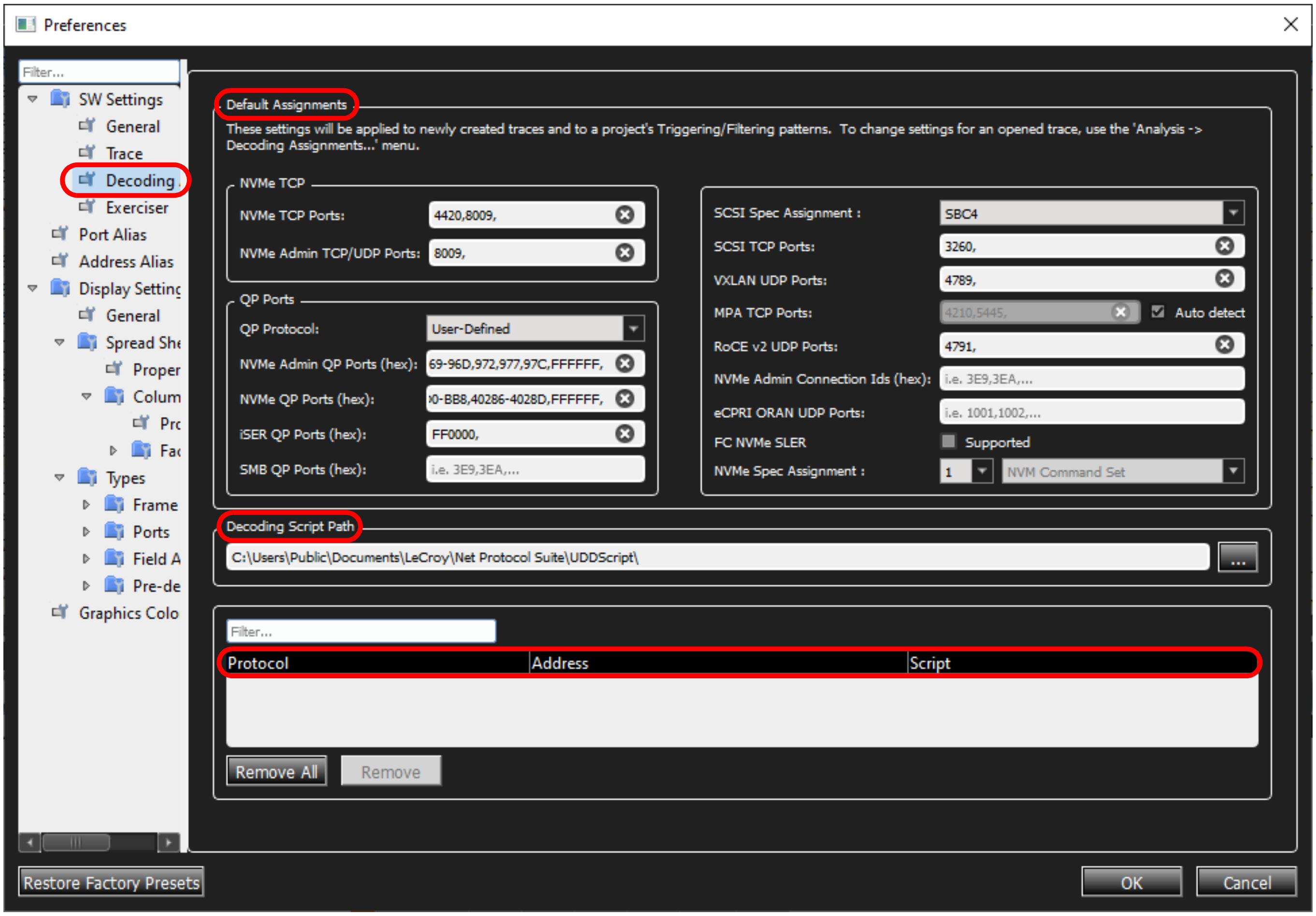


Figure 3.52: Decoding Assignments

Description of Settings: Default Assignments

- SCSI Spec Assignment: Select which SCSI command set to apply for decoding of SCSI commands.
- SCSI TCP Ports: Set which TCP ports are assigned for the iSCSI protocol.
- VXLAN UDP Ports: Set which UDP ports are assigned for the VXLAN protocol.
- MPA TCP Ports: Set which TCP ports are assigned for the MPA protocol on specific ports or selecting Automatic MPA Detection.
- IB BTH UDP Ports: Set which IB BTH UDP ports are assigned for the IB BTH protocol.
- NVMe QP Ports: Set which aligned port pairs (QP) are assigned for the NVMe protocol.
- iSER QP Ports: Set which aligned port pairs (QP) are assigned for the iSER protocol.

Description of Settings: Decoding Script Path

Script Path: Set the base script directory used for looking up user-defined decoding scripts. Refer to *5.1.1, Decoding Assignments* for details on assigning script decoders.

Description of Settings: Protocol, Address and Script

You can selectively Remove a single protocol or Remove All.

- Ethernet: ARP
- Ethernet: LLDP
- IP: UDP
- IP: LLDP
- IP: HOPORT
- RROCE
- MAD over RROCE

These settings can also be controlled from the Main Toolbar: 5.1.1, *Decoding Assignments* on a trace by trace basis.

SCSI Spec Assignment

The Decoding Assignments allow the user to configure SCSI command set assignments (see 3.53, *SCSI Spec Assignments*), well-known port numbers assignments, and decoding script assignments.

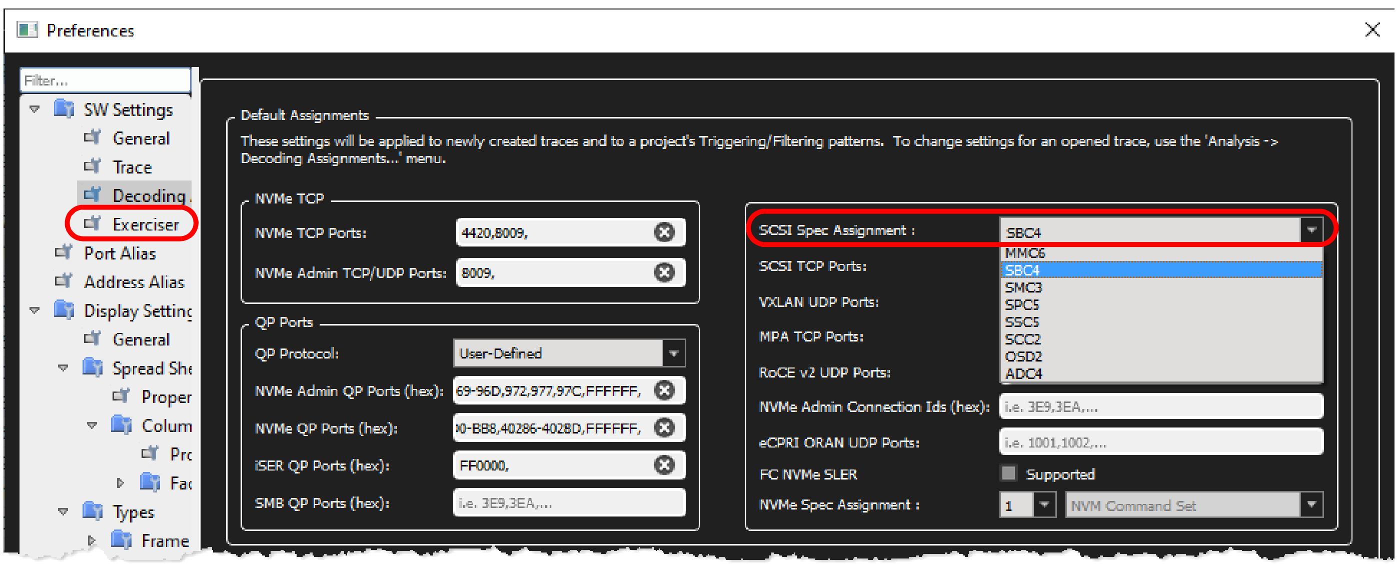


Figure 3.53: SCSI Spec Assignments

Automatic MPA Detection

The MPA TCP Ports can be set to the default ports of 4210 and 5445 or Automatic MPA Detection, which changes the MPA TCP ports from the assigned ports to any port.

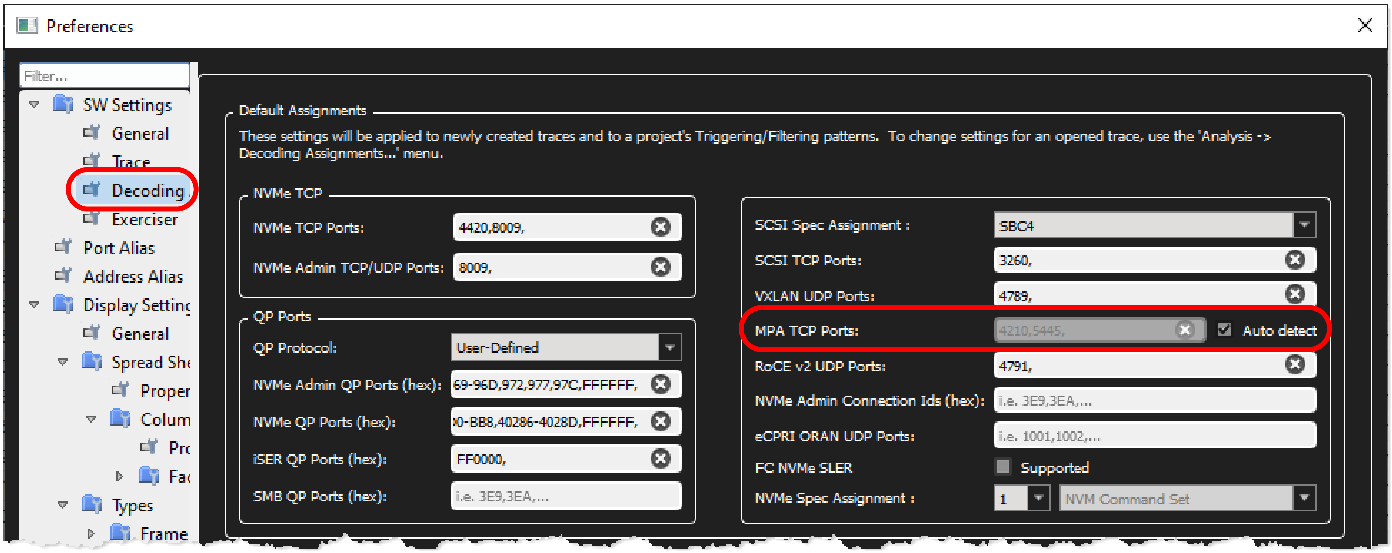


Figure 3.54: Automatic MPA Detection

NVMe Spec Assignment

Decoding Assignments allows you to configure which NVMe QP ports are detectable and to select the NVMe Spec Assignment. You can select to decode per NVMe spec 1 or NVMe spec 2, which allows you to choose the NVM Command Set, Key Value Command Set, or Zoned Namespace Command Set. See Figure 3.55.

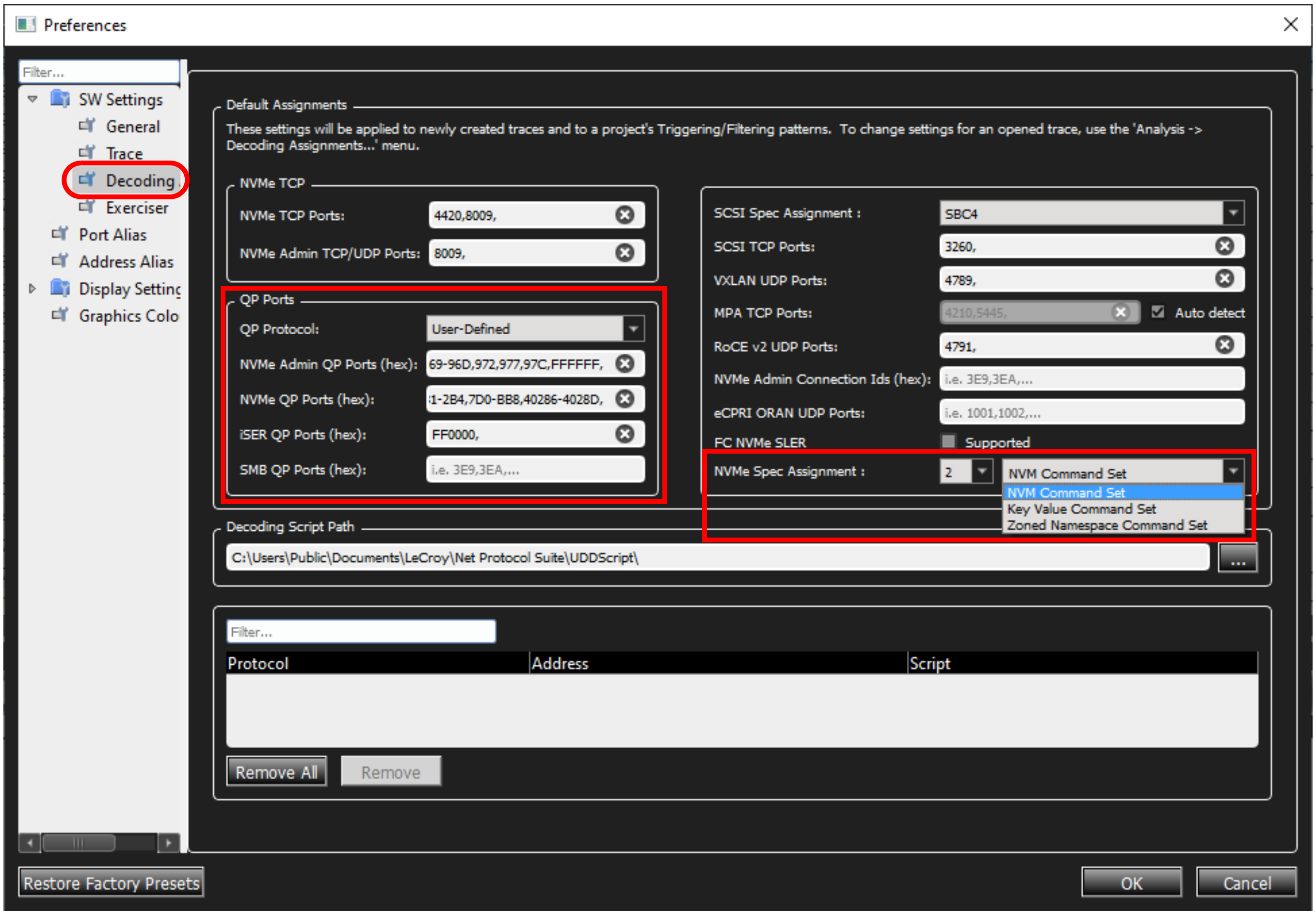


Figure 3.55: Preferences – NVMe QP Ports

Port Alias

Port Alias allows you to assign a meaningful name to each port to assist in interpreting the results displayed in the trace view. You can set the alias name for each port. Double click an Alias Name then enter a preferred name. See Figure 3.56, below.

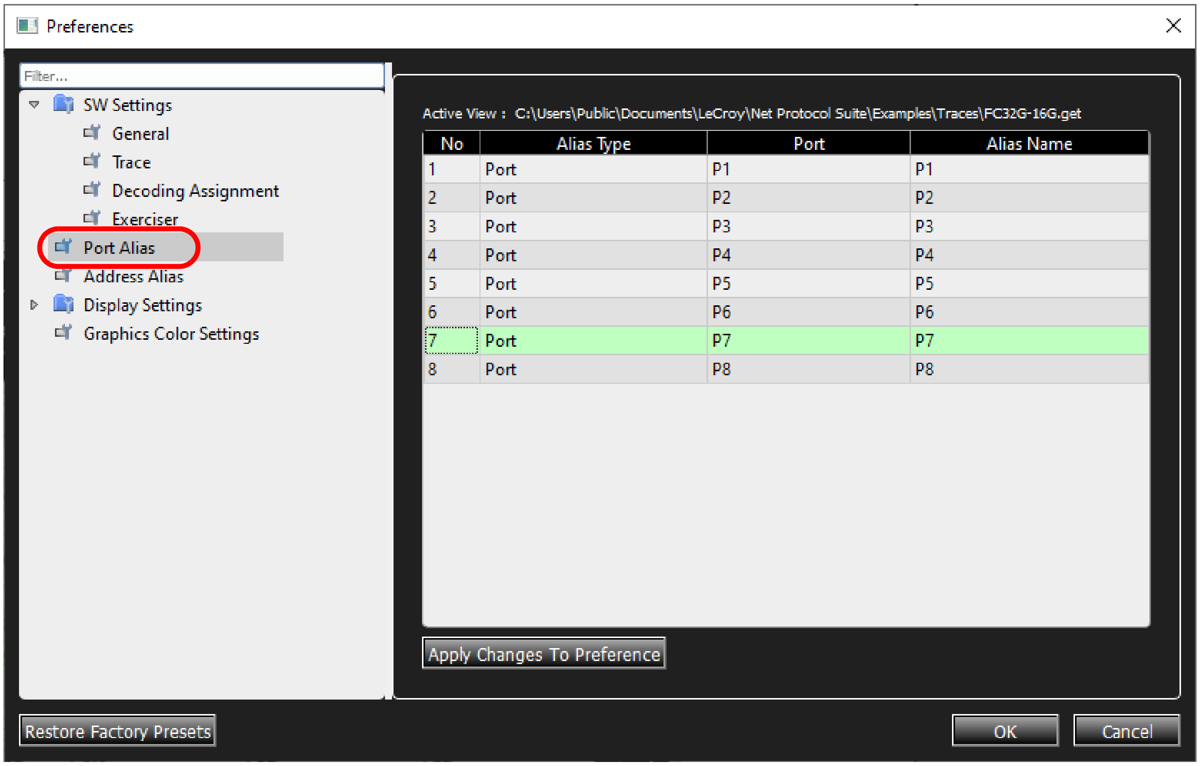


Figure 3.56: Port Alias Window

Address Alias

Address Alias allows you to assign a meaningful name to each address to assist in interpreting the results displayed in the trace view You can set the alias name for each address. Double click an Alias Name and enter a new name. See Figure 3.57.

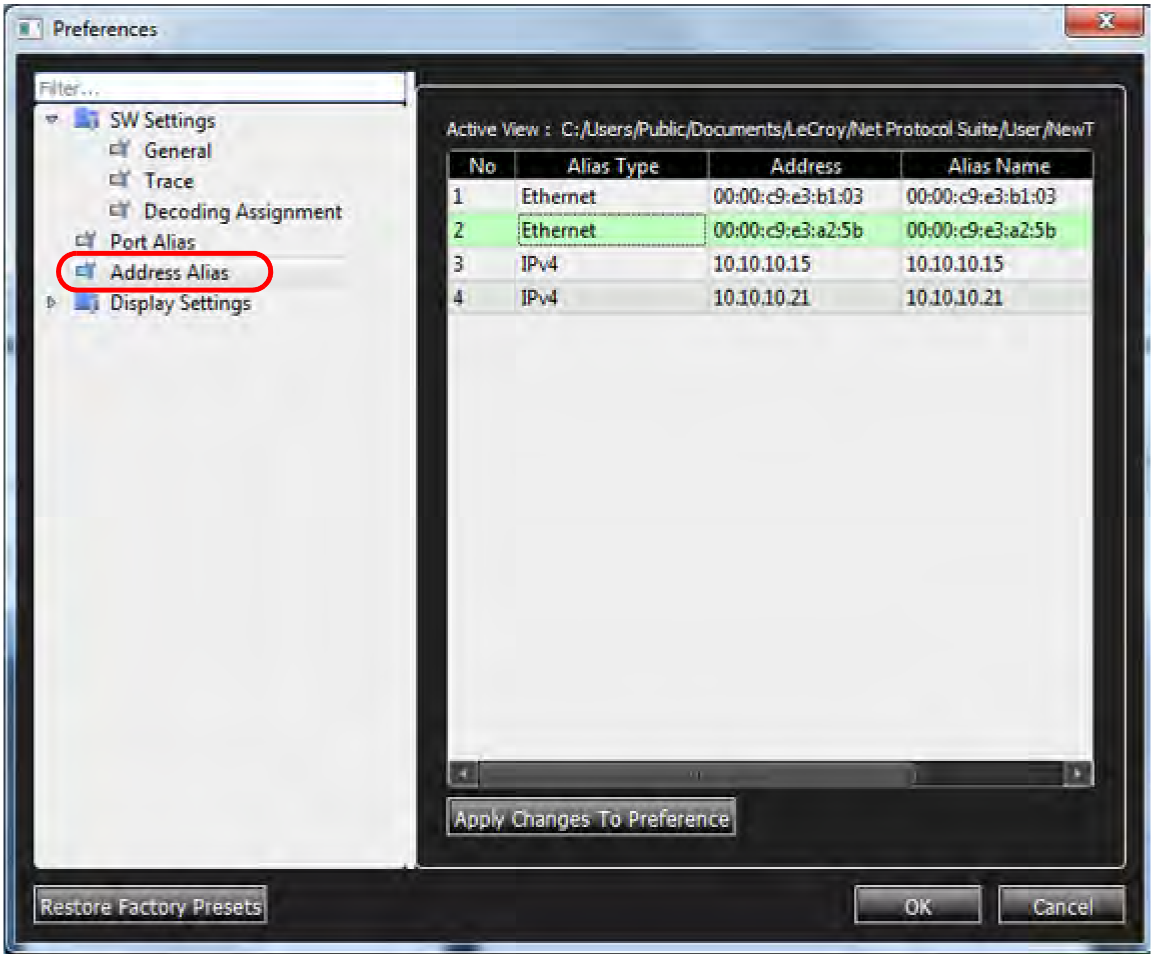


Figure 3.57: Address Alias Window

3.2.2.4 Display Settings

General

In *General* you can select the Time options and the Data Payload options from the drop-down lists. See Figure 3.58.

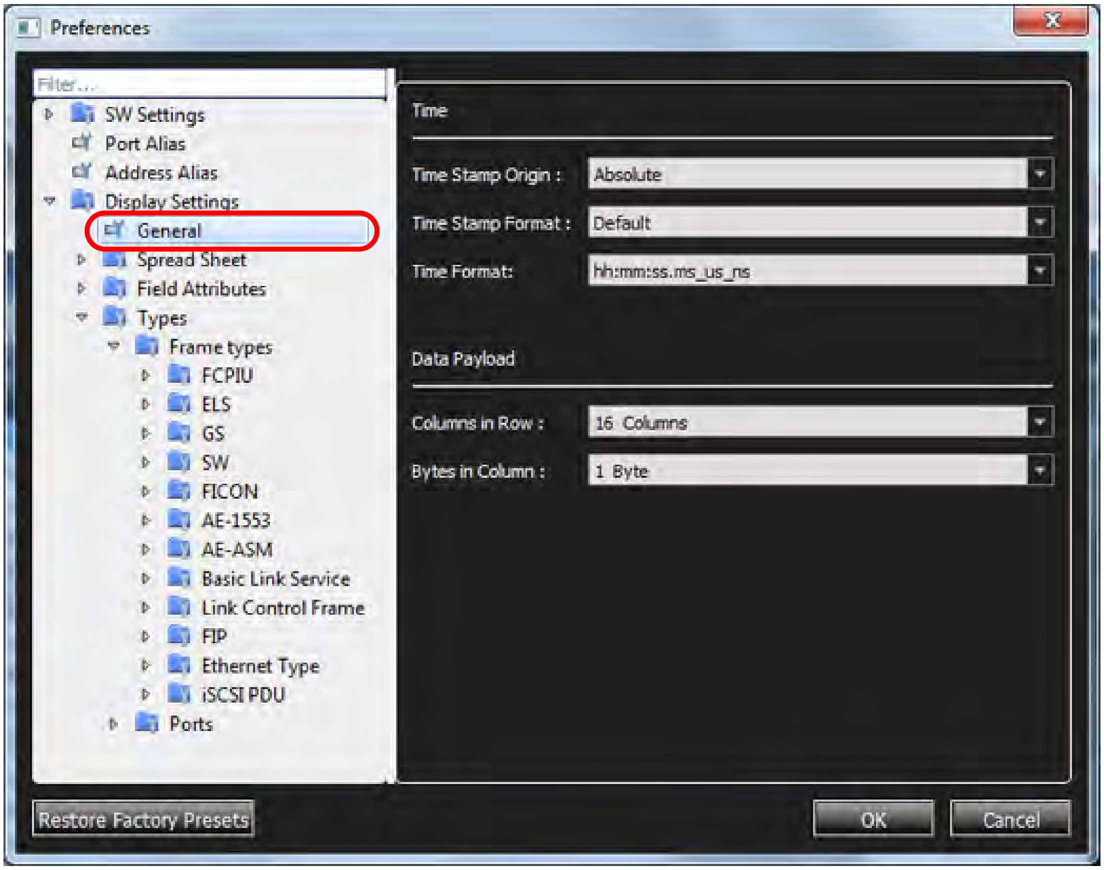


Figure 3.58: General Display Settings Window

Spreadsheet Property Settings

Under *Spreadsheet*, click **Property** and select a **Color Setting** option for row and column from the list. See Figure 3.59, below.

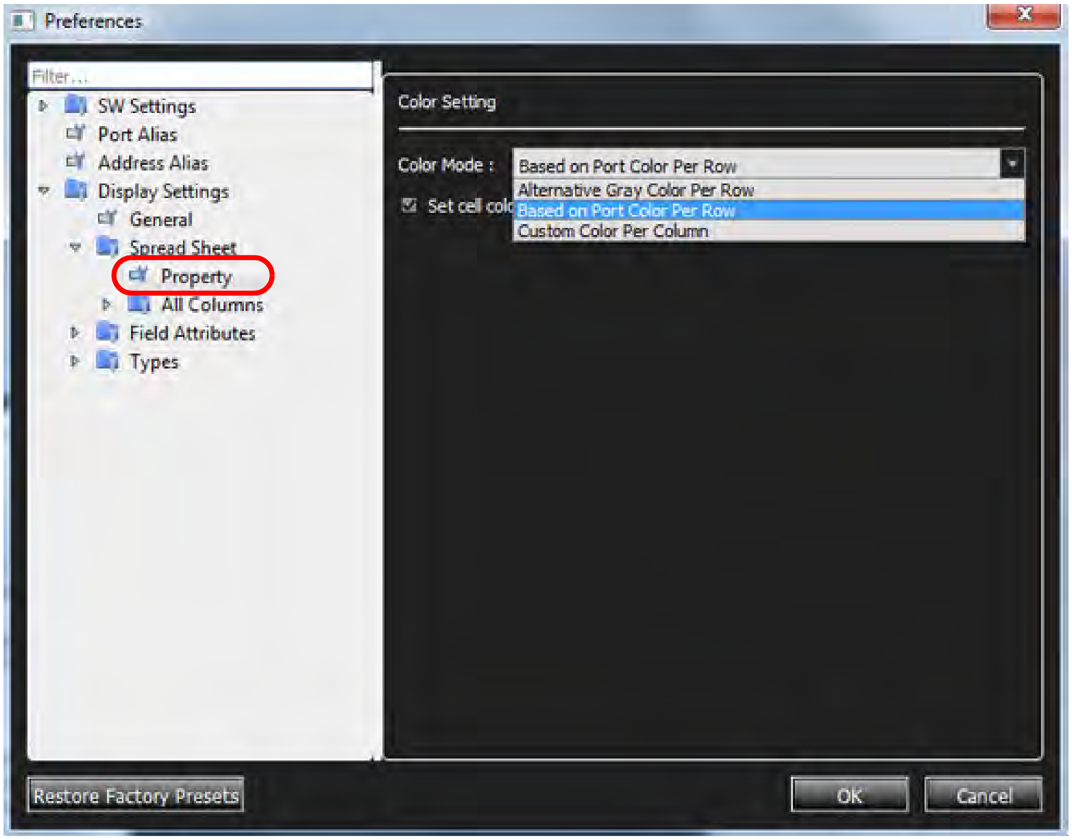


Figure 3.59: Display Settings Spreadsheet Property Window

NOTE: From S/W version 1.85 onward the default color setting for the entire row is based on the port color. See Figure 3.60 as an example.

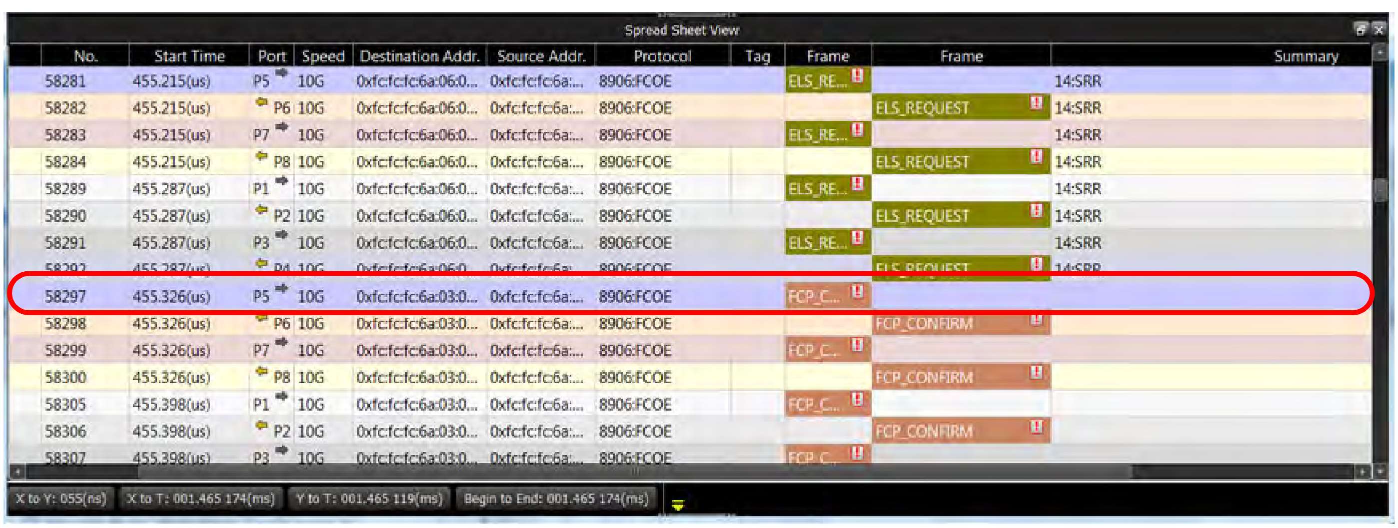


Figure 3.60: Row Color Based on Port Number

To see all of the default column headings, select **All Columns → Columns** for a Trace opened in Spreadsheet View. See Figure 3.61.

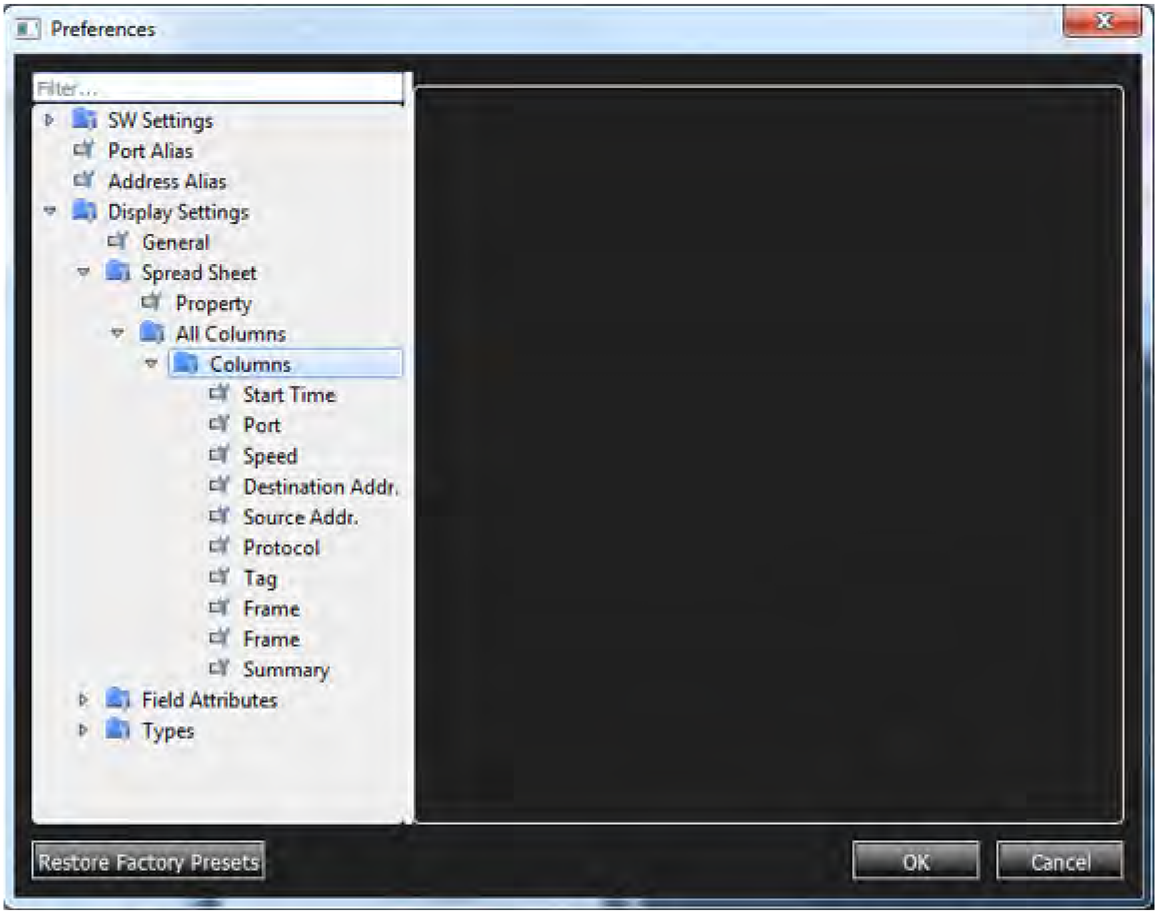


Figure 3.61: Preferences, Display Settings

If you load a previously saved Trace, you will see the following Spreadsheet View (Figure 3.62):

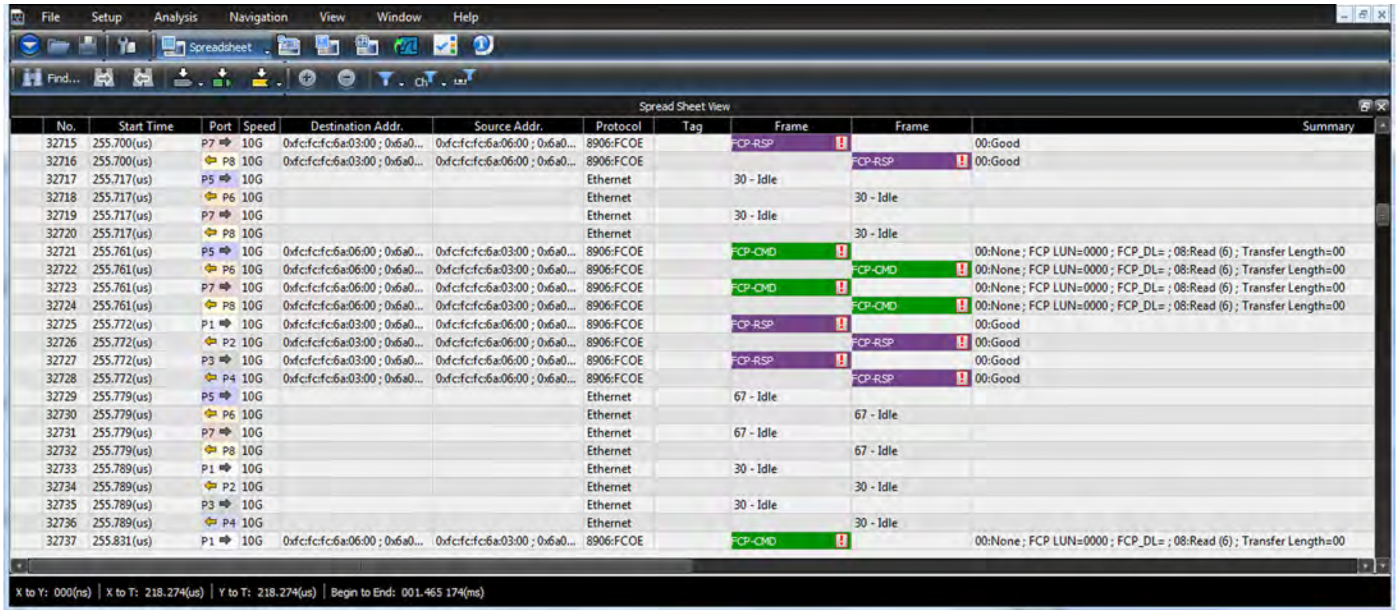


Figure 3.62: Spreadsheet View: Default Column Settings

Change Column Headings

1. To modify column headings and widths, navigate to the *Preferences* window (Figure 3.63).

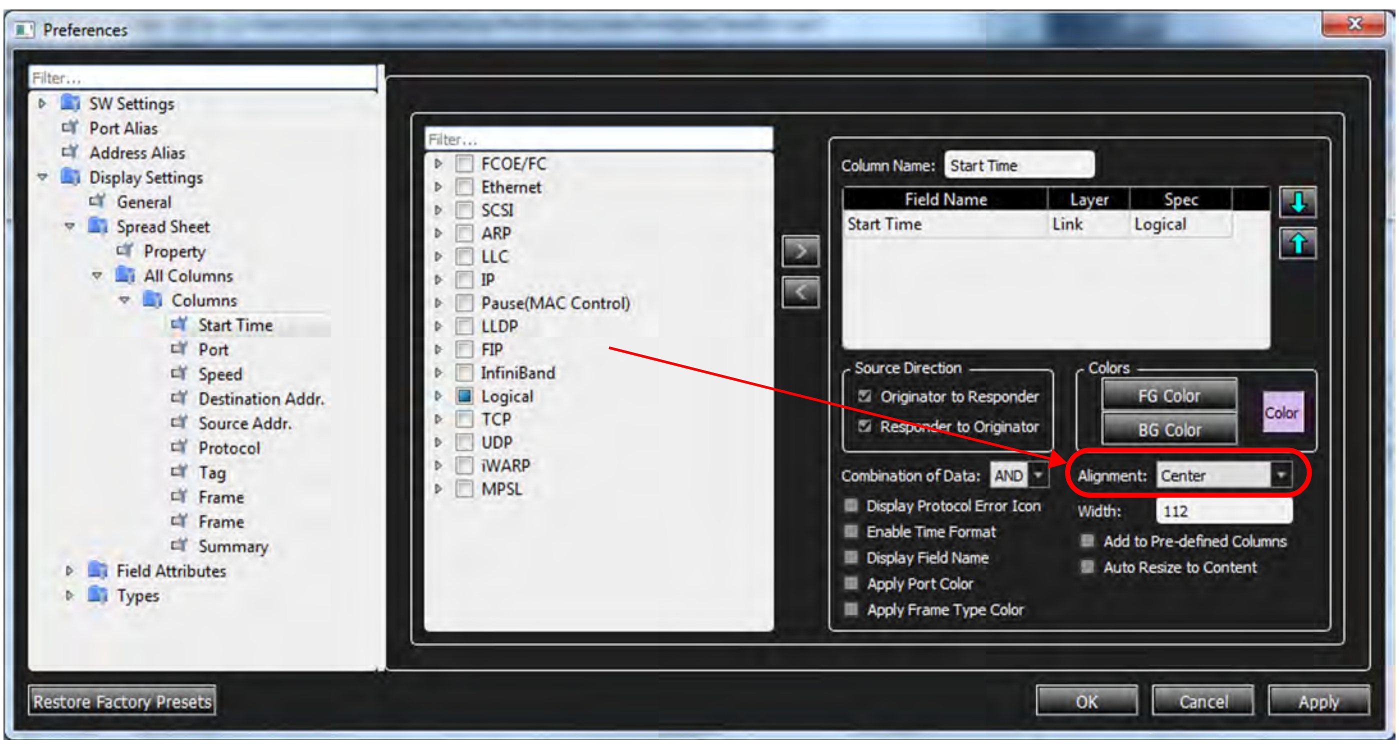


Figure 3.63: Preferences Window

In this example, only the Alignment to Center from Left was changed; however, you can select any of the Columns in the Preferences window pane and change their characteristics.

- Column Name
- Filter
- Source Direction
- Colors
- Combination of Data
- Alignment
- Width

2. Once you have changed the Columns, open a Trace and see the results.

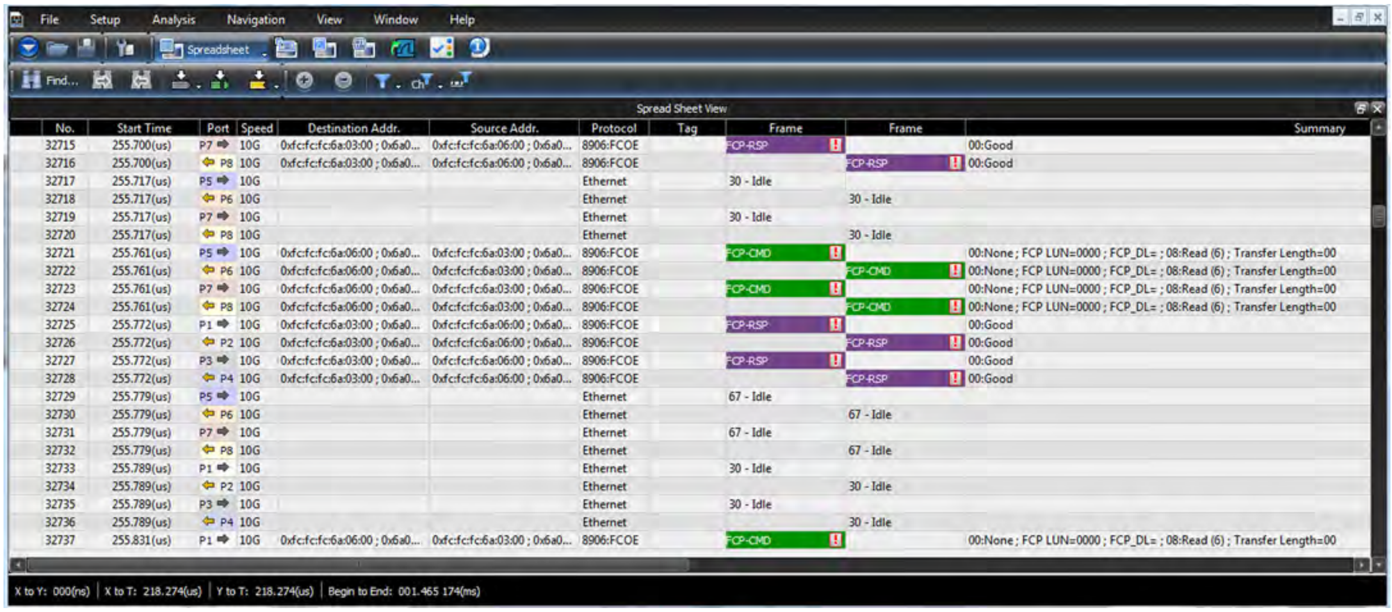


Figure 3.64: Start Time Display is Changed through Preferences

Figure 3.65 is a very simple example of what you can do. It shows changed column widths, column titles, and the filters used for the displayed column information.

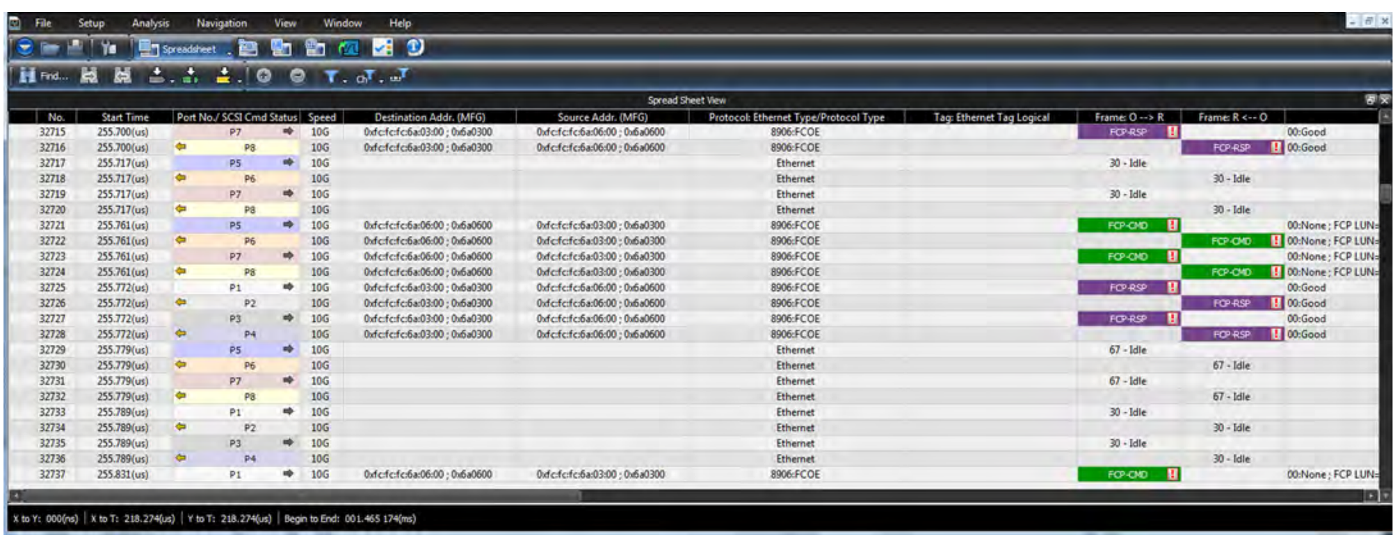


Figure 3.65: Many Changes Made to Column Headings

3. To Save the changes made to the Column Headings, delete the Trace and the Project panes, so that only NetSuite Protocol Tool is open. See figures 3.66 and 3.67.

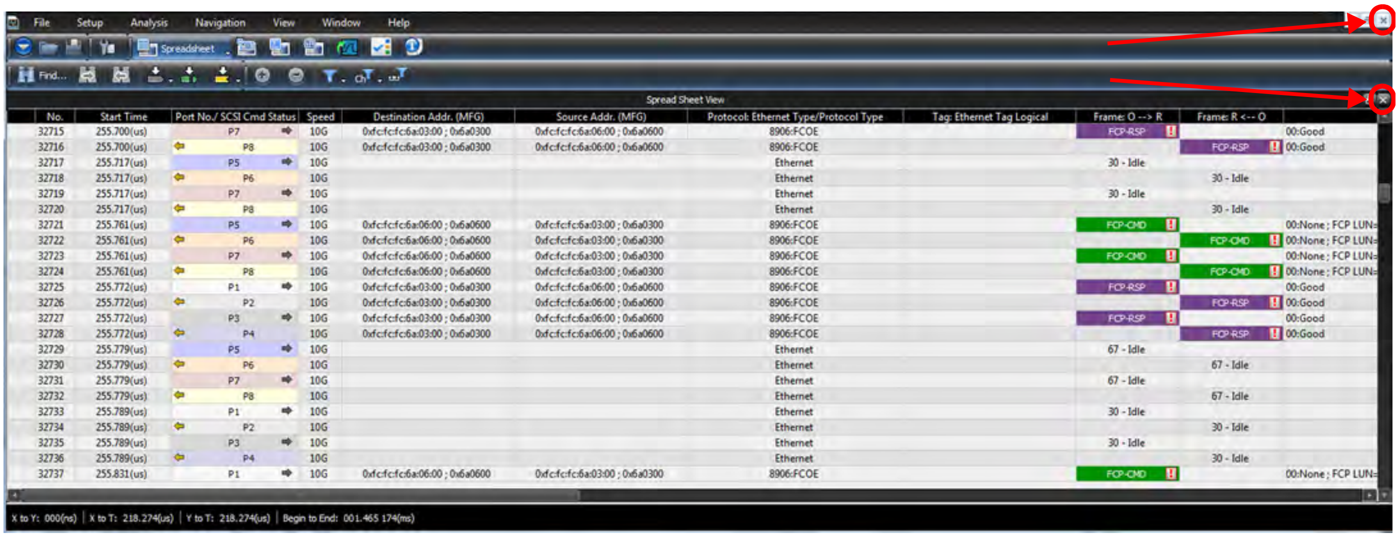


Figure 3.66: Deleting Trace and Project Windows

This leaves only the Net Suite Protocol tool running. See Figure 3.67.

Save a Set of Column Settings

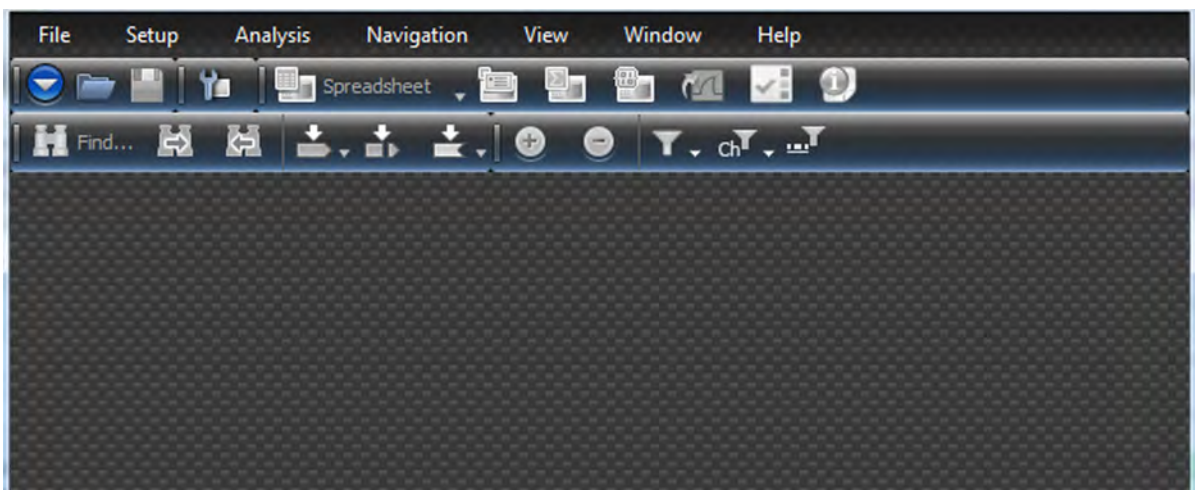


Figure 3.67: Trace and Project Deleted from Net Suite Protocol Dialog

1. Select **Preferences → Display Settings → All Columns → Columns**.

   The dialog window appears containing the **Save** and **Load** buttons (Figure 3.68). Use these buttons to save a set of column changes or load a previously saved set of Column changes.

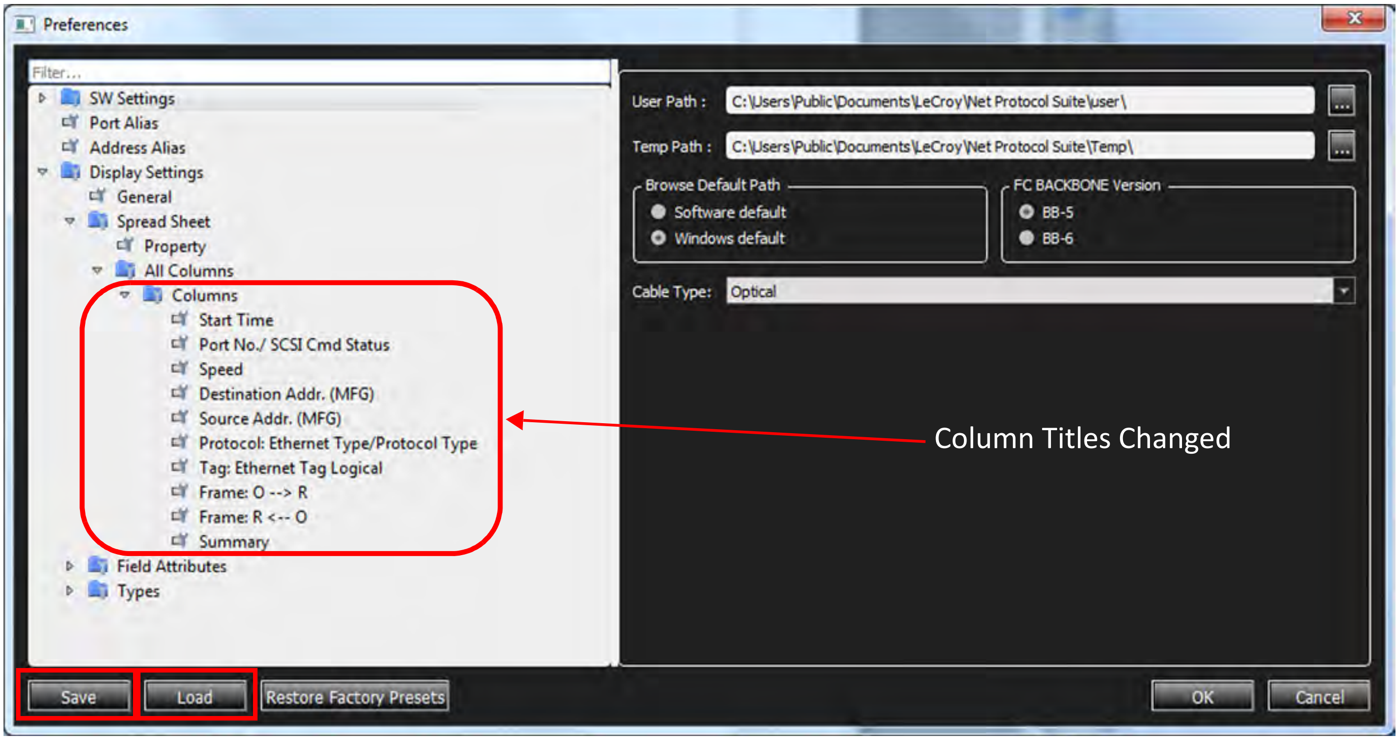


Figure 3.68: Save and Load a Set of Column Settings

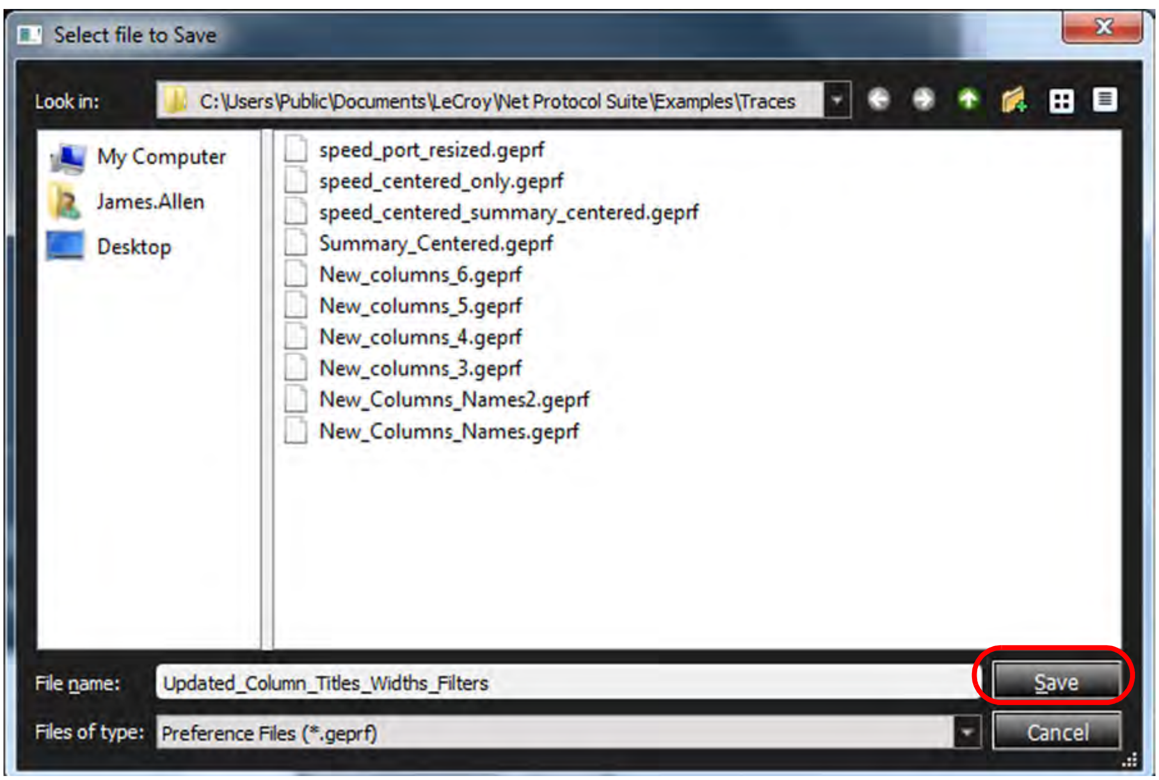


Figure 3.69: Saved Sets of Column Settings

2. To store the set of Column settings, select **Save**.

The following dialog box pops up (Figure 3.70), which verifies the Column Settings have been Saved.

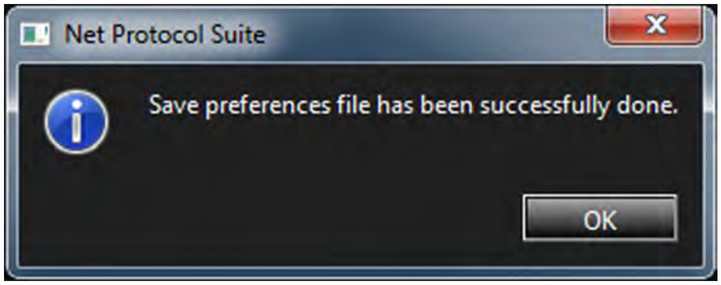


Figure 3.70: Confirmation of Column Settings

Load a Set of Column Settings

1. Launch the Net Protocol Suite tool (Figure 3.67).
2. Select **Preferences → Display Settings → All Columns → Columns**. A dialog box appears with **Save** and **Load** buttons.
3. Use the **Save** and **Load** buttons to Load a previously Saved set of Column changes. See Figure 3.68.

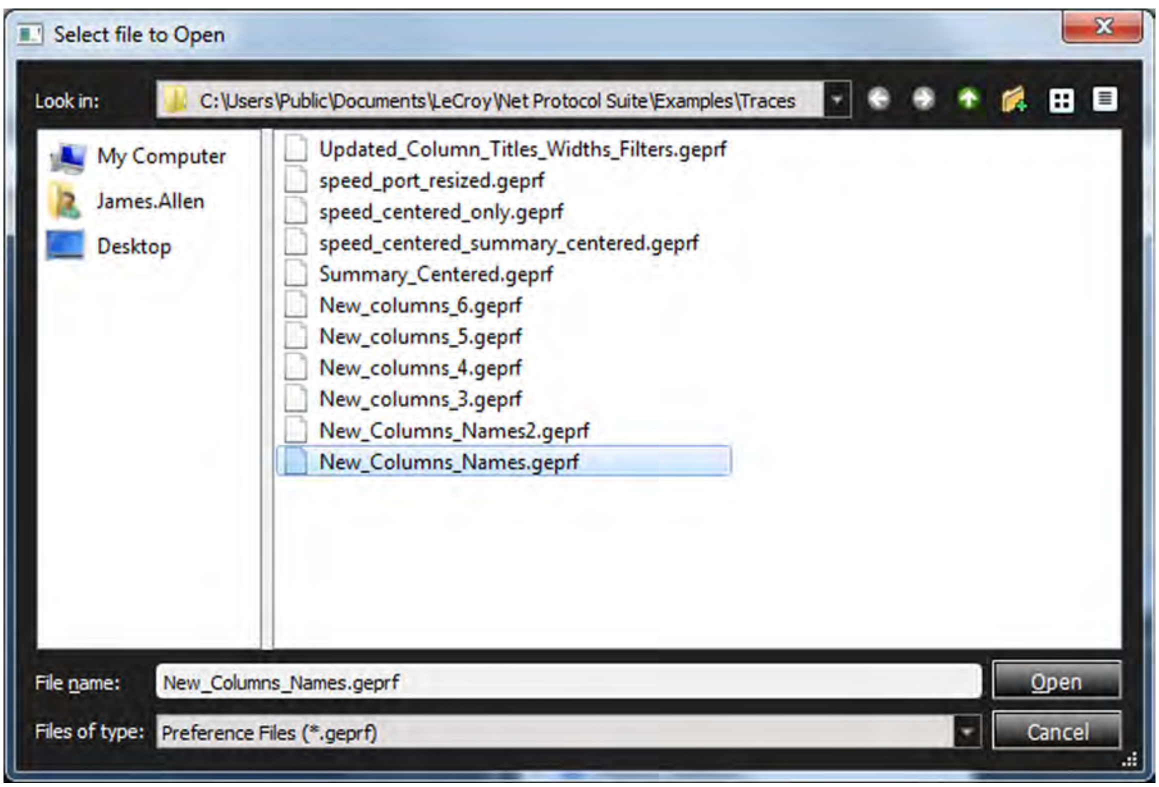


Figure 3.71: Sets of Columns Settings Available to Load

- When the set of Columns settings is successfully loaded, the following pop-up box appears (Figure 3.72).

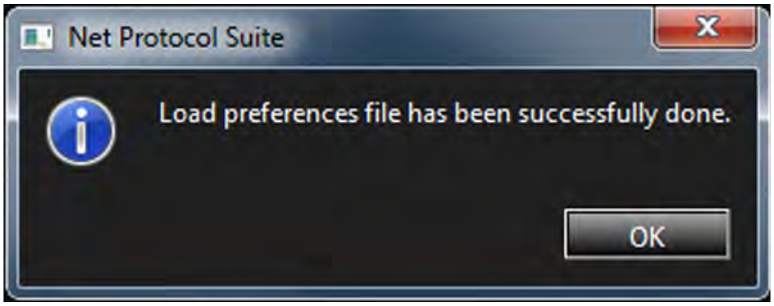


Figure 3.72: Set of Column Changes Loaded Successfully

- When you load a Trace, the set of Columns settings you selected is displayed (Figure 3.73).

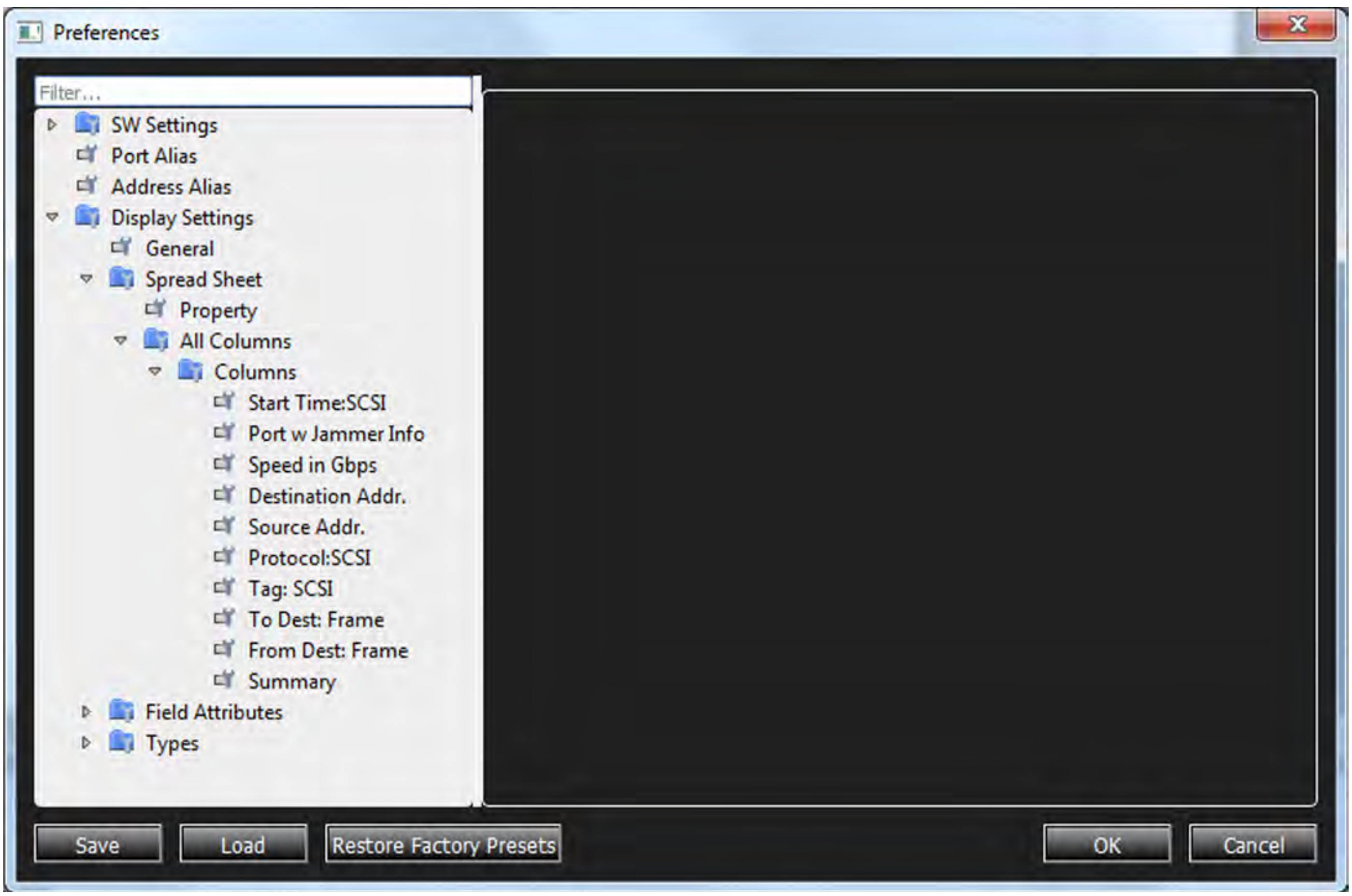


Figure 3.73: New Set of Columns Loaded

- When you load a Trace, a new set of Columns is displayed (Figure 3.74).

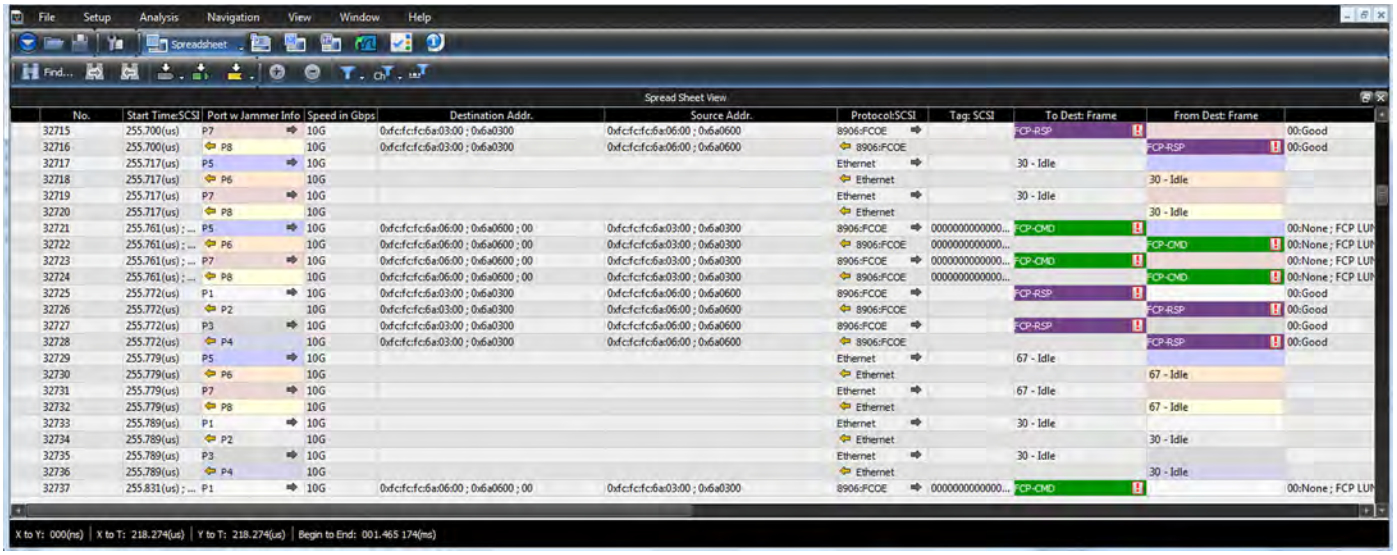


Figure 3.74: Trace Loaded with New Set of Column Headings

3.2.2.5 Display Settings – Field Attributes

In Field Attributes you can click a **Trigger Pattern** and choose the following:

- Format
  - Hexidecimal
  - Decimal
  - Binary
  - ASCII
  - IP
  - Reverse DWORD
  - MAC
  - OUI
- Byte Order
  - Right Align
  - Left Align
- Time Format
  - TBD
  - [Zulu]
- Bit Order
  - LSB-->MSB
  - MSB-->LSB
- Field Header Setting (Preferred Name)
  - In Frame Inspector View
  - In Spreadsheet View

Field Setting, **Color Setting**, and **Field Header Setting** options from the drop-down lists. See the figure below.

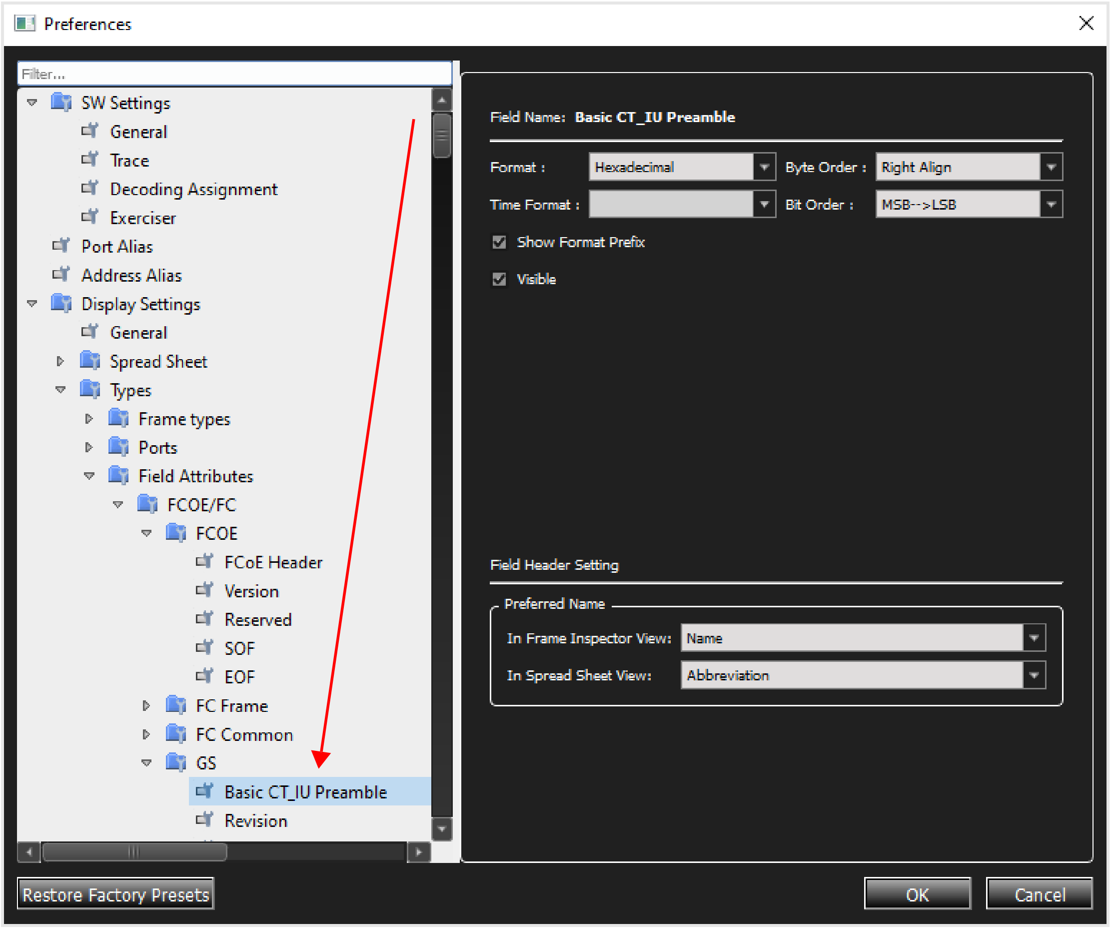


Figure 3.75: Display Settings Field Attributes Window

3.2.2.6 Display Settings – Types

In Frame types you can select the foreground and background Color Setting by clicking on the relevant button. See Figure 3.76 below.

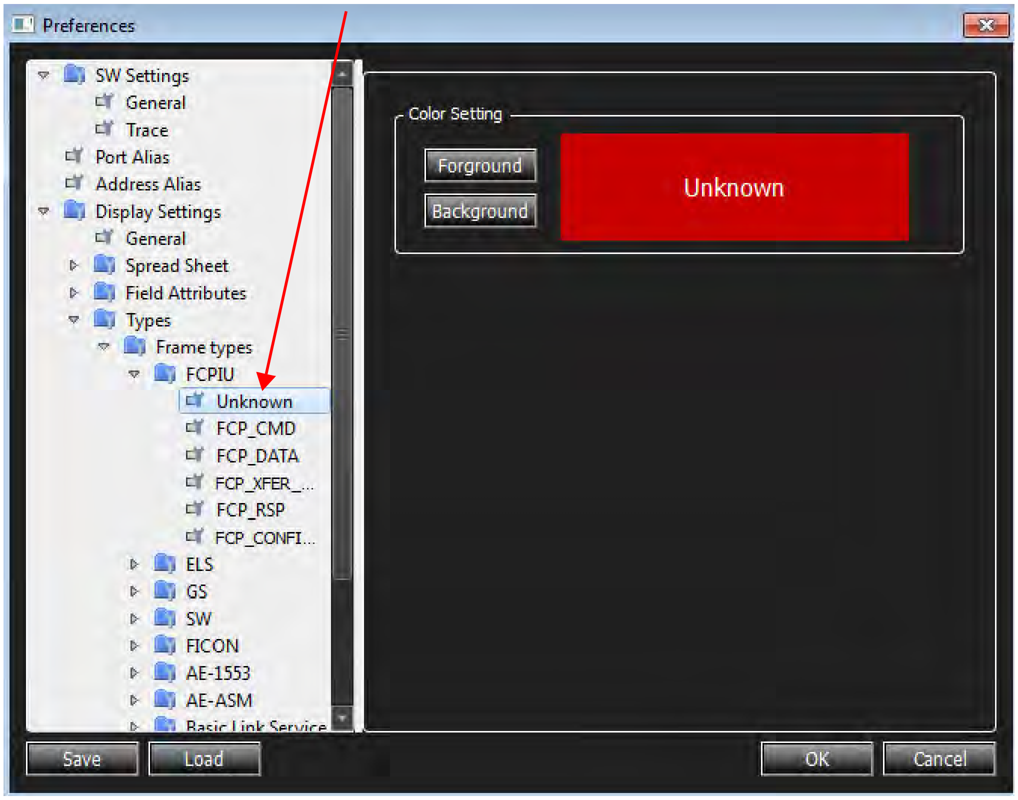


Figure 3.76: Display Settings Frame Types

In Ports you can select the foreground and background Color Setting by clicking on the relevant button. See Figure 3.76.

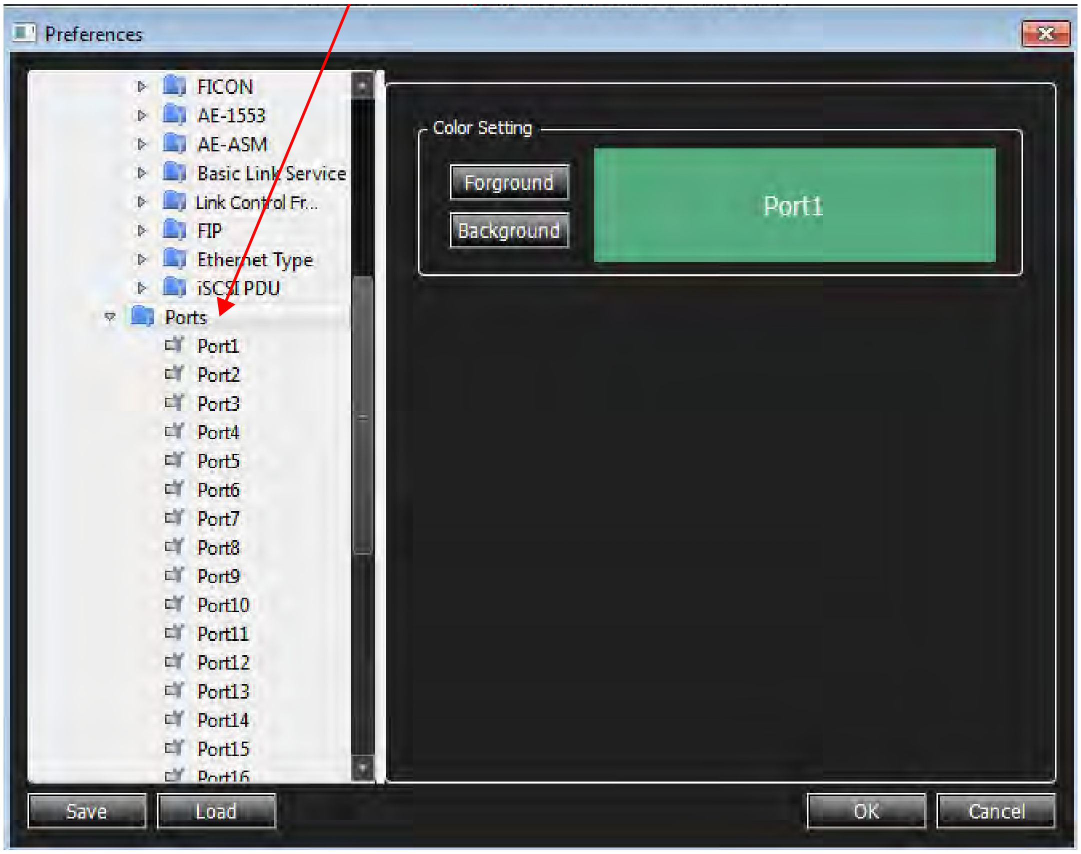


Figure 3.77: Display Settings Ports

3.2.2.7 Show/Hide Format Prefix

In the Spreadsheet View, you can Show or Hide Format Prefixes such as Hexadecimal, Decimal, Binary, ASCII or IP. The following provide and example for using this feature.

1. From Spreadsheet View, click the preferences icon to the left of the Spreadsheet View button in the main tool bar (Figure 3.78). The Preferences dialog window opens (Figure 3.79).

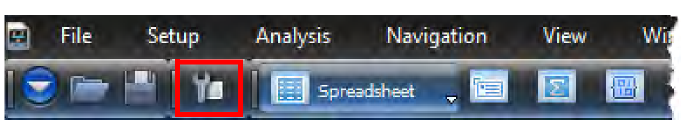


Figure 3.78: Select Preferences for Spreadsheet View

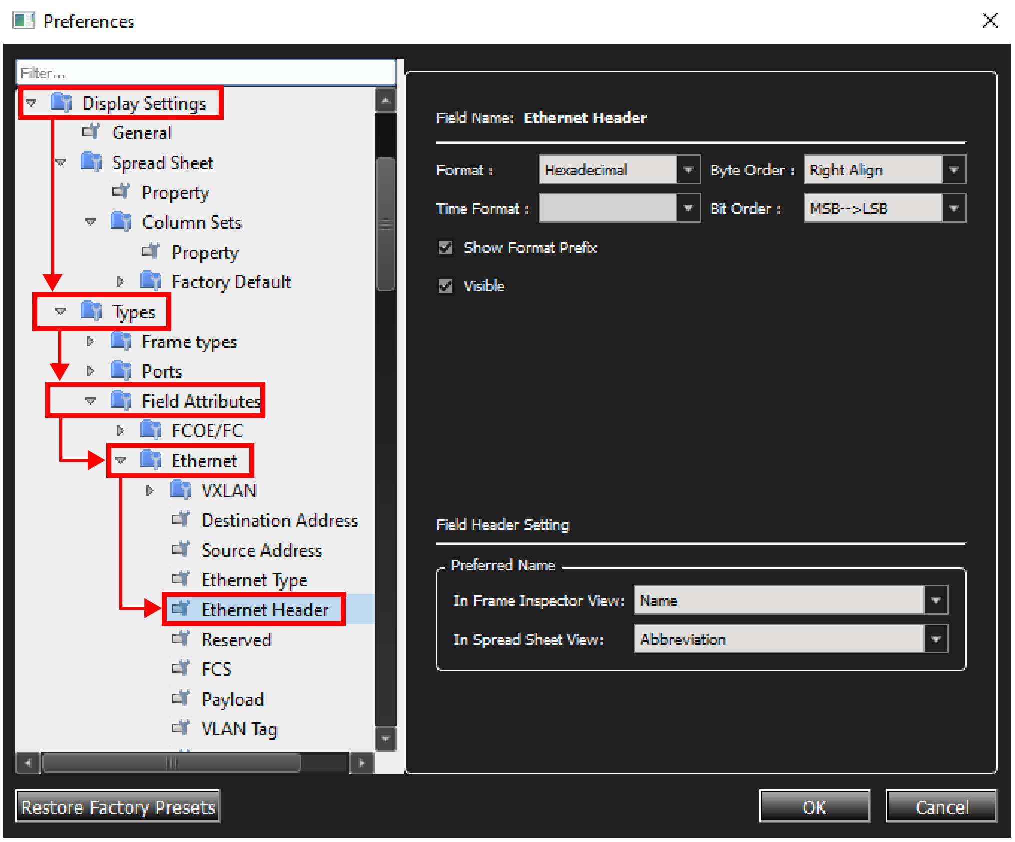


Figure 3.79: Preferences Dialog Window – Spreadsheet View

2. If needed, expand the filter. For example, **Display Settings → Types → Field Attributes → Ethernet** (Figure 3.79).

3. Select **Ethernet Header**, then select the desired **Format** (e.g., **Hexidecimal**) from the Format drop-down list (Figure 3.80).

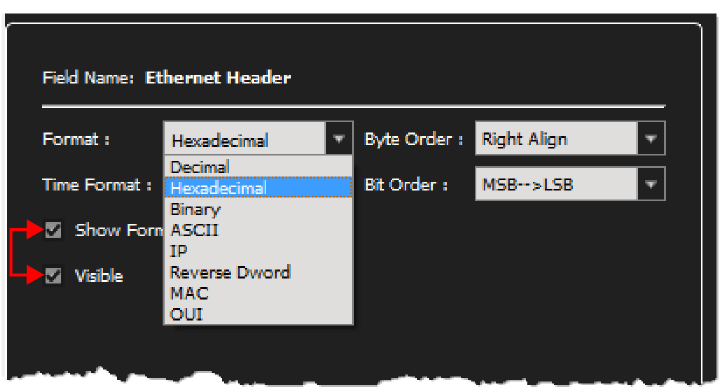


Figure 3.80: Preferences – Format Drop-Down List

4. To display this format, check the boxes for **Show Format** and **Visible**.

   - For Show Hexadecimal Format Prefix, “0x” is pre-pended to the data (Figure 3.81).

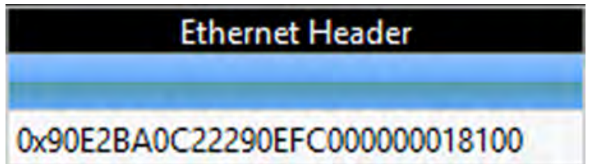


Figure 3.81: Example – Show Hexadecimal Prefix

- If you uncheck the Show Format Prefix box, the Hexadecimal Format Prefix will be removed. See figures 3.81 and 3.82.

5. When you are satisfied with your settings, click **OK**.

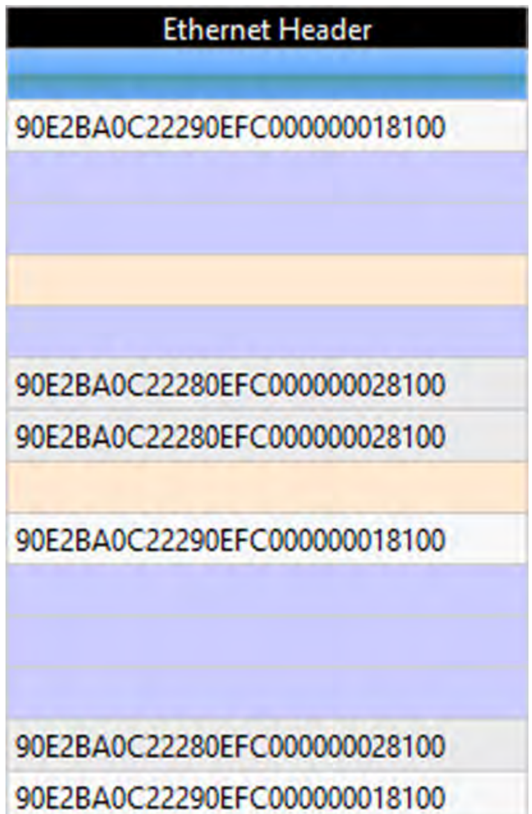


Figure 3.82: Example – Hide Hexadecimal Prefix

NOTE: This functionality applies to every column with appropriate data.

3.2.2.8 Launch CrossSync Control Panel

Click on Launch CrossSync Control Panel to bring up the CrossSync Control Panel allows you to select analyzers for synchronization and manage the recording process. It supports a wide combination of Teledyne LeCroy's flagship analyzers including PCI Express, USB, DDR, Serial ATA (SATA), Serial Attached SCSI (SAS), Fibre Channel (FC) and Ethernet.

CrossSync is Teledyne LeCroy's analyzer synchronization solution that enables time-aligned display of protocol traffic from multiple daisy-chained analyzers showing event traffic from multiple high-speed serial busses. A lightweight software control panel allows users to select analyzers for synchronization and manage the recording process. Captured traffic is displayed using the latest analyzer software (in separate windows) with all the protocol specific search and reporting features.

Captured events are displayed in separate windows that share a common time scale. Navigating the traffic in either direction will scroll to the same timestamp in a synchronized window. When using the CrossSync option, users can access the full complement of analysis capabilities available within the individual Teledyne LeCroy software. Search, reporting, and decoding all operate normally.

This feature is available with the Teledyne LeCroy Net Protocol Suite software application.

Please refer to the *CrossSync Control Panel User Manual* for more information.

See Figure 3.83.

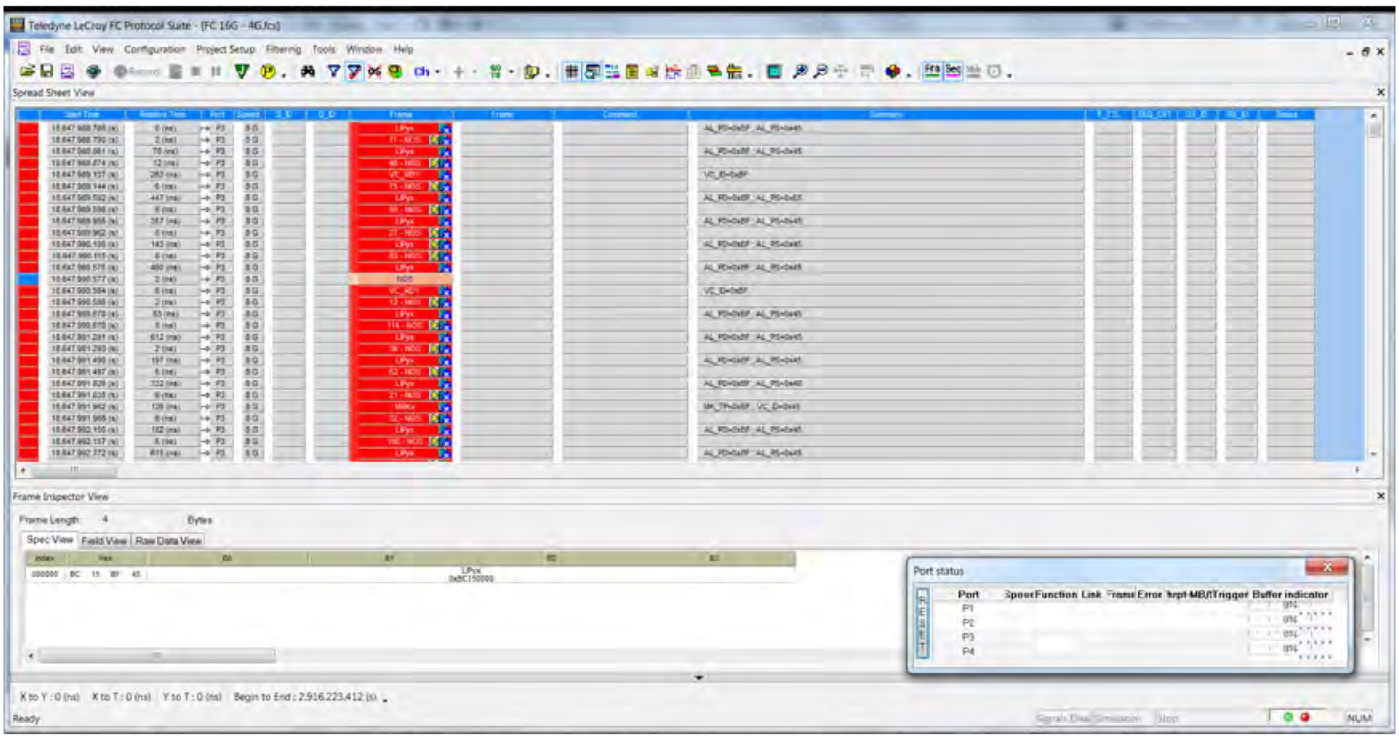


Figure 3.83: CrossSync Control Panel

3.2.3 Analysis

The Analysis menu has the following options to view trace files and specify SCSI decoding assignments:

- Decoding Assignments (see 3.2.3.1, *Decoding Assignments*)
- Spreadsheet View (see 3.2.3.2, *Spreadsheet View*)
- Exchange View (see 3.2.3.3, *Exchange View*)
- Frame Inspector View (see 3.2.3.4, *Frame Inspector View*)
- Traffic Summary View (see 3.2.3.5, *Traffic Summary View*)
- Data View (see 3.2.3.6, *Data View*)
- Bus Utilization (see 3.2.3.7, *Bus Utilization View*)
- Link State View (see 3.2.3.8, *Link State View*)

- Trace Expert (see 3.2.3.8, *Link State View*)
- Trace Information (see 3.2.3.10, *Trace Information*)
- Verification Script (see 3.2.3.11, *Verification Script*)
- RTT Pairs (see 3.2.3.12, *RTT Pairs*)

See Figure 3.84.

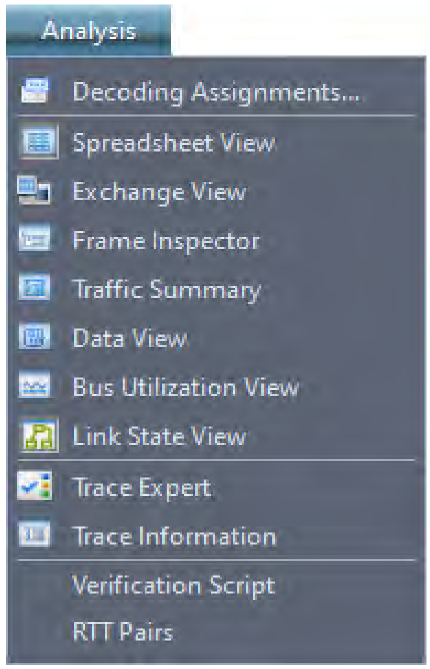


Figure 3.84: Analysis Menu

3.2.3.1 Decoding Assignments

Click on **Analysis** and select **Decoding Assignments** to display the **Decoding Assignments** dialog.

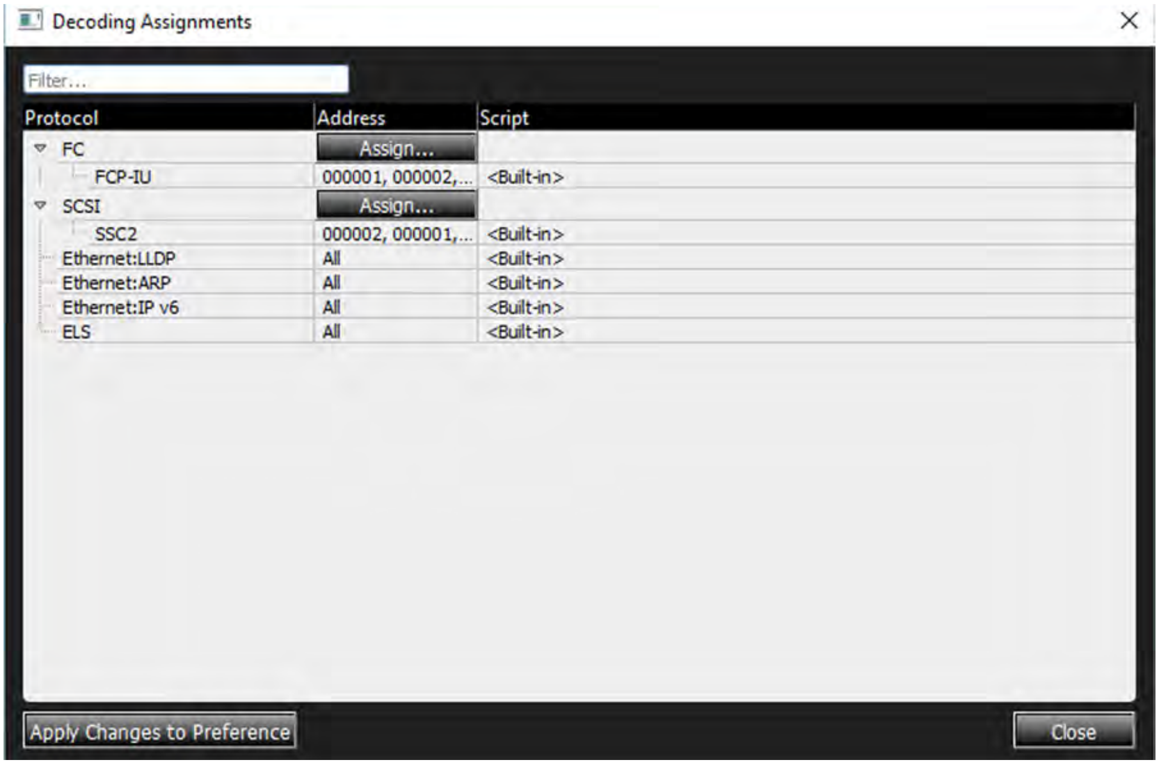
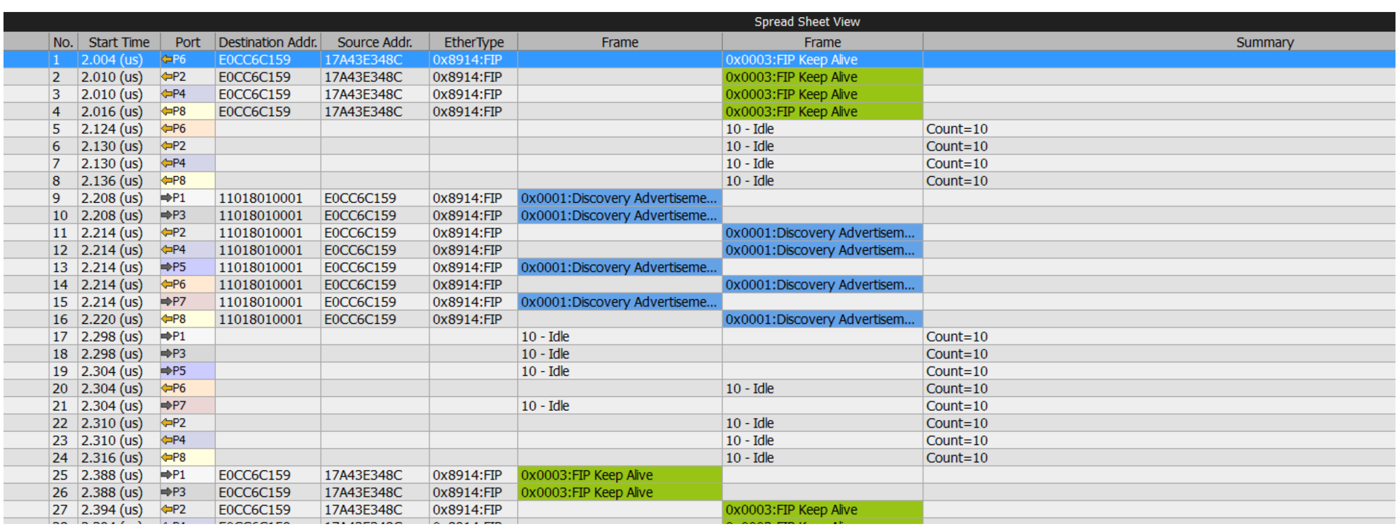


Figure 3.85: Decoding Assignments Dialog

For more details on Decoding Assignments see 5.1.1, *Decoding Assignments*.

3.2.3.2 Spreadsheet View

Click on **Analysis** and select **Spreadsheet View** or click the Spreadsheet icon to display the Spreadsheet View.



Spread Sheet View

No.	Start Time	Port	Destination Addr.	Source Addr.	EtherType	Frame	Frame	Summary
1	2.004 (us)	P6	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
2	2.010 (us)	P2	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
3	2.010 (us)	P4	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
4	2.016 (us)	P8	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
5	2.124 (us)	P6					10 - Idle	Count=10
6	2.130 (us)	P2					10 - Idle	Count=10
7	2.130 (us)	P4					10 - Idle	Count=10
8	2.136 (us)	P8					10 - Idle	Count=10
9	2.208 (us)	P1	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
10	2.208 (us)	P3	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
11	2.214 (us)	P2	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
12	2.214 (us)	P4	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
13	2.214 (us)	P5	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
14	2.214 (us)	P6	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
15	2.214 (us)	P7	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
16	2.220 (us)	P8	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
17	2.298 (us)	P1				10 - Idle		Count=10
18	2.298 (us)	P3				10 - Idle		Count=10
19	2.304 (us)	P5				10 - Idle		Count=10
20	2.304 (us)	P6					10 - Idle	Count=10
21	2.304 (us)	P7				10 - Idle		Count=10
22	2.310 (us)	P2					10 - Idle	Count=10
23	2.310 (us)	P4					10 - Idle	Count=10
24	2.316 (us)	P8					10 - Idle	Count=10
25	2.388 (us)	P1	E0CC6C159	17A43E348C	0x8914:FIP	0x0003:FIP Keep Alive		
26	2.388 (us)	P3	E0CC6C159	17A43E348C	0x8914:FIP	0x0003:FIP Keep Alive		
27	2.394 (us)	P2	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	

Figure 3.86: Spreadsheet View

Spreadsheet View displays Protocol Fields and Frames by time. Refer to 5.2.1, *Spreadsheet View* for more information.

3.2.3.3 Exchange View

In Exchange View the elements of a event are grouped together hierarchically rather than sequentially. See Figure 3.87.

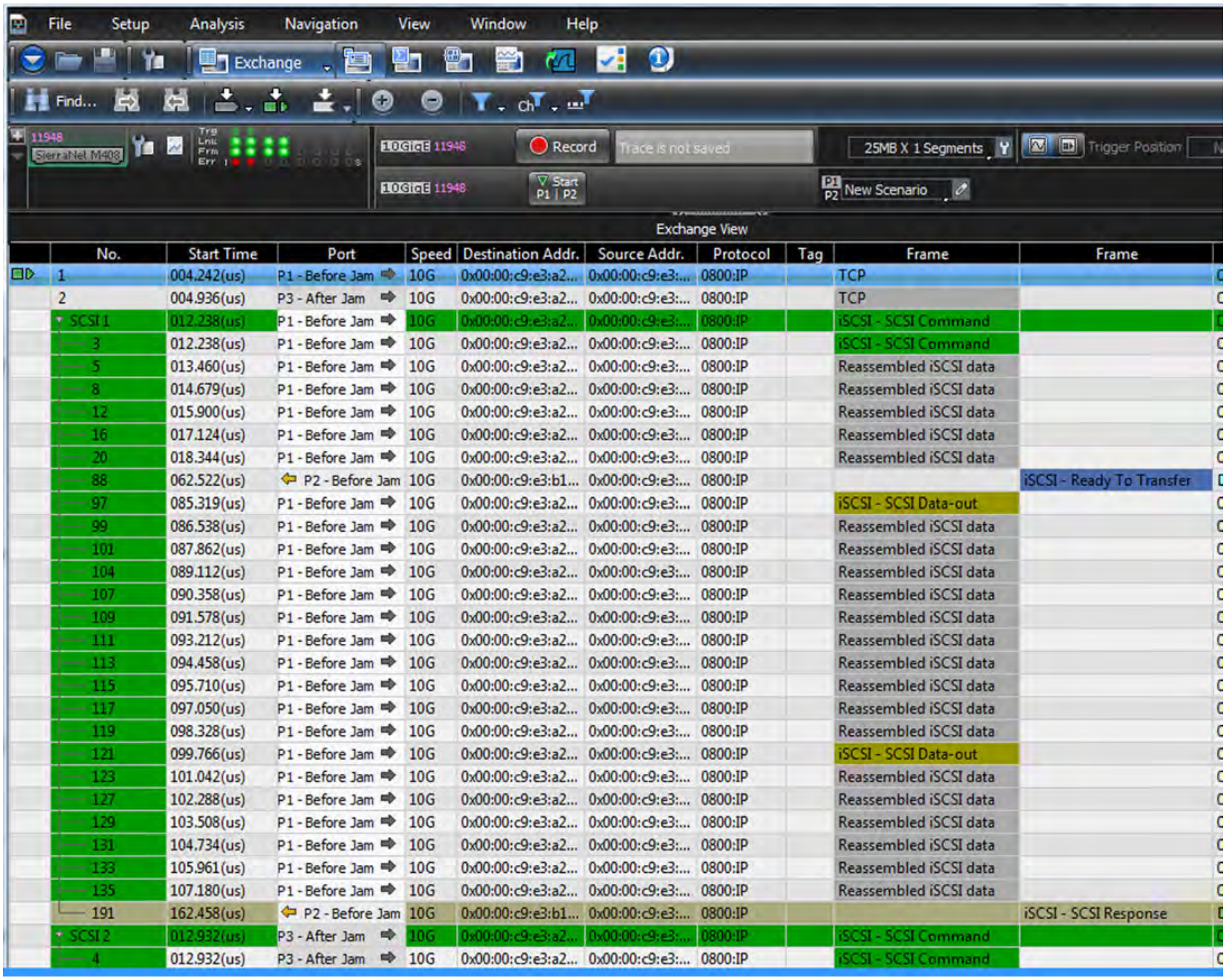


Figure 3.87: Exchange View, Events Arranged Hierarchically vs. Sequentially SCSI CMMD #1

NOTE: Exchange View only works when both sides of a link are captured on a single port pair.

For more details on Exchange View see 5.2.2, *Exchange View*.

3.2.3.4 Frame Inspector View

Click on **Analysis** and select **Frame Inspector View** or click the  icon to display the Frame Inspector View.

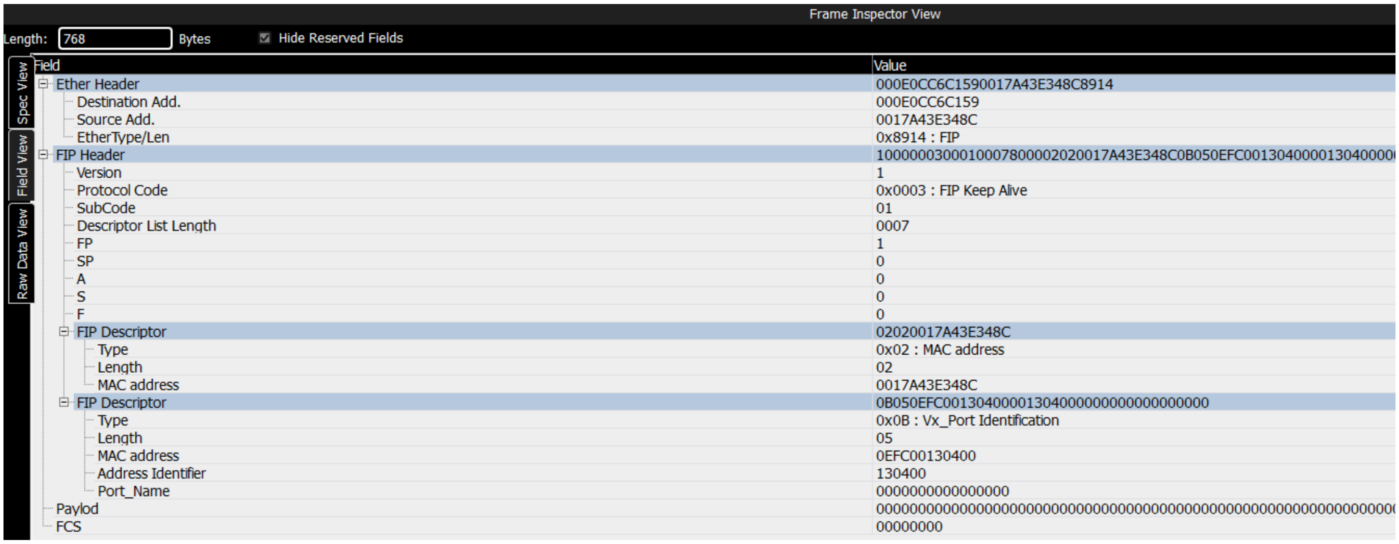


Figure 3.88: Frame Inspector View

Frame Inspector View displays detail information about a frame highlighted in Spreadsheet view. Refer to *5.2.3, Frame Inspector View* for more information.

3.2.3.5 Traffic Summary View

Click on **Analysis** and select **Traffic Summary View** or click the  icon to display the Traffic Summary View.

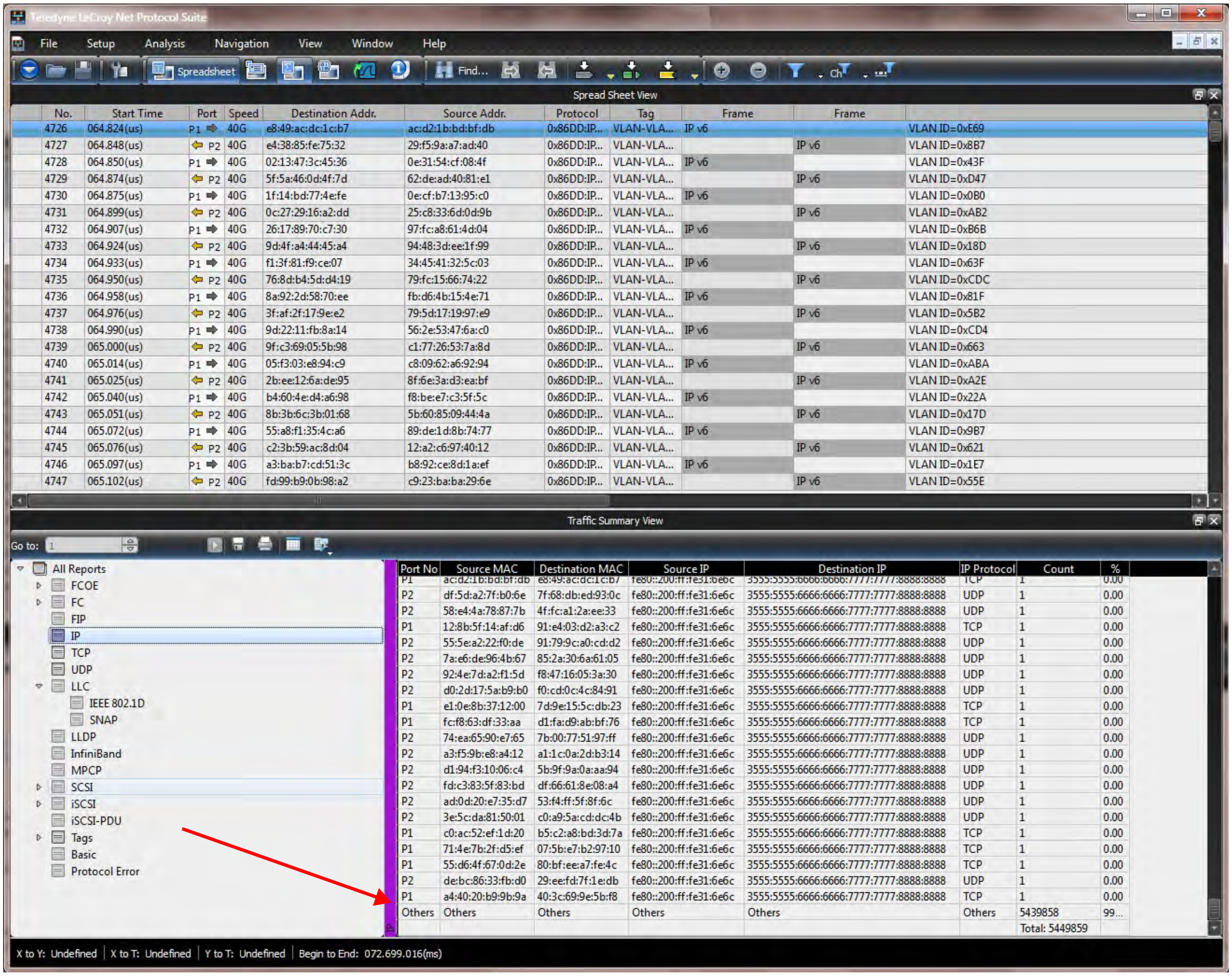


Figure 3.89: Traffic Summary View

The Traffic Summary View for each captured signal can be viewed. This Summary View displays the statistics of commands, the type of command and the total count. For each command it displays the percent of the total count. See 5.2.4, *Traffic Summary View* for more information.

The software collects up to 10,000 unique pairs for the reports. Anything beyond that is grouped into the *Others* category as shown in Figure 3.89 above.

Multi-Column Sorting

In order to address multi column sorting in traffic summary, the Shift key must be pressed. This is done by pressing the shift key while clicking on the header section, this will sort the columns one-by-one in the priority order.

In the case of multi-column sorting, the sort priority order will be shown in the form of indexes as part of the header title.

3.2.3.6 Data View

Click on **Analysis** and select **Data View** or click the icon to display the Data View (see Figure 3.90).

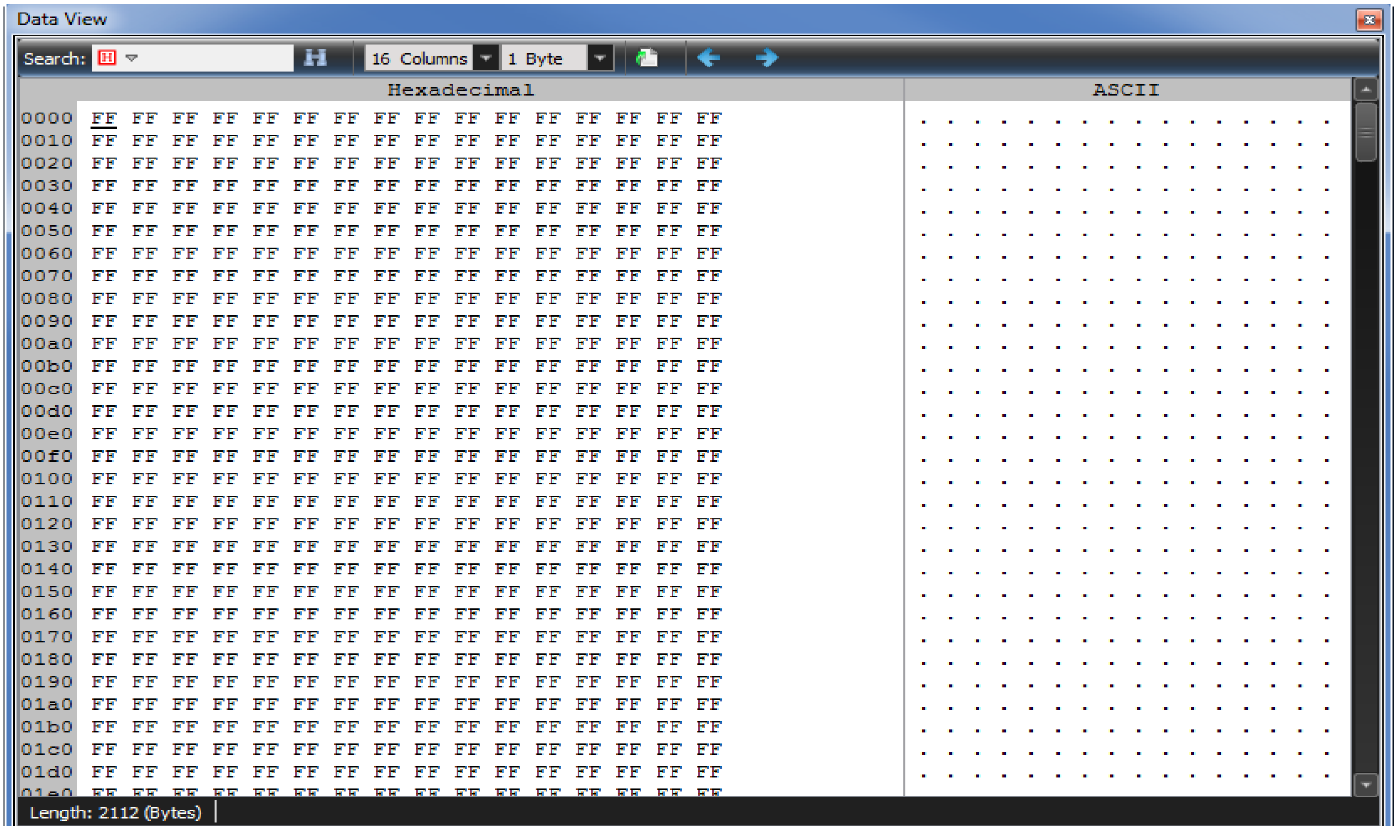


Figure 3.90: Data View

The Data View displays information in Hexadecimal and ASCII format. Refer to 5.2.5, *Data View* for more information.

3.2.3.7 Bus Utilization View

The Bus Utilization View displays both an Error Count and Link Utilization over a specific time frame. See Figure 3.91.

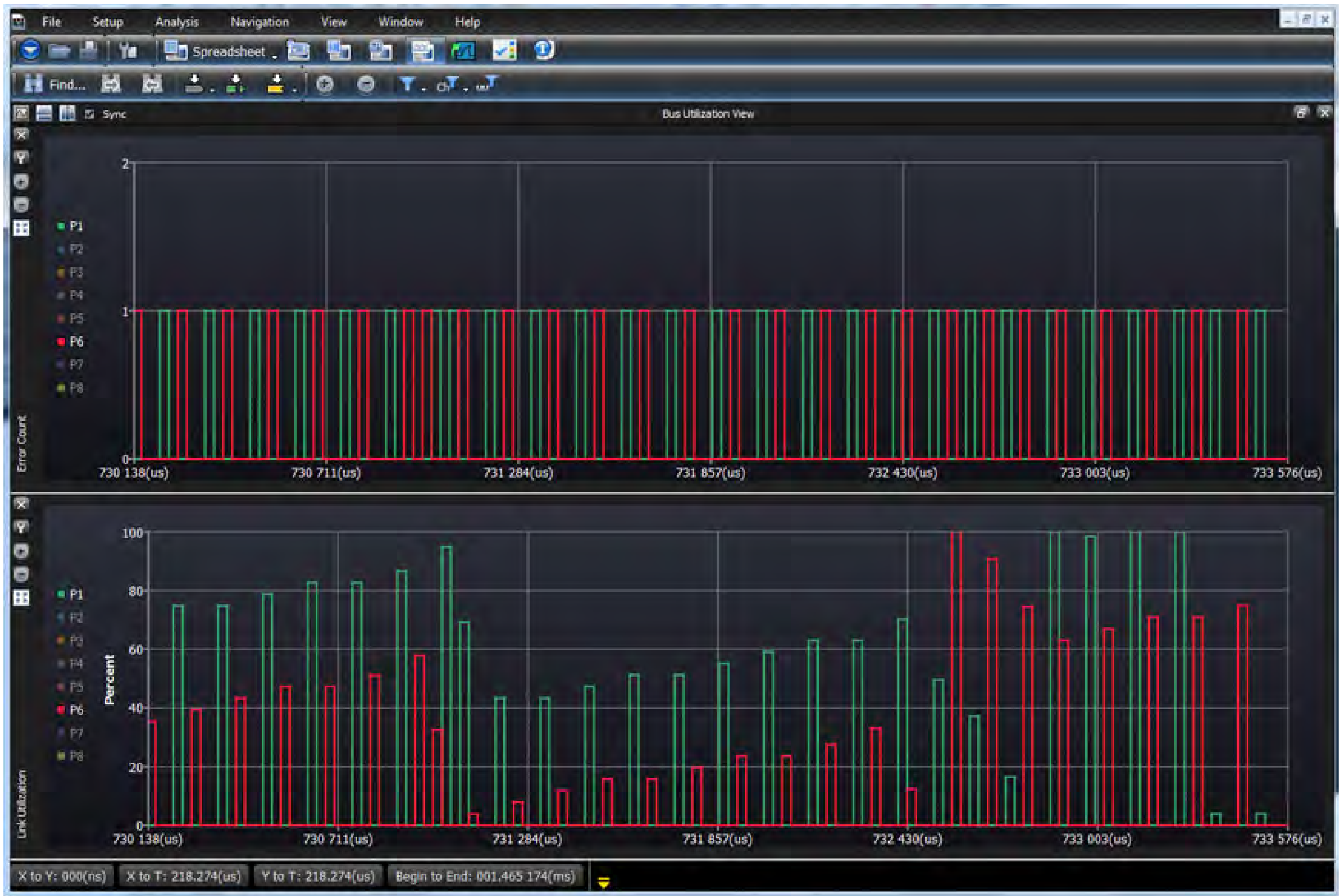


Figure 3.91: Typical Bus Utilization View (Ports P1 and P6 Showing)

For a more detailed explanation of Bus Utilization see 5.2.6, *Bus Utilization View*.

3.2.3.8 Link State View

Link State View is used for debugging Auto Negotiation and Link Training in Ethernet, and Speed Negotiation and TX Training in Fibre Channel. The Link Viewer is intended to show events chronologically. Transitions will not be shown on this view. All the errors that occur in the Trace will be shown in the Event Viewer.

Link State View can be enabled by selecting the Link State View  icon in the main toolbar (between Bus Utilization and Export to Wireshark). It has four main views:

- ❑ Timeline View
- ❑ Listing/State Diagram View
- ❑ Navigation View

See Figure 3.92.

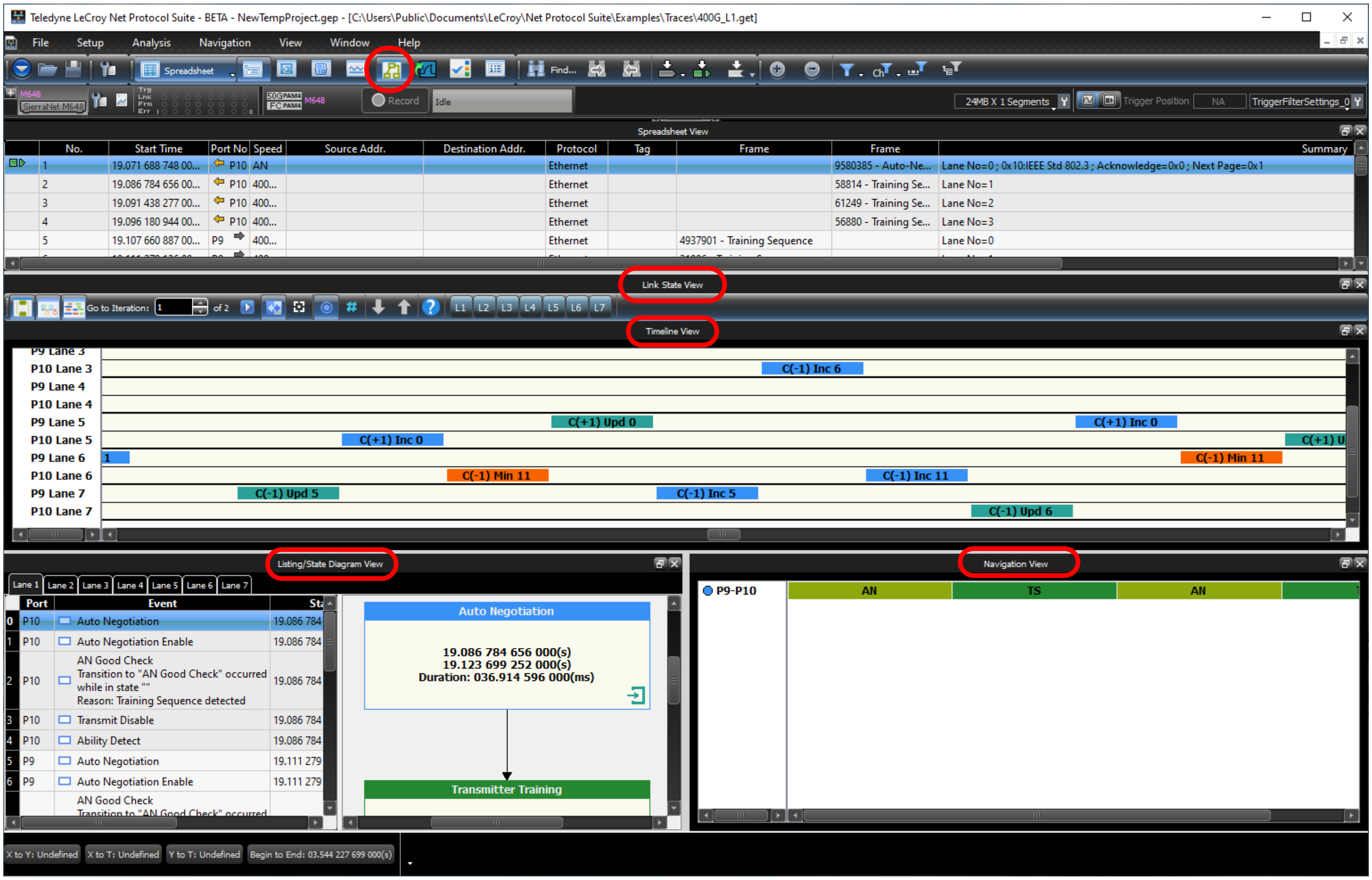


Figure 3.92: Link State Views

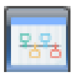
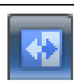
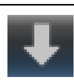
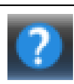
Link State View Toolbar

The Link State View also has its own toolbar of functions (Figure 3.93).

Figure 3.93: Link State View Toolbar

Table 3.2 describes the buttons and icons for the Link State View toolbar.

Table 3.2: Toolbar Buttons & Icons for Link State View

Button/Icon	Description
	Listing/State Diagram View. List of Ports in the captured trace (used to select a port pair). See *Listing/State Diagram View*.
	Toggle Navigation View – Show or hide the Navigation pane. See *Listings View Pane*.
	Toggle Timeline View – Displays color-coded metrics for each lane.
	Go to Iteration—Select from available iterations (appears in the Navigation View and Navigation panes).
	
	Synchronize Views. Use to time synchronize items in Spreadsheet View with item in Link State View. See *Synchronize Views*.
	Fit in Views: Use this to zoom back in when view is expanded.
	Show Final State. Goes to Final State.
	Show/Hide Number of Transitions (flow diagram/diagram view)
	Next. Move to Next Event). See *Go To Next Event*.
	Previous. Move to the Previous Event. See *Go To Previous Event*.
	Help. Displays a table of the icons, buttons, Markers, Legend (colors), and Controllers used in Link State View. See Figures 3.94 and 3.95.
	Show/Hide port lanes.

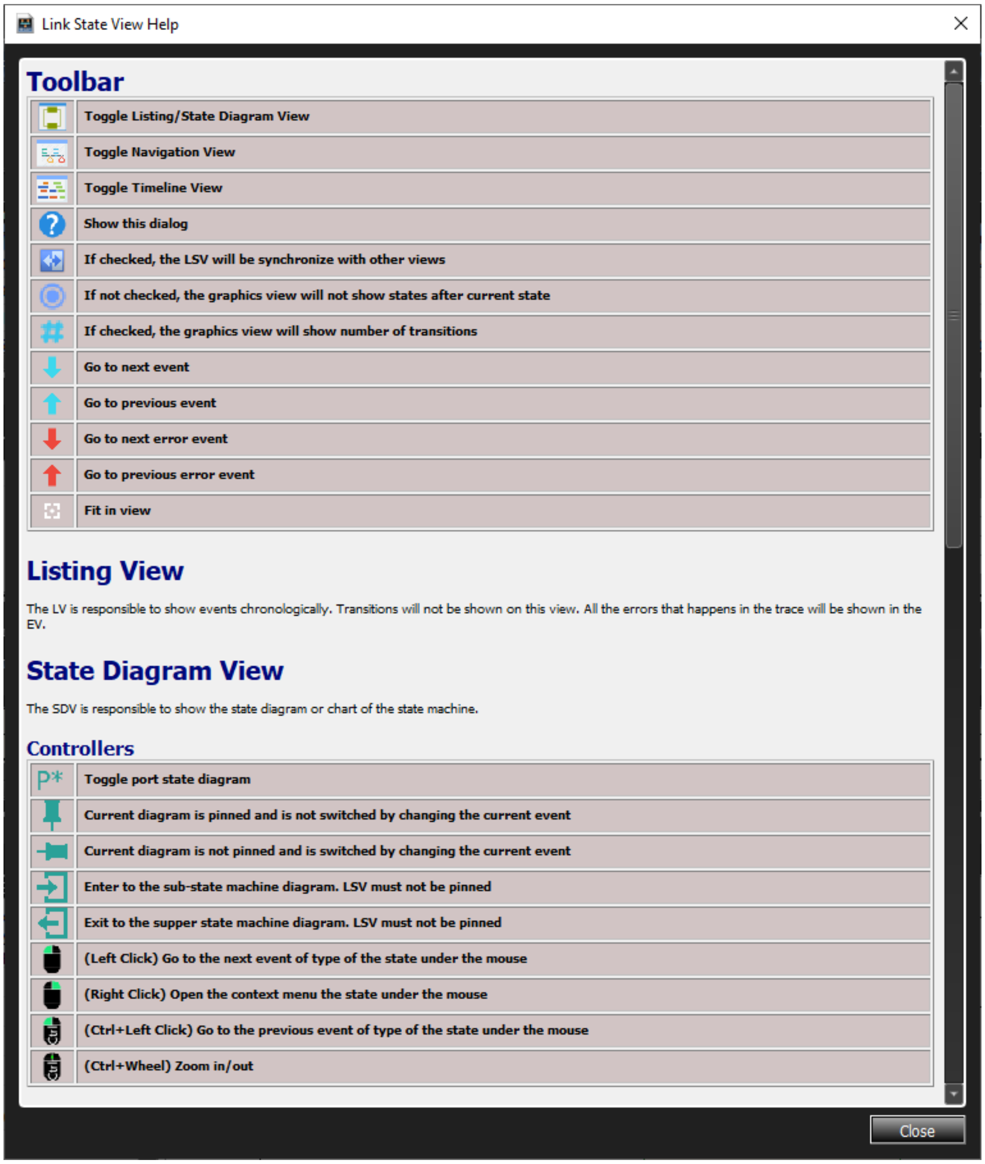


Figure 3.94: Link State View Help Table-1

Figure 3.95: Link State View Help Table-2

Listing/State Diagram View

Displays the list of active ports captured in the current trace, Event, Start and Stop, and the Duration; and the current State diagram (Figure 3.96).

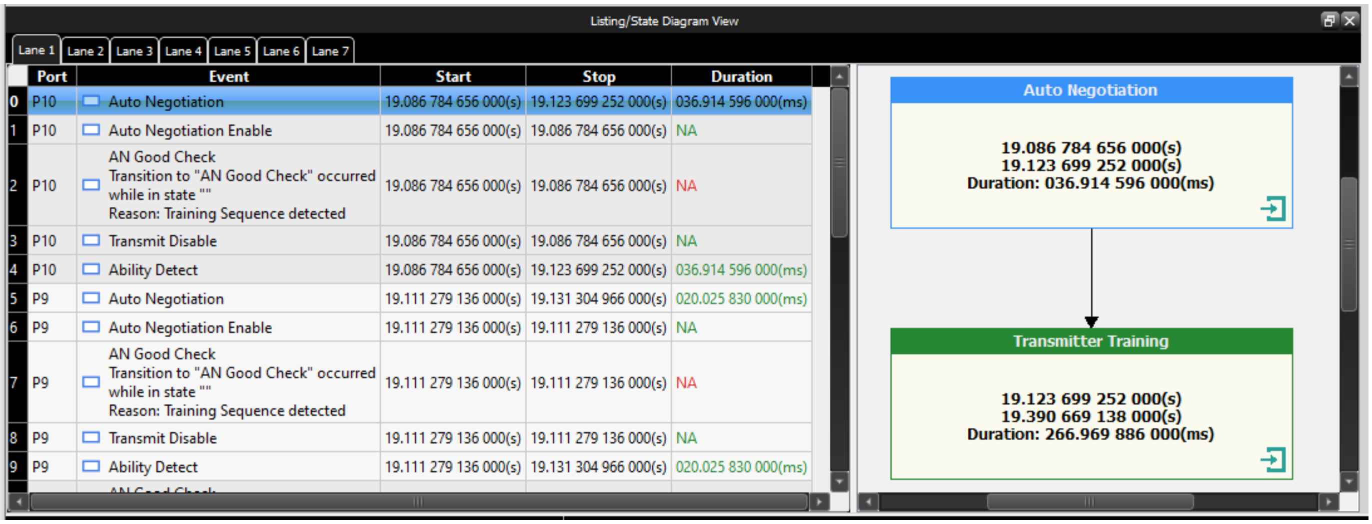


Figure 3.96: Listing/State Diagram View

Listings View Pane

The Listings View pane displays the port number, Event, Start and Stop time, Duration, and tabs for each lane (Figure 3.97).

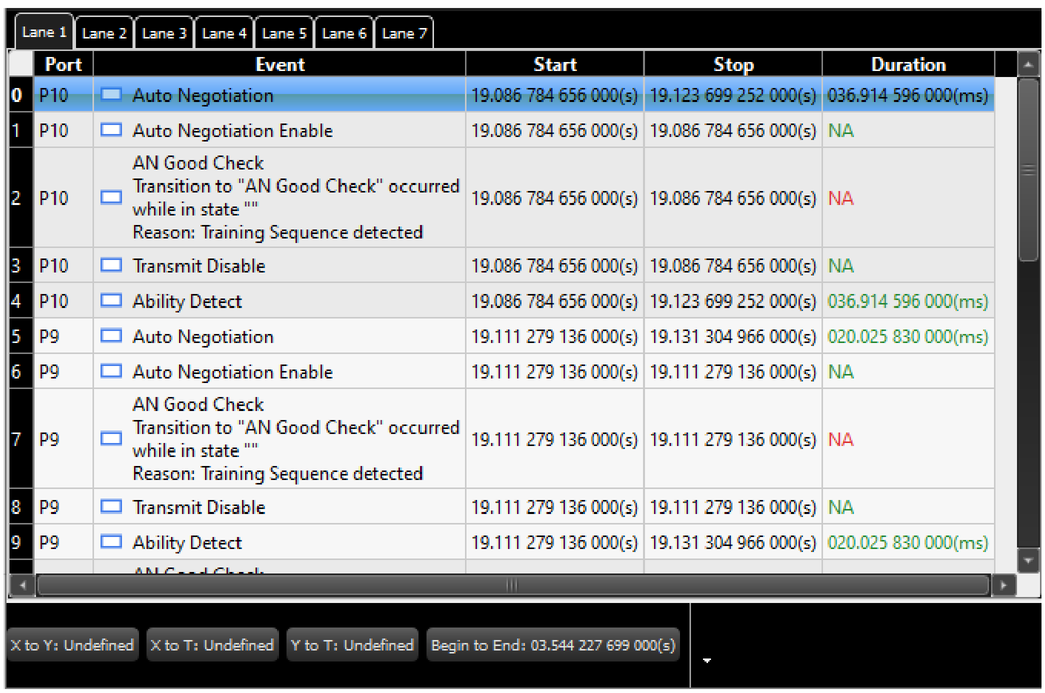


Figure 3.97: Listings View Pane

- The tabs for lanes 1 through 7 display the current-state diagram view for the selected port (Figure 3.97).
- Click the  icon for Auto Negotiation or Transmitter Training to a detailed diagram for the selected activity (Figure 3.99).
- Click the  icon to collapse the detail view.

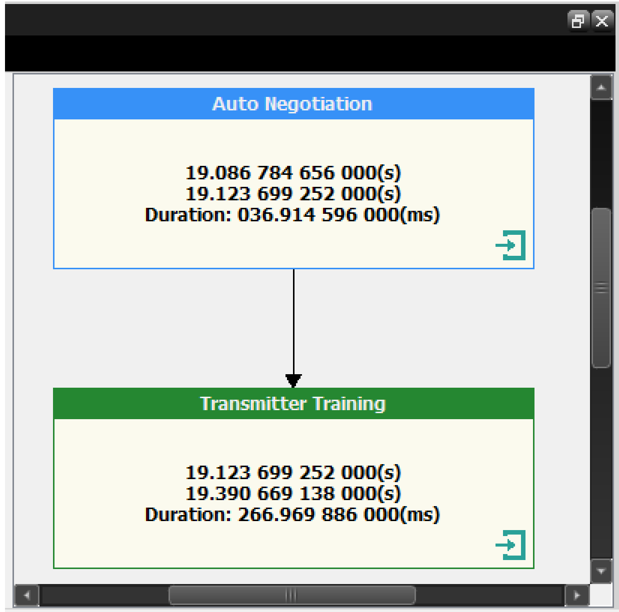


Figure 3.98: High-Level State Diagram for Selected Port

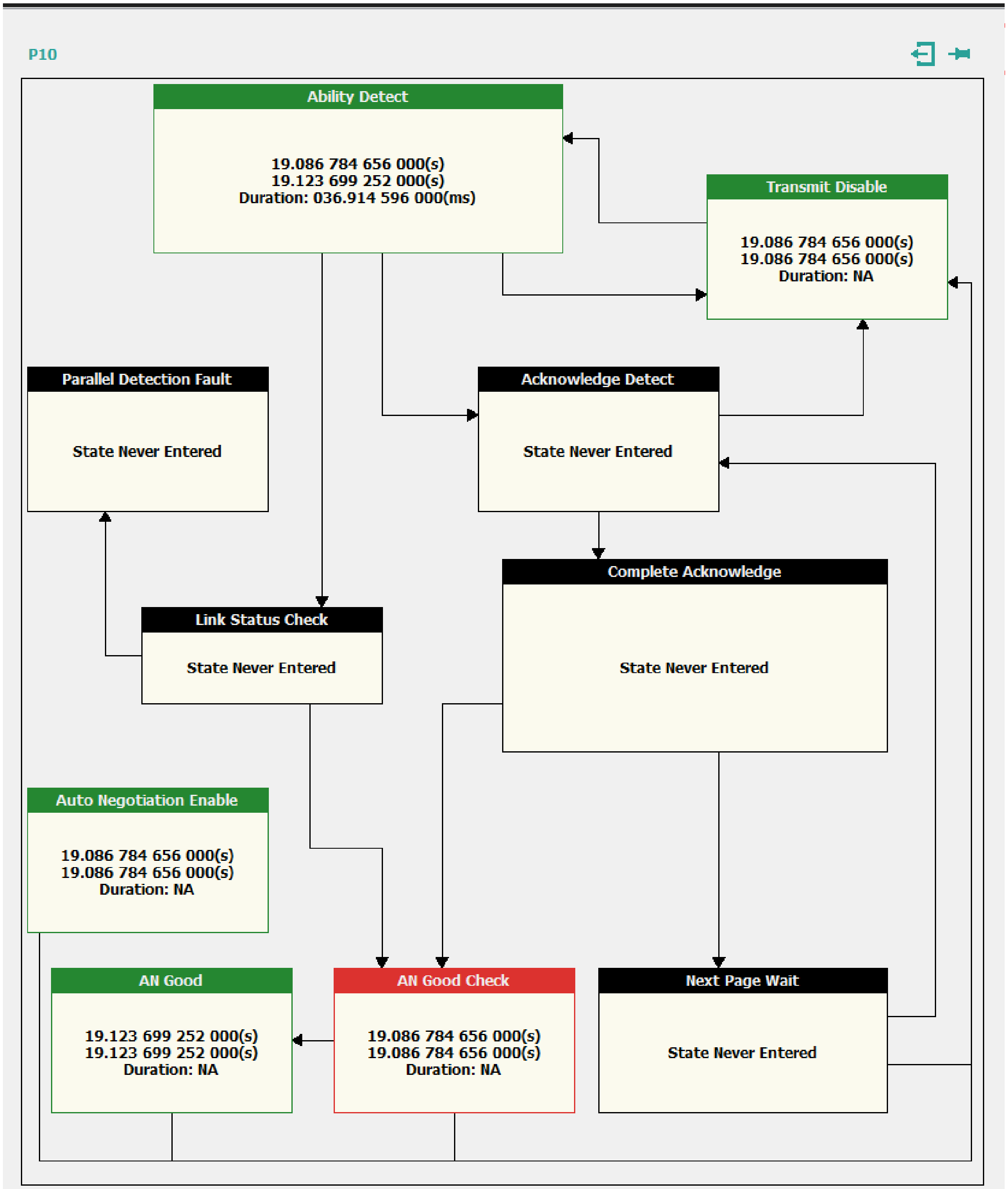


Figure 3.99: State Diagram Detail View for Selected Activity

Timeline View Pane

Shows Training transactions for each lane (Figure 3.100). To view the metrics within the color blocks, you must zoom in. To do this, hold down the **Ctrl** key and turn the mouse scroll wheel.

NOTE: When multiple consecutive increment or decrement requests are found, the accumulated distance from the starting point (either positive or negative) will be reported.

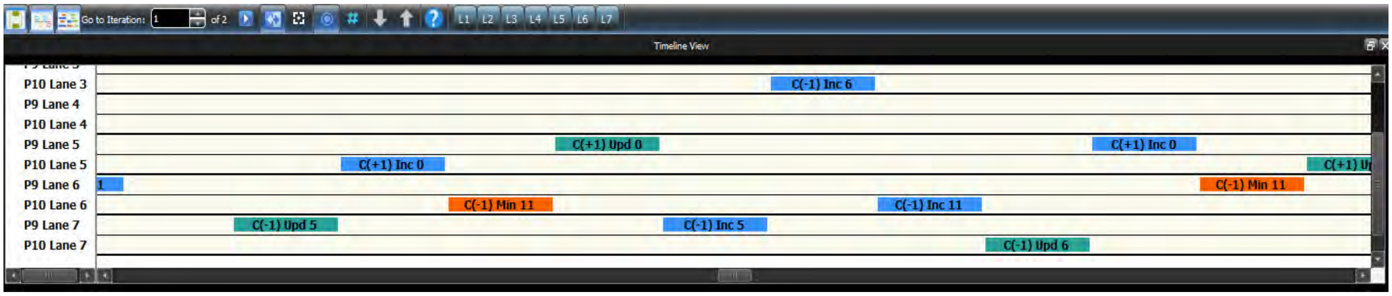


Figure 3.100: Timeline View

Navigation View Pane

This shows Negotiation activity of the ports for the captured trace: Auto-Negotiation, Training Sequence, and PCS (Figure 3.101).

Selecting one of the ports causes the Navigation View and State Diagram panes to shift to display that particular event. See Figure 3.102.

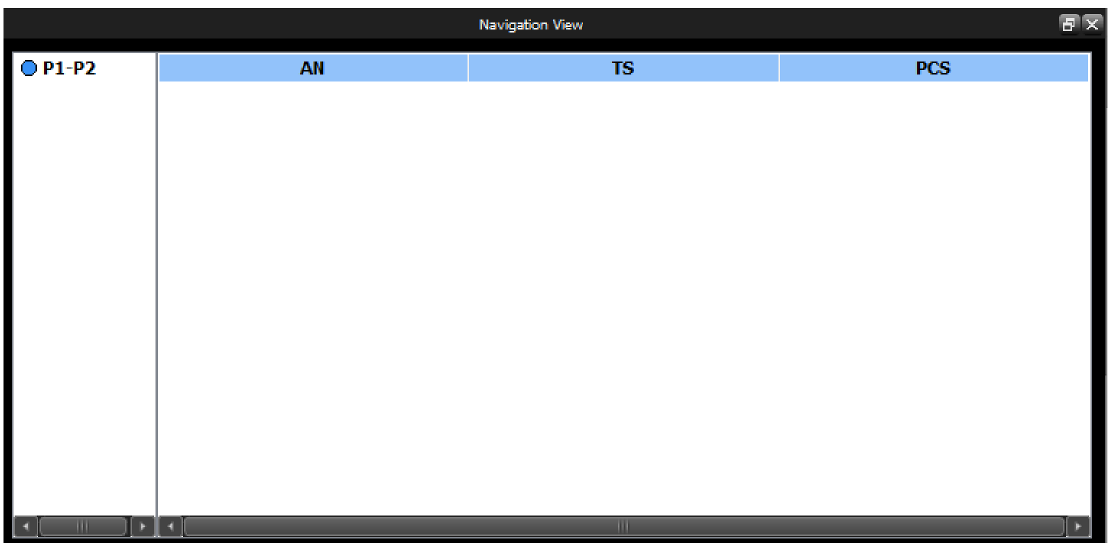


Figure 3.101: Navigation View Pane

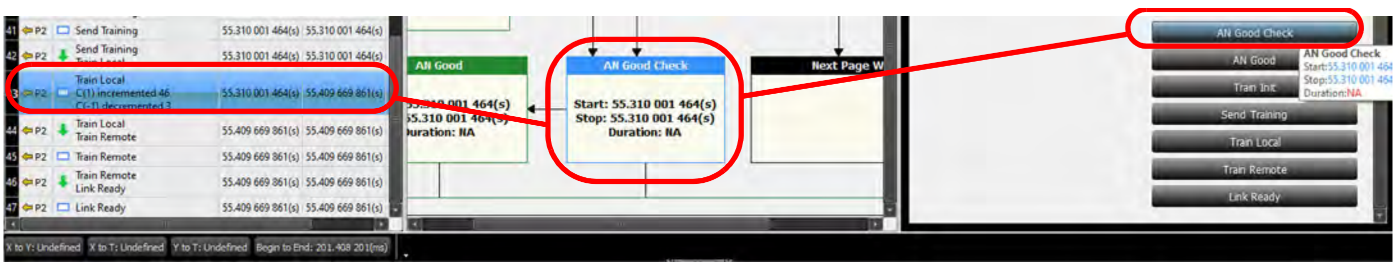


Figure 3.102: One Specific Block in the Interaction Pane

Synchronize Views

Synchronized all Views: Trace, Event, State Diagram and Interactions (Figure 3.103).

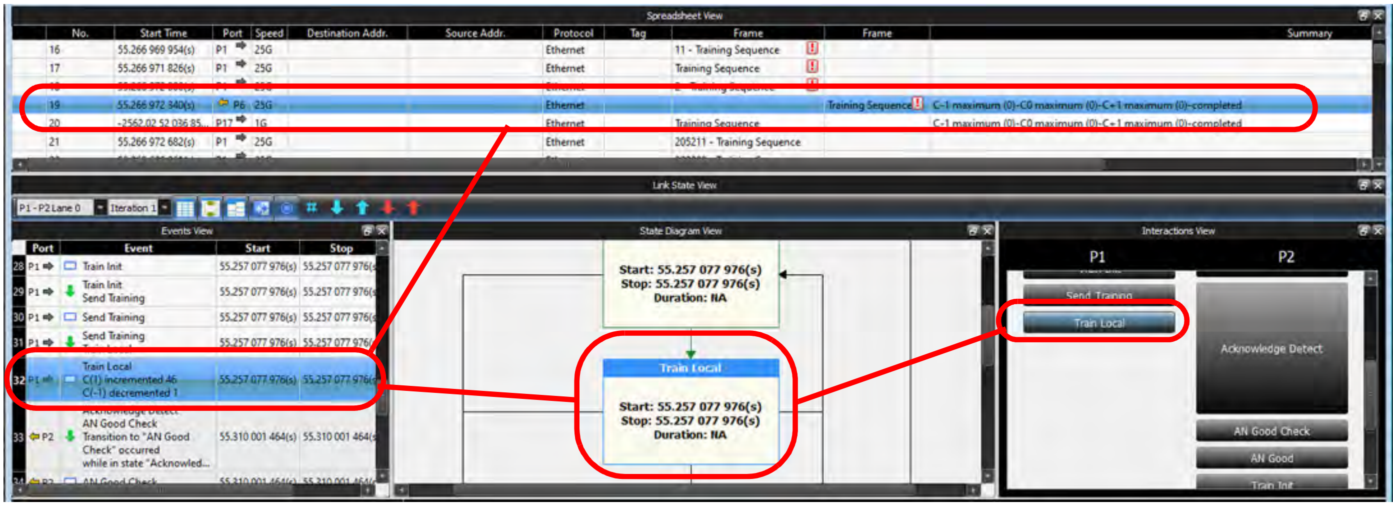


Figure 3.103: Synchronize Views—Trace, Listings, State, and Timeline

Go to Final State in Selected Event

Displays Final State in the selected Event. See Figure 3.104.

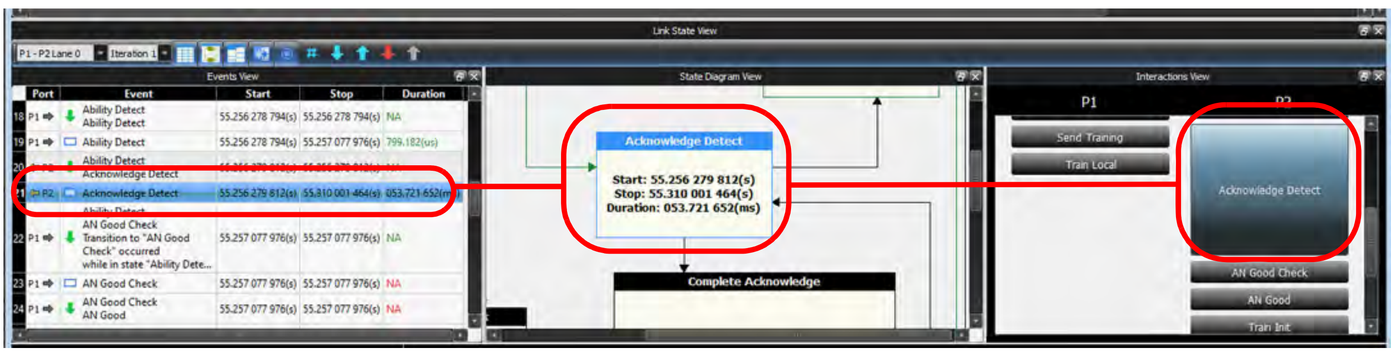


Figure 3.104: Final State in Selected Event

Show/Hide Number of Transitions

Show/Hide the number of Transitions in the State Diagram. See Figure 3.105.

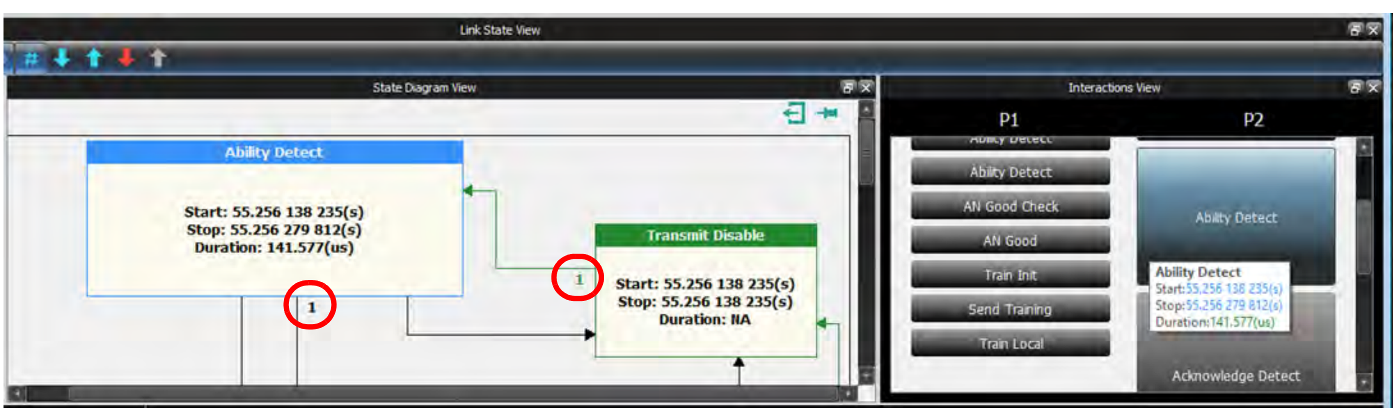


Figure 3.105: Show/Hide Number of Transitions in State Diagram

Go To Next Event

Display moves to Next Event. See Figure 3.106.

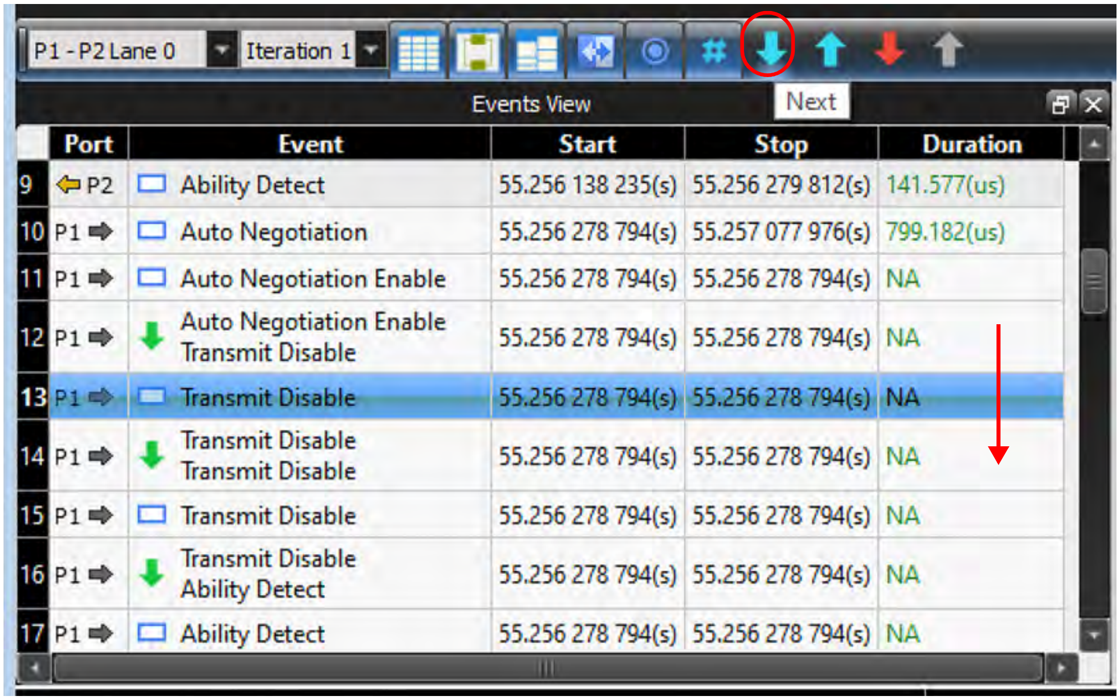


Figure 3.106: Go to Next Event

Go To Previous Event

Display goes to Previous Event. See Figure 3.107.

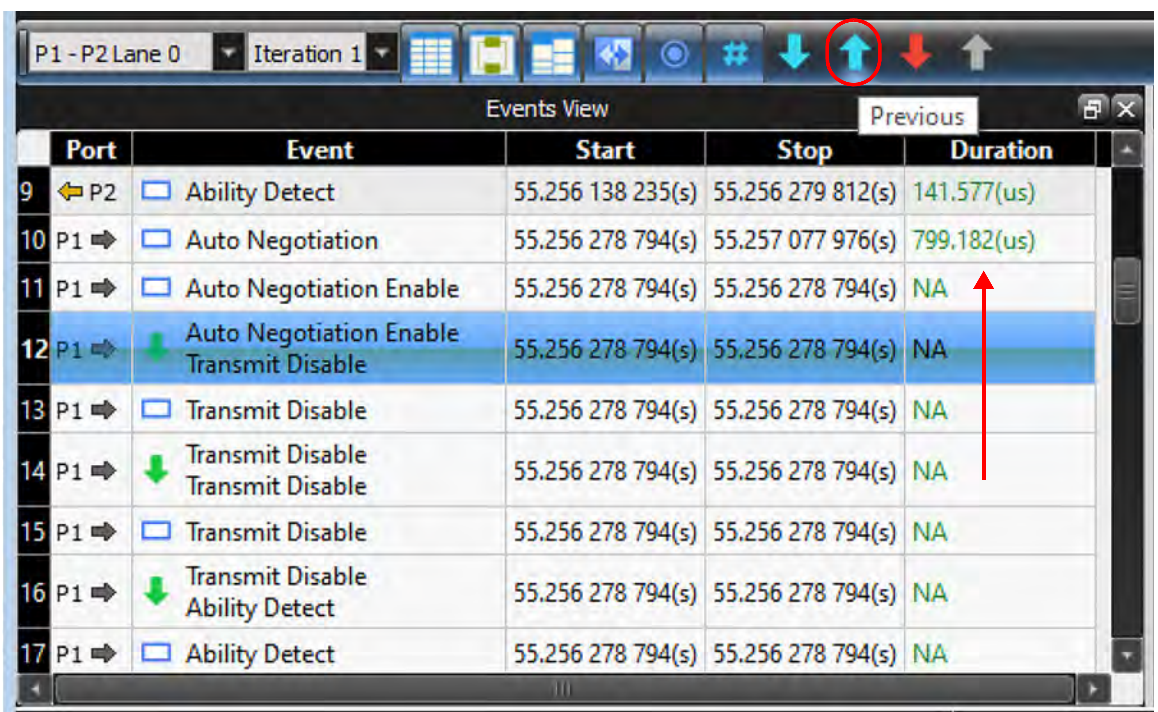


Figure 3.107: Go to Previous Event

Go To Next Error

Display moves to Next Error. See Figure 3.108.

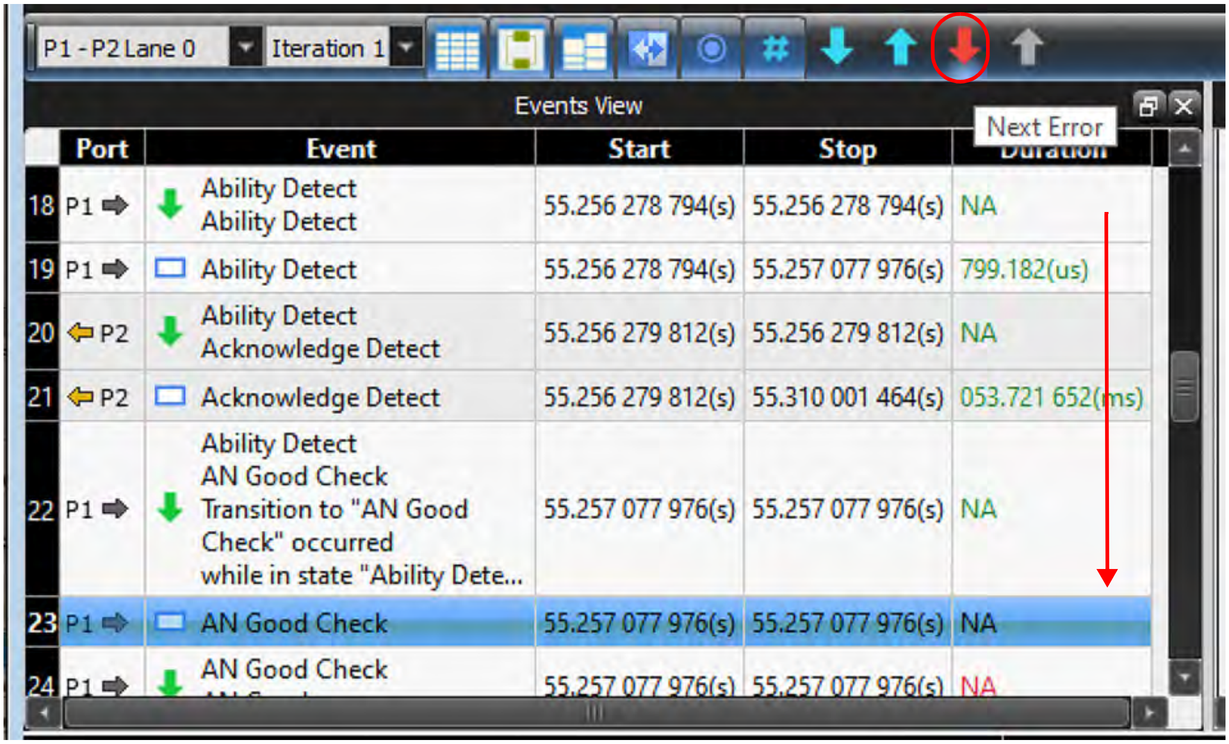


Figure 3.108: Display moves to Next Error

Go To Previous Error

Display moves to Previous Error. See Figure 3.109.

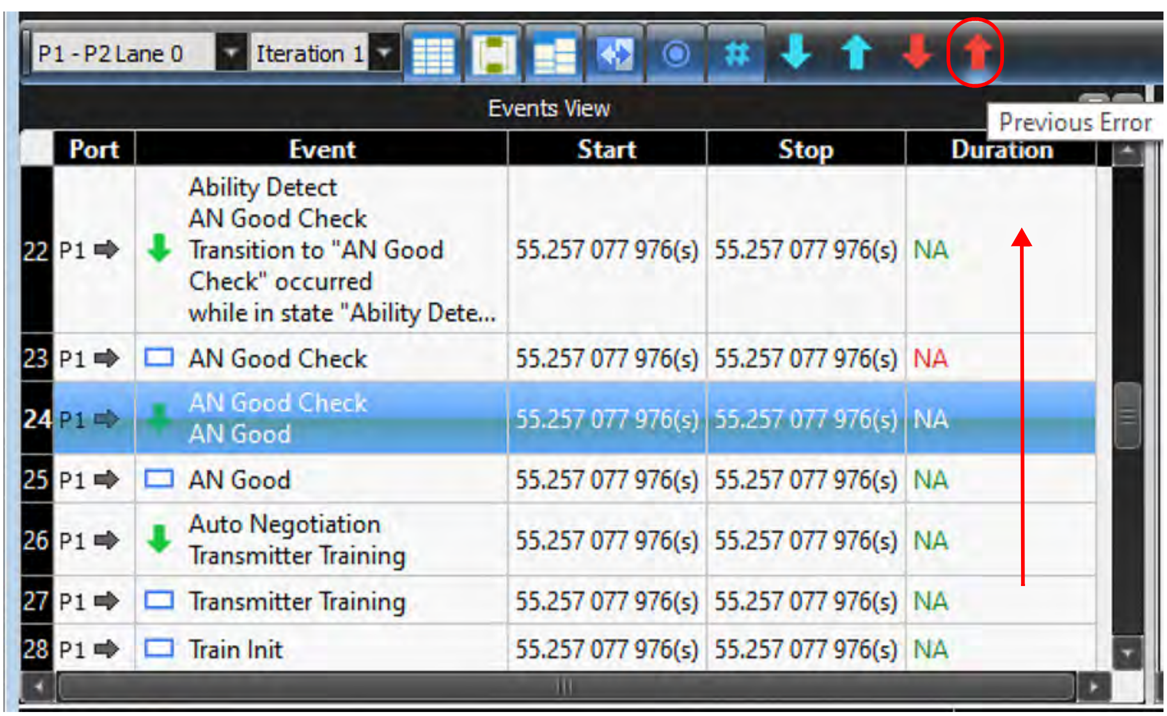


Figure 3.109: Display moves to Previous Error

3.2.3.9 Trace Expert

Trace Expert generates the following reports and analysis for the currently loaded trace:

- Performance Analysis
- Error Reports
- Trace Analysis Statistics
- Trace Information

For more details about Trace Expert see *5.2.8, Trace Expert*.

3.2.3.10 Trace Information

Click on **Analysis** and select **Trace Information** or click the  icon to display the trace Information dialog (see figures 3.110 and 3.111). You can click on the hyperlinks—**File info**, **Hardware info**, **Project info** or **License info**—to navigate to that section. Click **Open Trace Project** to open the project in which the trace was captured.

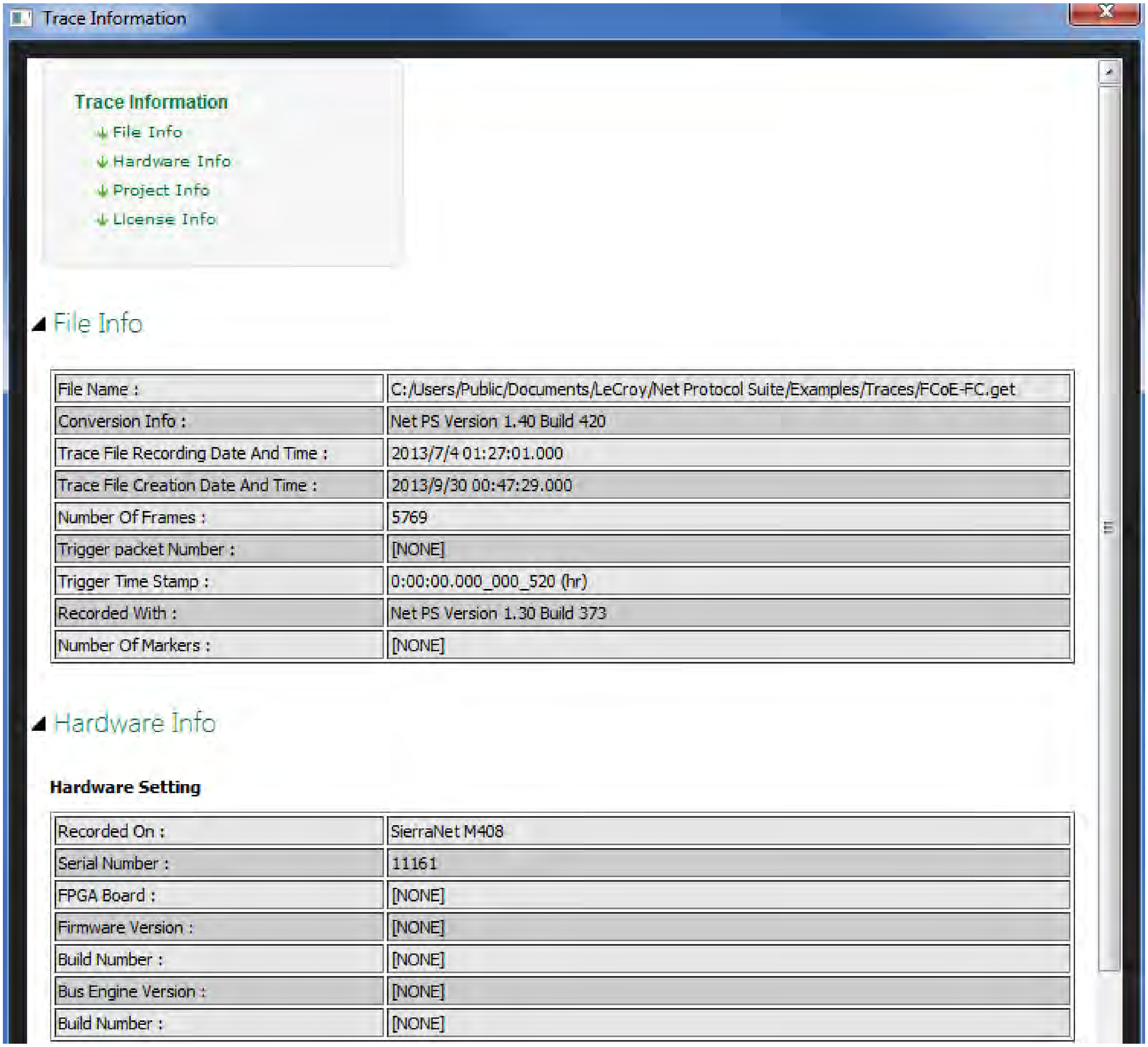


Figure 3.110: Trace Information Window 1

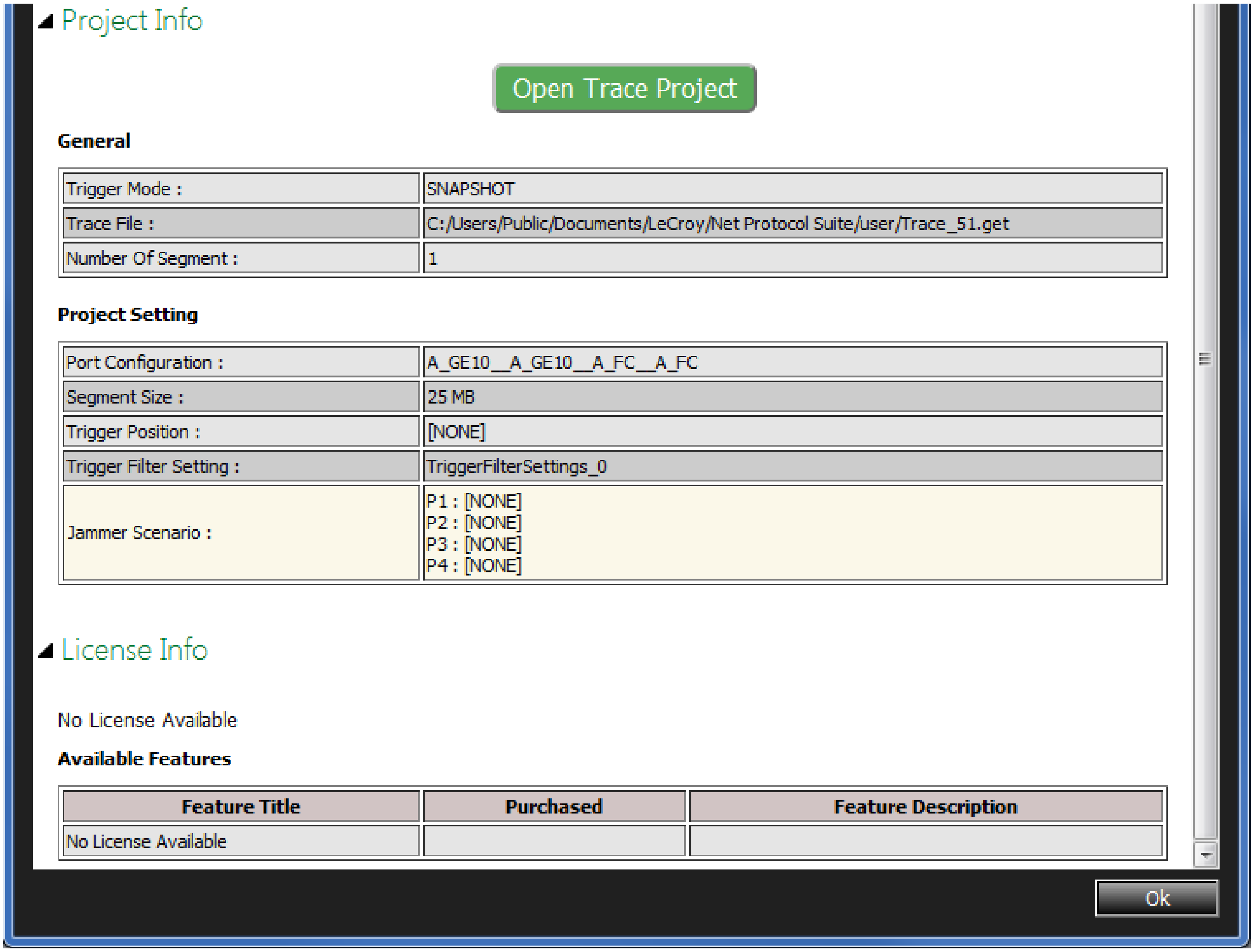


Figure 3.111: Trace Information Window 2

3.2.3.11 Verification Script

The Verification Script Engine allows you to select from available traces and execute verification scripts on them.

For more details see *5.3, Verification Script Engine (VSE)*.

3.2.3.12 RTT Pairs

Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

For more detail see *5.4, Round Trip Time (RTT) Pairs*.

3.2.4 Navigation

The Navigation menu option enables the user to navigate the application (see Figure 3.112). You can go to the trigger, marker or where the cursor is located. Markers can also be added and removed. Find menu options are available as shown in the screen capture below.

NOTE: The menu options listed in the Navigation menu can also be selected when you right-click anywhere on the screen, see *5.2.1.7, Markers*.

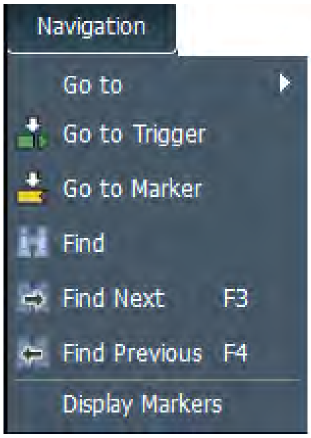


Figure 3.112: Navigation Menu Option

For more details on the Navigation Options see *5.5, Navigation Toolbar Icons*.

3.2.5 View

The View menu has the following options:

- Zoom in – Allows you to zoom in the view.
- Zoom out – Allows you to zoom out the view.
- Hide/Show – Displays the Filter dialog box enabling you to configure filters applied to the trace view.
- Hide/Show non-Frames – Shows/Hides the Idles in the trace view.
- Toolbars – Allows you to customize the toolbar display (see Figure 3.113).
- Menu Bar-Selecting and deselecting this option toggles between showing and hiding the menu bar. Press the Alt key to do the same. See *3.2, Menu Bar Options*.
- Restore Default View – Restores view so only Spreadsheet View and Frame Inspector View are displayed.

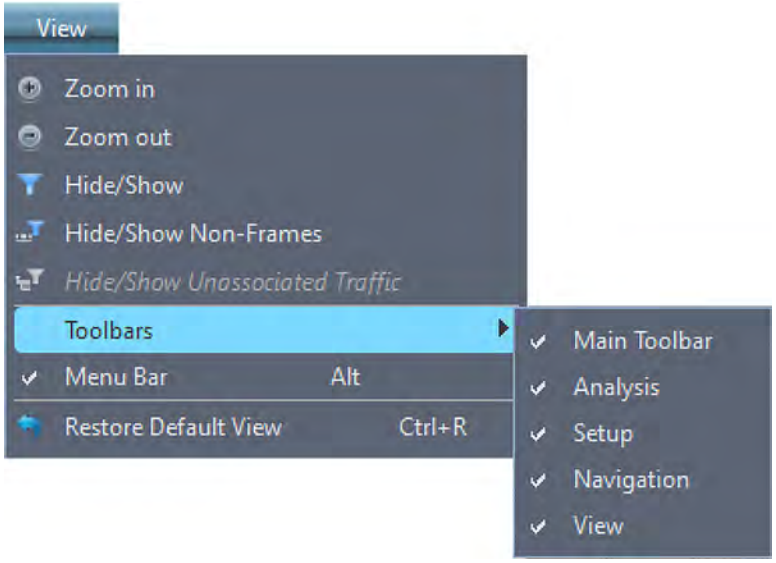


Figure 3.113: View Menu Options

For more details abut the View tab see 5.6, *View: Pull Down Menu*.

3.2.6 Window

See Figure 3.114.

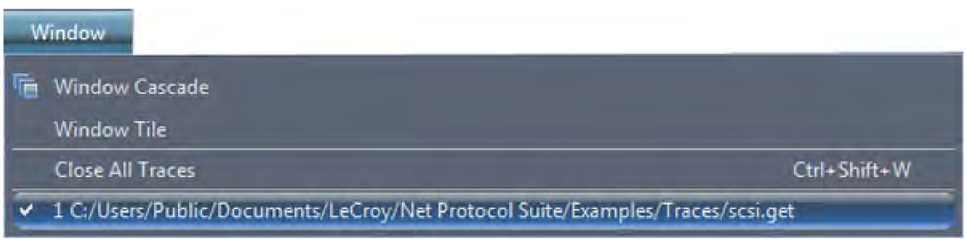


Figure 3.114: Window Tab

Window – Allows you to configure your display. It has the following options:

- Window Cascade: Displays open Views in available Main Display window.
- Window Tile: Displays open Views in Full Size Main Display window.
- Close All Traces - closes all open traces, see Figure 3.115.

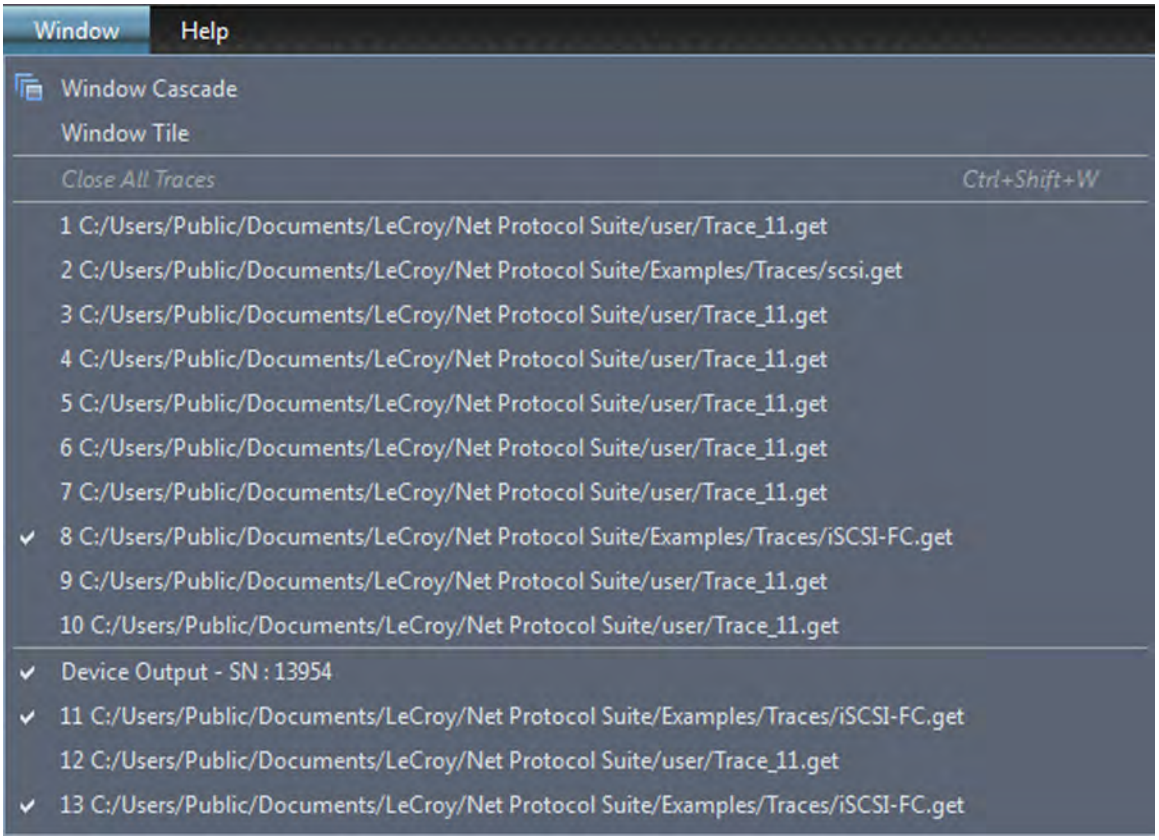


Figure 3.115: Window Dialog with Open Traces, Recent Traces and Active Devices

3.2.7 Help

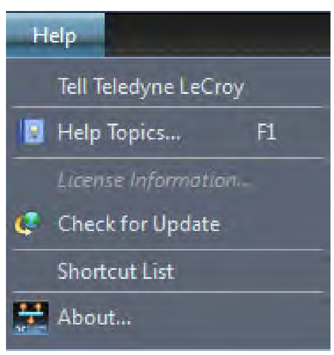


Figure 3.116: Help Menu Option

3.2.7.1 Tell Teledyne LeCroy

To report a problem to Teledyne LeCroy Support via e-mail, select **Help → Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.

3.2.7.2 Help Topics

Displays online help. You can also select F1.

3.2.7.3 License Information

Open the license information dialog (see Figure 3.117) to display a list of named features supported by the current software version. Named features that are not enabled on your system are indicated by No in the Purchased column. Whether or not named features are enabled depends on the license key stored in your analyzer. If you try to use a feature for which you do not yet have a license, the program displays the License Protection Message. To use the feature, you must purchase a license.

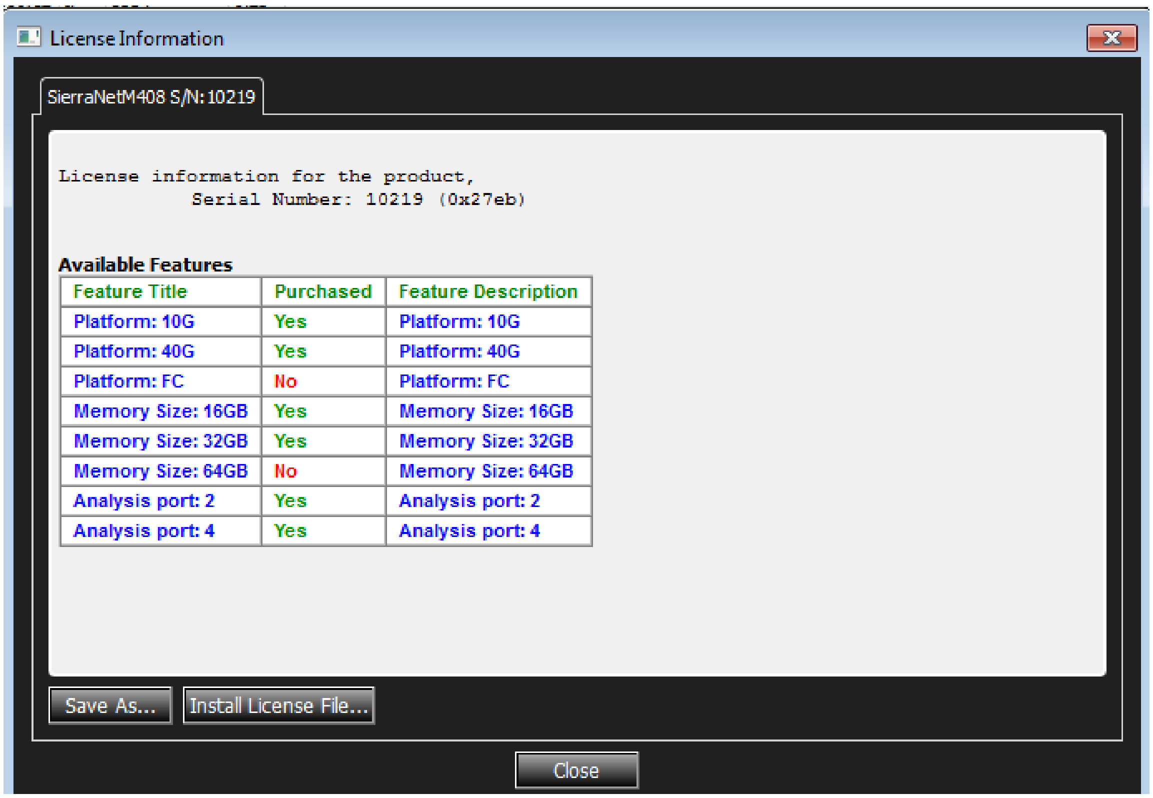


Figure 3.117: Typical License Information Window

A current license agreement with Teledyne LeCroy entitles the Analyzer owner to continued technical support and access to software updates as they are published on the Teledyne LeCroy website (https://teledynelecroy.com/sw/netprotocolsuite/). When you obtain a license key, from the Help menu in the License Information dialog, select **Install License File** to display the Open License dialog. Enter the path and filename for the license key, or browse to the directory that contains the license key and select the *.lic file. Click Open.

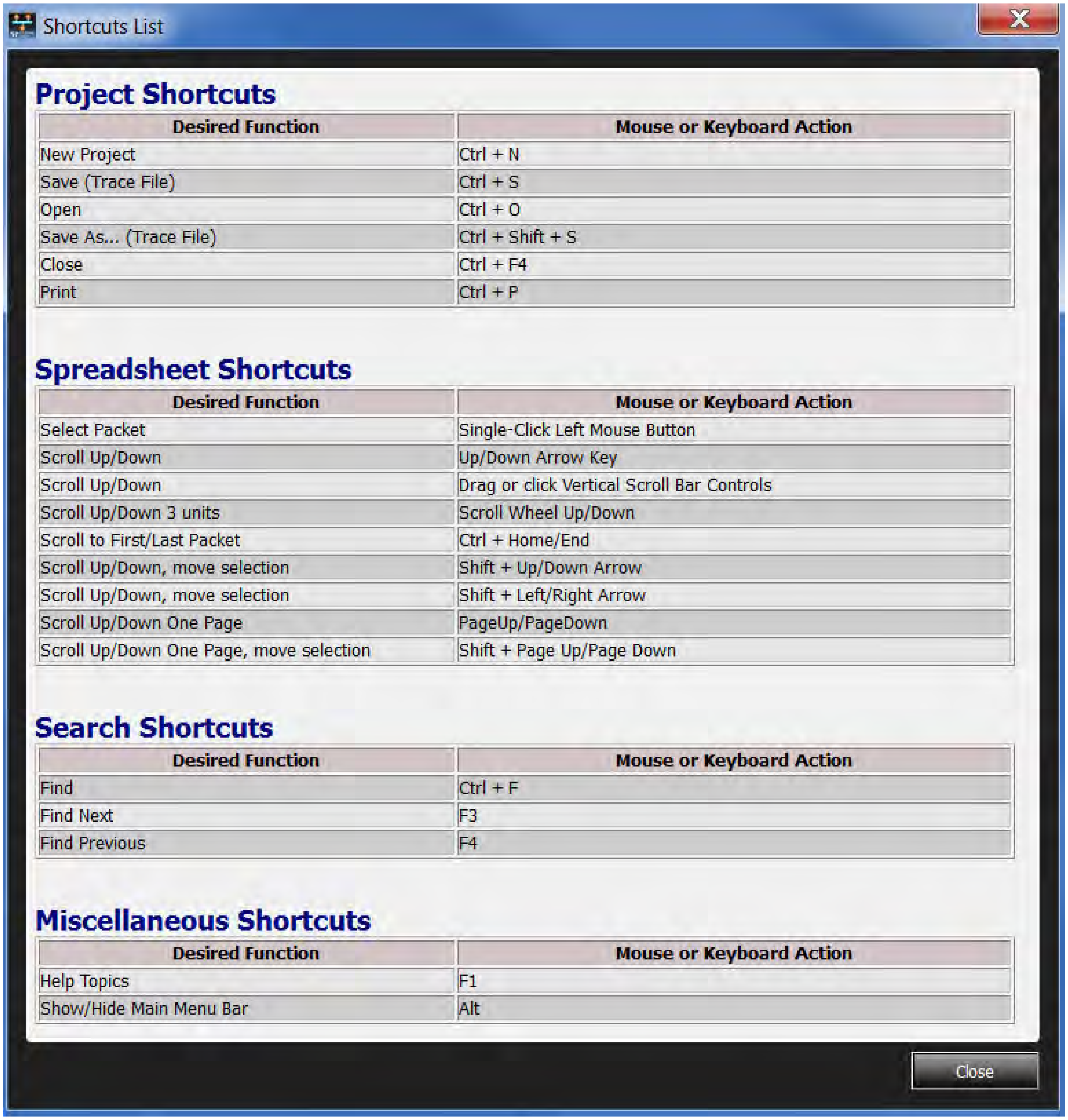
3.2.7.4 Check for Updates

Check whether a new software version is available. If so, you can download from the Teledyne LeCroy web site: https://teledynelecroy.com/sw/netprotocolsuite/

You can check for updates at application startup.

3.2.7.5 Shortcut List

Displays a list of keyboard shortcuts. See Figure 3.118.



Shortcuts List

Project Shortcuts

Desired Function	Mouse or Keyboard Action
New Project	Ctrl + N
Save (Trace File)	Ctrl + S
Open	Ctrl + O
Save As... (Trace File)	Ctrl + Shift + S
Close	Ctrl + F4
Print	Ctrl + P

Spreadsheet Shortcuts

Desired Function	Mouse or Keyboard Action
Select Packet	Single-Click Left Mouse Button
Scroll Up/Down	Up/Down Arrow Key
Scroll Up/Down	Drag or click Vertical Scroll Bar Controls
Scroll Up/Down 3 units	Scroll Wheel Up/Down
Scroll to First/Last Packet	Ctrl + Home/End
Scroll Up/Down, move selection	Shift + Up/Down Arrow
Scroll Up/Down, move selection	Shift + Left/Right Arrow
Scroll Up/Down One Page	PageUp/PageDown
Scroll Up/Down One Page, move selection	Shift + Page Up/Page Down

Search Shortcuts

Desired Function	Mouse or Keyboard Action
Find	Ctrl + F
Find Next	F3
Find Previous	F4

Miscellaneous Shortcuts

Desired Function	Mouse or Keyboard Action
Help Topics	F1
Show/Hide Main Menu Bar	Alt

Close

Figure 3.118: Shortcuts List

3.2.7.6 About

Displays Teledyne LeCroy SierraNet Protocol Suite software version information.

3.3 Toolbar Options

Table 3.3: Toolbars & Options (Sheet 1 of 2)

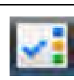
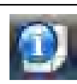
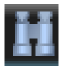
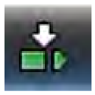
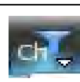
Toolbar	Icon	Description
Main Toolbar		Hide/Display Menu Bar. Click to hide or display the Menu Bar. See *3.2, Menu Bar Options*.
		Open file icon. Click to open a file. See *3.2.1, File*.
		Save trace icon. Click to save a trace. See *3.2.1, File*.
Setup Toolbar		Preferences icon. Click to set the software and display settings. See *3.2.2.2, Preferences*.
Analysis Toolbar		Spreadsheet View icon. See *5.2.1, Spreadsheet View*.
		Frame Inspector View icon. See *5.2.3, Frame Inspector View*.
		Traffic Summary icon. *5.2.4, Traffic Summary View*
		Data View icon. *5.2.5, Data View*
		Bus Utilization icon. See *5.2.6, Bus Utilization View*.
		Export to Wireshark. Click to export trace to Wireshark and launch the Wireshark application. Wireshark must be installed on the PC. Wireshark is a free application available at www.wireshark.org. (see *5.2.7, Export to Wireshark*).
		Trace Expert icon. Click to generate a variety of reports about the loaded Trace. See *5.2.8, Trace Expert* for more details.
		Displays the Trace information dialog. (see *5.2.9, Trace Information*).

Table 3.3: Toolbars & Options (Sheet 2 of 2)

Toolbar	Icon	Description
Navigation Toolbar		Find icon. You can search for specific Triggers and specify the From, Domain, Direction and Logic. See 5.5.1, *Find*.
		Find Next icon. Searches for the next instance.
		Find Previous icon. Searches for the previous instance.
		Go to icon. Click on white down arrow to bring up Event Dialog (see 5.5.2, *Go To Event*). Click on small white triangle (to right of icon) to bring up Go To Event dialog. See Figure 5.155.
		Go to Trigger icon. Click to go to the trigger point in the trace. See Figure 5.157.
		Go to Marker icon. Click on white down arrow and orange pointer to bring up the Marker list dialog. See 5.5.4, *Go to Marker*. Click on the small white triangle (to the right of the icon) to bring up the list of Markers. See Figure 5.159.
View Toolbar		Zoom in icon. Expands the Spreadsheet or Exchange View. See 5.6.1, *Zoom In*.
		Zoom out icon. Compresses the Spreadsheet or Exchange View. See 5.6.2, *Zoom Out*.
		Filter icon. Click on blue funnel to Enable Hide/Show. Click the small white triangle to open the filter dialog. See 5.6.3, *Enable Hide/Show (Filter Events)*.
		Ports icon. Click to select a port. See 5.6.3.5, *Ports*.
		Idles icon. Click to show/hide idles in a trace. See 5.6.4, *Show/ Hide Non-Frames*.
Analyzer Configuration Settings Icons		Device External Trig Setting icon. Click to open the Device Settings dialog. See 4.1.2.6, *External Trigger*.
		Recording Setting icon. Click to open the Recording Setting dialog. See 4.1.5, *Recording Settings Pane*.
		Trigger Filter Settings icon. Click to open the Trigger Filter Settings dialog. See 4.2.1.5, *Patterns and Data Capture Setup*.

Chapter 4

Recording Configuration with Real Time Traffic

To perform Protocol Analysis, the system defines and runs an analysis project for either Ethernet or Fibre Channel (FC), depending on the licensed features of the Analyzer to which you are connected. An analysis project defines what to capture, what the analyzer triggers on, and the memory settings. You can save defined projects as project ***.gep** files for later use. A captured trace is saved in a file with the **.get** extension.

After you install the Analyzer software (see 2.1.1, *Installation of the Net Protocol Suite Software*) and set up the Analyzer (see 2.2, *Hardware Setup*):

1. Launch the software (see 2.5, *Using the Net Protocol Suite Software*) to display the main window.
2. Configure the analyzer (see *Analyzer Startup – New Project*).

The Main Menu displays the Menu Bar, the Tool Bars and the selected analyzer configuration (Figure 4.1).

Figure 4.1: Teledyne LeCroy Net Protocol Suite Main Window

4.1 Analyzer Settings

The Teledyne LeCroy Net Protocol Suite Analyzer Settings panel in the application has five functional sections as shown below. The application is designed such that the user starts from the left pane and moves to the right pane to connect to a device and record a capture as listed below.

Figure 4.2: Analyzer Settings Panel

① *Device Pane*: Enables adding and assigning a device

② *Port Status Pane*: View the port status

③ *Session Control Pane*: Starts and stops recording

④ *Recording Settings Pane*: Manages the recording settings such as Number of Segments and Segment Size

⑤ *Trigger/Filter Settings Pane*: Enables Trigger Filter settings

4.1.1 Device Pane

The Device pane allows you to add or remove a device in the chain of attached devices and assign each device to a different project (Figure 4.3). First, add a device before activating it:

1. Click **Setup** → **Device Management.**
2. To select a device, drag-and-drop it onto a device in the Project Device Pane.

You can have multiple projects assigned to different devices. A single project will automatically connect to an active device. Right-click on a device and select **Activate** to start the device. Click the **X** icon to disconnect the device.

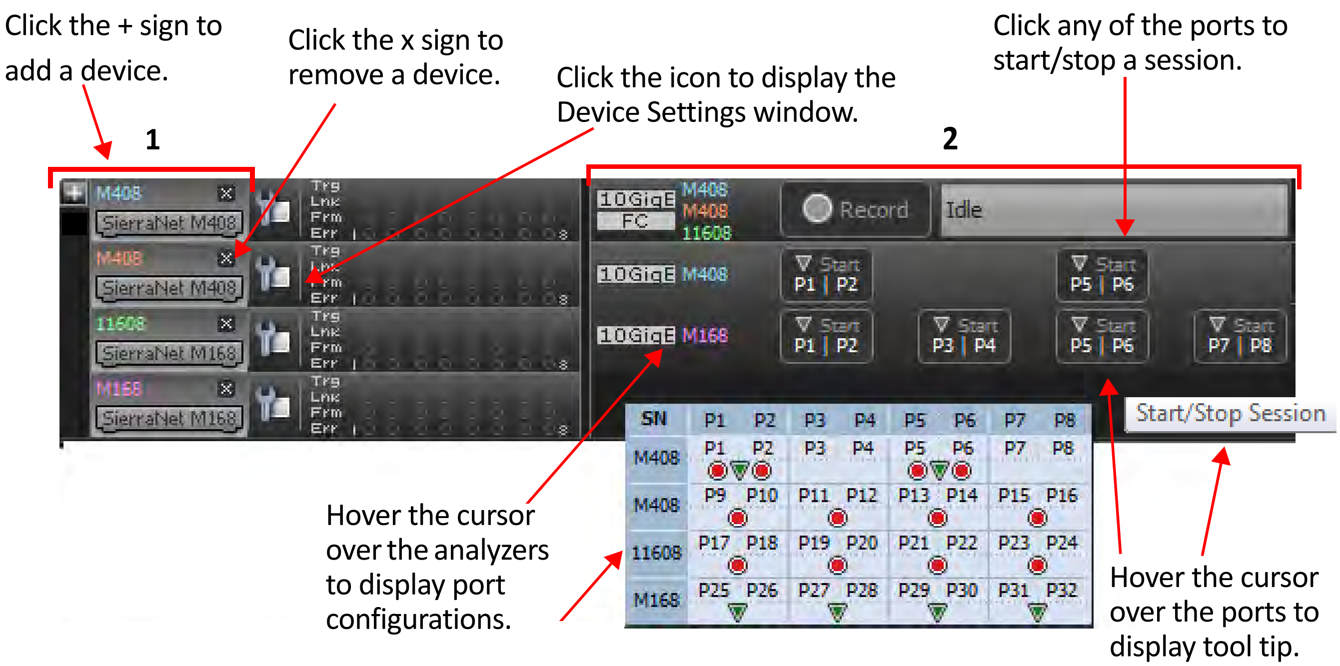


Figure 4.3: Device Pane Displaying Multiple Devices

① Presents a physical representation of the analyzers

② Presents a logical representation of the analyzers

Perform the following steps to add a device.

1. Click **Setup → Device Management.**

   The **Device Management** window appears (Figure 4.4).

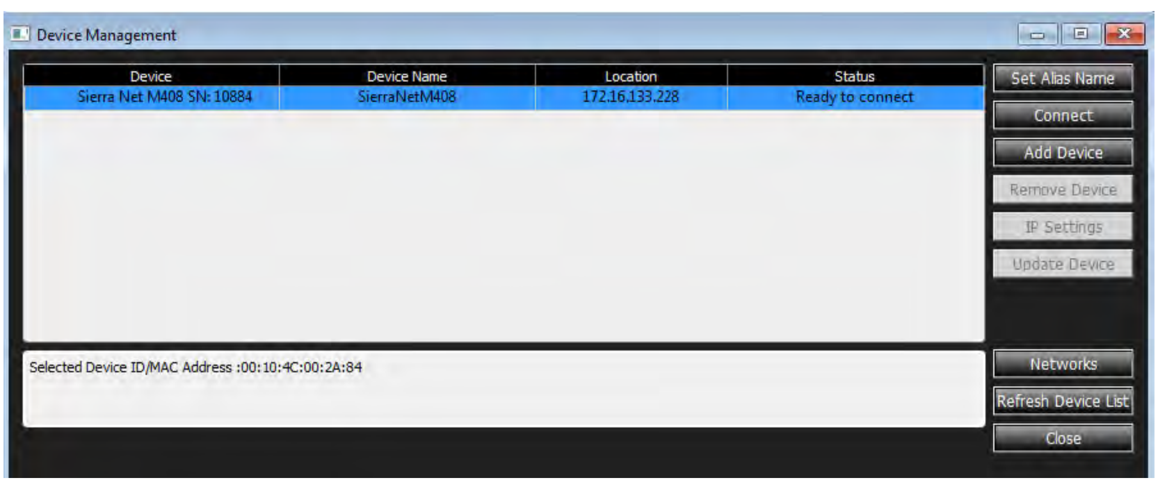


Figure 4.4: Device Management Window

2. Click on the selected Device, then click **Connect**.

4.1.2 Device Settings

The Device Settings window configures the External Trigger and Probe Calibration settings for each device supported by the Net Protocol Suite. For the M648, you can also set up the FEC counter, See 4.1.2.2, *M1288 Calibration*, 4.1.2.4, *M648 Auto Calibration* and 4.1.2.6, *External Trigger* for more information.

4.1.2.1 M1288 Device Settings

The Device Settings window configures the following:

- External Trigger settings (see Figure 4.5)
- Probe/Transceiver settings (see Figure 4.6 and Figure 4.7)

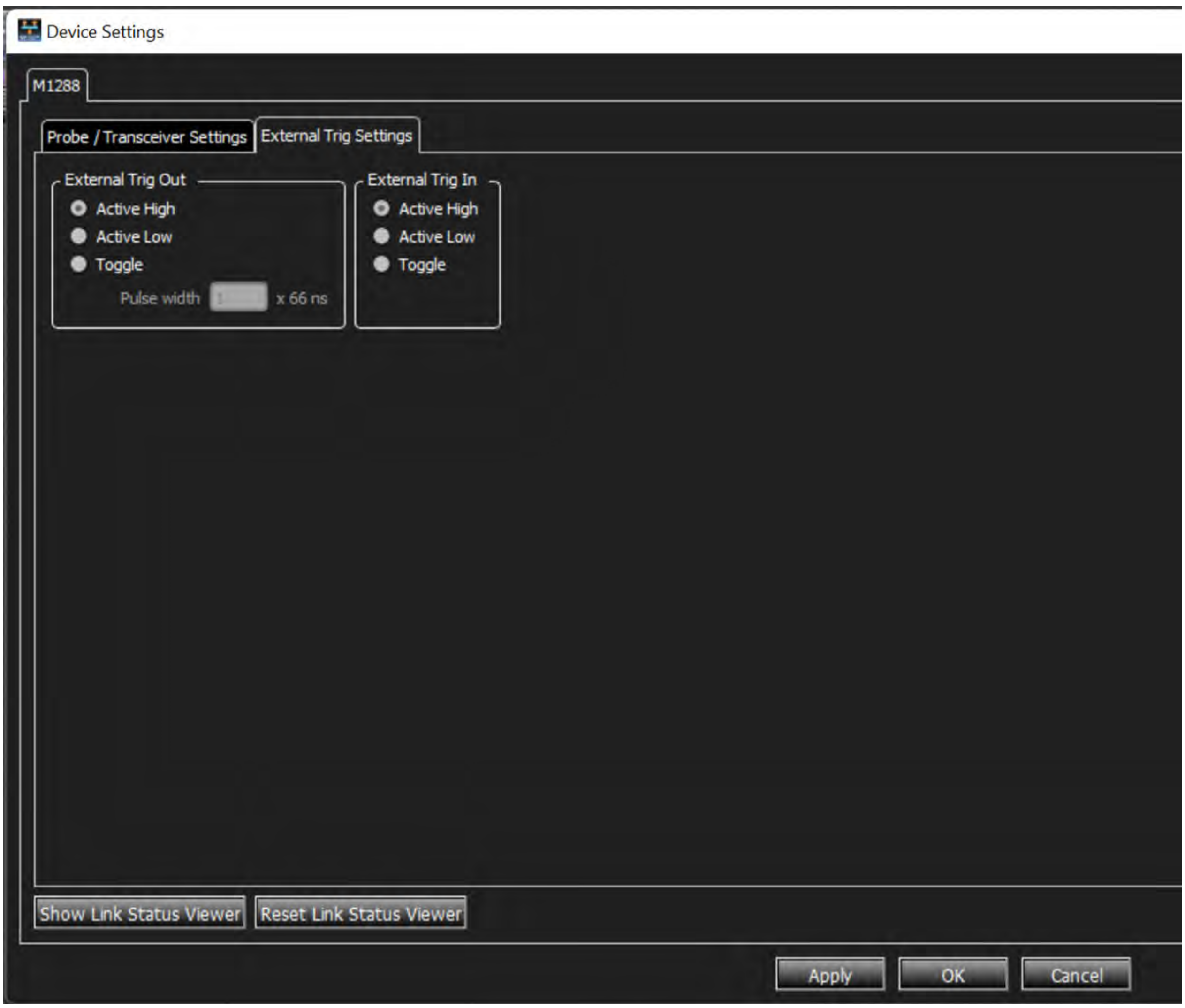


Figure 4.5: External Trigger Settings

For the M1288, you can set the following parameters per Port and per Lane(Figure 4.6):

- To Analyzer:
  - DC Gain

- EQ Gain

- To DUT:
  - DC Gain
  - EQ Gain

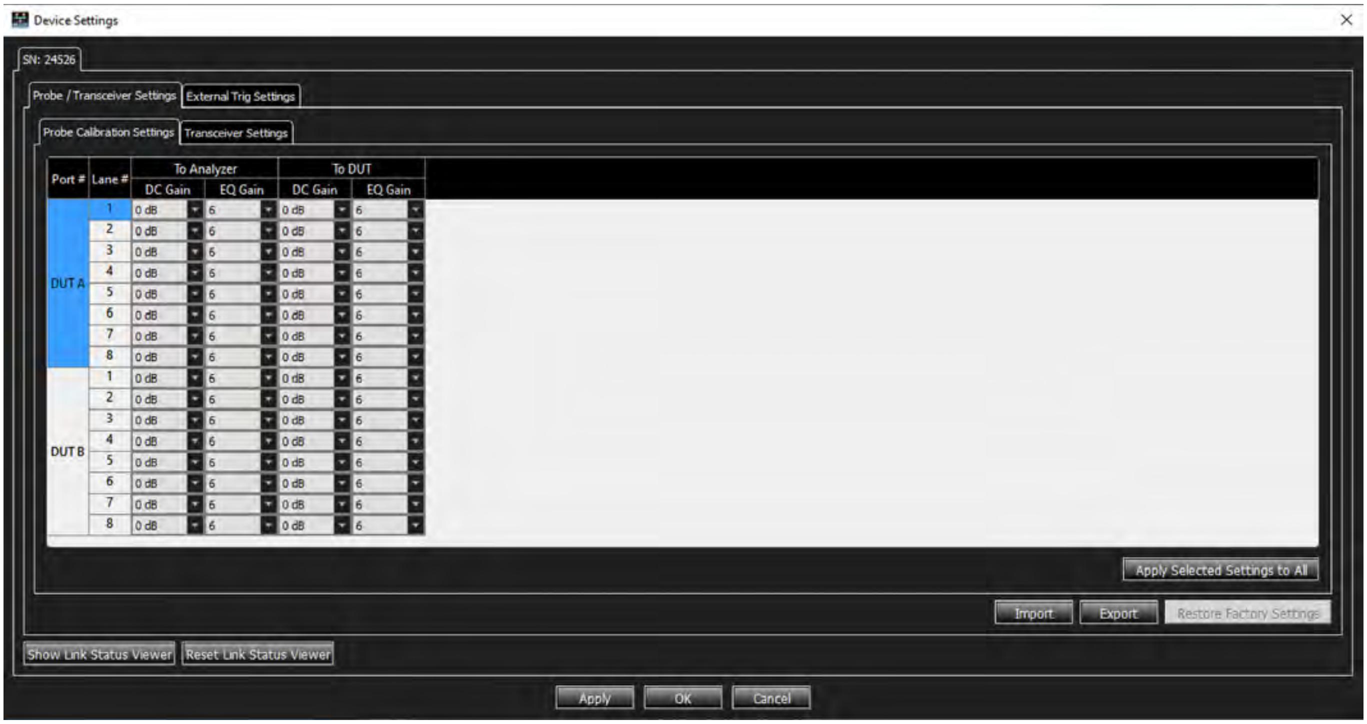


Figure 4.6: M1288 Probe Calibration Settings

The following options are available for each lane of the M1288 (See Figure 4.7):

- TX Drv Amp: 585 to 998
- TX Emp Pre: 0 to -18.69
- TX Emp Pre2: 0 to -7.09
- TX Emp Pre3: 0 to -7.09
- TX EMP Post: 0 to -18.69
- TX Inhibit: On or Off
- TX Polarity: Pos or Neg
- RX CDR Hold: On or Off
- RX Polarity: Pos or Neg
- GTM RST: Reset
- PCS Loopback: On or Off
- Xcvr Rate Select: Default

The options are:

- Apply the selected settings to all lanes,

- Import settings from a stored file,

- Export the current settings to a saved file for use in the future, or
- Restore to the Factory Settings.

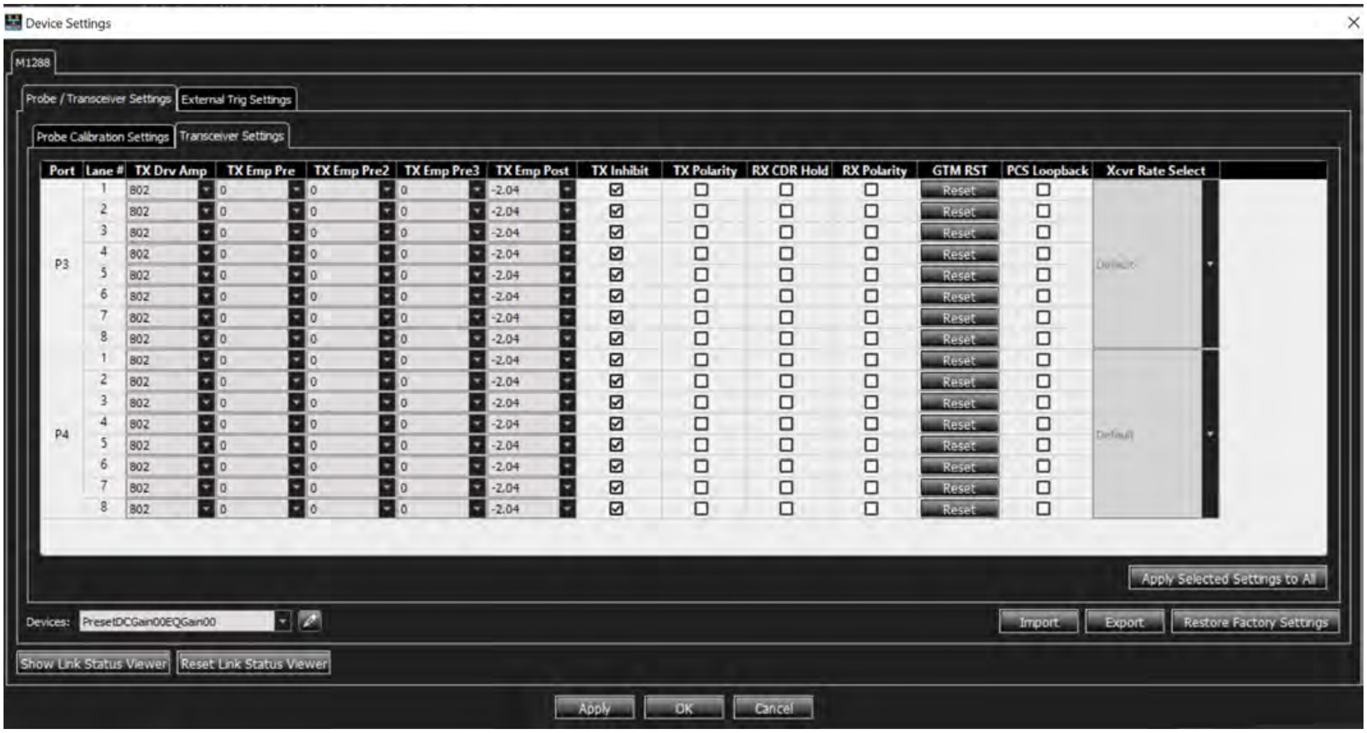


Figure 4.7: M1288 Transceiver Settings

4.1.2.2 M1288 Calibration

The M1288 probes come pre-calibrated and, in many cases, will not need additional field calibration. Following these instructions, along with using a worksheet to track the calibration settings, will help perform the field calibration. There are two calibrations possible:

1. DUT path calibration. This should be performed first, if necessary.
2. Analyzer path calibration.

M1288 DUT Path Calibration

Calibrate the DUT path first before proceeding to calibrating the Analyzer side of the probe.

1. To perform the DUT path calibration, you will need a SierraNet M1288 analyzer, the Net Protocol Suite software, and the M1288 Calibration spreadsheet.
2. Connect and add the M1288 probe to the Net Protocol Suite software (see Figure 4.3 for more information). The Add Device to Project window displays (Figure 4.8).

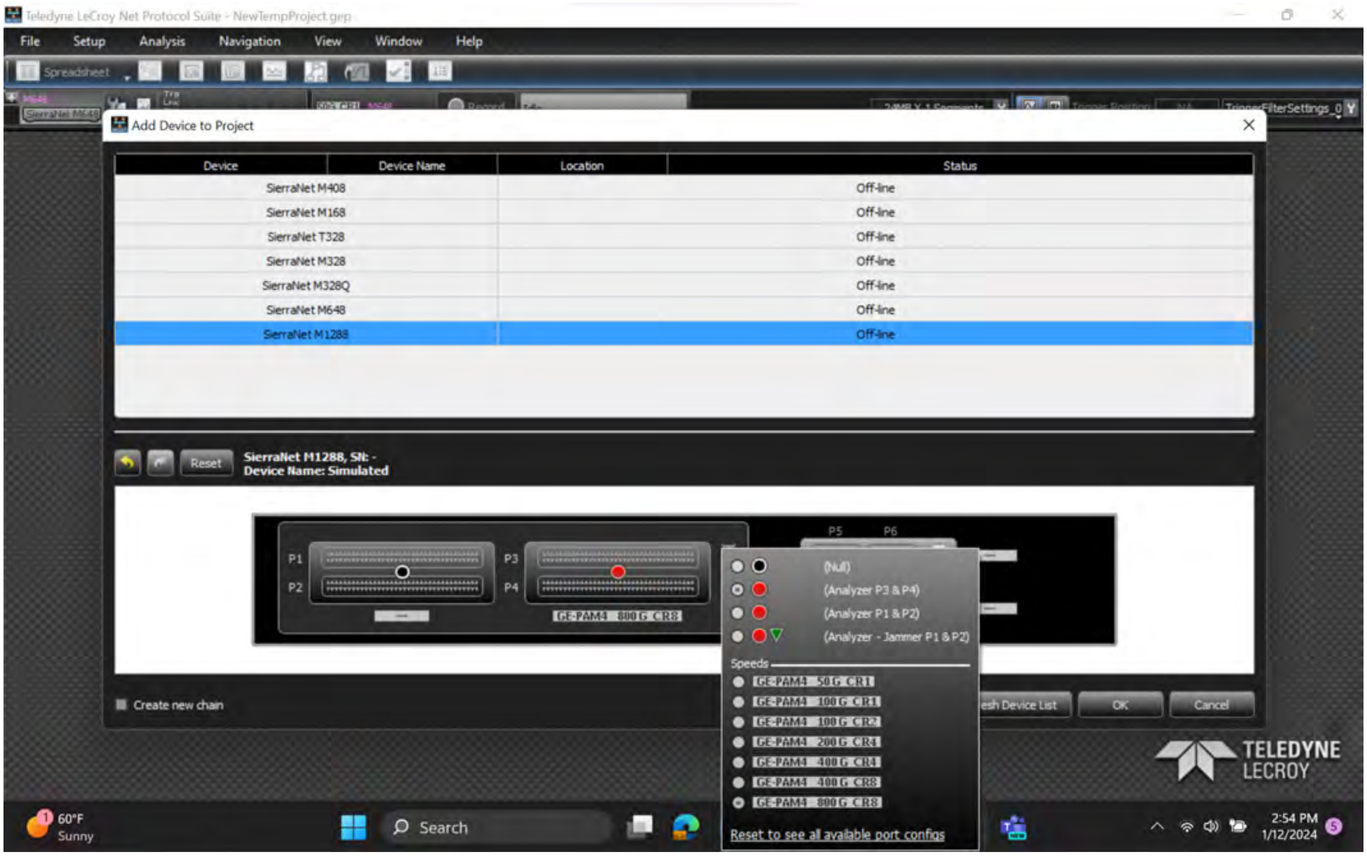


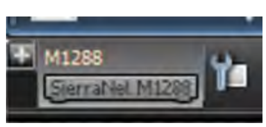
Figure 4.8: M1288 Configure Ports P3 and P4

3. Configure ports P3 and P4 in 8x100G mode (if supported). This enables each lane to be calibrated independently. This also assumes that:
   a. The DUT has a mechanism to read the BER values, OR
   b. The DUT path doesn't need calibration, just the analyzer path. If the DUT path doesn't need calibration, skip to the *M1288 Analyzer Path Calibration* section.

NOTE: If one or more of the DUTs do not support a BER reading, then contact psgsupport@teledyne.com for assistance using the analyzer to assess the link quality.

---

4. Verify the probe middle ('Status') LED is flashing (you are connected to the probe). If the Status LED is Blue or Red, please contact Support at psgsupport@teledyne.com.
5. Open the Device Settings window by clicking the wrench icon next to the device.



6. To find the quickest calibration setting, test the values in this order:
   a. For 100G Base speeds: (0/8, 0/10, 0/12, -2/8, -2/10, -2/12) and
   b. For 50G Base speeds: (0/16, 0/18, 0/20, -2/16, -2/18, -2/20) .
   c. If the goal is to find the best calibration settings, then run through more settings (possibly skipping the -4 setting).
   d. Change one value at a time, so in a thorough search, start with 0/6 and move up to 0/24, once at 0/24, the process can begin again at either -2/24 and work down or -2/6 and work up.
7. Enter the BER reading in the spreadsheet for any lanes that come up with a BER reading. Once the calibration is complete, the table automatically marks the lowest BER in each row as green, therefore identifying the best setting .
8. By changing all lanes to the same setting, all the values can be quickly tested and then the spreadsheet will show the best setting for each individual value. The DUT Calibration - Example tab in the Calibration Workbook should help make it clearer how the process works.
9. For lanes that don't come up, leave the field blank.

M1288 Analyzer Path Calibration

Once the lanes are showing good at the DUT side and the links are up (with valid PCS traffic running), calibrate the Analyzer path, as needed. The Link Status dialog makes this easy:

1. Click the Show Link Status Viewer button in the Device Status window. See Figure 4.9.

Figure 4.9: M1288 Device Settings: Show Link Status Viewer

2. The Link Status window displays on the main Net Protocol Suite window, as shown in Figure 4.10.

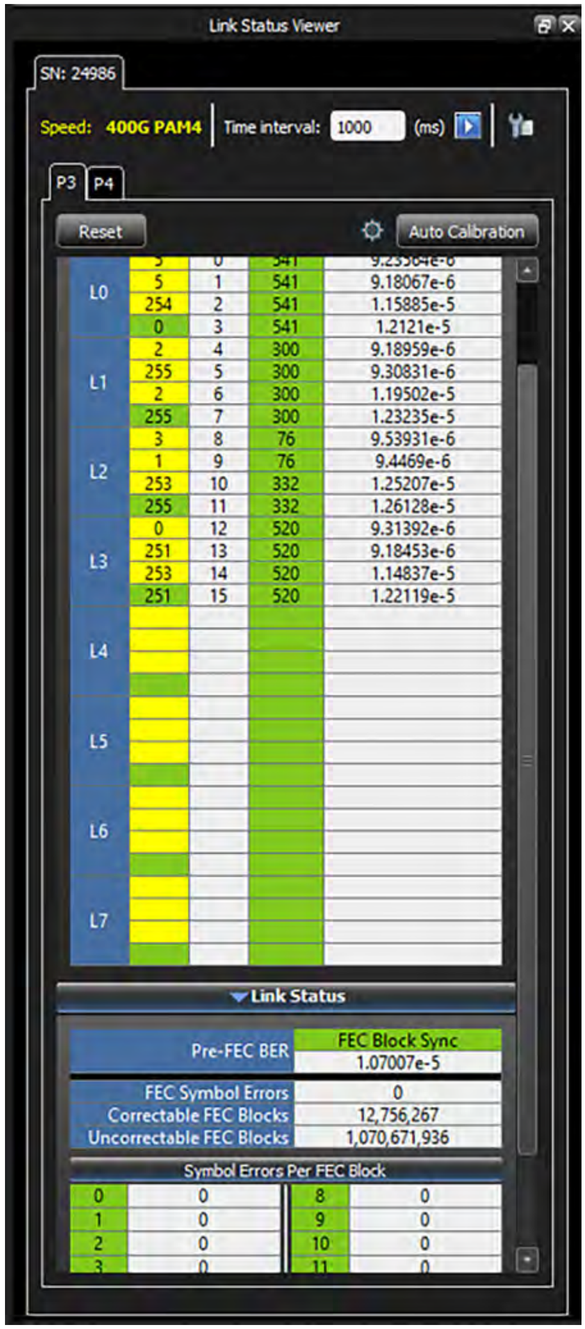


Figure 4.10: Link Status Window

3. For calibrating the analyzer path, detect lanes that have higher BER, and manipulate them one by one, in a similar manner to the DUT path described above in *M1288 DUT Path Calibration*.

4.1.2.3 M648 Device Settings

The Device Settings window configures the following:

- External Trigger settings (see Figure 4.11)
- Probe/PHY settings (see Figure 4.12 and Figure 4.13)
- Forward Error Correction (FEC) Counter settings

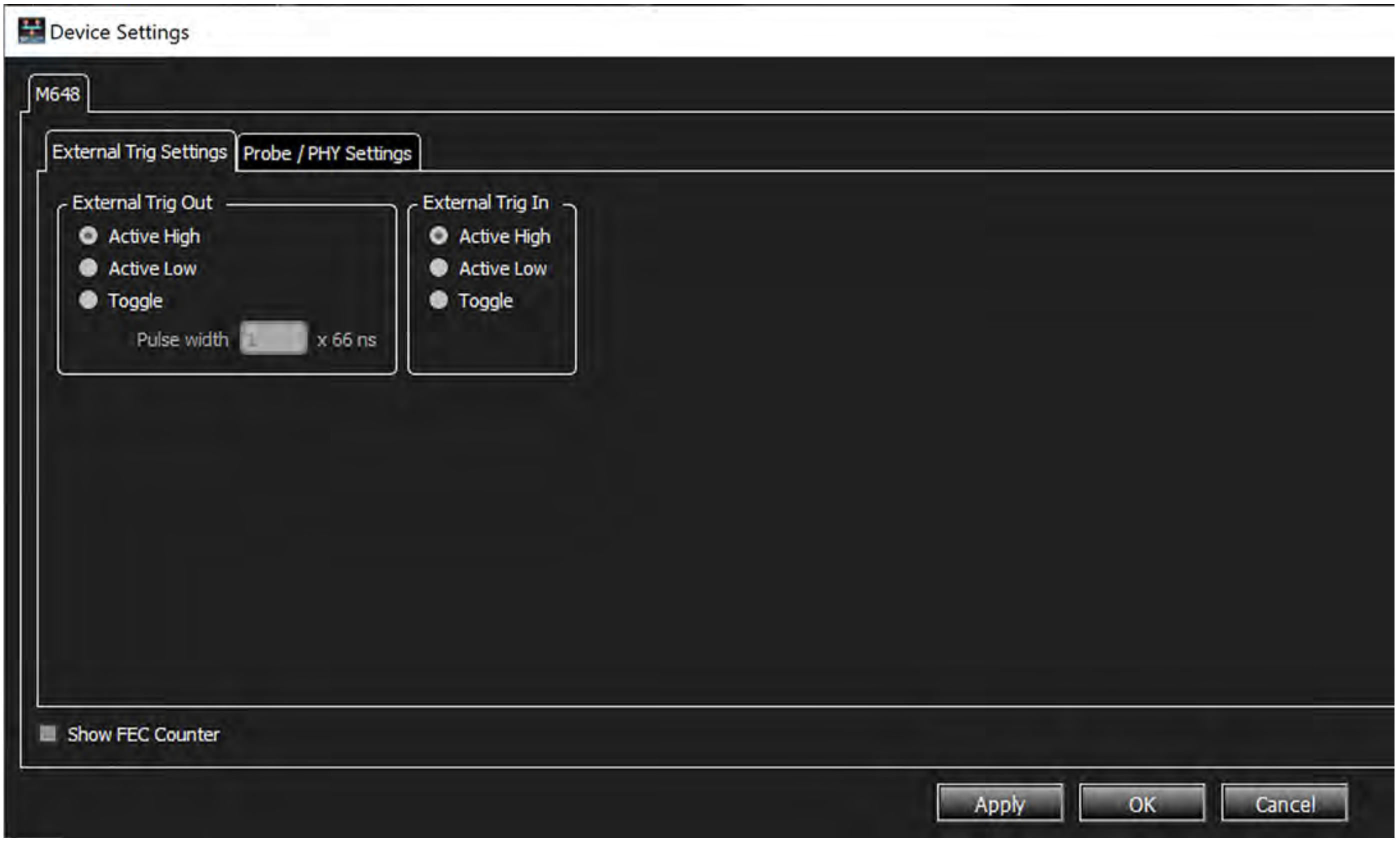


Figure 4.11: M648: External Trigger Settings

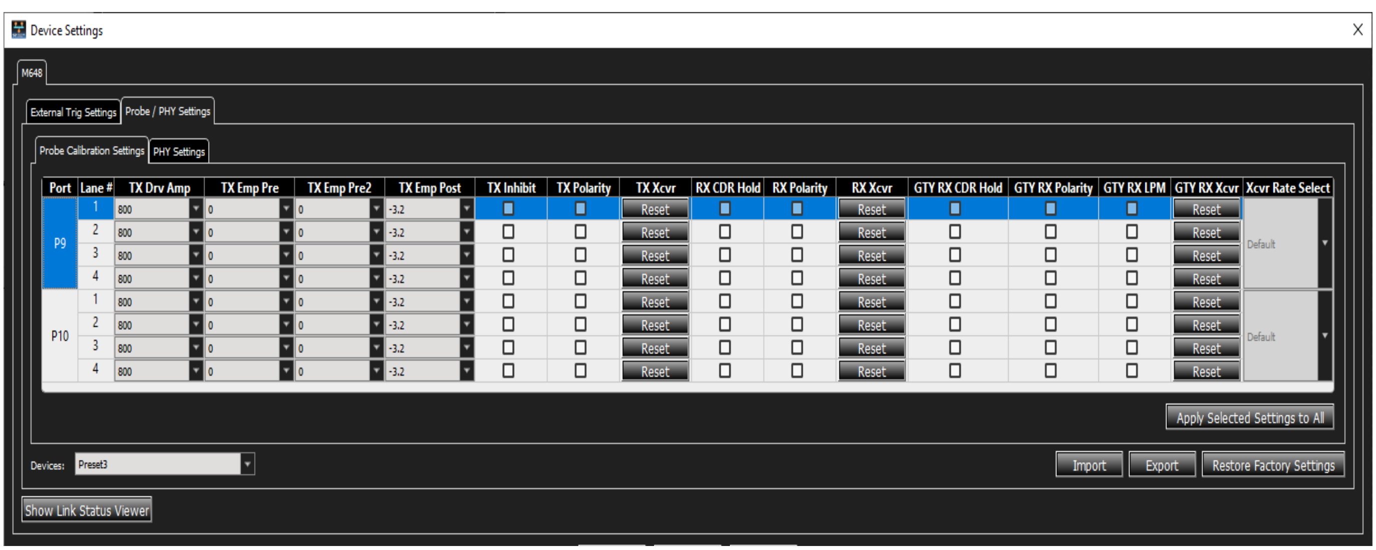


Figure 4.12: M648 Probe Calibration Settings

For the M648 Probe Calibration you can set the following options for each lane:

- TX Drv Amp: 250 to 1025
- TX Emp Pre: 0 to -9.2
- TX Emp Pre2: 0 to -2.7
- TX EMP Post: 0 to -9.2
- TX Inhibit: On or Off
- TX Polarity: Pos or Neg
- TX Xcvr: Reset
- RX CDR Hold: On or Off
- RX Polarity: Pos or Neg
- RX Xcvr: Reset
- GTY RX CDR Hold: On or Off
- GTY RX Polarity: Pos or Neg
- GTY RX LPM: On or Off
- GTY RX Xcvr: Reset

You can apply the selected settings to all lanes, Import settings from a stored file, Export the current settings to a saved file for use in the future or Restore the Factory Settings.

Figure 4.13: M648 PHY Calibration Settings

For the M648 you can set the following parameters per Port and per Lane:

- CTLE Gain DUT
- Amp Gain DUT
- CTLE Gain ANA
- Amp Gain ANA

For the M648 Probe and PHY Calibration settings, you can select Presets from the Devices drop-down list (Figure 4.14). You can also click the edit button to rename a selected Preset.

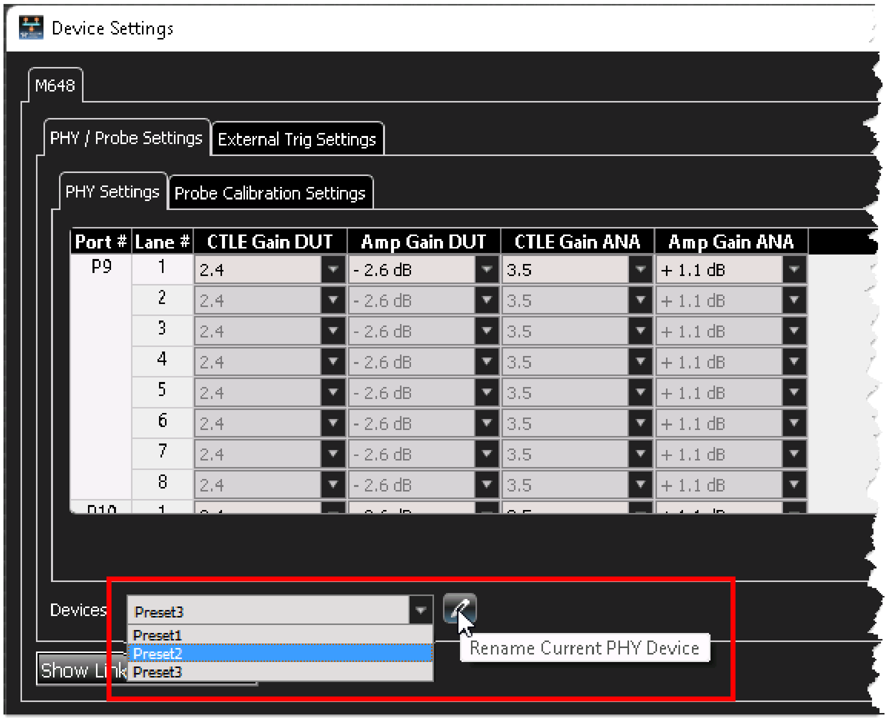


Figure 4.14: M648 Probe/PHY Calibration Device Presets

4.1.2.4 M648 Auto Calibration

If you need to ease the process of finding a combination of Probe Settings that will result in a clean link, you can use the Auto Calibration option. his process first goes through all available known Presets to determine if one of them results in a clean link. If not, it will then loop through all possible combinations of Probe Settings, until it finds a setting that does.

This is found by clicking the **Show Link Status Viewer** button on the Device Settings window, shown in Figure 4.12. To use Auto Calibration, click **Auto Calibration** (Figure 4.15). The icon to the left of the Auto Calibration button changes to yellow when the first possible calibration value is found, then changes to green when the best calibration value is found.

This process can be lengthy, as there are 73 x 8 x 8 = 4672 potential cases to try. The time each case takes is configurable; that is, the longer the Analyzer 'dwells' on each case, better results are produced. With the default dwell time, the worst-case Auto Calibration run could take up to 30 hours. However, in practice, most runs find adequate settings in between 30 minutes to 2 hours.

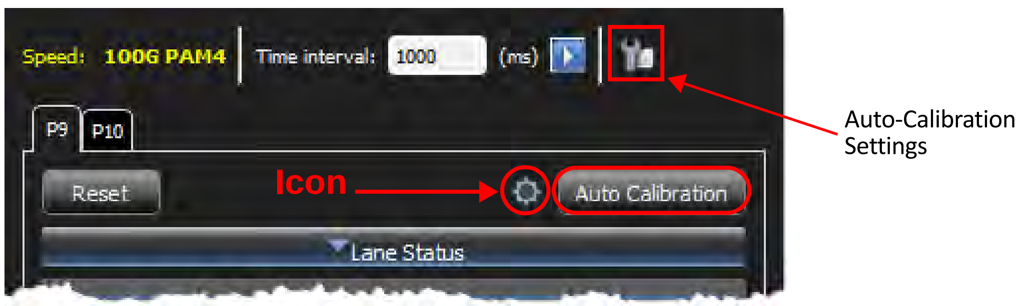


Figure 4.15: Link Status Window – Auto Calibration Option

To change the settings of the Auto Calibration, click the icon located next to the Time Interval. Figure 4.16 displays.

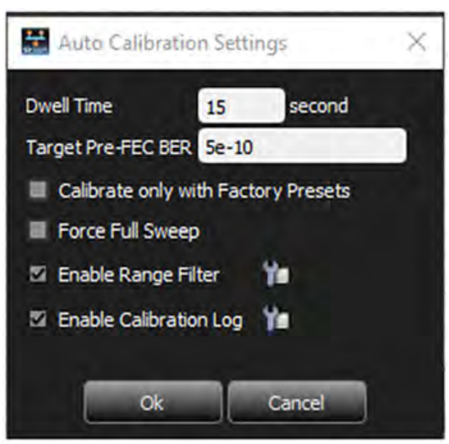


Figure 4.16: Auto Calibration Settings

Table 4.1: M648 Auto Calibration Settings

Setting	Description
Dwell Time	The time (in seconds) the Auto Calibration process monitors the link stability and accumulates the Pre-FEC BER. Making this longer will lengthen the total calibration time, but will yield better, more stable settings.
Target Pre-FEC BER	During the Auto Calibration process, the BER found will be compared to this value to determine if the link is good enough. Making this smaller will lengthen the total calibration time, as more settings will be attempted in an effort to reach the lower BER.
Calibrate only with Factory Presets	This allows for a quicker calibration process, as the Software will only attempt previously known settings, saved as Factory Presets. If none of these Presets satisfies the calibration in terms of link stability time or BER, the best Preset will be chosen and additional settings will not be attempted. When this is unchecked, if no Presets satisfy the calibration requirements, the Auto Calibration will go ahead to systematically attempt each combination of PHY settings variables, potentially taking many hours to complete.
Force Full Sweep	When the Auto Calibration process find settings that satisfy the required parameters in terms of link stability and BER, it will stop the calibration and use those settings. Checking this option will force the process to keep searching for even better results, until all combinations have been attempted. This will take many hours to complete.
Enable Range Filter	Enable Range Filter: Check this box to add range filters to the Auto Calibration. See *M648 Range Filter* for more information.
Enable Calibration Log	Enable Calibration Log: Check this box to log results for each attempted setting . See *M648 Auto Calibration Log* for more information.

Table 4.2 shows how to use the various settings together. There are only certain combinations you can use to search for the best BER.

Table 4.2: Auto Calibration Combinations

Combination	Result
Calibrate only with Factory Presets + Force Full Sweep	Adding Force Full Sweep with Factory Presets forces the system to check all the factory presets for the best Pre-Fec BER (the set BER or below) instead of stopping when it finds the first instance.
Calibrate only with Factory Presets + Enable Range Filter	N/A. This combination is invalid. The Range Filter will be ignored.
Force Full Sweep + Enable Range Filter	Adding Force Full Sweep with Enable Range Filter forces the system to check all the settings in the range for the best Pre-Fec BER (the set BER or below) instead of stopping when it finds the first instance.
Calibrate only with Factory Presets + Force Full Sweep + Enable Range Filter	N/A. This combination is invalid. The Range Filter will be ignored.

M648 Range Filter

The Range Filter option allows you to choose a specific range in which to search for the Target Pre-Fec BER. You can select a range of the following:

- Amp Gain DUT
- Amp Gain ANA
- CTLE Gain DUT

To enable range filtering:

1. In the Auto Calibration Setting dialog, check the box next to **Enable Range Filter.**
2. To edit the range filter values, click the icon to the right of Enable Range Filter. The Range Filter Settings dialog displays, as shown in Figure 4.17.
3. Change the lower and upper limits. Click **OK**.

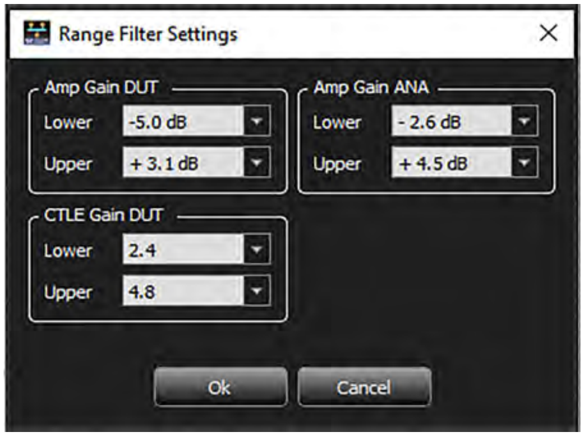


Figure 4.17: Range Filter Settings

NOTE: Range Filter does not work if you also select **Use Factory Presets**.

M648 Auto Calibration Log

You can change the default path for the log file and append a new file to prevent overwriting the previous file.

1. From the Auto Calibration settings dialog, click the check box for **Enable Calibration Log**, then click the wrench icon  to the right. See Figure 4.18.

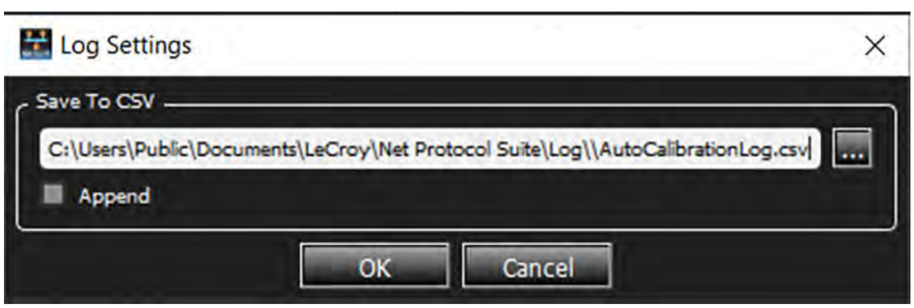


Figure 4.18: Log Settings for Auto Calibration

2. To change the default path, enter a new path or click  and browse for a file location.
3. To prevent overwriting the previous file, click the **Append** check box.

NOTE: When using Append, you can distinguish between new and old data; the software enters a timestamp at the beginning of each new set of data.

---

4. Once you are satisfied with your changes, click **OK**. The Link Status window reappears.

5. Click **Auto Calibration** to start the Auto Calibration.

The following is a snippet from the end of an actual log file. It shows auto-calibration attempting different Presets and reaching status OK when BER is adequate. See Table 4.3 for an explanation of result codes.

```
Preset10,_1-5-1-2,SAMPLING,size 13,5e-4
Preset10,_1-5-1-2,SAMPLING,size 14,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset10,_1-5-1-2,UNSTABLE_LINK,BestStableTime 0ms,5e-4
Preset11,_1-6-1-2,SAMPLING,size 1,0e+0
Preset11,_1-6-1-2,SAMPLING,size 2,2e-8
Preset11,_1-6-1-2,SAMPLING,size 3,0e+0
Preset11,_1-6-1-2,SAMPLING,size 4,1e-8
Preset11,_1-6-1-2,SAMPLING,size 5,0e+0
Preset11,_1-6-1-2,SAMPLING,size 6,3e-8
Preset11,_1-6-1-2,SAMPLING,size 7,0e+0
Preset11,_1-6-1-2,SAMPLING,size 8,2e-8
Preset11,_1-6-1-2,SAMPLING,size 9,0e+0
Preset11,_1-6-1-2,SAMPLING,size 10,3e-9
Preset11,_1-6-1-2,SAMPLING,size 11,0e+0
Preset11,_1-6-1-2,SAMPLING,size 12,1e-8
Preset11,_1-6-1-2,SAMPLING,size 13,0e+0
Preset11,_1-6-1-2,SAMPLING,size 14,2e-8
Preset11,_1-6-1-2,OK,,1e-9
Preset11,_1-6-1-2,OK,,3e-8
```

Figure 4.19 is an example of a log output in Excel. The log is filtered to only show results that were OK and sorted by the Pre-FEC BER. This combination produces the following results:

- Results = OK for Presets 3, 8, 9, and 11.
- Preset 11 shows the lowest Pre-FEC BER.

Therefore, Preset 11 was chosen as optimal.

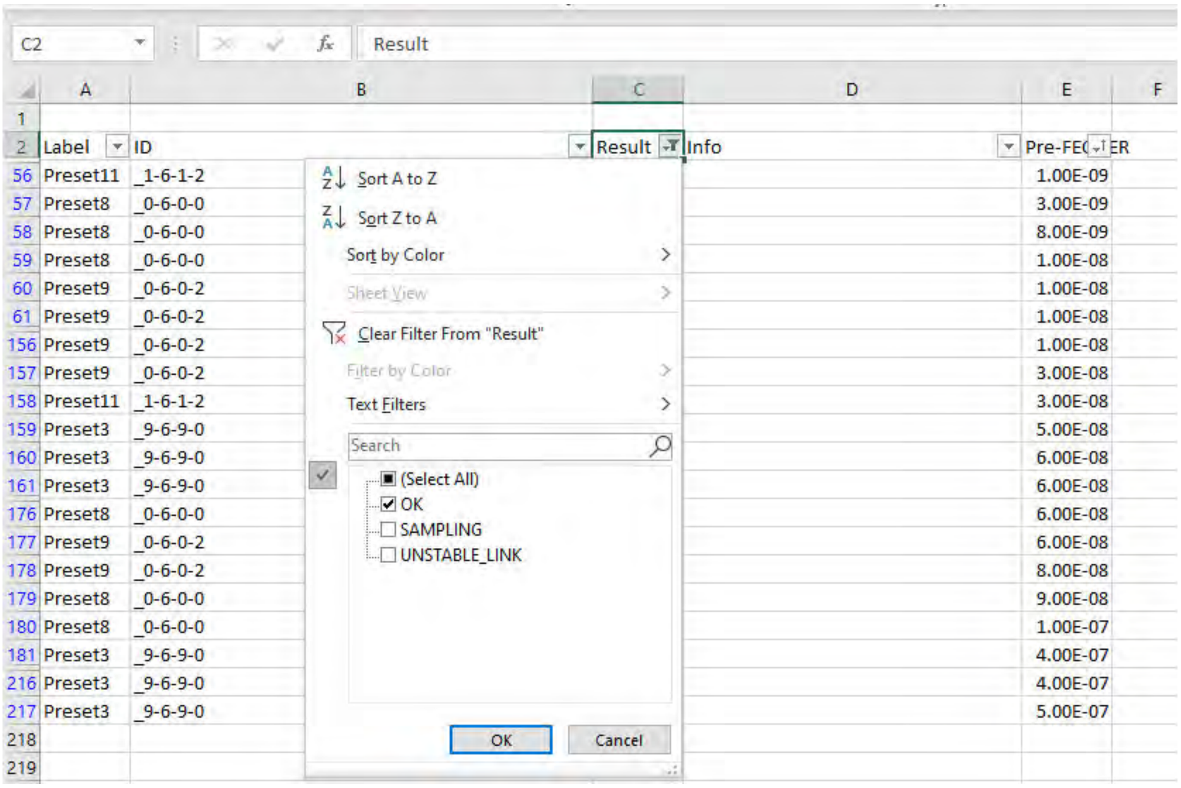


Figure 4.19: M648 Auto Calibration Results Log

Table 4.3: M648 Calibration Log Status Codes

Result	Information	Description
SAMPLING	Dwell time sampling	Auto Calibration is still sampling Link Status to meet Dwell time setting.
NO_LINK	Setting skipped due to no link	Received Loss of Sync Link Status
UNSTABLE_LINK	Setting skipped due to unstable link during dwell time	Link Status is neither Idle nor Frames throughout dwell time, and there are up to x ms time where Status is Linked (Idle or Frame).
BAD_LINK	Setting skipped due to high error	Status is linked but there are x Uncorrectable FEC errors detected.
OK	Setting is added to Candidate list	Link is stable and Uncorrectable FEC error is 0.
ACCEPT	Candidate is added to Preset list	Link is stable, Uncorrectable FEC error is 0, and Pre-FEC BER is below target value.

4.1.2.5 Probe Calibration (for SierraNet M408 and SierraNet M168)

In the Device Settings window, select the **Probe Calibration Settings** tab. Depending on the project’s protocol configuration, the Device Settings tab appears slightly different.

These settings are meant for advanced users to tune the performance of the Analyzer receiver ports, the Jammer receiver and transmitter ports, and the Analyzer DUT link pass-through path. In most cases, the default settings will perform well and should be used as-is.

40 GigE Configurations

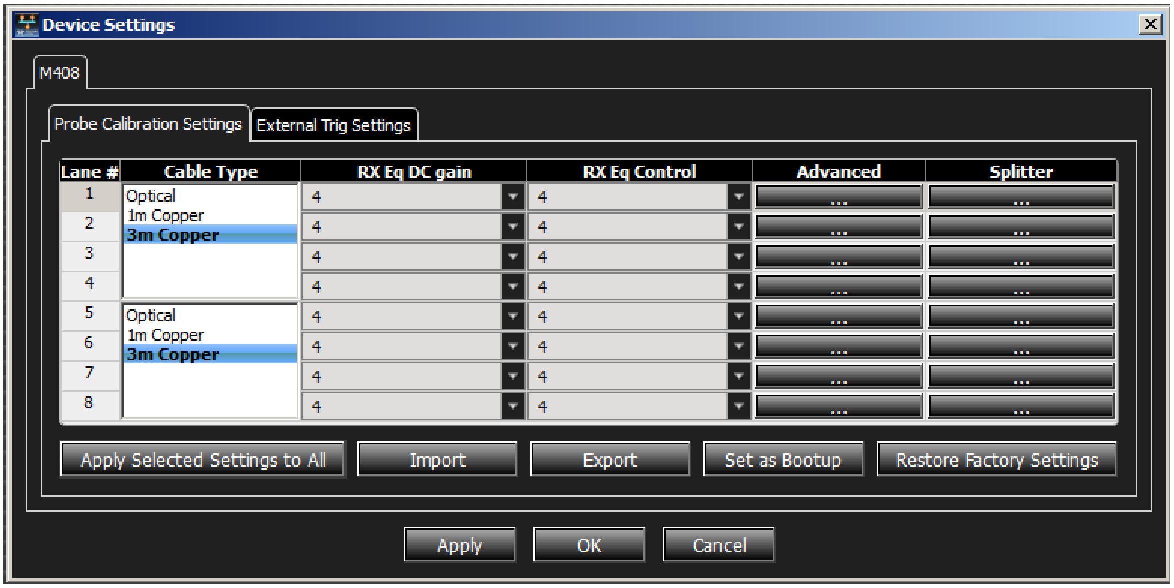


Figure 4.20: Device Settings Window for 40 GigE Device

You can manually calibrate the probe settings. Set the parameters for the following:

- Cable Type: Select Optical, 1m, 2m, 3m, or 5 meter Copper. (See 2.2.6.1, *Cables to Use with M408/M168 Analyzer*).
- RX Eq DC gain: Select a value from the drop-down list.
- RX Eq Control: Select a value from the drop-down list.
- Advanced: Displays the Advanced Probe Setting window (Figure 4.21). Enter the desired values for each of the parameters.
- Splitter: Displays the Splitter Settings window (Figure 4.22).
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.
- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.

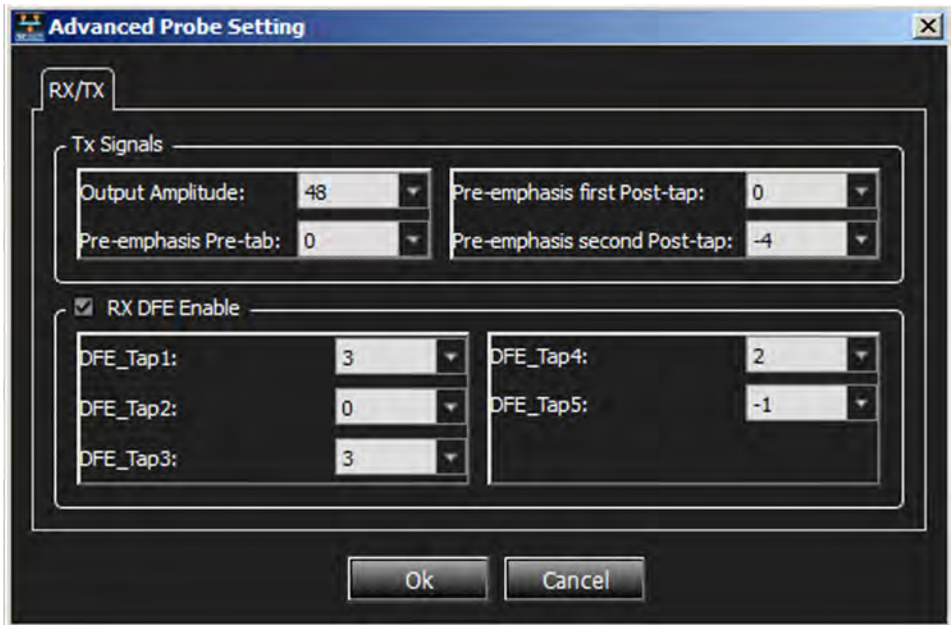


Figure 4.21: Advanced Probe Setting Window for 40 GigE Device

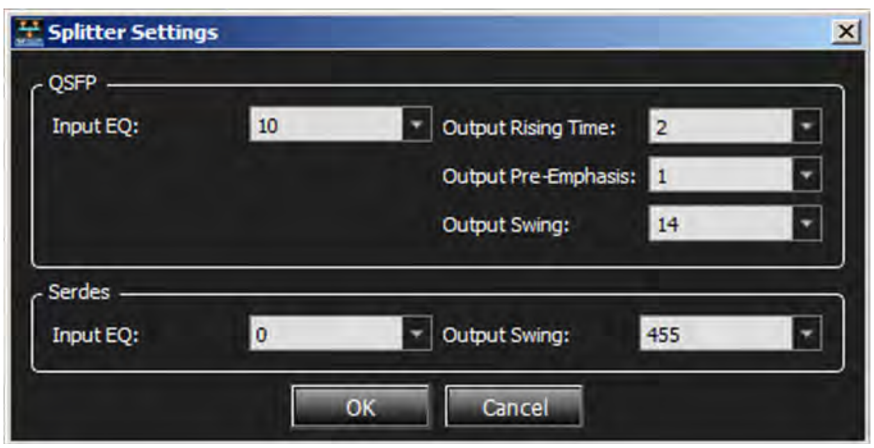


Figure 4.22: Splitter Settings Window for 40 GigE Device

10 GigE Configurations

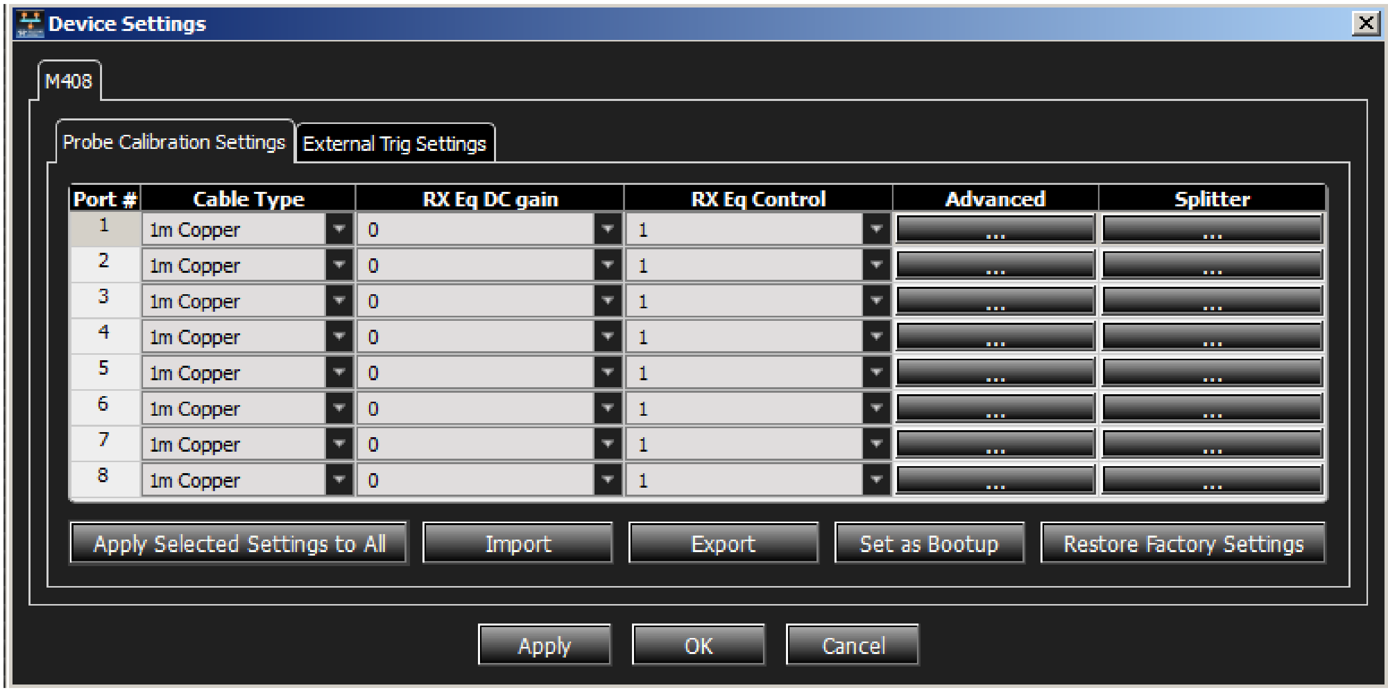


Figure 4.23: Device Settings Window for 10 GigE Device

You can manually calibrate the probe settings. To do this, set the parameters for the following:

- Cable Type: Select 1m, 3m, or 5m Copper. (See 2.2.6.1, *Cables to Use with M408/ M168 Analyzer*).
- RX Eq DC gain: Select a value from the drop-down list.
- RX Eq Control: Select a value from the drop-down list.
- Advanced: Displays the Advanced Probe Setting window (Figure 4.24). Enter the desired values for each of the parameters.
- Splitter: Displays the Splitter Settings window (Figure 4.25).
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.
- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.

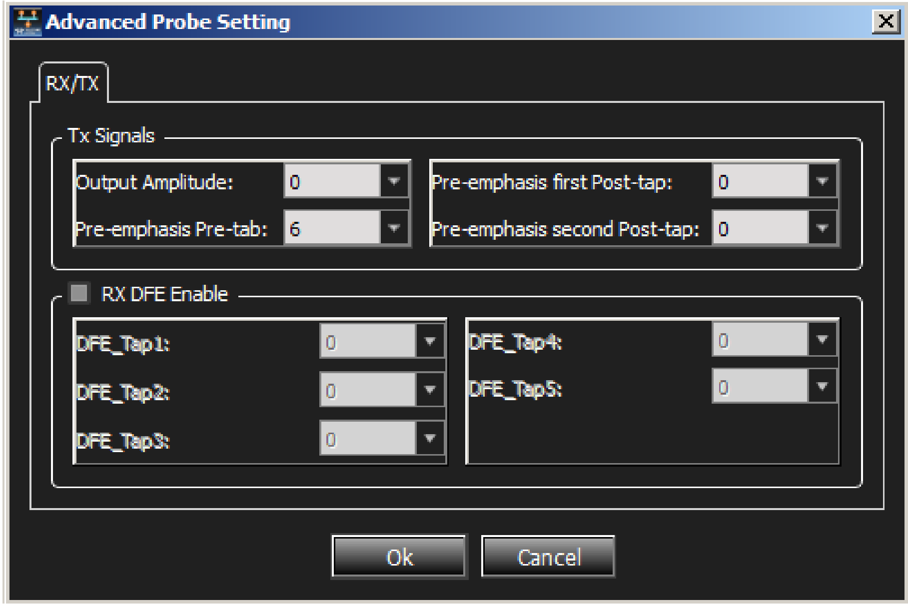


Figure 4.24: Advanced Probe Setting Window for 10 GigE Device

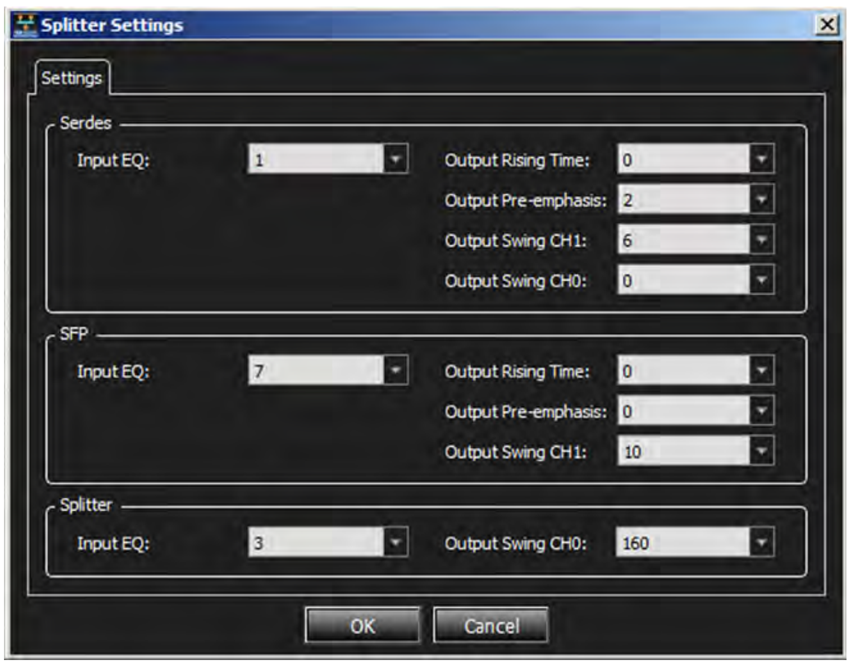


Figure 4.25: Splitter Settings Window for 10 GigE Device

FC Configurations

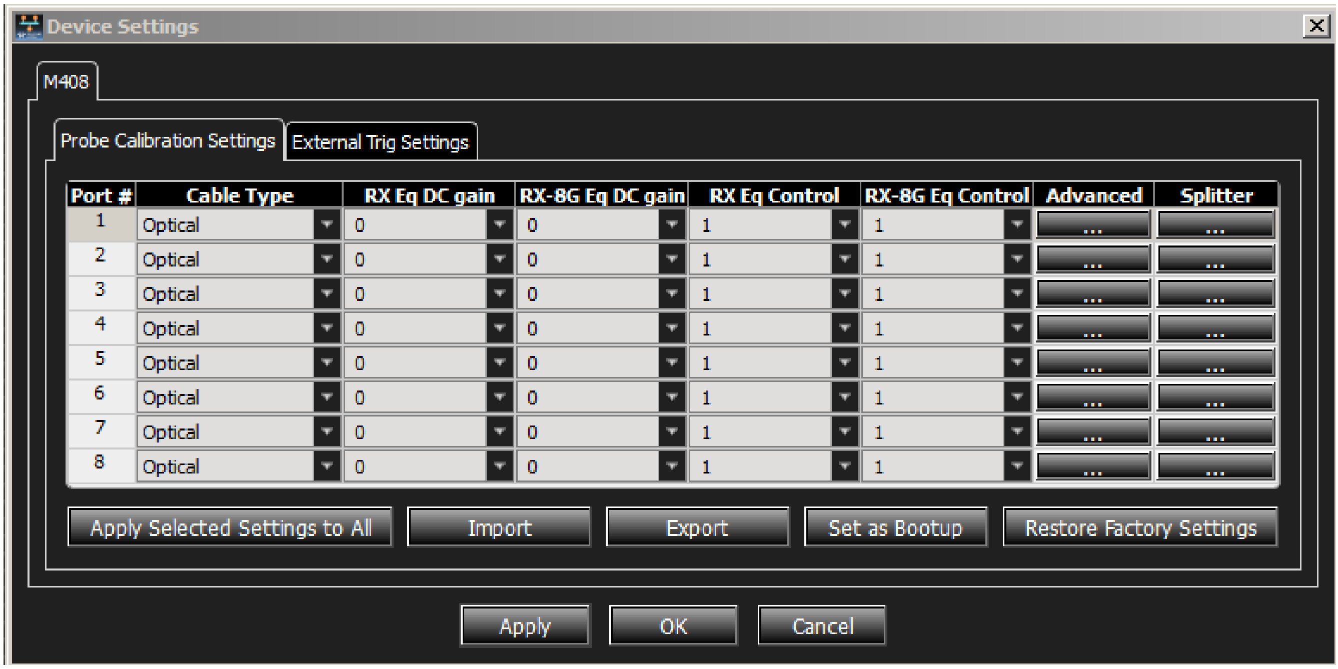


Figure 4.26: Device Settings Window for FC Devices

You can manually calibrate the probe settings. Set the parameters for the following:

- Cable Type
- RX Eq DC gain: Select value from the drop-down list.
- RX-8G Eq DC gain: Select value from the drop-down list.
- RX Eq Control: Select value from the drop-down list.
- RX-8G Eq Control: Select value from the drop-down list.
- Advanced: Displays the Advanced Probe Setting window with the RX/TX tab selected (Figure 4.27). Enter the desired values for each of the parameters. Select the RX/TX 8G tab (see Figure 4.28) and enter the desired values for each of the parameters.
- Splitter: Selecting **Splitter** displays the Splitter Settings window. (See Figure 4.29.) Enter the desired values for each of the parameters. Select the 8G tab (see Figure 4.30) and enter the desired values for each of the parameters.
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.
- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.

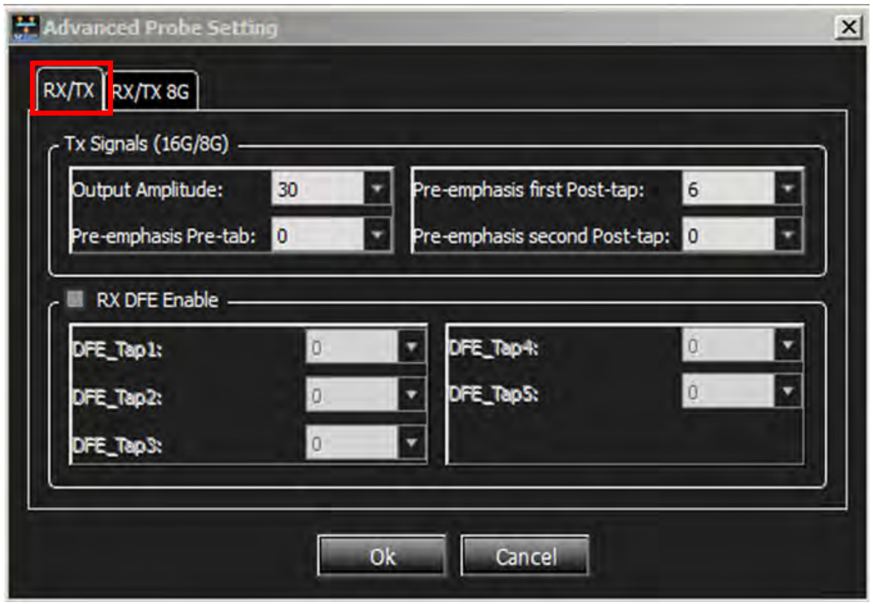


Figure 4.27: Advanced Probe Setting Window for FC Device – RX/TX

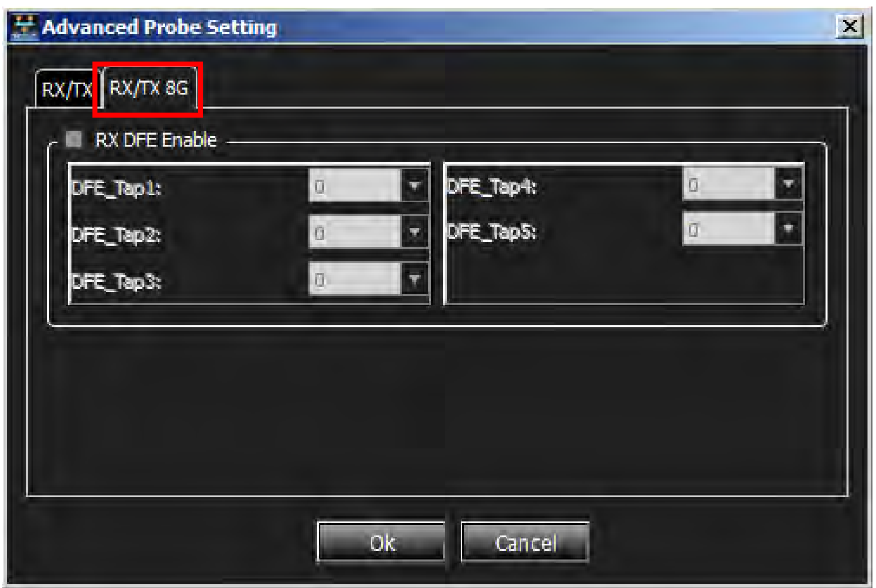


Figure 4.28: Advanced Probe Setting Window for FC Device – RX/TX 8G

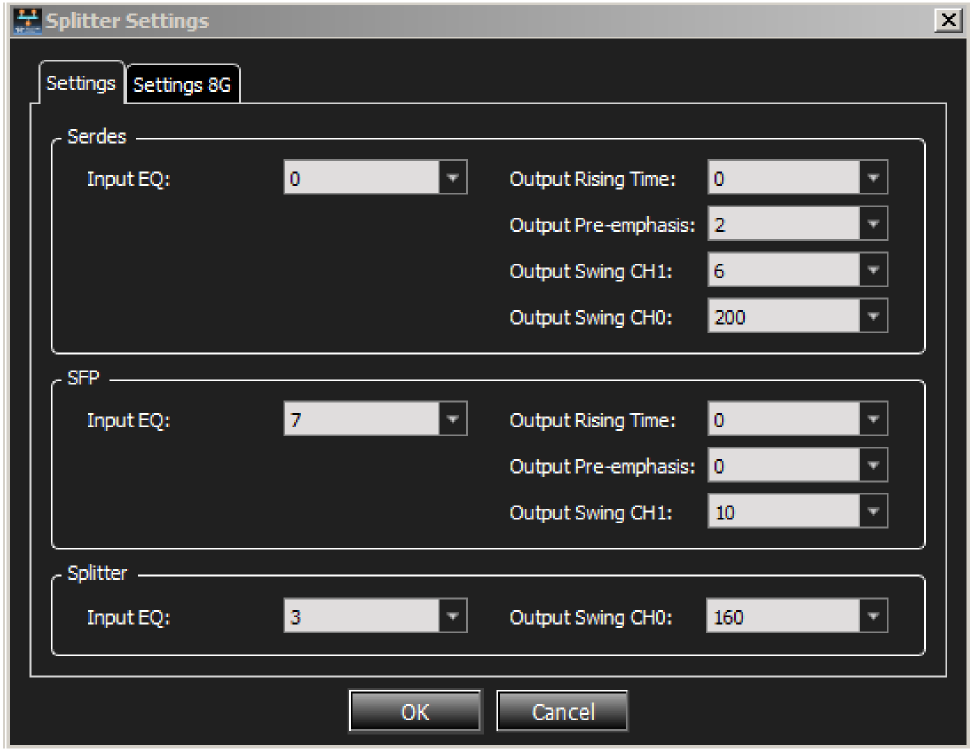


Figure 4.29: Splitter Settings Window for FC Device

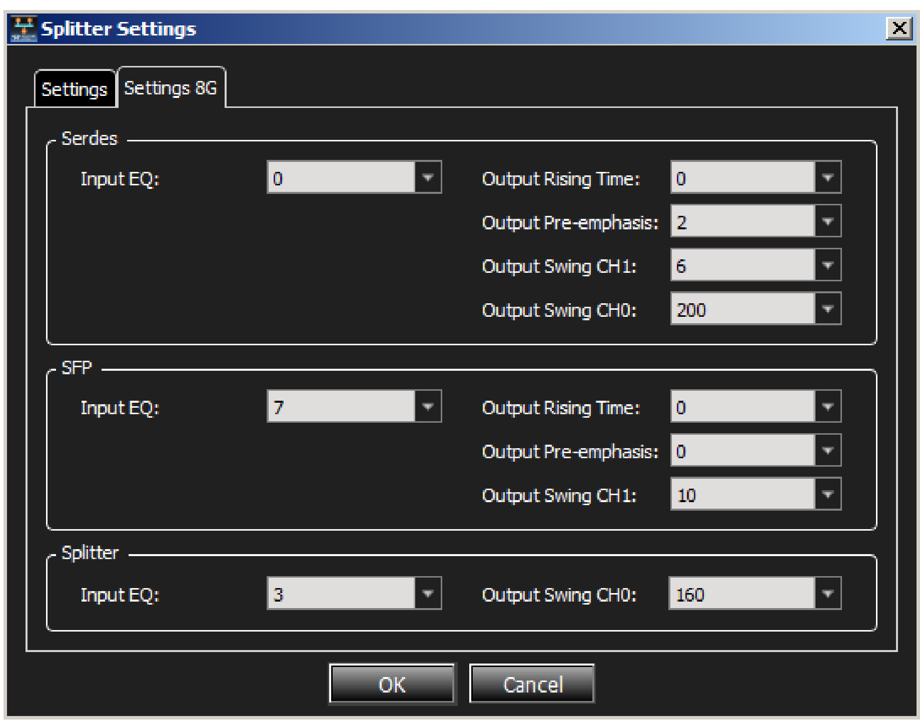


Figure 4.30: Splitter Settings window for FC Device – 8G Tab

4.1.2.6 External Trigger

External Trigger In and Out connectors appear on the front panel.

- Use *External Trigger In* to trigger the analyzer from an external source, such as a scope or other test equipment: Attach the source to the input for *External Trigger In*, then set up the analyzer to trigger on the *External Trigger In* signal, as described below.
- The *External Trigger Out* can be used to trigger other equipment when the analyzer detects a specified sequence of events on the probed links.

NOTE: This window applies to all configurations.

- In Device Settings, select the **External Trig Settings** tab.

  This shows the External Trig Out Setting and External Trig In Setting as Active, Active Low, or Toggle (Figure 4.31).

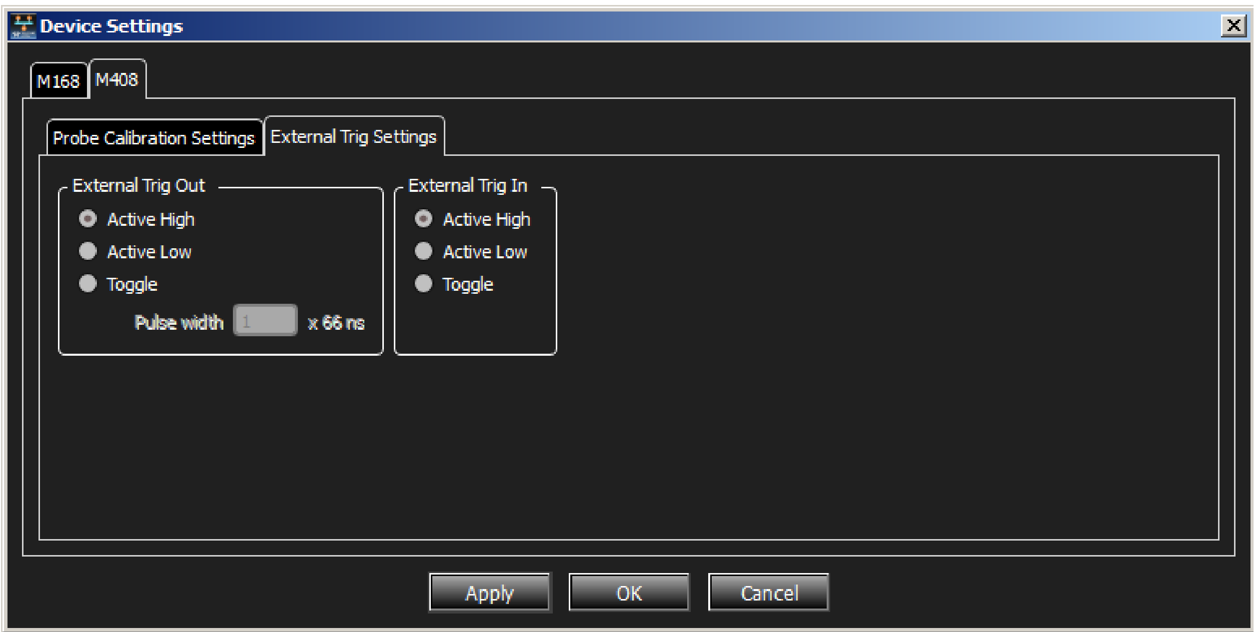


Figure 4.31: External Trigger Settings Window

External Trig Out Setting

The Analyzer can send a Low or High external signal any time a trigger occurs.

Select the External Trig Out Setting: **High Active**, **Low Active**, or **Toggle** from High to Low or Low to High once (3.3 V output).

Enter the External TrigOut pulse width.

External Trig In Setting

An external Low or High input signal can cause triggering.

Select the External Trig In Setting: **Active High**, **Active Low**, or **Toggle** from High to Low or Low to High once (3.3 V input).

The nominal External Trigger voltage is 0.818 volts. Trigger In can work with 1 volt to 5 volts input voltage.

Range Filter Settings

4.1.3 Port Status Pane

The Port Status pane (Figure 4.32) displays the status of the link on each port (Trigger, Link, Frame, and Error).

Figure 4.32: Port Status Panel

Trigger LEDs

Null	No Trigger
Green	Trigger

Link LEDs

Null	No Link
Red	Rx power differential greater than 200 uW detected between the port pairs.
Colored	Link establish; decoding of LED color coding is exactly the same as HW Link LED. See 1.5.1.1, *M648 LEDs*.

Frm LEDs

Null	No Activity
Green	Activity (AN/Training or frame)

Err LEDs

Null	No error(s)
Red	Error(s)

4.1.3.1 Dashboard of Per-Port Status

If you roll your cursor over the Port Status panel, additional information appears (Figure 4.33). You will see the serial number of the product as well as the Status of the following functions per port:

- Trigger
- Link
- Speed
- Frame
- Error
- Forward Error Correction (FEC)
- Function

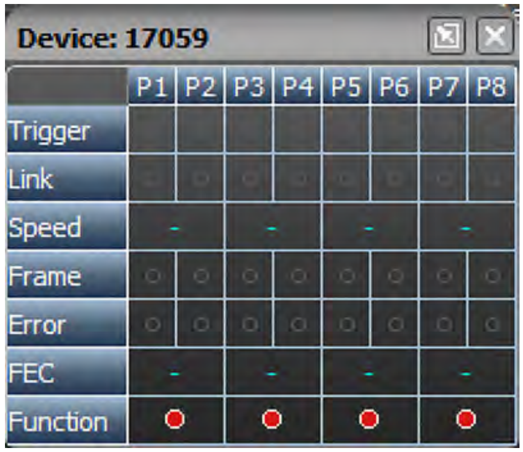


Figure 4.33: Detailed Per Port Status of Current Device

If you right click in the Port Status Pane the following menu pops up (see Figure 4.34).

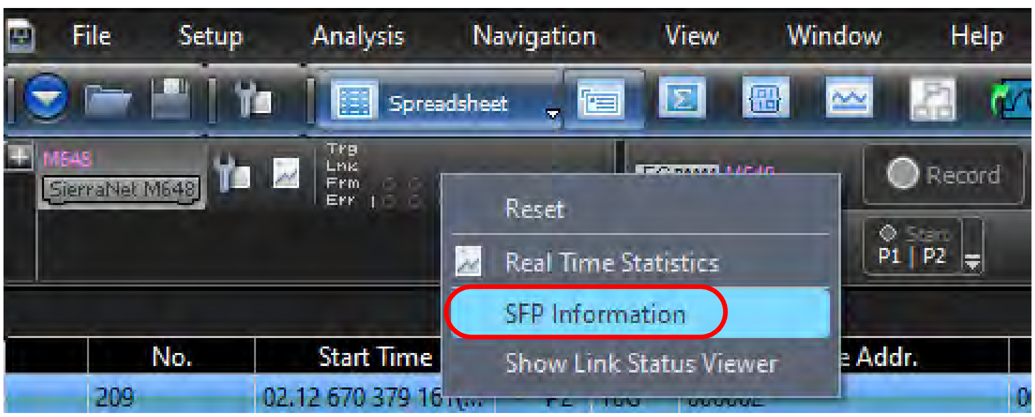


Figure 4.34: Port Status Menu

Select one of the four following options:

- Click **Reset** to reset the LED history.
- Click **Real Time Statistics** to bring up the Real Time Statistics window (see 4.4.1, *Real Time Statistics*).
- Click **SFP Information** to check both the information about the “Small Form-Factor Pluggable” connection (see 4.1.3.2, *Small Form-Factor Pluggable (SFP) Connection*) and the Rx and Tx Power Levels per Port (see 4.1.3.3, *Tx/Rx Power Tab*).
- Click **Show Link Status Viewer** to display the Link Status of the connected ports.

4.1.3.2 Small Form-Factor Pluggable (SFP) Connection

When you select **SFP Information**, the following window appears (see Figure 4.35).

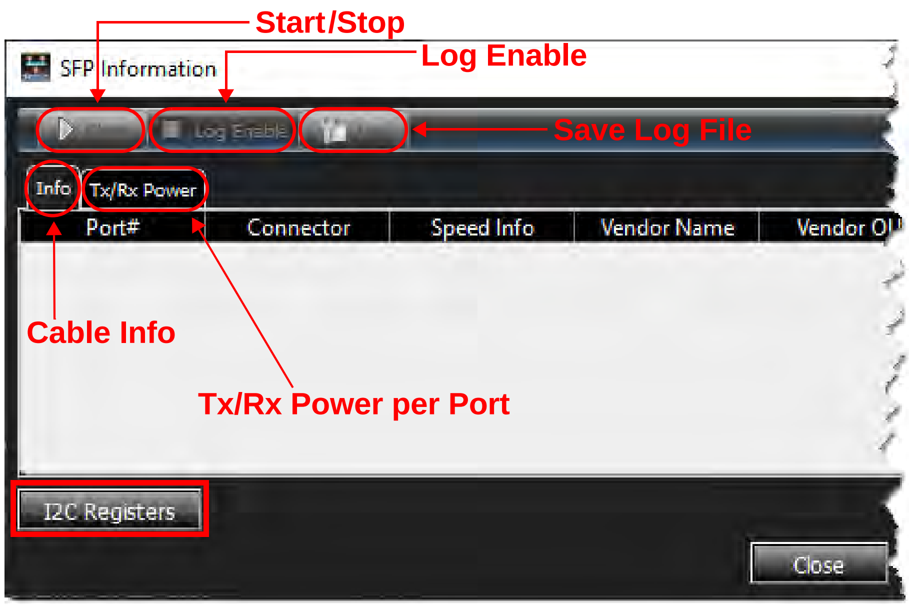


Figure 4.35: Blank SFP Information Window

When connected to a unit with cables plugged in (Figure 4.36), you can click the **Start** button to *Read* the information from the cables.

To view the cable information, select the **Info** tab and **Start** (Figure 4.36):

- Port #
- Connector
- Vendor Name
- Vendor OUI
- PartNum
- SerialNum
- Compliance

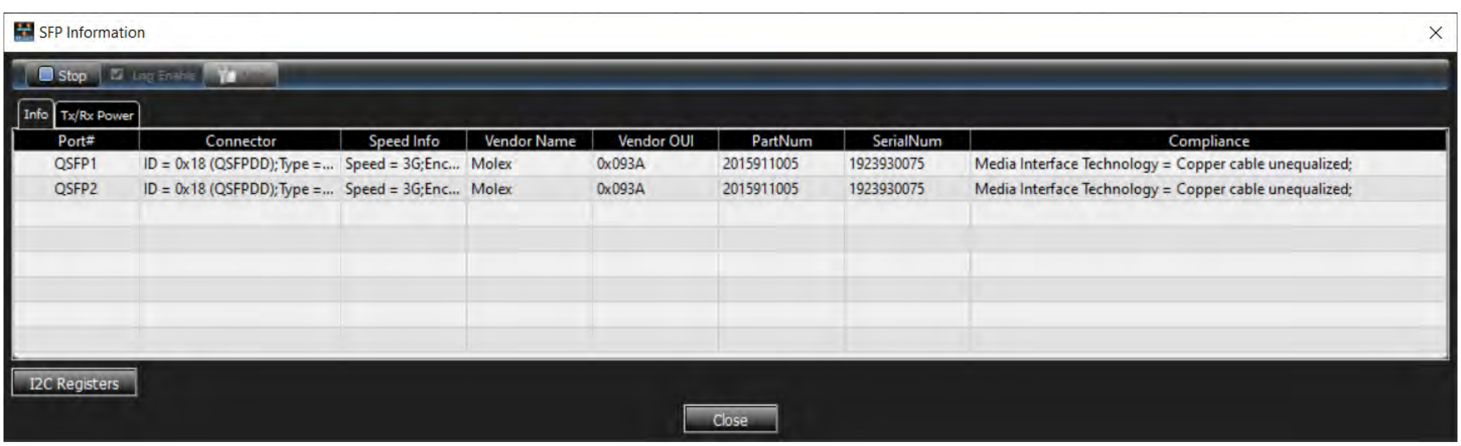


Figure 4.36: SFP Information Window

To view the Tx and Rx power per port, select the **Tx/Rx Power** tab and **Start** (Figure 4.37).

4.1.3.3 Tx/Rx Power Tab

There are three functions in the window:

- Port #
- Rx Power
- Tx Power

Figure 4.37 shows six ports are active.

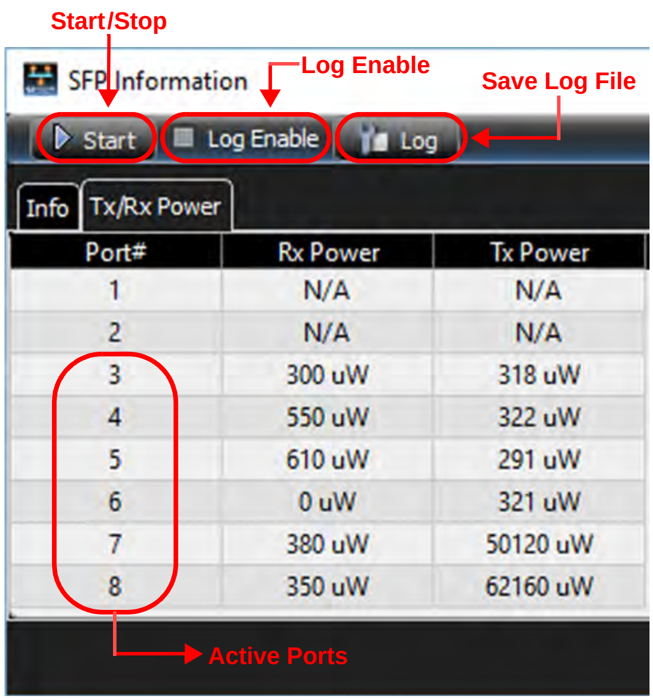


Figure 4.37: Start Viewing Active Ports

1. To set up a Log file to keep a record of the power readings, check **Log Enable** and click **Start**.

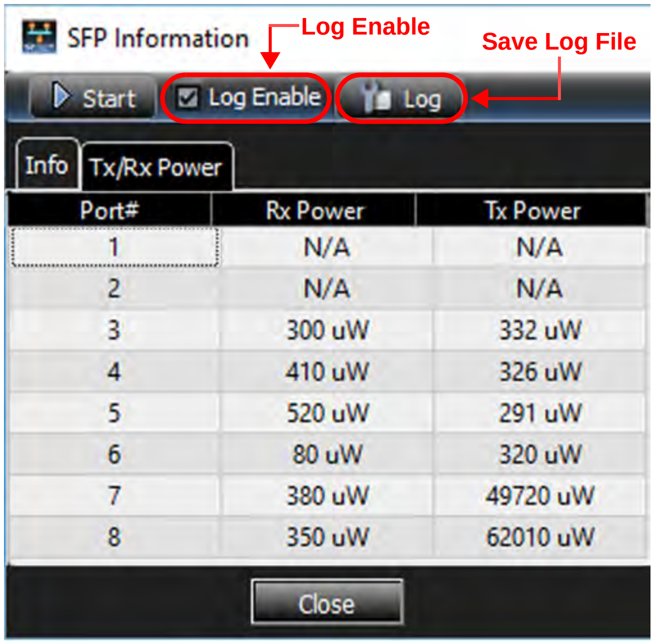


Figure 4.38: Enable Log File/Save Log File

2. To save your log file, select the **Log** tab . A dialog box appears where you can navigate to the Log File folder for Net Protocol Suite software (Figure 4.39).

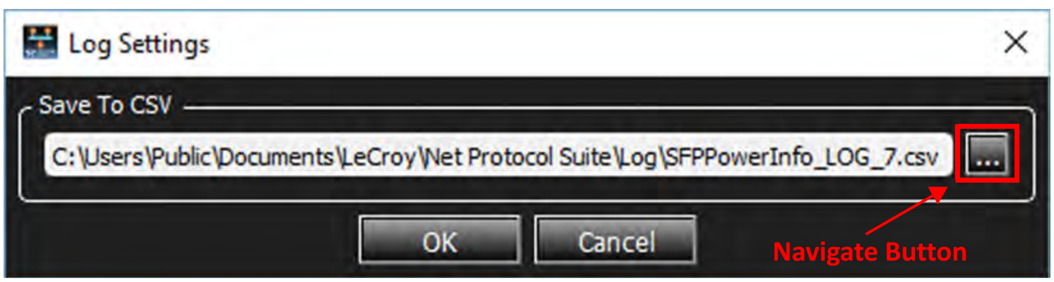


Figure 4.39: Path to Log Files for Net Protocol Suite

3. Click the **Navigate Button** . The Log Settings window appears (Figure 4.40).

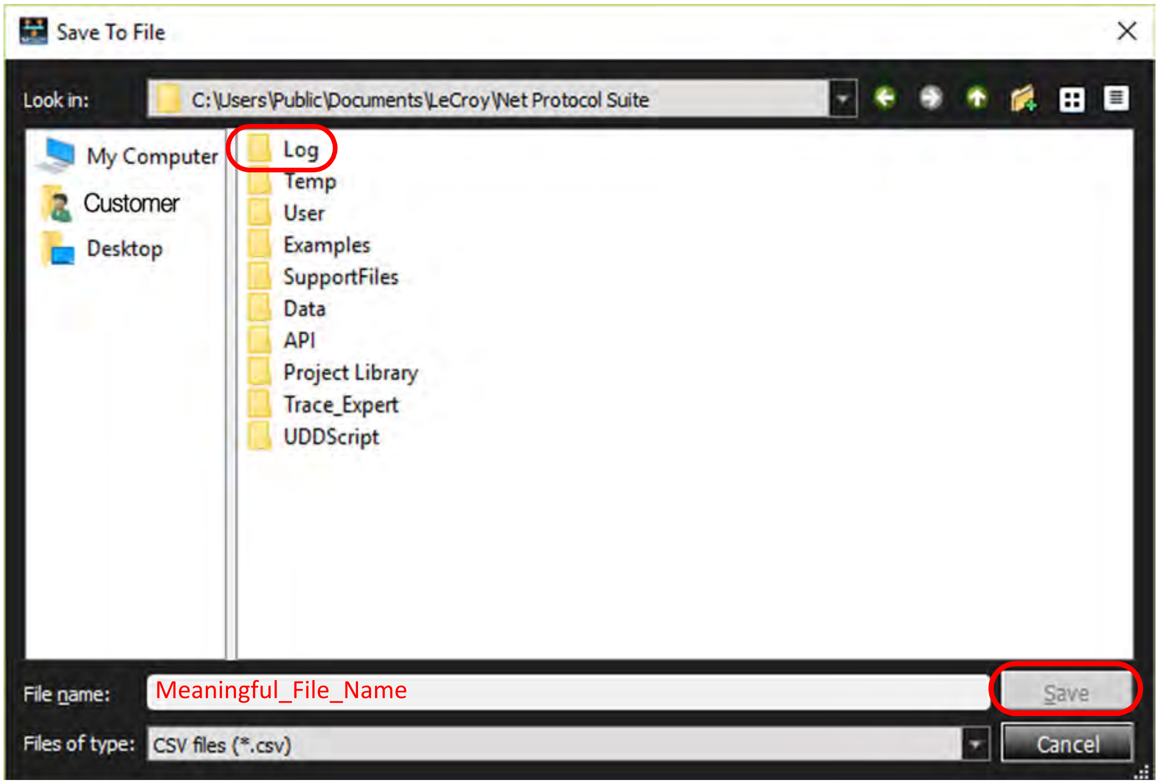


Figure 4.40: Save to File Window – Path to Log Folder

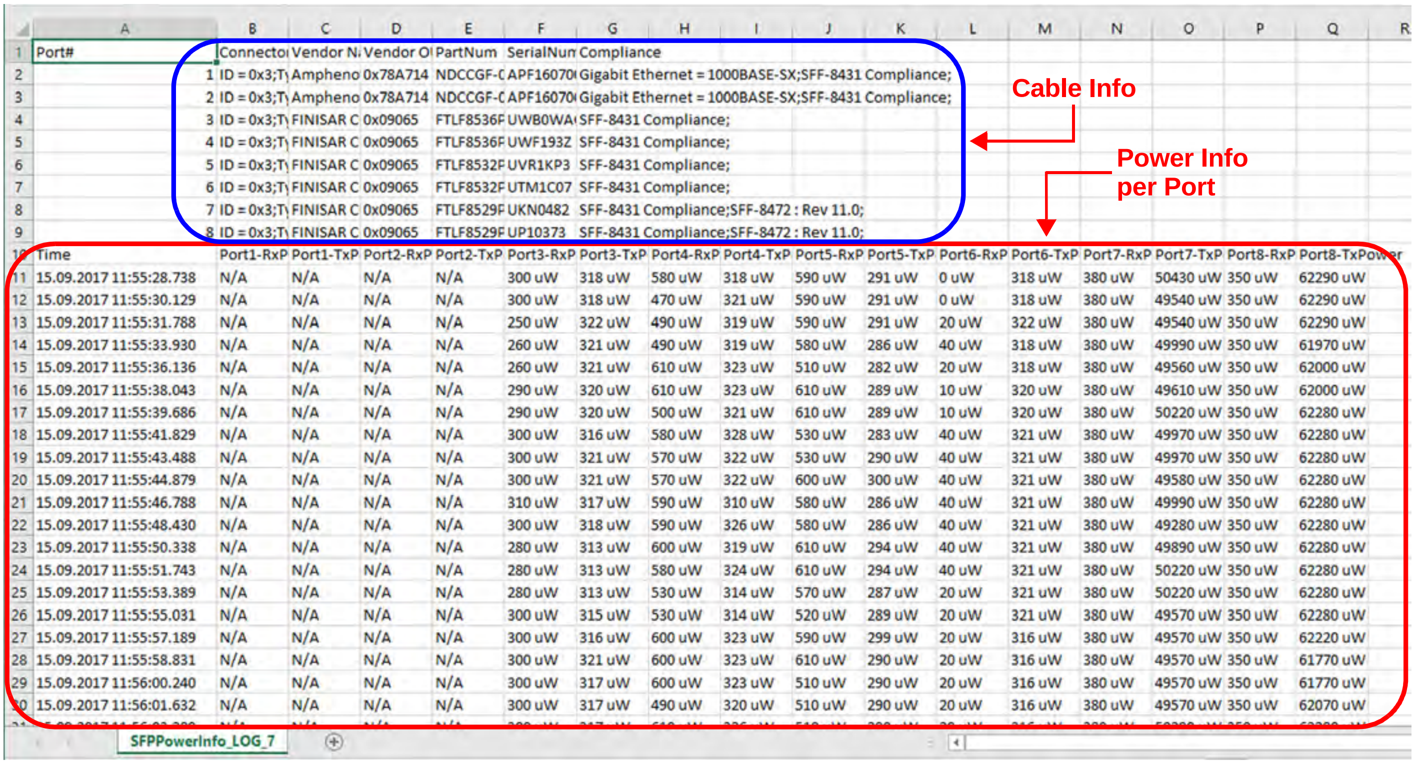
4. Enter a meaningful file name, then click **Save**.

5. Once you have created the log file, return to the original **Rx/Tx Power** window and click **Start**.

   - With the **Log Enabled**, the power readings are saved (Figure 4.41).

Figure 4.41: Saved SFP and Real Time Power Log Files

- The data is stored in comma separated value (CSV) format. An example log file is shown in Figure 4.42.

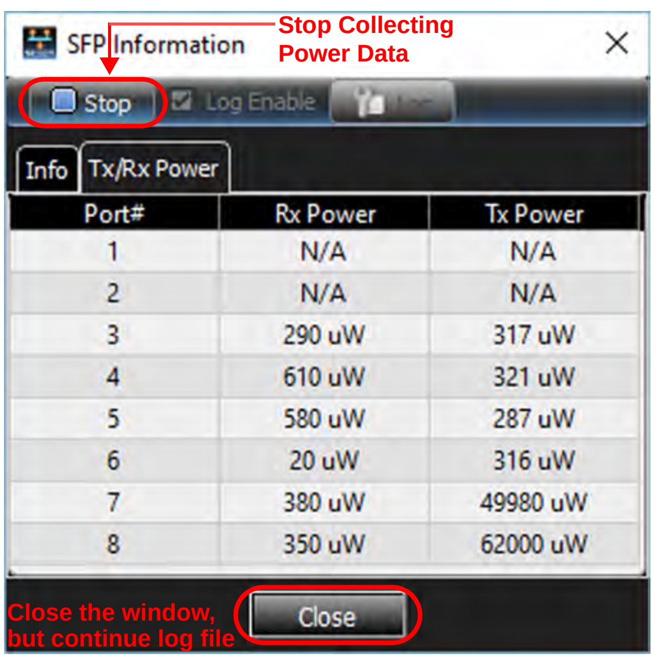


Port#	Connecto	Vendor N	Vendor O	PartNum	SerialNum	Compliance
1	ID = 0x3;T	Ampheno	0x78A714	NDCCGF-(	APF16070	Gigabit Ethernet = 1000BASE-SX;SFF-8431 Compliance;
2	ID = 0x3;T	Ampheno	0x78A714	NDCCGF-(	APF16070	Gigabit Ethernet = 1000BASE-SX;SFF-8431 Compliance;
3	ID = 0x3;T	FINISAR C	0x09065	FTLF8536F	UWB0WA	SFF-8431 Compliance;
4	ID = 0x3;T	FINISAR C	0x09065	FTLF8536F	UWF193Z	SFF-8431 Compliance;
5	ID = 0x3;T	FINISAR C	0x09065	FTLF8532F	UVR1KP3	SFF-8431 Compliance;
6	ID = 0x3;T	FINISAR C	0x09065	FTLF8532F	UTM1C07	SFF-8431 Compliance;
7	ID = 0x3;T	FINISAR C	0x09065	FTLF8529F	UKN0482	SFF-8431 Compliance;SFF-8472 : Rev 11.0;
8	ID = 0x3;T	FINISAR C	0x09065	FTLF8529F	UP10373	SFF-8431 Compliance;SFF-8472 : Rev 11.0;

Time	Port1-RxP	Port1-TxP	Port2-RxP	Port2-TxP	Port3-RxP	Port3-TxP	Port4-RxP	Port4-TxP	Port5-RxP	Port5-TxP	Port6-RxP	Port6-TxP	Port7-RxP	Port7-TxP	Port8-RxP	Port8-TxPower
15.09.2017 11:55:28.738	N/A	N/A	N/A	N/A	300 uW	318 uW	580 uW	318 uW	590 uW	291 uW	0 uW	318 uW	380 uW	50430 uW	350 uW	62290 uW
15.09.2017 11:55:30.129	N/A	N/A	N/A	N/A	300 uW	318 uW	470 uW	321 uW	590 uW	291 uW	0 uW	318 uW	380 uW	49540 uW	350 uW	62290 uW
15.09.2017 11:55:31.788	N/A	N/A	N/A	N/A	250 uW	322 uW	490 uW	319 uW	590 uW	291 uW	20 uW	322 uW	380 uW	49540 uW	350 uW	62290 uW
15.09.2017 11:55:33.930	N/A	N/A	N/A	N/A	260 uW	321 uW	490 uW	319 uW	580 uW	286 uW	40 uW	318 uW	380 uW	49990 uW	350 uW	61970 uW
15.09.2017 11:55:36.136	N/A	N/A	N/A	N/A	260 uW	321 uW	610 uW	323 uW	510 uW	282 uW	20 uW	318 uW	380 uW	49560 uW	350 uW	62000 uW
15.09.2017 11:55:38.043	N/A	N/A	N/A	N/A	290 uW	320 uW	610 uW	323 uW	610 uW	289 uW	10 uW	320 uW	380 uW	49610 uW	350 uW	62000 uW
15.09.2017 11:55:39.686	N/A	N/A	N/A	N/A	290 uW	320 uW	500 uW	321 uW	610 uW	289 uW	10 uW	320 uW	380 uW	50220 uW	350 uW	62280 uW
15.09.2017 11:55:41.829	N/A	N/A	N/A	N/A	300 uW	316 uW	580 uW	328 uW	530 uW	283 uW	40 uW	321 uW	380 uW	49970 uW	350 uW	62280 uW
15.09.2017 11:55:43.488	N/A	N/A	N/A	N/A	300 uW	321 uW	570 uW	322 uW	530 uW	290 uW	40 uW	321 uW	380 uW	49970 uW	350 uW	62280 uW
15.09.2017 11:55:44.879	N/A	N/A	N/A	N/A	300 uW	321 uW	570 uW	322 uW	600 uW	300 uW	40 uW	321 uW	380 uW	49580 uW	350 uW	62280 uW
15.09.2017 11:55:46.788	N/A	N/A	N/A	N/A	310 uW	317 uW	590 uW	310 uW	580 uW	286 uW	40 uW	321 uW	380 uW	49990 uW	350 uW	62280 uW
15.09.2017 11:55:48.430	N/A	N/A	N/A	N/A	300 uW	318 uW	590 uW	326 uW	580 uW	286 uW	40 uW	321 uW	380 uW	49280 uW	350 uW	62280 uW
15.09.2017 11:55:50.338	N/A	N/A	N/A	N/A	280 uW	313 uW	600 uW	319 uW	610 uW	294 uW	40 uW	321 uW	380 uW	49890 uW	350 uW	62280 uW
15.09.2017 11:55:51.743	N/A	N/A	N/A	N/A	280 uW	313 uW	580 uW	324 uW	610 uW	294 uW	40 uW	321 uW	380 uW	50220 uW	350 uW	62280 uW
15.09.2017 11:55:53.389	N/A	N/A	N/A	N/A	280 uW	313 uW	530 uW	314 uW	570 uW	287 uW	20 uW	321 uW	380 uW	50220 uW	350 uW	62280 uW
15.09.2017 11:55:55.031	N/A	N/A	N/A	N/A	300 uW	315 uW	530 uW	314 uW	520 uW	289 uW	20 uW	321 uW	380 uW	49570 uW	350 uW	62280 uW
15.09.2017 11:55:57.189	N/A	N/A	N/A	N/A	300 uW	316 uW	600 uW	323 uW	590 uW	299 uW	20 uW	316 uW	380 uW	49570 uW	350 uW	62220 uW
15.09.2017 11:55:58.831	N/A	N/A	N/A	N/A	300 uW	321 uW	600 uW	323 uW	610 uW	290 uW	20 uW	316 uW	380 uW	49570 uW	350 uW	61770 uW
15.09.2017 11:56:00.240	N/A	N/A	N/A	N/A	300 uW	317 uW	600 uW	323 uW	510 uW	290 uW	20 uW	316 uW	380 uW	49570 uW	350 uW	61770 uW
15.09.2017 11:56:01.632	N/A	N/A	N/A	N/A	300 uW	317 uW	490 uW	320 uW	510 uW	290 uW	20 uW	316 uW	380 uW	49570 uW	350 uW	62070 uW

Figure 4.42: Example Log File

- This example shows the time each reading was taken and the active ports, as well as the cables attached to the analyzer.
- Power readings were taken about every 1.5 seconds and will continue until you **Stop** the logging. See Figure 4.43.



Port#	Rx Power	Tx Power
1	N/A	N/A
2	N/A	N/A
3	290 uW	317 uW
4	610 uW	321 uW
5	580 uW	287 uW
6	20 uW	316 uW
7	380 uW	49980 uW
8	350 uW	62000 uW

Figure 4.43: **Tx/Rx Power** Being Logged

6. Click **Close** to close the window. The power data remains logged until you reopen the **Tx/Rx Power** and click the **Stop** button.

4.1.3.4 I2C Write/Read Registers

This feature allows you to manually Add, Edit, and Delete I2C Registers. When new I2C settings get programmed manually for specific modules (whether Optic or DAC), the software logs these and automatically programs them the next time the same module (i.e., same part number) is detected, so that the link comes up automatically.

To create a new I2C Register, do the following:

1. From the main screen, right-click on the Port Status area , then select **SFP Information** from the drop-down menu. The SFP Information window appears (Figure 4.44).

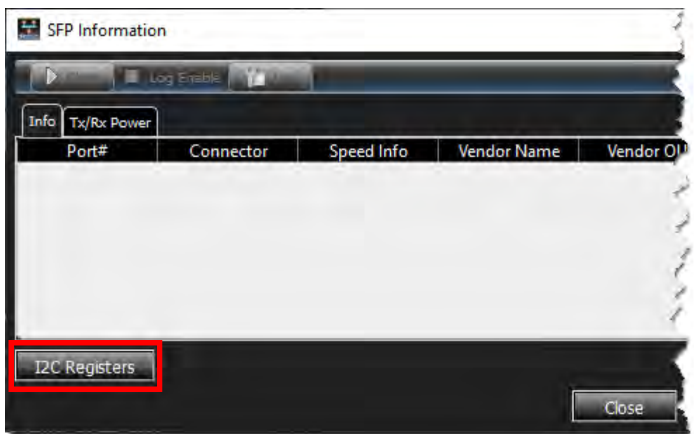


Figure 4.44: SFP Information Window

2. Click the **I2C** button at the bottom left corner of the SFP Information window. The Transceiver Modules I2C Write/Read dialog window appears (Figure 4.45).

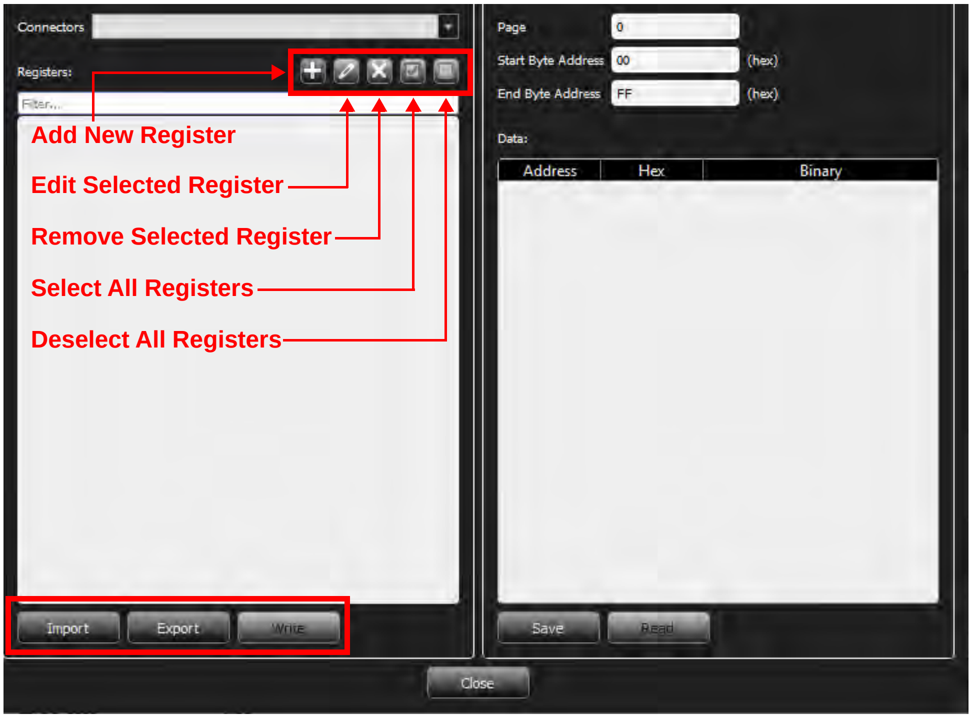


Figure 4.45: Transceiver Modules I2C Write/Read Dialog Window

3. Click **Add** . The Add New Register dialog box appears (Figure 4.46).

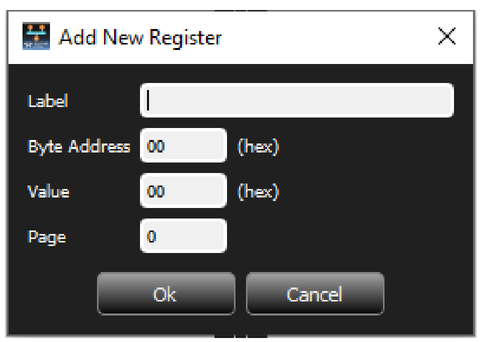


Figure 4.46: Add New Register Dialog Box

4. Enter a **Label**, **Byte Address**, **Value**, and **Page** for the New Register.
5. Repeat steps 1 through 4 as needed.
6. When you are satisfied with your entries, click **OK**.

   You can click **Cancel** at any time to close the New Register dialog box and return to the Write/Read dialog window.

NOTE: When different modules are used, the unit must be deactivated and reactivated so that the changes will be detected and the proper settings applied.

---

7. If you need to delete a Register, highlight it and click the **Delete** button.

8. To modify a Register, do the following:
   a. Highlight the Register you need to modify and click the **Edit Selected Register** button.
   b. Make the necessary corrections in the Edit Register dialog box and click **OK**.
9. To Export a Register, do the following:
   a. Highlight a Register and click **Export**. The Export Connector Registers window appears (Figure 4.47).

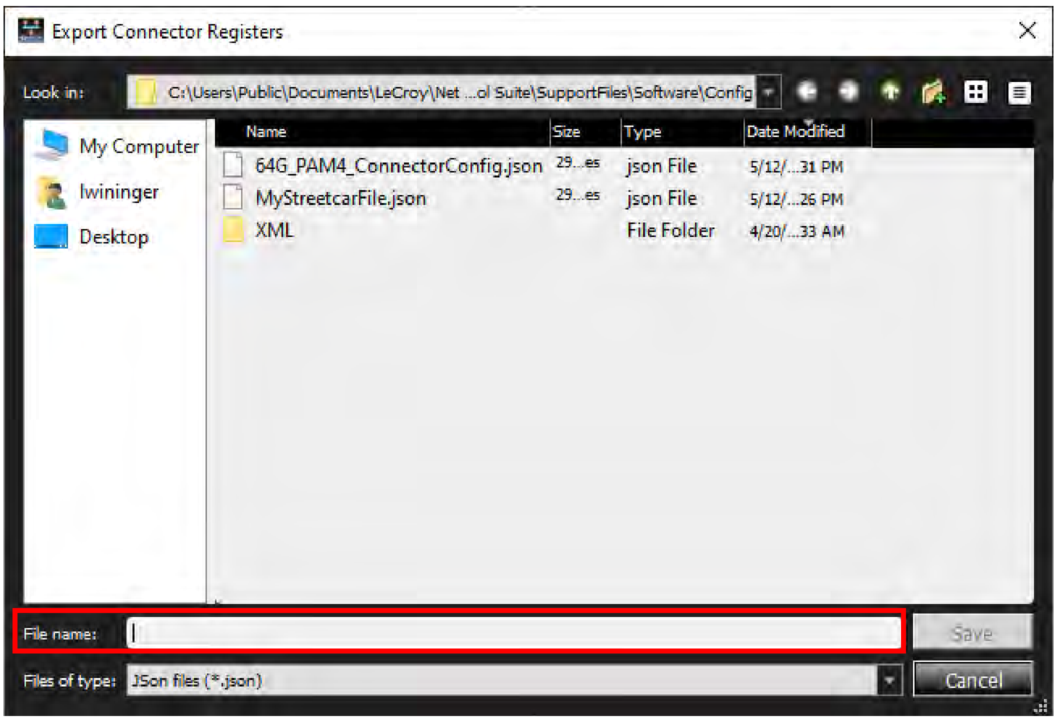


Figure 4.47: Export Connector Registers Window

   b. Enter a path and file name in the **File name** field, then click **Save**. The register is saved as a JSON file.
   c. To overwrite an existing file, highlight it and click **Save**. A confirmation prompt appears (Figure 4.48). If you are sure you wish to overwrite the file, click **Yes**.

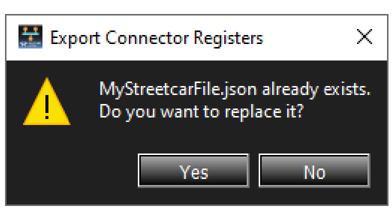


Figure 4.48: Overwrite File Confirmation

Write a Register to the Transceiver Modules

To Write to the Transceiver Modules, click the **Write** button at the bottom of the left pane.

NOTE: *Write* writes the values, one by one, for checked Registers.

Read any Register or range from the Transceiver Modules

To Read any Register or range:

1. From the Transceiver Modules in the right pane, enter the **Page**, **Start Byte Address**, and **End Byte Address**.
2. Click the **Read** button at the bottom of the right pane.

NOTE: You can also click **Save** to save the read results to a file.

4.1.4 Session Control Pane

Use the Session Control pane to start and stop a recording. There is also a session status pane that shows the current status of the session. See Figure 4.49.

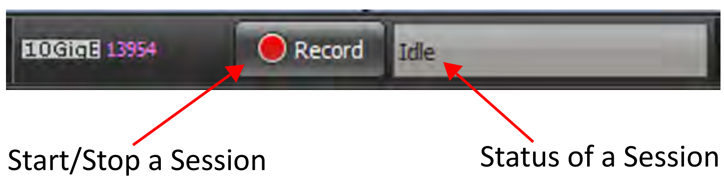


Figure 4.49: Session Control Pane

Snapshot mode is the default mode of operation of the analyzer see 4.1.6.1, *Snapshot Mode*, but Event Trigger mode allows the user to set an Event Trigger and allows control over the timing of the recording of data. See 4.1.6.2, *Event Trigger Mode*.

4.1.4.1 Snapshot Mode Recording Overview

When "Idle" is displayed in the Session Status Pane (SSP), this means the analyzer is idle and not recording or saving data (Figure 4.50). The analyzer is waiting to start recording.

Figure 4.50: Session Status Pane Before Recording Starts

- ❑ Click the **Record** button.
  - ■ You may receive a pop-up Warning message depending on the state of the analyzer.

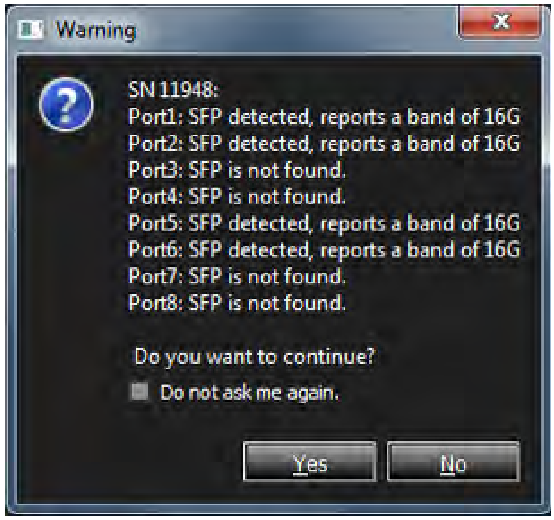


Figure 4.51: Warning Message

- Click **Yes** to Start Recording a Trace.

❑ Wait for the buffer to fill with raw data (Recording)

In the default Snapshot mode, when the Record button is clicked, the analyzer is automatically triggered, the “Record” button turns into a “Stop” button and the status is “Recording” (the analyzer is storing the data in a local buffer). See Figure 4.52.

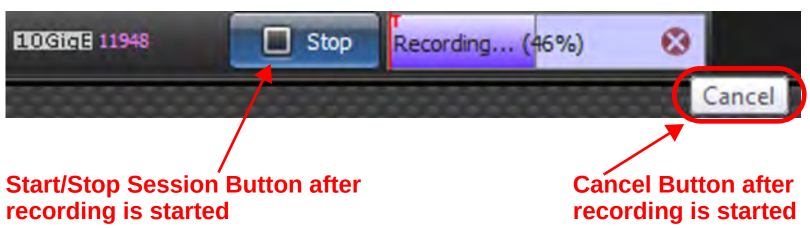


Figure 4.52: Analyzer Recording Data

NOTE: The Cancel button terminates Recording and no Trace data is stored.

If the **Stop** button is clicked, the analyzer will stop recording data and move automatically to the next step in the sequence (Indexing). See Figure 4.53.

❑ When the buffer is full, the analyzer processes the data (Indexing).

Recording continues within the limits set by the buffer size. When the buffer is full, recording stops and the analyzer starts turning the raw data into a meaningful database. See Figure 4.53.

When “Indexing” is displayed, it means the application is creating an index of the captured Trace data while it still resides in the recording memory buffer. This functionality is a necessary preparation stage for opening the Trace in Quick View mode.

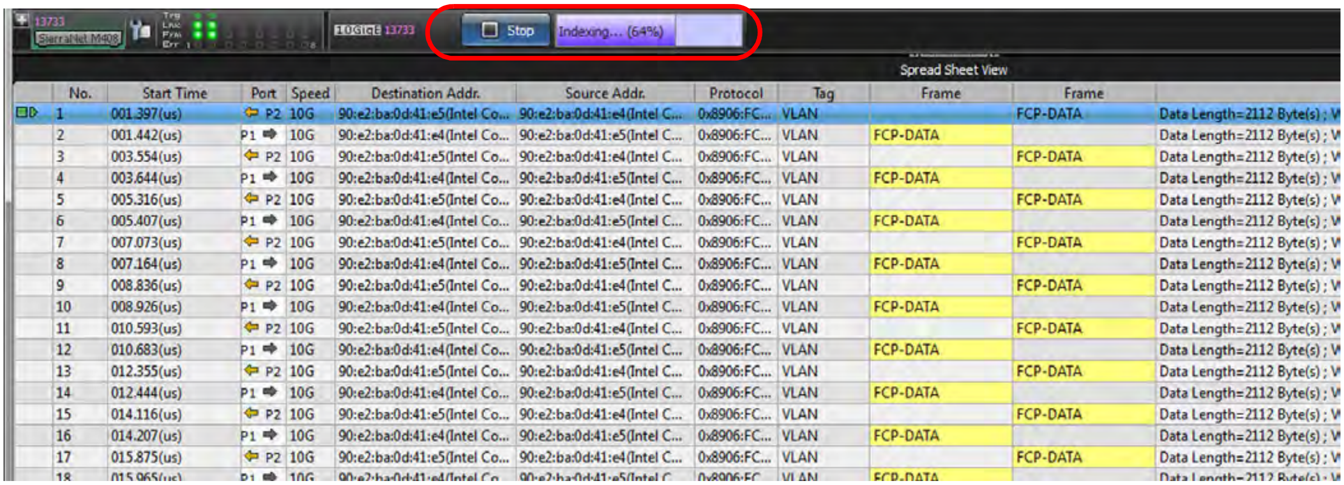


Figure 4.53: SSP While Host is Indexing Recorded Data from the Analyzer’s Memory

- After the data is Indexed, the Record button turns on, but the Session Status Panel says Trace is not Saved (Figure 4.54). When “Trace is Not Saved” is displayed, this means that the trace is opened for viewing in Quick View mode, but it has not been saved to disk.

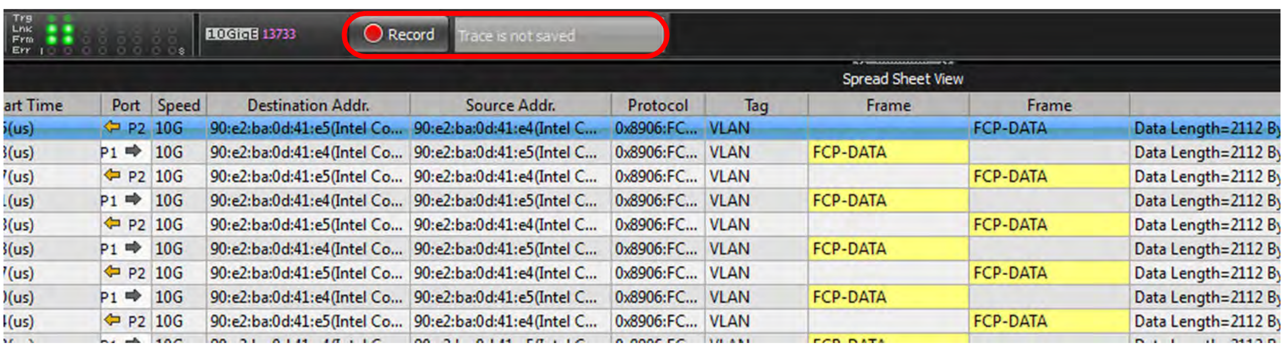


Figure 4.54: SSP Trace Data has not been Saved to Host Memory

- You can choose to store the processed data for later use (Save Trace As), or to discard the trace by starting a new recording.

To save the trace:

1. Select **File** → **Save Trace As**. See Figure 4.55.

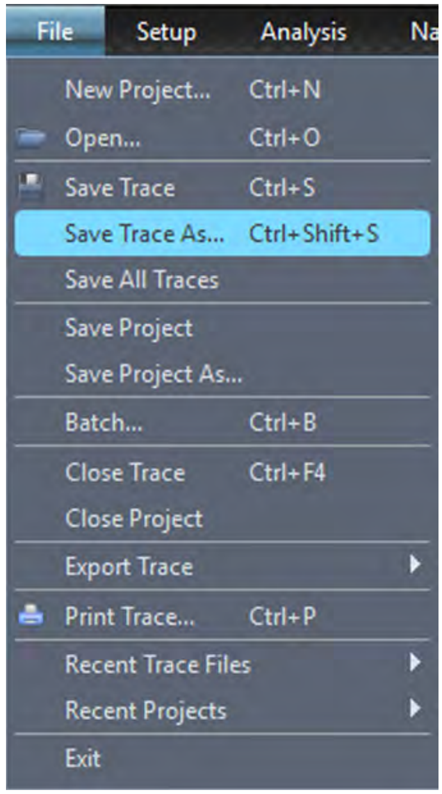


Figure 4.55: Save Trace As

2. Click **Save Trace As**.

- A window appears showing a path to the location of the Saved Trace (Figure 4.56). There is a default label for the Trace, but you can change it if needed.

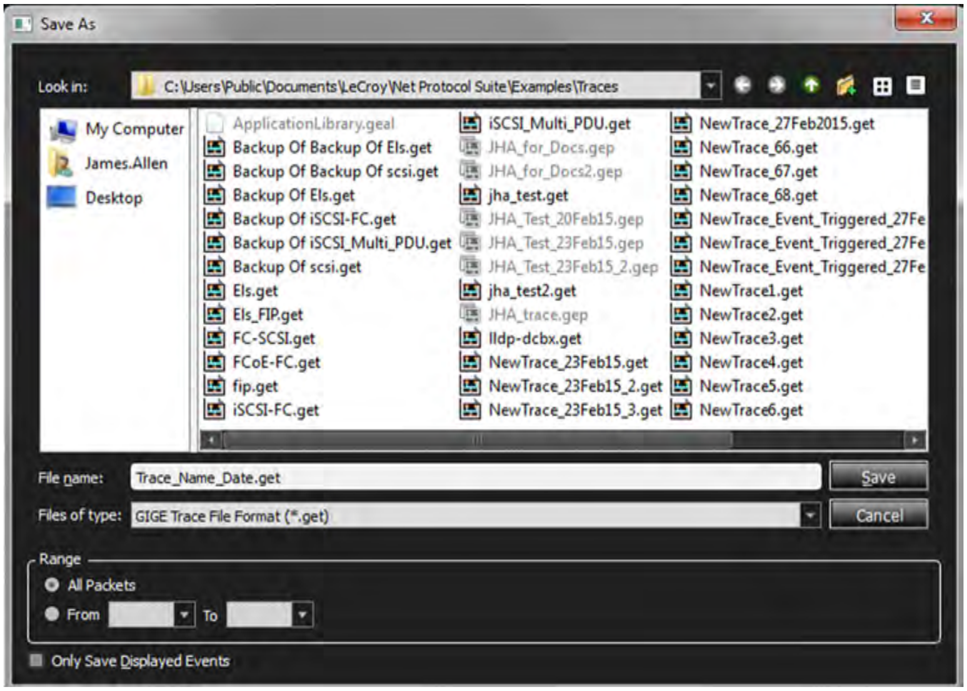


Figure 4.56: Saving a Trace File on Host Computer

- The analyzer saves Trace data to the Host Computer (Figure 4.57). When "Saving" is displayed, this means the Trace has been captured and is being saved from the analyzer recording memory buffer to a file on the host PC.

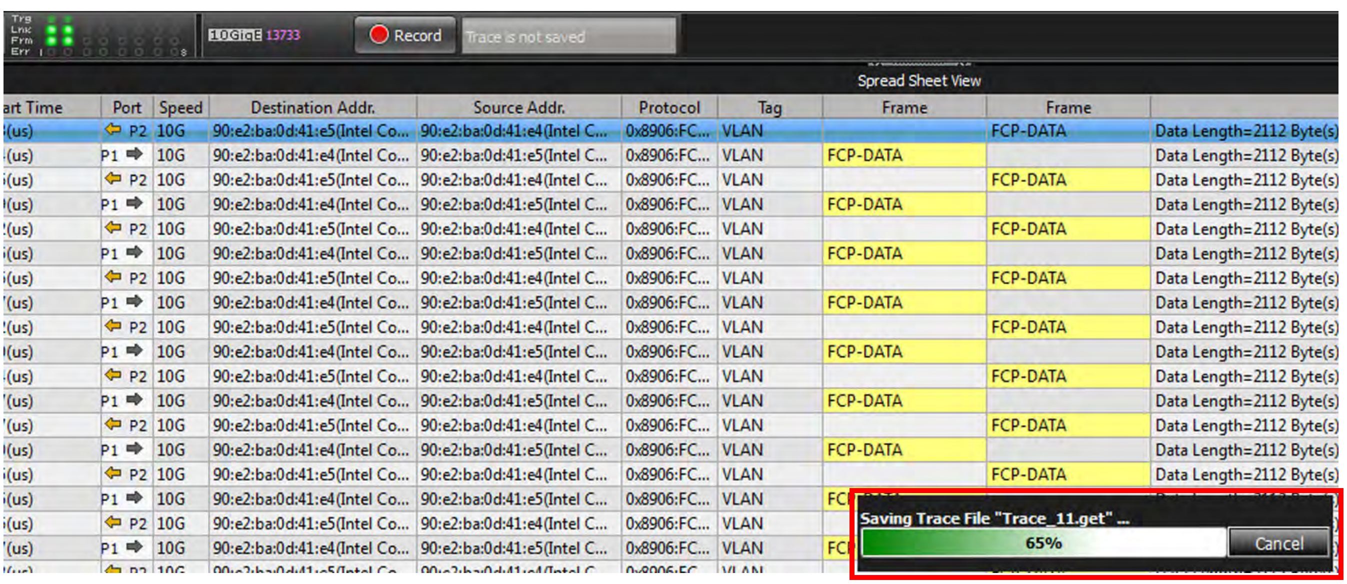


Figure 4.57: Analyzer Saving Data Trace to Host Computer

- Once the Trace is Saved, you can start the process over again. See Figure 4.58.

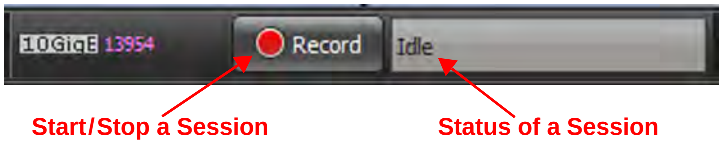


Figure 4.58: Session Control Pane

4.1.4.2 Event Trigger Mode Recording Overview

The sequence for Event Trigger Mode is:

- Define an Event Trigger (define an Event and define where in the buffer memory it will occur).

  Recording continues in a circular manner within the limits set by the buffer size until an Event Trigger is detected that meets the Trigger conditions specified in the Triggering Options and the defined amount of data has been recorded after the Event Trigger.

- The analyzer is waiting to start recording (Idle). See Figure 4.59.

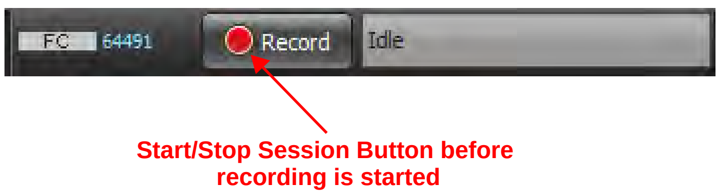


Figure 4.59: Session Status Pane Before Recording Starts

- Click the Record button.
- Wait for the Event Trigger to occur. While it is waiting for the Event Trigger, the analyzer is recording raw data and the Status Pane displays “Waiting for Trigger”. See Figure 4.60.

NOTE:
- If the “Stop” button is clicked, the analyzer will ignore the Event Trigger, stop recording data and move automatically to the next step in the sequence (Indexing). See Figure 4.44: .
- If the “Cancel” button is clicked, the analyzer will terminate the recording and no data will be stored.

Figure 4.60: SSP While Analyzer is Waiting for Trigger

- The Event Trigger occurs.

  Trigger LEDS are turned on and the analyzer records data after the trigger. The analyzer continues recording raw data until the buffer is full (Recording). see Figure 4.61.

Figure 4.61: SSP While Analyzer is Recording Data After an Event Trigger

- When the buffer is full the analyzer will process the data (Indexing). See Figure 4.62. When “Indexing” is displayed, this means the application is creating an index of the captured trace data while it still resides in the analyzer’s recording memory buffer. This functionality is a necessary preparation stage for opening the trace in Quick View mode.

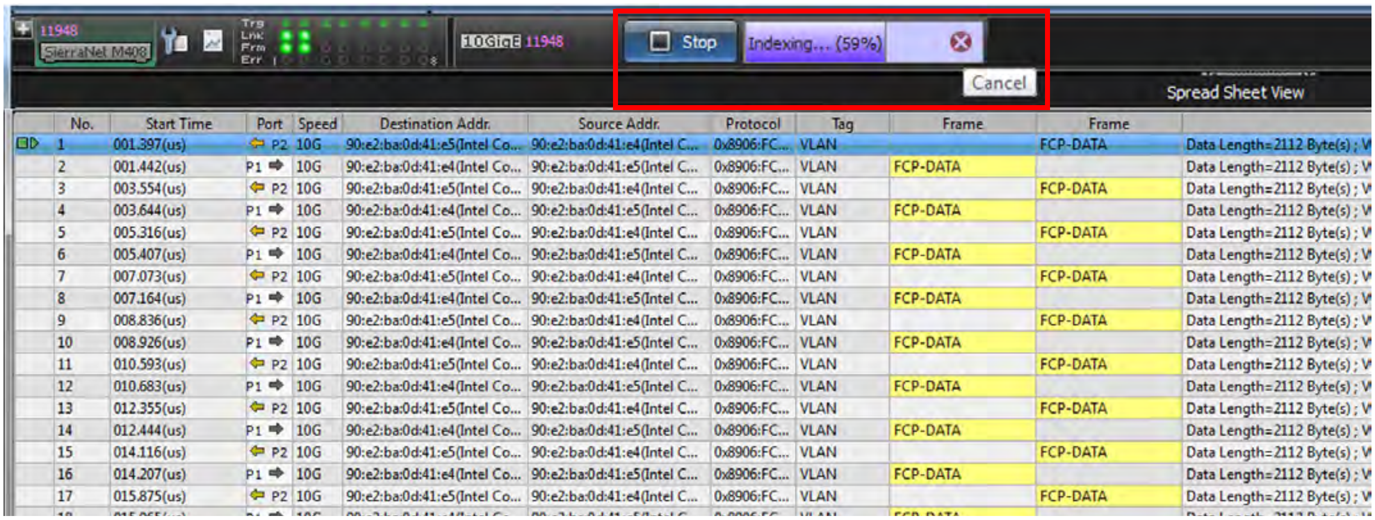


Figure 4.62: SSP While Host is Indexing Recorded Data from Analyzer Memory

- After the data is Indexed, the Record button turns back on, but the Session Status Panel shows “Trace is not Saved”. See Figure 4.63. “Trace is Not Saved” means that the trace is opened for viewing in Quick View mode, but it has not been saved to disk.

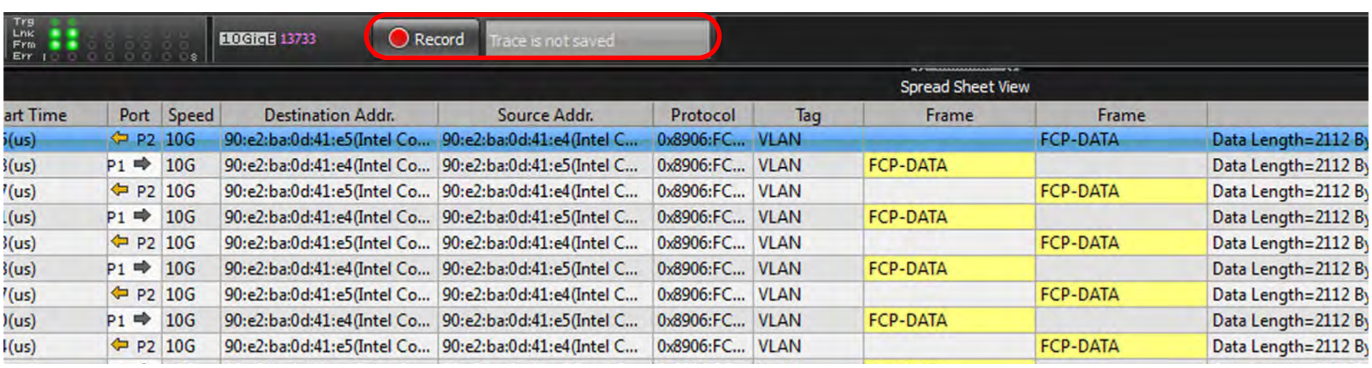


Figure 4.63: SSP Trace Data has not been Saved to Host Memory

- You can choose to store the processed data for later use (Save Trace As), or discard the Trace by starting a new recording.

4.1.4.3 Recording Status as Buffer Fills

You can see the buffer being filled in the following set of sequential images (see Figure 4.64 through Figure 4.67:

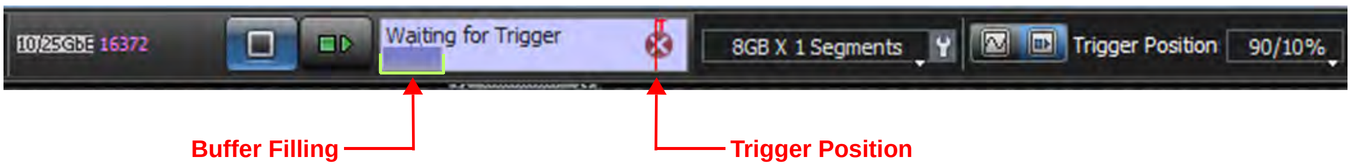


Figure 4.64: Buffer Filled Up About 25% of Triggering Position

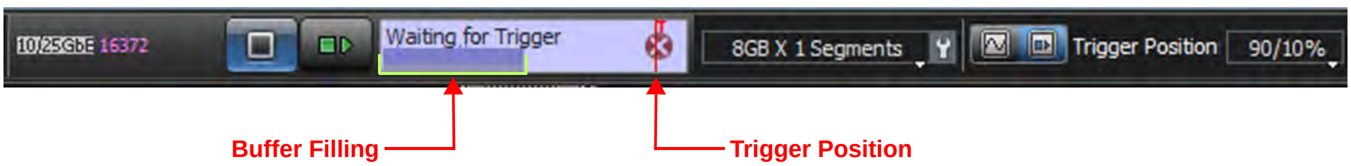


Figure 4.65: Buffer Filled Up About 50% of Triggering Position

Figure 4.66: Buffer Filled Up About 75% of Triggering Position

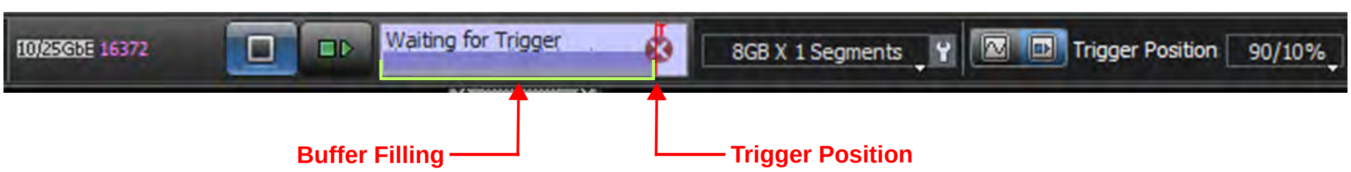


Figure 4.67: Buffer Filled Up About 100% of Triggering Position

4.1.4.4 Save Trace As

1. To save the Trace, click **File** → **Save Trace As**. See Figure 4.68.

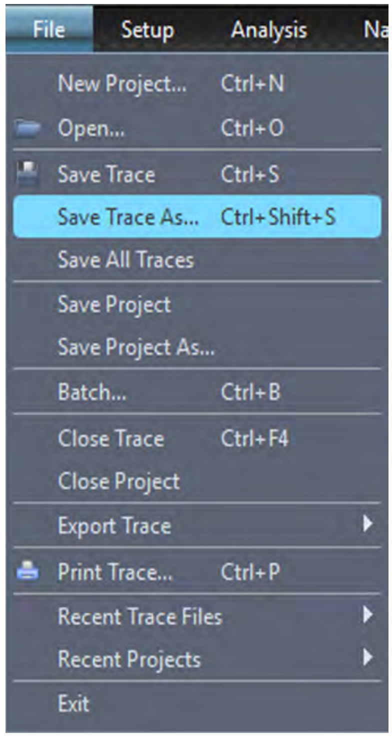


Figure 4.68: Save Trace As

A window appears showing a path to the location of the Saved Trace (Figure 4.69). There is a default label for the Trace, but you have the option to change it.

2. If needed, enter an appropriate path.
3. When you are finished, click **Save**.

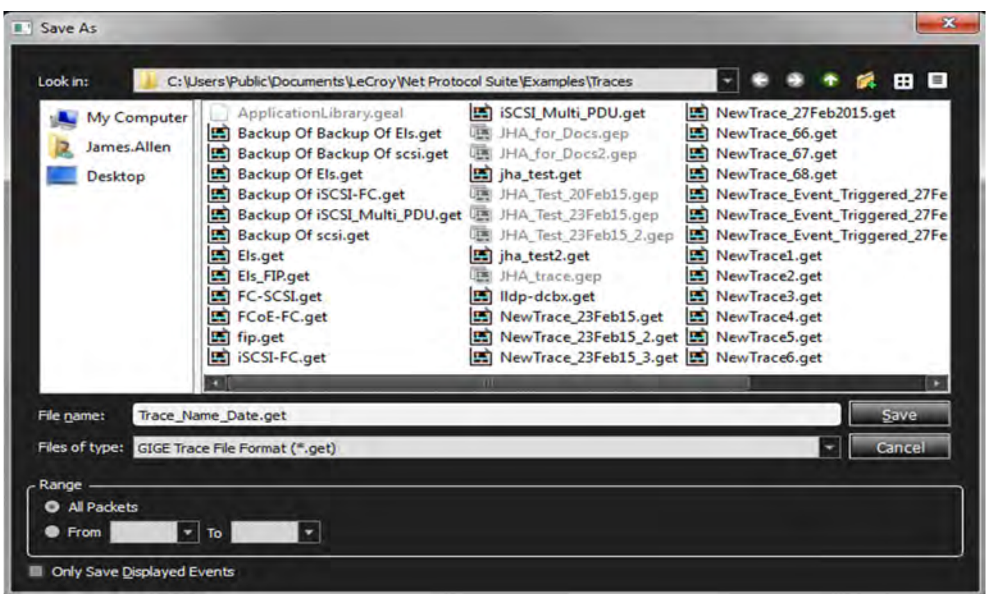


Figure 4.69: Saving a Trace File on Host Computer

- The analyzer saves Trace data to the Host Computer. See Figure 4.70.
- “Saving” means the Trace has been captured and is being saved from the Analyzer recording memory buffer to a file on the host PC.

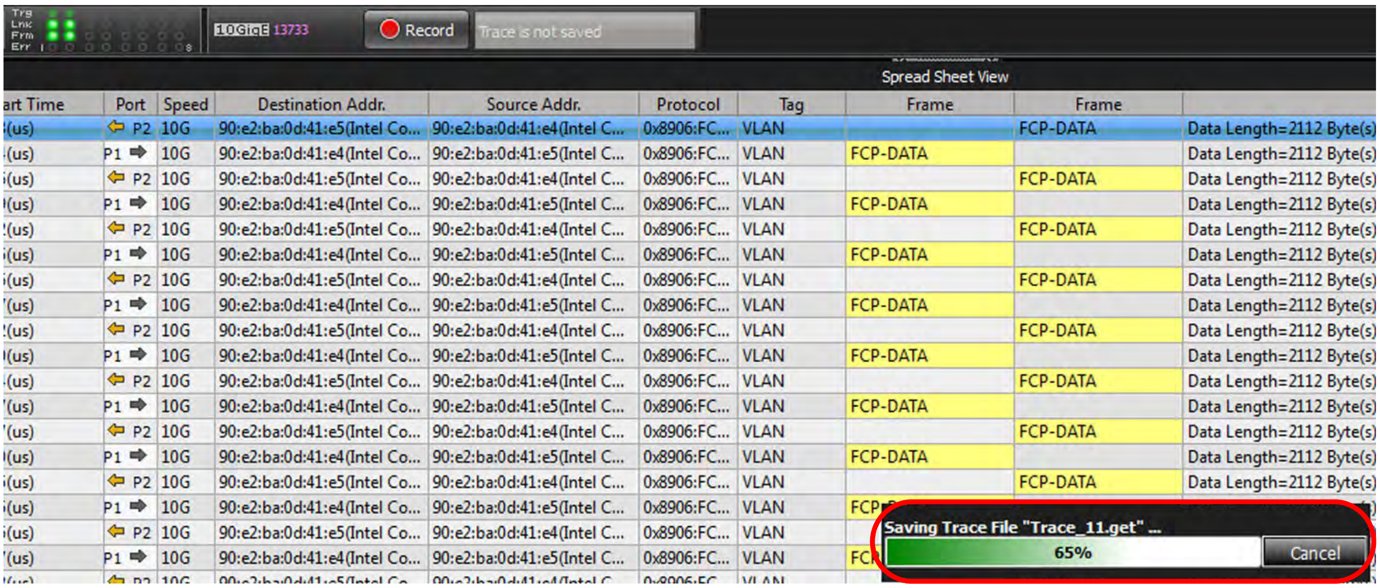


Figure 4.70: SSP While Analyzer is Saving Data from a Trace to a File in Host Memory

- You can then start the process over again. See Figure 4.71.

Figure 4.71: Session Control Pane

4.1.4.5 Event Trigger Recording Progress

A red vertical line illustrates the location of the Trigger Position you have selected in Trigger and Filter Settings.

- ❑ Pre-Trigger progress is indicated by **Waiting for Trigger** in the field to the left of the Trigger Position.

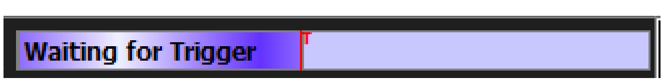


Figure 4.72: Pre-Trigger

- ❑ After the trigger occurs **Recording** is displayed in the field to the left of the Trigger Position indicating the progress of the recording.

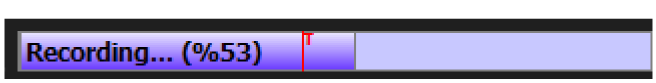


Figure 4.73: Post-Trigger.

- ❑ To save the file for later use, select **File** → **Save**

4.1.4.6 Interrupting the Recording Process (Unplugging Cables)

When a captured trace is not saved and the USB cable is removed, the software displays an error message that unsaved traces will be closed. If you ignore the message and again plug in and unplug the USB cable, the software might get into an unstable state.

When the Ethernet cable is removed, the application detects the event after a delay of approximately 2.5 to 3 minutes. During this delay the device status remains ready and an attempt to capture a trace might result in error messages such as: “PCI configuration failed”, or “HAL error”. If this occurs, you need to power cycle the analyzer to allow detecting the device in the device list and continue capturing.

4.1.5 Recording Settings Pane

Use the Recording Settings (Figure 4.74) pane to select and set the number and size of segments and save a new trace file. (See 4.1.6.3, *Buffer Size and Segments*.)

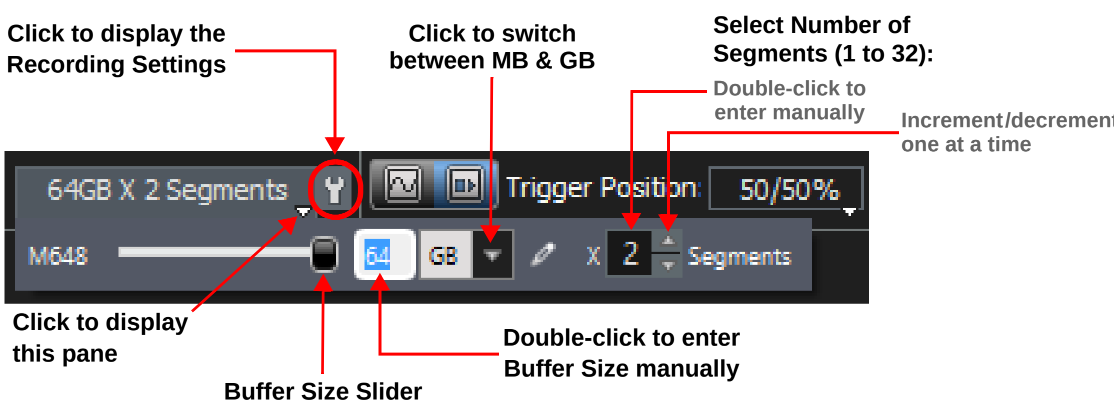


Figure 4.74: Recording Settings Pane

NOTE: Because each analyzer has different capabilities and depending on which analyzer you are using, Recording Settings will have different options.

NOTE: In the M168/M408 the memory buffer is shared between Host and Device ports, while in the M328 Host and Device ports are using only half of the buffer. In the M328 half of the memory buffer is shared between the Host side of all ports and the other half of the memory buffer is shared between the Device side of all ports.

In the case where both the Host and Device ports have similar traffic, the memory buffer would be filled (~24 MB); however, in an unbalanced case the captured trace size would be different between the M168/M408 and the M328.

For Example, if one side is sending only Idles (Fill words) and the other side has Frames:

- In the M168/M408, since the memory buffer is shared between the Host and Device of the same port, the Analyzer would capture almost the full 24MB buffer size.
- In the M328, one side would capture 12 MB (Frames) and the other side would capture packed Idles that use less buffer space and may have <1MB in size.

In this unbalanced case, the M328 would capture less than 13 MB of traffic.

4.1.5.1 M1288 – Recording Settings

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window.

Figure 4.75: M1288 Recording Settings

Table 4.4: Recording Settings Window

Condition	Setting	Description
Trace Path	Trace File	Location of Saved Trace. Click the **...** to rename and/or change file location. You can save the trace data in two different modes: Indexed and Decoded, or Raw (check the Only Save Data box for Raw). Indexed and Decoded: Trace data saved as a .get file with Indexing and Decoding. See Figure 4.75.
Only Save Data (Raw file format)	Checked/ Unchecked	Raw: Trace data saved as a .geraw file without Indexing and Decoding. Saving a trace as Raw data will speed up saving the trace to host memory. The Raw data file can be indexed and decoded at a later date to view the Trace file. The option, Only save data (Raw file format), is available for all Sierra Net products (M1288, M648, M408, M168, T328 and M328). See Figure .
Number of Segment	1-32	Select the segment number.
Set as Default		Save the Recording Settings you selected as the default.
Restore Factory Settings		To revert to Factory Settings, select Restore Factory Settings.
Setting Tab		
Speed	Speed of DUT	For the selected ports in use, choose the DUT speed.
Training Signal Pack Mode	Unpacked, Packed	Setting the Training Signal Pack Mode to Unpacked enables the selected Lanes to record all Training Sequence details, including PRBS. This could require much more buffer space, so should only be used when needed (the default is Packed).
Precoding	Disable, Enable, Auto	Precoding tells the analyzer how to decode the traffic. For Digitally Retimed ports (DRT, Ports P1 and P2), the Precoding setting also affects the traffic on the M1288's Tx, going to the DUT. When Precoding is set to **Off**, the trace only shows PCS data, if the traffic is NOT precoded. When Precoding is set to **On**, the trace only shows PCS data, if the traffic is precoded. **NOTE:** On DRT ports, the analyzer will send the traffic out as precoded, even if the received traffic was not precoded (APT traffic through the probe will not be affected).
Lane Number	Lane number(s)	Select which lane(s) to unpack. **NOTE:** In some port configurations, not all lanes Training Signals can be Unpacked.
PE Detection Tab		

Table 4.4: Recording Settings Window

Condition	Setting	Description
Protocol Errors	Checked/ Unchecked	See Figure 4.77 for all the Protocol Errors available.
Check All	Checked/ Unchecked	Check this box to select all Protocol Errors.

Figure 4.76: M1288 Recording Settings: Raw File Format

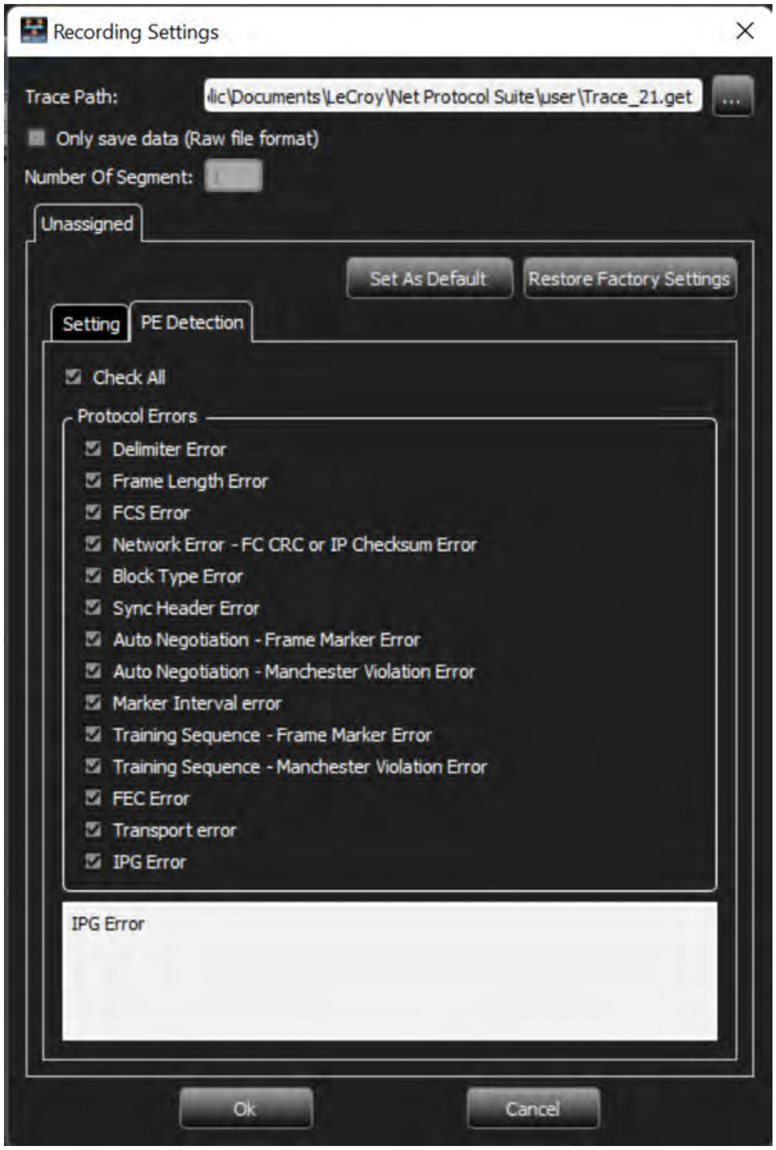


Figure 4.77: M1288 Recording Settings: PE Detection Tab

4.1.5.2 M408 – 10GbE Recording Settings

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window. You can save the trace data in two different modes:

- Indexed and Decoded (trace data saved as **.get** file with Indexing and Decoding) see Figure 4.78.
- Raw (trace data saved as **.geraw** file without Indexing and Decoding) (Figure 4.79). Saving trace as RAW data will speed up saving the trace to host memory. The RAW data file can be indexed and decoded at a later date to view the Trace file.

The option, **Only save data (Raw file format)**, is available in all Sierra Net products (M408, M168, T328 and M328).

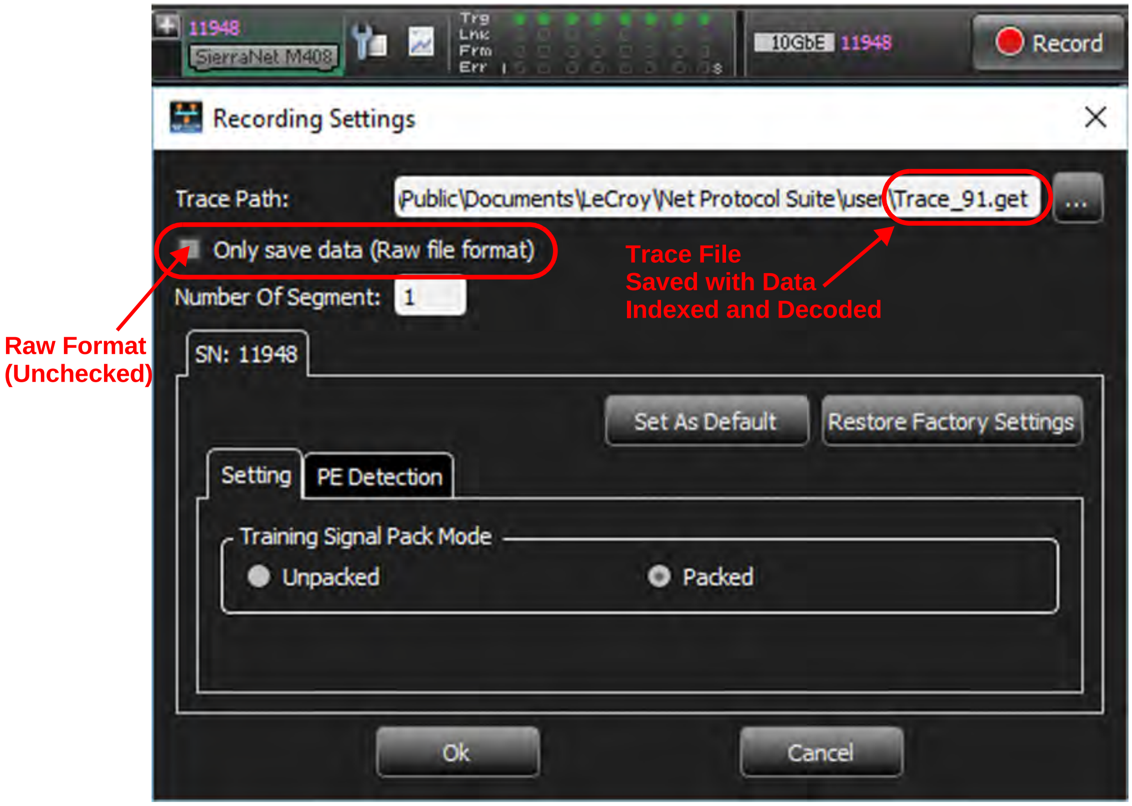


Figure 4.78: Recording Settings Window – M408 10GbE

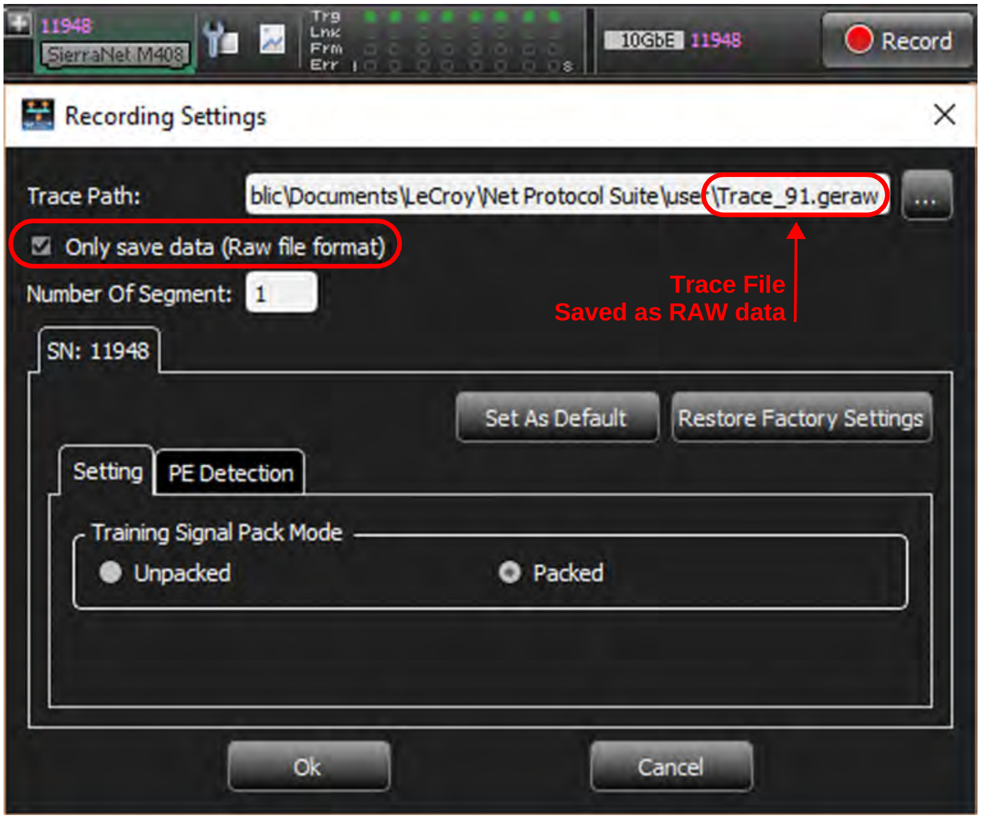


Figure 4.79: Recording Settings Window – M408 10GbE

The Recording Settings window allows you to select conditions on which the analyzer will trigger, including:

- **Trace Path**: Location of Saved Trace
- **Number of Segments**: 1 – 32
- **Setting**: Training Signal Pack Mode, Unpacked or Packed
- **PE Detection**: See Figure .
- **Set As Default**: You can save the Recording Settings you selected as the default.
- **Restore Factory Settings**: If you want to revert to Factory Settings, select **Restore Factory Settings**.

Protocol Error (PE) Detection Tab: M408 → 10GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. You can save the trace in two different formats (see Figure 4.80):

- **Indexed and Decoded** (trace data saved as **.get** file with Indexing and Decoding).
- **Raw file format** (trace data saved as **.geraw** file without Indexing and Decoding). Saving trace as RAW data will speed up saving the trace to host memory. The RAW data file can be indexed and decoded at a later date to view the Trace file.
- **Set As Default**: You can save the Recording Settings you selected as the default.

- **Restore Factory Settings**: If you want to revert to the Factory Settings, select **Restore Factory Settings**.

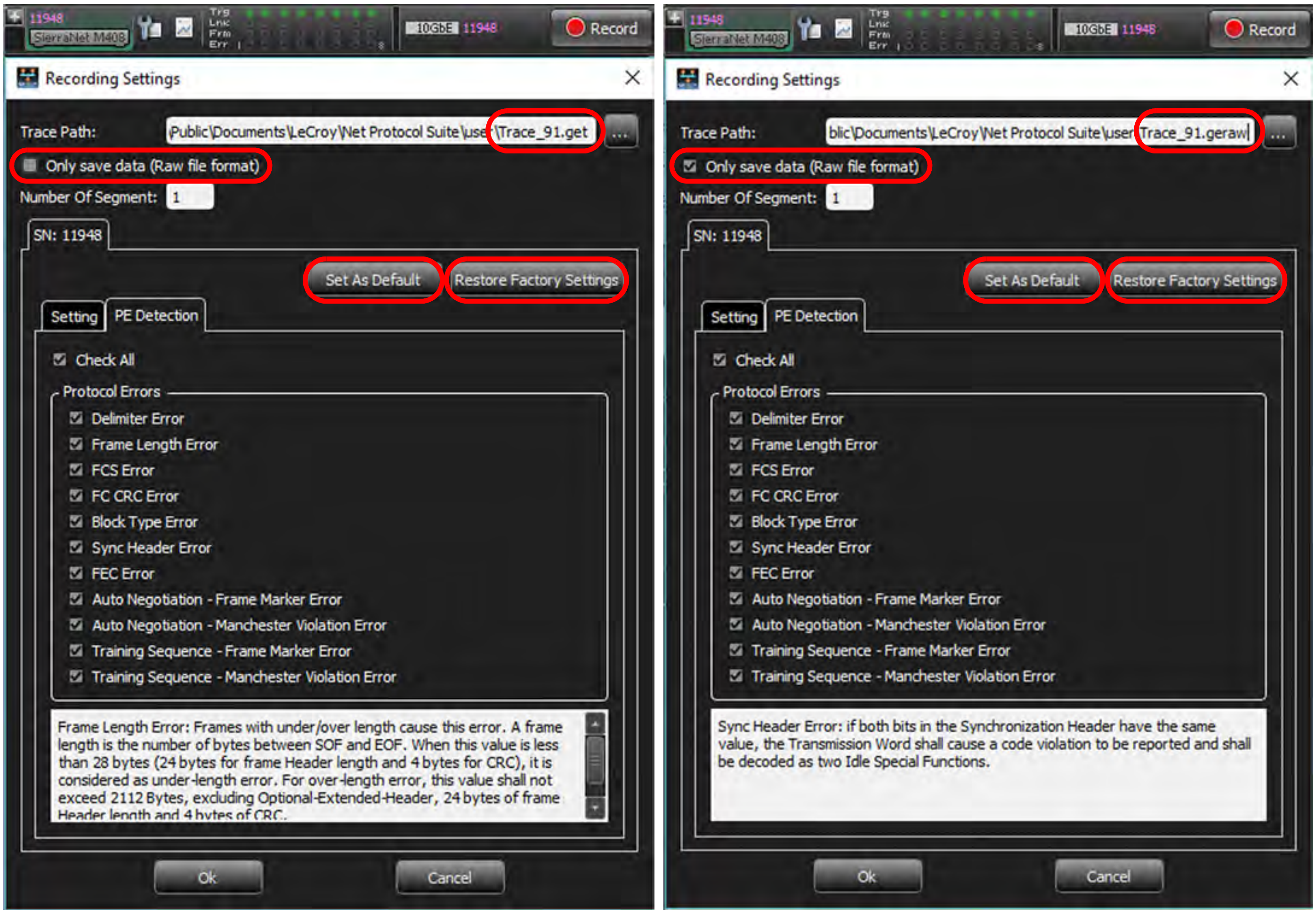


Figure 4.80: PE Detection Tab for M408

4.1.5.3 Recording Settings – M408 40GbE

Click the Recording Settings icon  to display the Recording Settings/PE Detection window.

You can save the trace in two different formats (Figure 4.81):

- Indexed and Decoded, generating a **.get** file
- Raw file format, generating a **.geraw** file

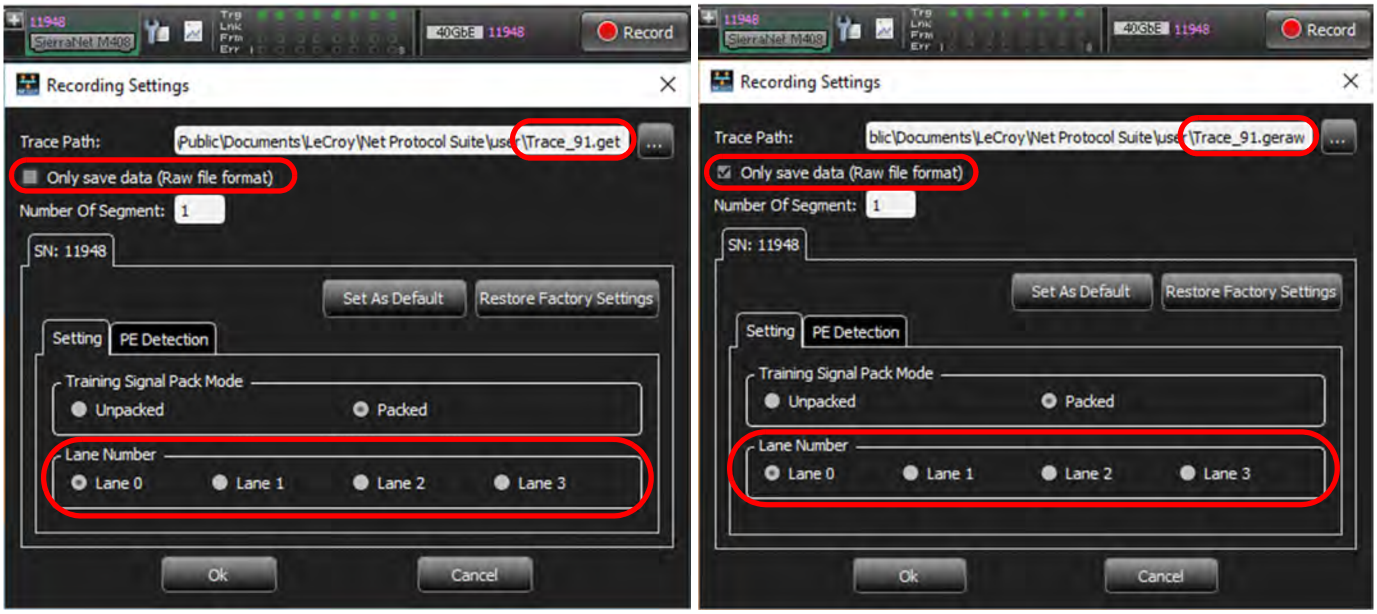


Figure 4.81: Recording Settings

Recording Settings enables you to select the conditions on which the analyzer will trigger, including:

- **Trace Path**: Location of Saved Trace
- **Number of Segments**: 1 – 32
- **Setting**
  - Training Signal Pack Mode: Unpacked or Packed
  - Lane Number: 0 – 3
- **PE Detection**: See below
- **Set As Default**: You can save the Recording Settings you've set as the default.
- **Restore Factory Settings**: If you want to revert to the Factory Settings you can select the **Restore Factory Settings** button.

PE Detection Tab – M408 40GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **M408 40GbE** options are similar to the **M408 10GbE** options (Figure 4.80).

4.1.5.4 Recording Settings – M408 FC

Click the Recording Settings icon  to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (Figure 4.82):

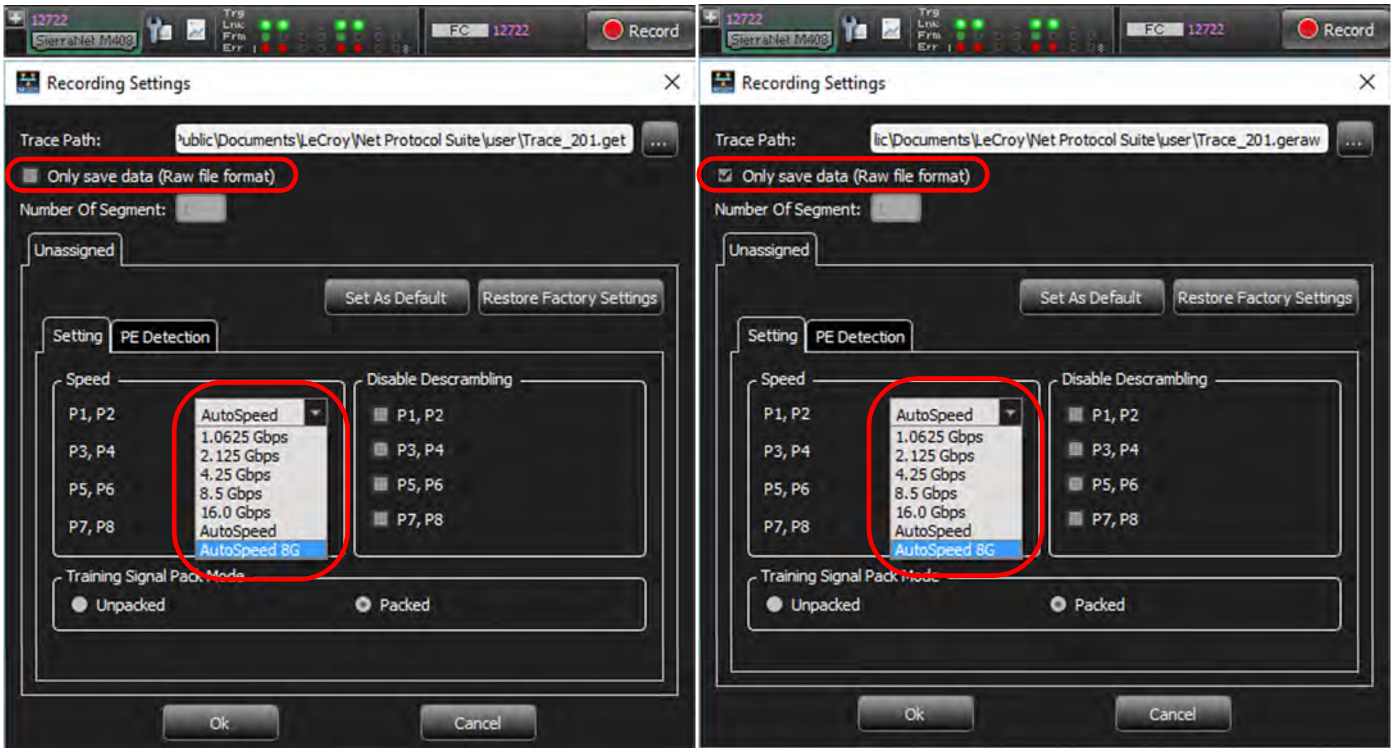


Figure 4.82: Recording Settings Window – M408 FC

Recording Settings enables you to select conditions on which the analyzer trigger, including:

- **Trace Path**: Location of Saved Trace
- **Number of Segments**: 1 – 32
- **Setting**
  - **Speed**: Port Pairs: P1, P2; P3, P4; P5, P6; P7,P8 → 1.0625 Gbps, 2.125 Gbps, 4.25 Gbps, 8.5 Gbps, 16.0 Gbps, AutoSpeed or AutoSpeed 8G
  - **Disable Descrambling**: By Port Pair → P1, P2; P3, P4; P5, P6; P7,P8
  - **Training Signal Pack Mode**: Unpacked or Packed
- **PE Detection**: See *PE Detection Tab – M168 – FC*.
- **Set As Default**: You can save the Recording Settings you've set as the default.
- **Restore Factory Settings**: If you want to revert to Factory Settings, select **Restore Factory Settings**.

PE Detection Tab: M408 – FC

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored.

1. Select one or more protocol errors or click in the **Check All** box to select all.
2. Enter the Number of Segments in the field. The **M408 FC** options are similar to the **M408 10GbE** options (Figure 4.80).

4.1.5.5 Recording Settings: M168 – 10GbE

1. Click the Recording Settings icon to display the Recording Settings/PE Detection window.
2. You can save the trace in two different formats:
   - Indexed and Decoded, which generates a **.get** file
   - Raw file format, which generates a **.geraw** file (Figure 4.83)

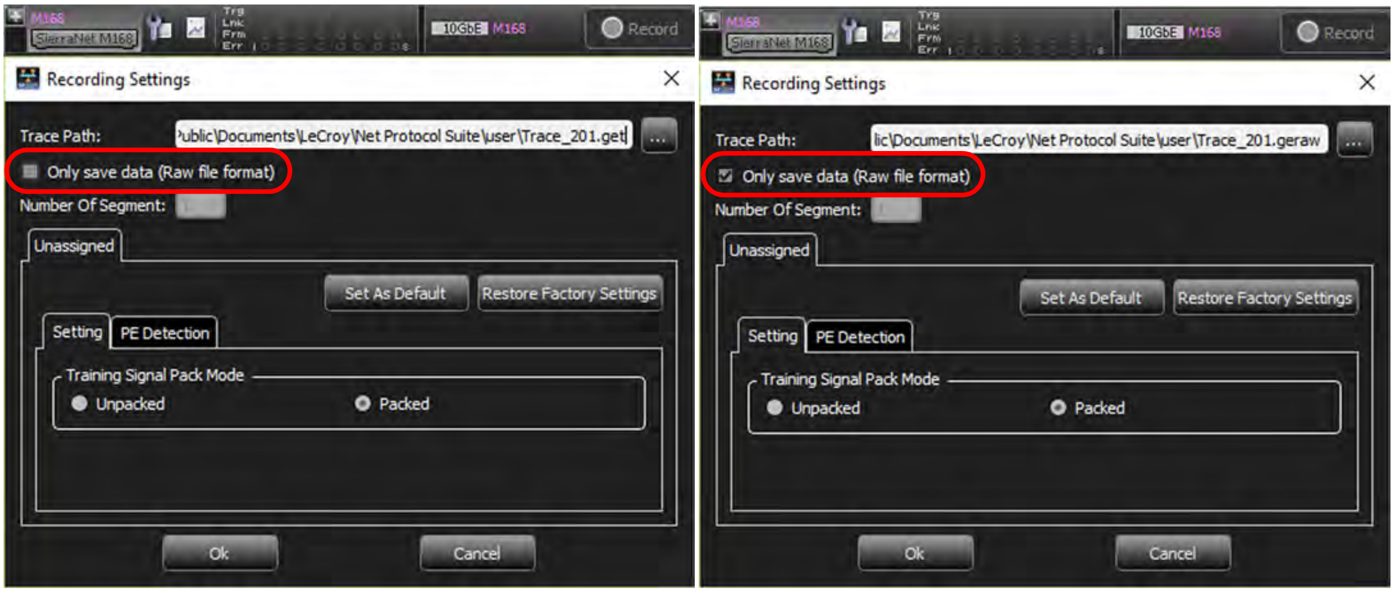


Figure 4.83: Recording Settings Window: M168 – 10GbE

The Recording Settings window allows you to select conditions on which the analyzer will trigger, including:

- **Trace Path**: Location of Saved Trace
- **Number of Segments**: 1 – 32
- **Setting**

  Training Signal Pack Mode: Unpacked or Packed
- **PE Detection**: See below
- **Set As Default**: You can save the Recording Settings you set as the default.
- **Restore Factory Settings**: If you want to revert to the Factory Settings you can select the “Restore Factory Settings” button.

PE Detection Tab: M168 – 10GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored.

1. Select one or more protocol errors or select the **Check All** box to select all.
2. Enter the Number of Segments in the field. The **M168 10GbE** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.6 Recording Settings – M168 – FC

Click the Recording Settings icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (see Figure 4.83):

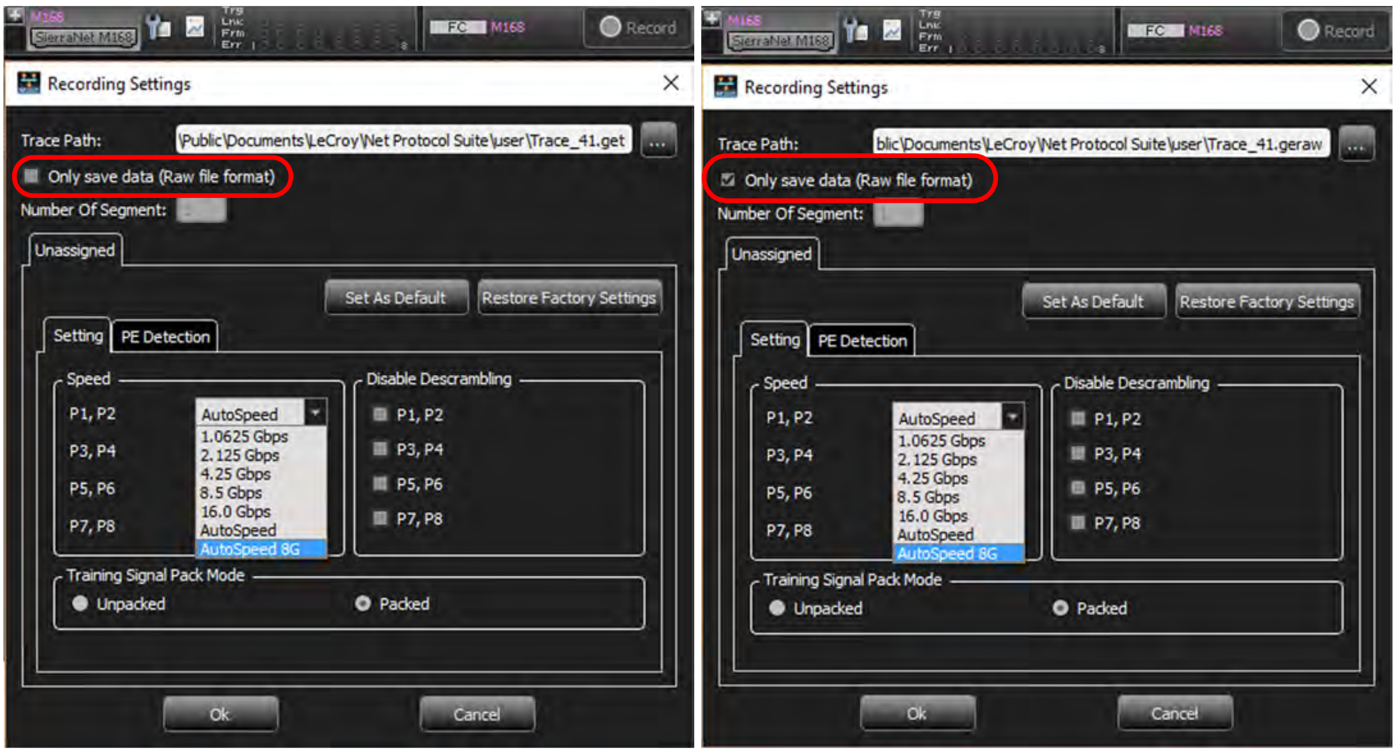


Figure 4.84: Recording Settings Window – M168 → FC

The Recording Settings window allows you to select conditions on which the Analyzer will trigger, including:

- **Trace Path**: Location of Saved Trace
- **Number of Segments**: 1 – 32
- **Setting**
  - Speed: Port Pairs: P1, P2; P3, P4; P5, P6; P7,P8 → 1.0625 Gbps, 2.125 Gbps, 4.25 Gbps, 8.5 Gbps, 16.0 Gbps, AutoSpeed, AutoSpeed 8G
  - Disable Descrambling: Port Pairs → P1, P2; P3, P4; P5, P6; P7,P8
  - Training Signal Pack Mode: Unpacked or Packed
- **PE Detection**: See below
- **Set As Default**: You can save the Recording Settings you've set as the default.
- **Restore Factory Settings**: If you want to revert to the Factory Settings, you can select **Restore Factory Settings**.

PE Detection Tab – M168 – FC

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored.

1. Select one or more protocol errors or select the **Check All** box to select all.
2. Enter the Number of Segments in the field.

The **M168 FC** options are similar to the **M408 10GbE** options (Figure 4.80).

4.1.5.7 Recording Settings – T328 – 10/25GbE

Click the Recording Settings icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (Figure 4.85):

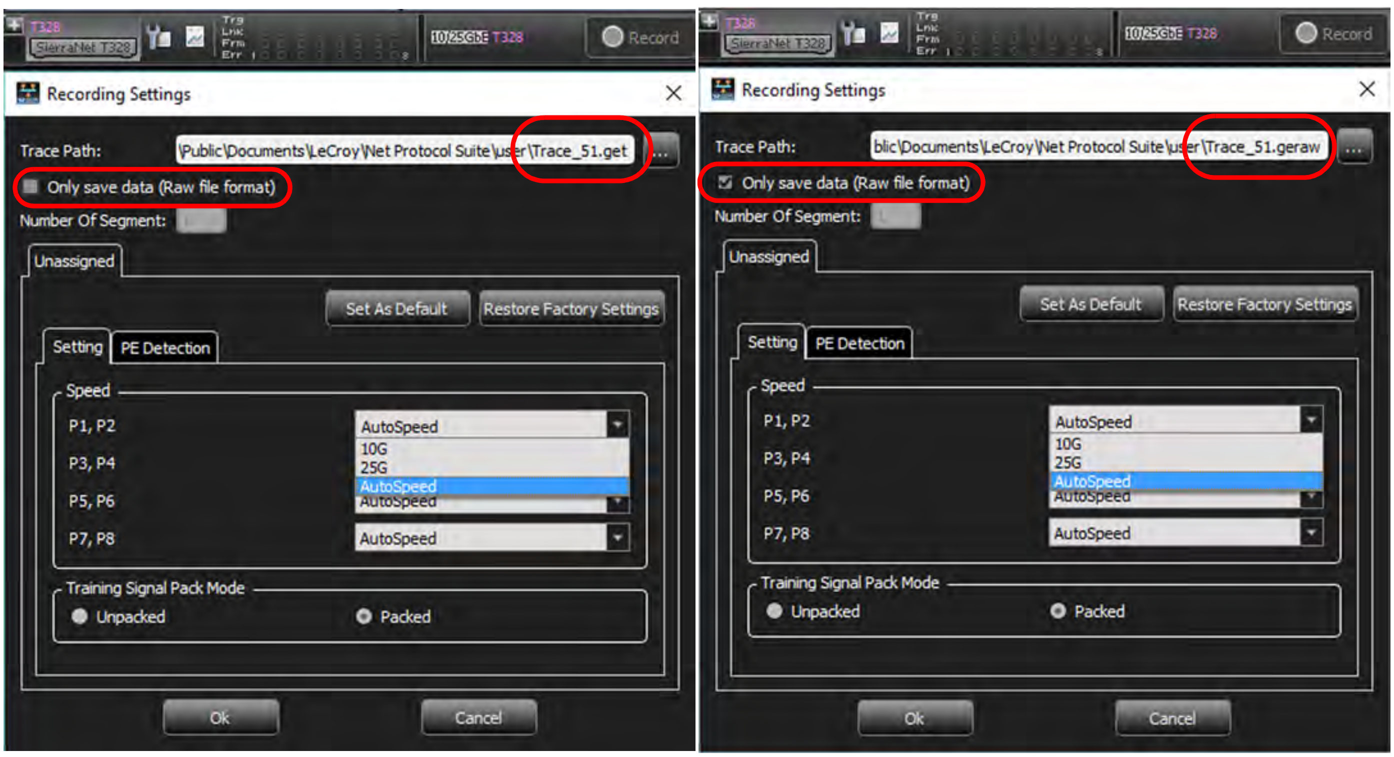


Figure 4.85: Recording Settings – T328 → 10/25GbE

Recording Settings enables you to select conditions on which the Analyzer will trigger, including:

- Trace Path: Location of Saved Trace
- Number of Segments: 1 – 32
- Setting
  - Speed per Port Pair: 10G, 25G or AutoSpeed
  - Training Signal Pack Mode: Unpacked or Packed
- PE Detection: See *PE Detection Tab: T328 – 10/25GbE*, below.

- ❑ Set As Default: You can save the Recording Settings you've set as the default.
- ❑ Restore Factory Settings: If you want to revert to the Factory Settings you can select the "Restore Factory Settings" button.

PE Detection Tab: T328 – 10/25GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **T328 10/25GbE** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.8 Recording Settings: T328 – 50GbE

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (see Figure 4.86).

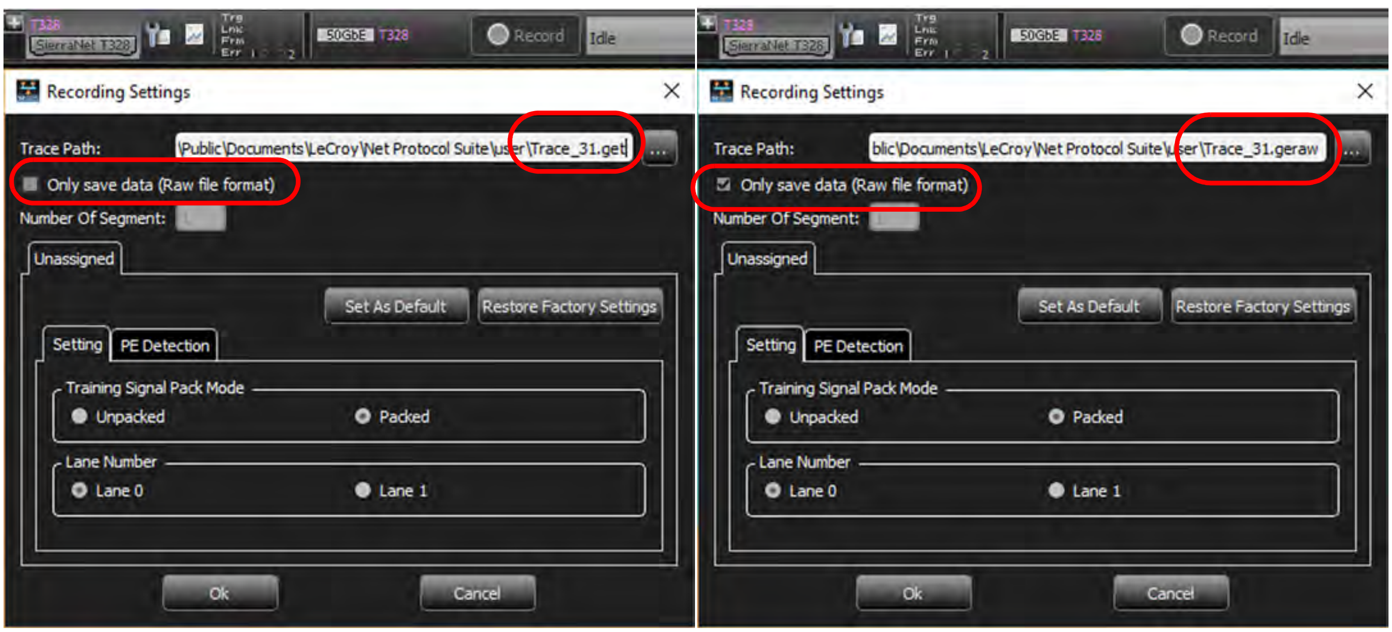


Figure 4.86: Recording Settings Window – T328 → 50GbE

Recording Settings enables you to select conditions on which the Analyzer will trigger, including:

- ❑ Trace Path: Location of Saved Trace
- ❑ Number of Segments: 1 - 32
- ❑ Setting
  - ■ Training Signal Pack Mode: Unpacked or Packed
  - ■ Lane Number: Lane 0 or Lane 1
- ❑ PE Detection: See *PE Detection Tab: T328 – 50GbE*, below.
- ❑ Set As Default: You can save the Recording Settings you've set as the default.

- ❑ Restore Factory Settings: If you want to revert to the Factory Settings you can select the “Restore Factory Settings” button.

PE Detection Tab: T328 – 50GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **T328 50GbE** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.9 Recording Settings: T328 – 40/100GbE

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file. The Recording Settings window will look a lot like Figure 4.85 but the transfer speeds will be 40/100GbE instead of 10/25GbE.

Recording Settings allows you to select conditions on which the Analyzer will trigger, including:

- ❑ Trace Path: Location of Saved Trace
- ❑ Number of Segments: 1 - 32
- ❑ Setting
  - ■ Training Signal Pack Mode: Unpacked or Packed
  - ■ Speed per Port Pair: 40G, 100G or AutoSpeed
  - ■ Lane 0 → 3
- ❑ PE Detection: See *PE Detection Tab – T328 – 40/100GbE*, below
- ❑ Set As Default: You can save the Recording Settings you’ve set as the default.
- ❑ Restore Factory Settings: If you want to revert to the Factory Settings you can select the “Restore Factory Settings” button.

PE Detection Tab – T328 – 40/100GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **T328 40/100GbE** options are similar to the **M408 10GbE** options (Figure 4.80).

4.1.5.10 Recording Settings: T328 – FC

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window. You can save the Trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (Figure 4.86).

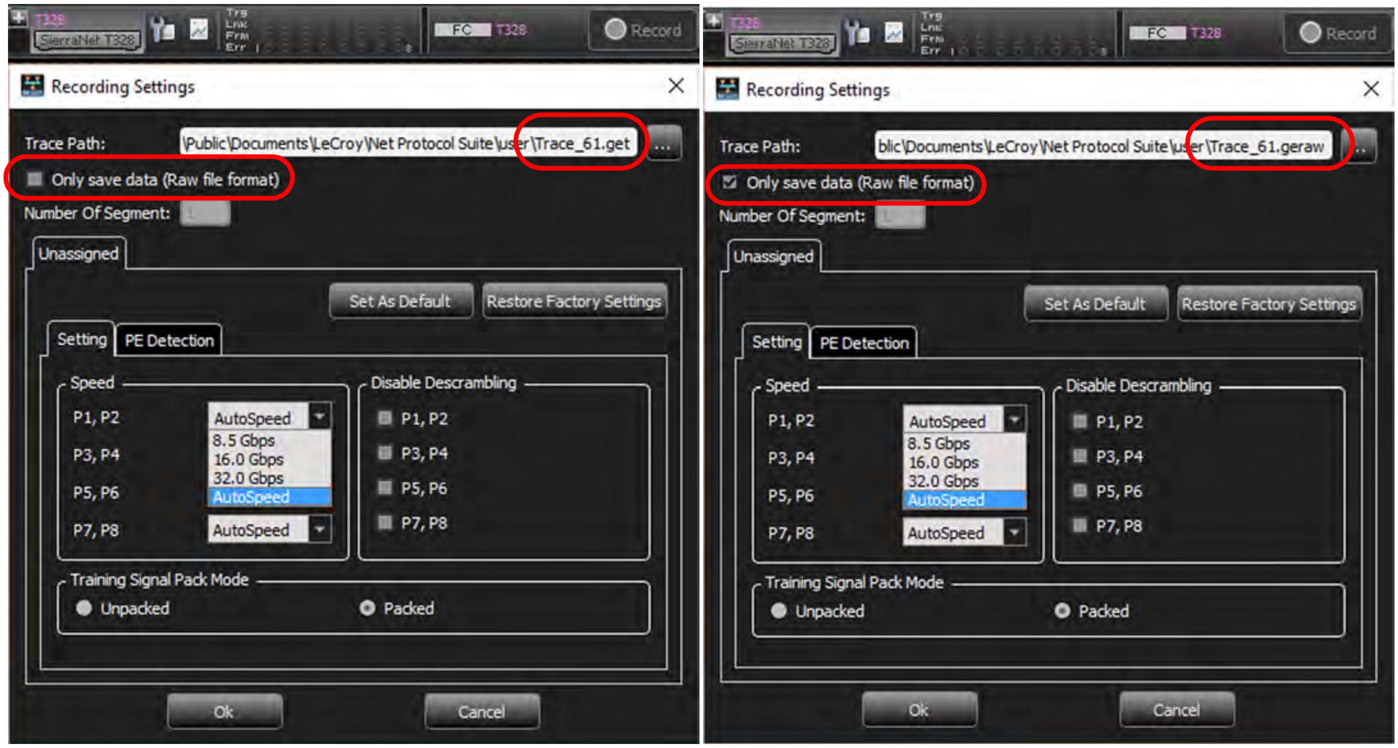


Figure 4.87: Recording Settings Window: T328 → FC

Recording Settings enables you to select conditions on which the Analyzer will trigger, including:

- Trace Path: Location of Saved Trace
- Number of Segments: 1 – 32
- Setting
  - Speed per Port Pair: P1/P2, P3/P4, P5/P6, P7/P8 → 8.5 Gbps, 16.0 Gbps, 32.0 Gbps or AutoSpeed
  - Disable Descrambling for Port Pairs: P1/P2, P3/P4, P5/P6, P7/P8
  - Training Signal Pack Mode: Unpacked or Packed
- PE Detection: See *PE Detection Tab – T328 – FC*, below.
- Set As Default: You can save the Recording Settings you've set as the default.
- Restore Factory Settings: If you want to revert to the Factory Settings you can select the “Restore Factory Settings” button.

PE Detection Tab – T328 – FC

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **T328 FC** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.11 Recording Settings: M328 – 10/25GbE

Click the **Recording Settings** icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a .geraw file (see Figure 4.86).

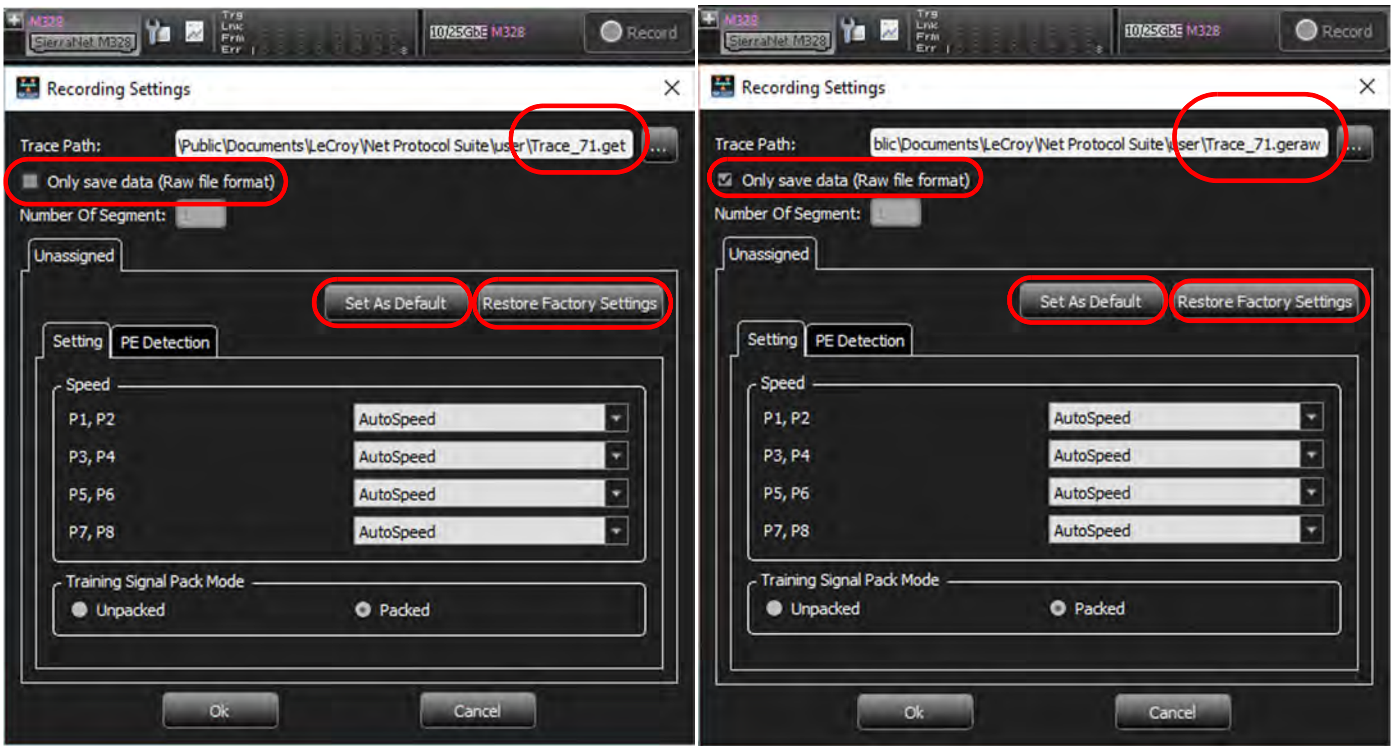


Figure 4.88: Recording Settings Window: M328 → 25GbE

The *Recording Settings* window allows you to select conditions on which the Analyzer will trigger, including:

- Trace Path: Location of Saved Trace
- Number of Segments: 1 - 32
- Setting
  - Speed: P1/P2, P3/P4, P5/P6, P7/P8 → AutoSpeed
  - Training Signal Pack Mode: Unpacked or Packed
- PE Detection: See below
- Set As Default: You can save the Recording Settings you've set as the default.
- Restore Factory Settings: If you want to revert to the Factory Settings you can select the "Restore Factory Settings" button.

PE Detection Tab: M328 – 10/25GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored.

1. Select one or more protocol errors or click in the **Check All** box to select all.

2. Enter the Number of Segments in the field.

   The **M328 10/25GbE** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.12 Recording Settings: M328 → 40/100GbE

Click the Recording Settings icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (see Figure 4.89).

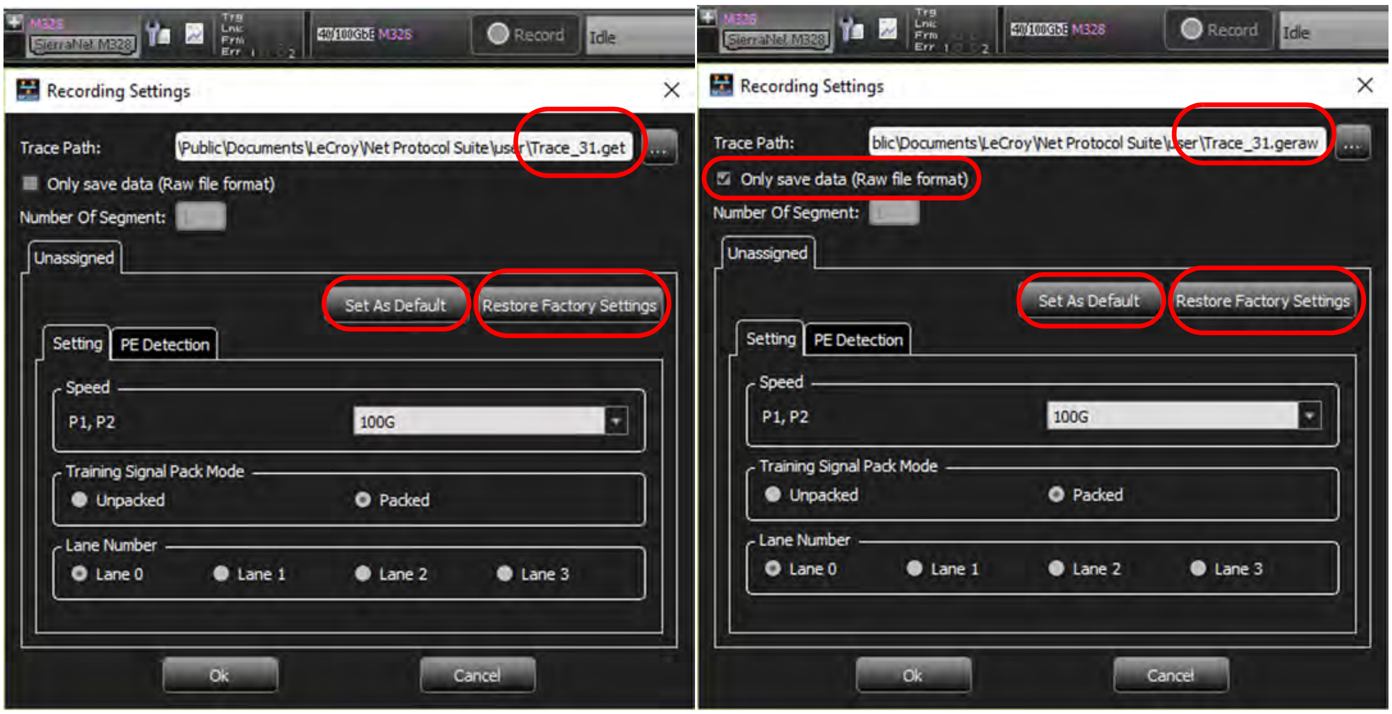


Figure 4.89: Recording Settings Window: M328 → 40/100GbE

Recording Settings allows you to select conditions on which the analyzer will trigger, including:

- Trace Path: Location of Saved Trace
- Number of Segments: 1 – 32
- Setting
  - Training Signal Pack Mode: Unpacked or Packed
  - Speed per Port Pair: 100G
  - Lane 0 → 3
- PE Detection: See below
- Set As Default: You can save the Recording Settings you've set as the default.
- Restore Factory Settings: If you want to revert to the Factory Settings you can select the "Restore Factory Settings" button.

PE Detection Tab: M328 → 40/100GbE

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **M328 40/100GbE** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.5.13 Recording Settings: M328 → FC

Click the Recording Settings icon to display the Recording Settings/PE Detection window. You can save the trace in two different formats: Indexed and Decoded generating a **.get** file or Raw file format generating a **.geraw** file (see Figure 4.90).

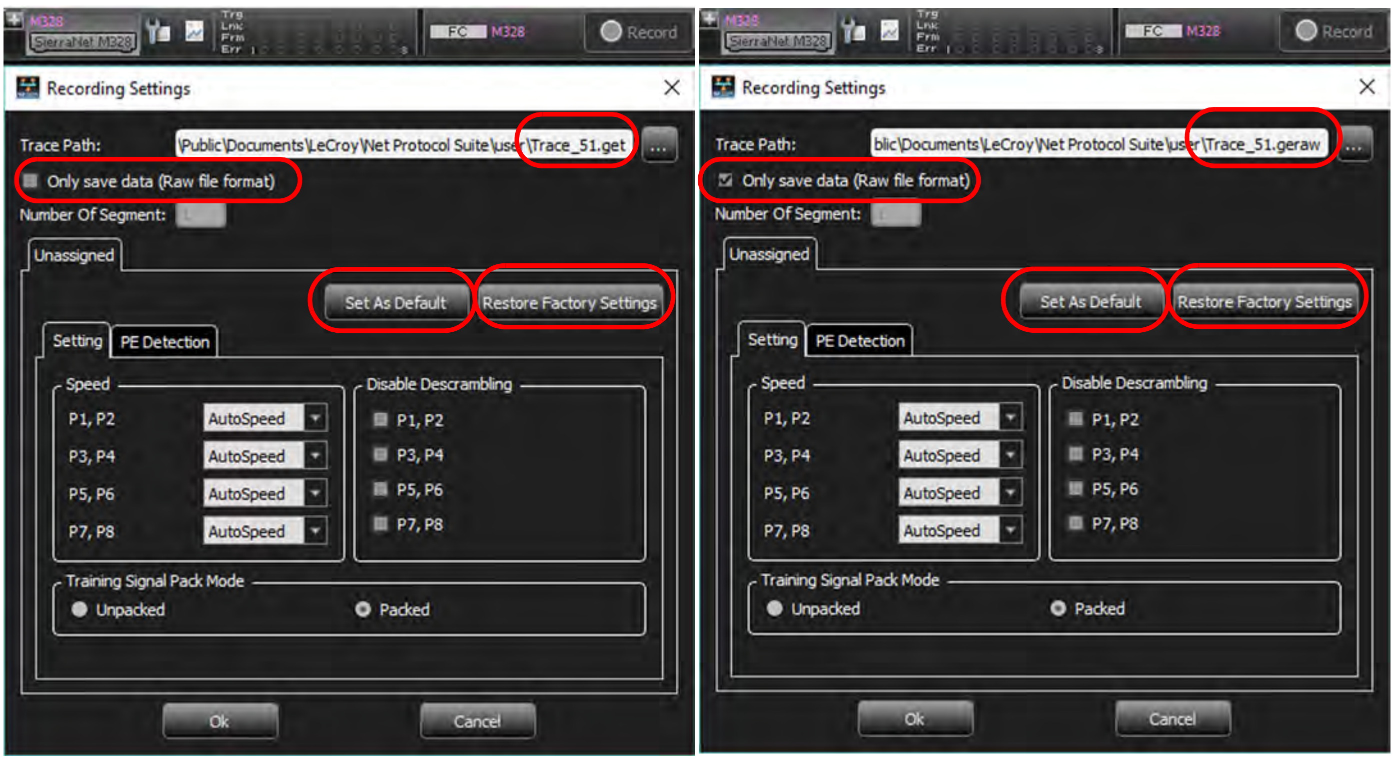


Figure 4.90: Recording Settings Window: M328 → FC

Recording Settings allows you to select conditions on which the analyzer will trigger, including:

- Trace Path: Location of Saved Trace
- Number of Segments: 1 - 32
- Setting
  - Training Signal Pack Mode: Unpacked or Packed
  - Speed per Port Pair: AutoSpeed
  - Lane 0 → 3
- PE Detection: See below

- Set As Default: You can save the Recording Settings you set as the default.
- Restore Factory Settings: If you want to revert to the Factory Settings you can select the “Restore Factory Settings” button.

PE Detection Tab: M328 – FC

The PE Detection Tab allows you to select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field. The **M328 FC** options are similar to the **M408 10GbE** options (see Figure 4.80).

4.1.6 Trigger/Filter Settings Pane

Use the Trigger/Filter Settings pane to select Snapshot or Event Trigger mode and choose the Trigger Filter settings. See figures below.

Figure 4.91: Trigger/Filter Settings Tool Bar

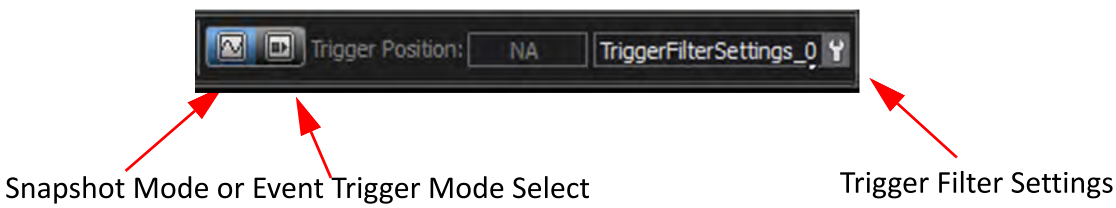
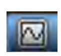
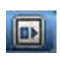
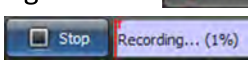


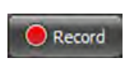
Figure 4.92: Default Trigger Snapshot Mode Selected

Clicking on the icon  puts the analyzer in Snapshot (default) mode.

Clicking on the icon  puts the analyzer in Event Trigger mode.

4.1.6.1 Snapshot Mode

A Snapshot is a fixed-length recording and is the default triggering mode. The size of this recording is set by the Buffer Size box (see 4.1.6.3, *Buffer Size and Segments*). Recording begins when  is clicked and ends when either the selected buffer size is filled or the  button is clicked while a recording is taking place.

If the cursor is hovered over the  button the Start/Stop Session icon will pop up, shown below:

4.1.6.2 Event Trigger Mode

In Event Trigger Mode, recording begins when you click  on the Tool Bar.

Recording continues in a circular manner within the limits set by the buffer size until an Event Trigger is detected that meets the Trigger conditions specified in the Triggering Options and the defined amount of data has been recorded after the Event Trigger.

NOTE: If no Event Trigger occurs, the data continues be written into memory and will over-write the previously written data until the recording session is manually stopped by clicking on the Record button again.

4.1.6.3 Buffer Size and Segments

The Analyzer Settings panel has the Recording Buffer pane where you can set the buffer size (megabytes or gigabytes), number of Segments, and the Segment size. See Figure 4.93.

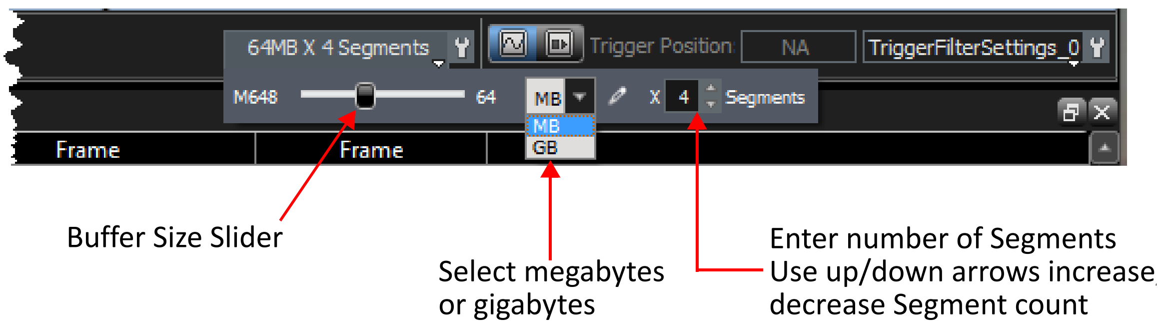


Figure 4.93: Segment Size and Number

The default is a buffer size of 24MB x 1 Segment. Setting multiple segments will trigger on the first occurrence of the trigger condition, fill the first segment, then automatically re-arm the trigger and repeat the remaining number of segments specified.

- Use the slider to increase/decrease the buffer size, then click the arrow to indicate MB or GB. You can set the size of each segment, up to the buffer size, divided by the number of segments.

  Maximum buffer size depends on the hardware. See Figure 4.74 for the T328, M328, M408 and M168).

- Enter an integer number of Segments, from 1 to 32 (default = 1), or click the up/down arrows to set the number of Segments.

The New Project window opens with default settings to Snapshot mode and 1 segment of 24MB. (The analyzer captures everything immediately, when the Record button is clicked without triggering on anything in particular.)

When the analyzer is changed to Event Trigger mode, each time a trigger condition occurs, the system records a new segment. When the same trigger automatically repeats, the system records the number of segments that you entered.

NOTE: If the size of a data traffic exceeds the buffer memory allocation, the project runs, but no data capture occurs. You must increase buffer memory size to a value greater than the data traffic size.

4.1.6.4 Trigger Position

Configuring an Event Trigger Position

Choosing the Event Trigger option enables the Trigger Position to be set manually. You can set the trigger position in the captured buffer as a percentage of the segment size. A trigger point of 1% means the trigger point will be near the first event in the buffer. See Figure 4.94.

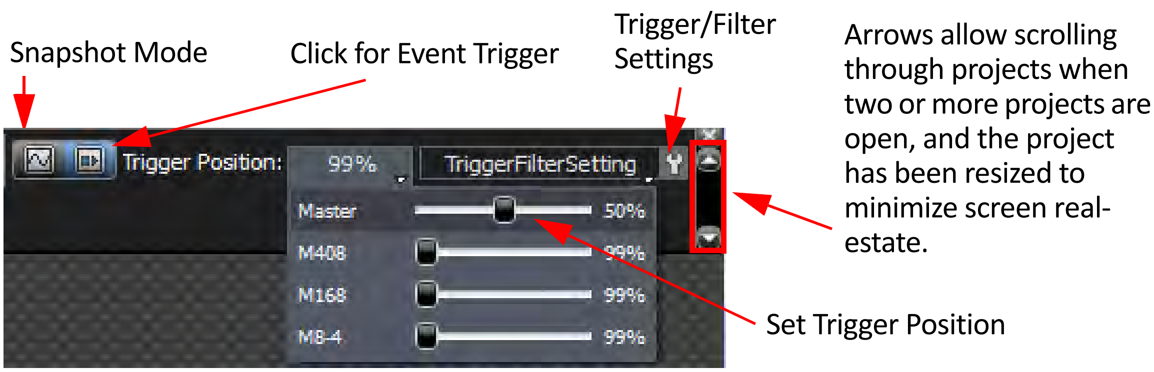


Figure 4.94: Trigger/Filter Settings Pane.

Pre-Trigger/Post-Trigger

You can set the amount of data to be captured before and after the trigger event, as a percentage of the data segment, between 1% and 99%. See Figure 4.95.

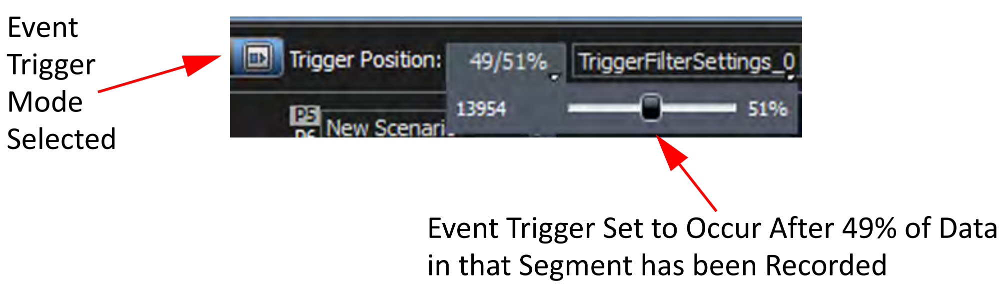


Figure 4.95: Trigger Position within the Segment

The Pre-trigger specifies a percentage of data prior to the triggering event. This feature allows the evaluation of bus activity leading up to and after the triggering event. Figure 4.96 illustrates the operation of pre-trigger in data memory.

You can adjust the amount of recording to be done post-trigger or select where you want the Trigger located within the defined buffer. You can adjust the Triggering Position between 1 and 99% post-trigger. As an example, if the buffer size is set to 16 MB, then for the following Trigger Position settings, the amount of pre-trigger and post-trigger data is:

- 95% post-triggering: 0.8 MB pre-trigger, 15.2 MB post-trigger
- 75% post-triggering: 4 MB pre-trigger, 12 MB post-trigger
- 50% post-triggering: 8 MB pre-trigger, 8 MB post-trigger
- 25% post-triggering: 12 MB pre-trigger, 4 MB post-trigger
- 5% post-triggering: 15.2 MB pre-trigger, 0.8 MB post-trigger

When a Trigger occurs, recording continues until the post-trigger amount of the buffer is filled or when **Stop** is selected.

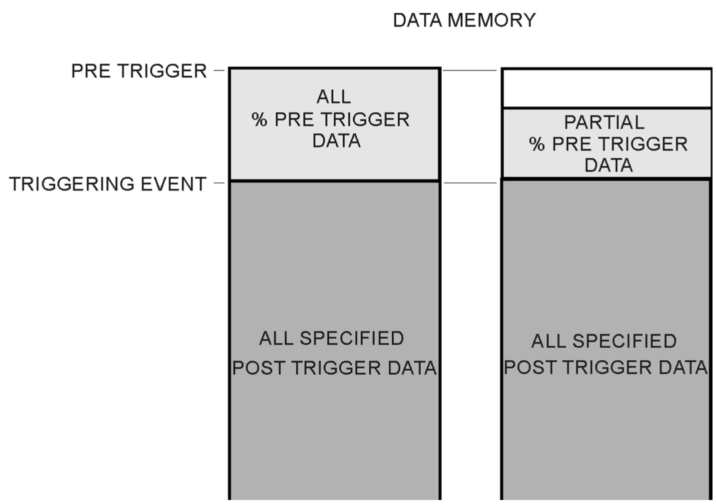


Figure 4.96: Pre-Trigger Example, 20% Pre-Trigger

In certain cases, when one port is recording traffic and filling up the memory much faster than another port, you might see traffic appearing only on one port for a while, and the other port's traffic will only appear later. This occurs as a function of the trigger position, and is normal, expected behavior of the analyzer.

4.2 Trigger Filter Settings in Easy Mode

Easy mode allows you to operate the analyzer with minimum setup. Use Easy Mode to get a comprehensive overview of your analyzer's capabilities. Easy mode allows only Trigger and Data captures.

The Trigger and Filter settings panes has parameters for triggering on selected triggers and filtering in (including) or filtering out (excluding) selected patterns. The window opens with default settings to capture everything on the bus. The analyzer captures everything immediately without triggering on anything in particular.

Configure an Event Trigger using the settings from the Trigger Filter Setting Pane (see Figure 4.94).

1. To create new trigger filter settings, click **TriggerFilterSettings** and select **New** from the drop-down menu (Figure 4.97). The Trigger Filter Settings window displays.

2. To set the when the Analyzer triggers, click **Trigger/Filter** . The Trigger Filter Settings window displays.

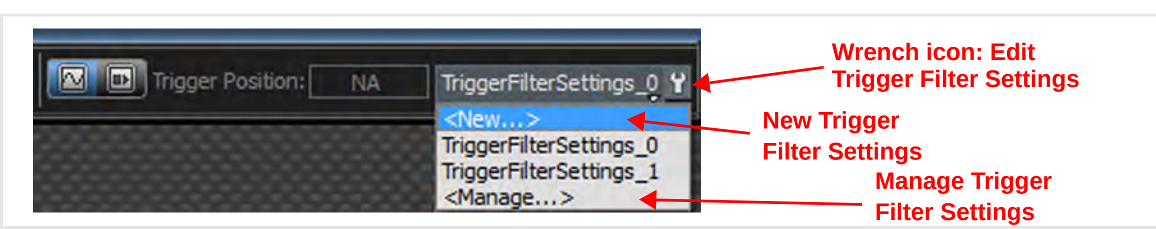


Figure 4.97: Generate a New Trigger Filter Setting

4.2.1 Trigger Filter Settings Window

Refer to Figure 4.98 to learn more about the Trigger Filter Settings.

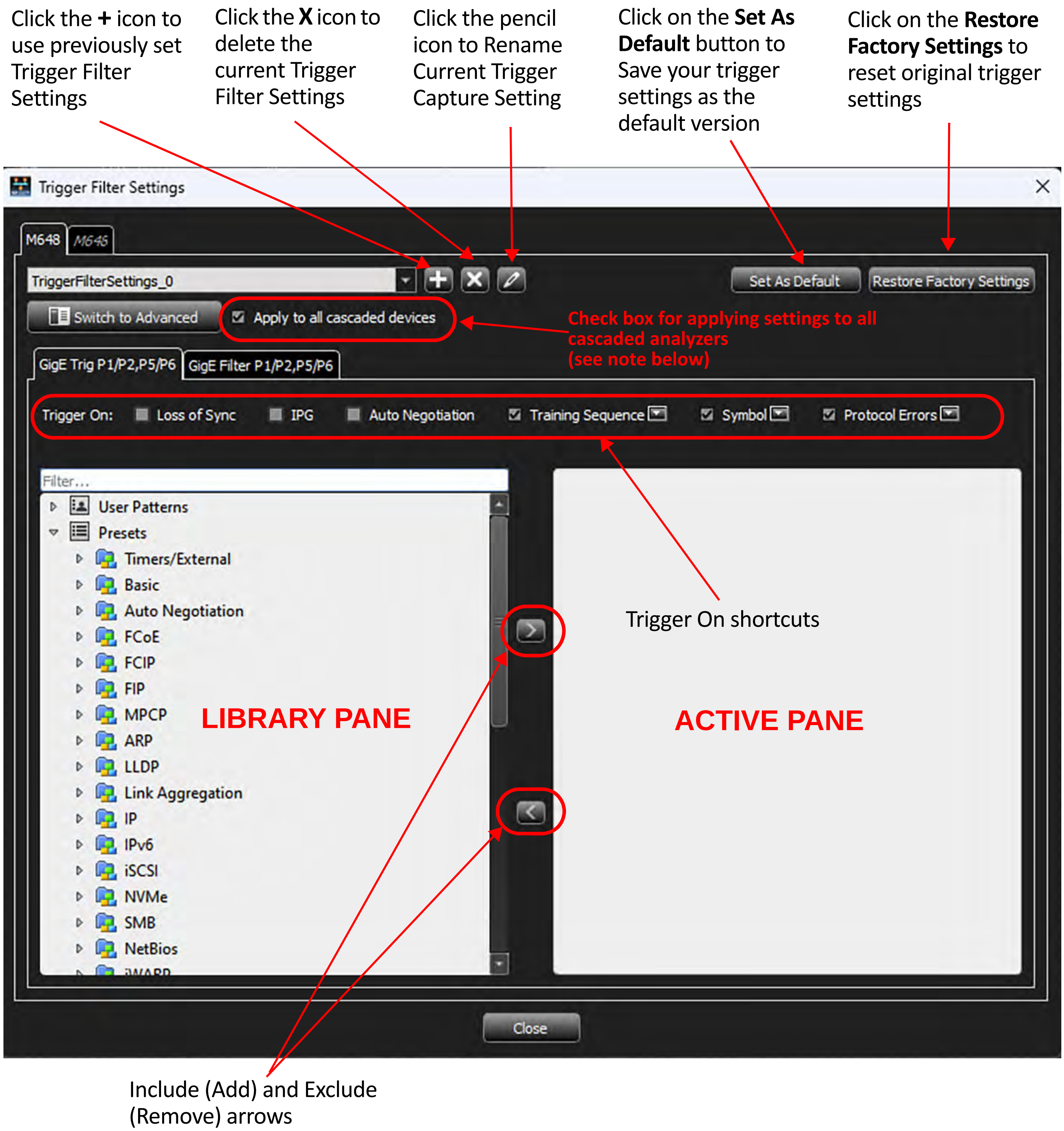


Figure 4.98: Trigger Filter Settings Window

NOTE: The “Apply to all cascaded devices” checkbox: When checked, the Trigger/ Filter settings applied to the first analyzer are also applied to any other analyzers which have been cascaded together. In this case, the settings for the M648 will be applied to the M646.

4.2.1.1 Trigger On Shortcuts

The Trigger On: section provides trigger shortcuts.

FCOE Options

- Loss of Sync
- IPG
- Auto Negotiation
- Training Sequence: NRZ/PAM4 options (both selected by default).
- Symbol: All the symbols are listed here, among which only two can be selected at any time.
- Protocol Errors: The protocol-errors are grouped as "Any/Frame/Symbol/Auto Negotiation/Training Sequence" for easy selection, ("Any error" is selected by default).

FC Options

- Connect/Disconnect: Connect or Disconnect options options available (both selected by default).
- Training Sequence: NRZ/PAM4 options (both selected by default).
- Protocol Error: The protocol-errors are grouped as "Any/Frame/Symbol/Training Sequence" for easy selection, ("Any error" selected by default.)

4.2.1.2 Patterns

1. Choose a pattern for capture from any of the categories.
2. Drill down through the category in the Library pane by double-clicking until reaching a filter.
3. Click the **Add >** button. If applicable, a dialog may display to further refine the filter. Once complete, click OK on the dialog to return to the Trigger Filter Settings window. The filter is now added to the Active Pane.
4. To remove a filter, highlight it in the Active Pane and either click the Remove button (<) or press the delete key on the keyboard. A dialog will display asking if you want to remove the pattern. Click Yes.

4.2.1.3 Trigger Tab

Drag and drop patterns from the Trigger Library Pane into the Active Pane. Use the Add and Remove arrows to move patterns between the Patterns Library and the Active pane (see Figure 4.98).

Setting an Event Trigger

1. With the Trigger Filter Settings open, select a pattern of interest. For example, FCOE-FCP_CONFIRM (Figure 4.99).
2. Click the **Add** button (**>**).

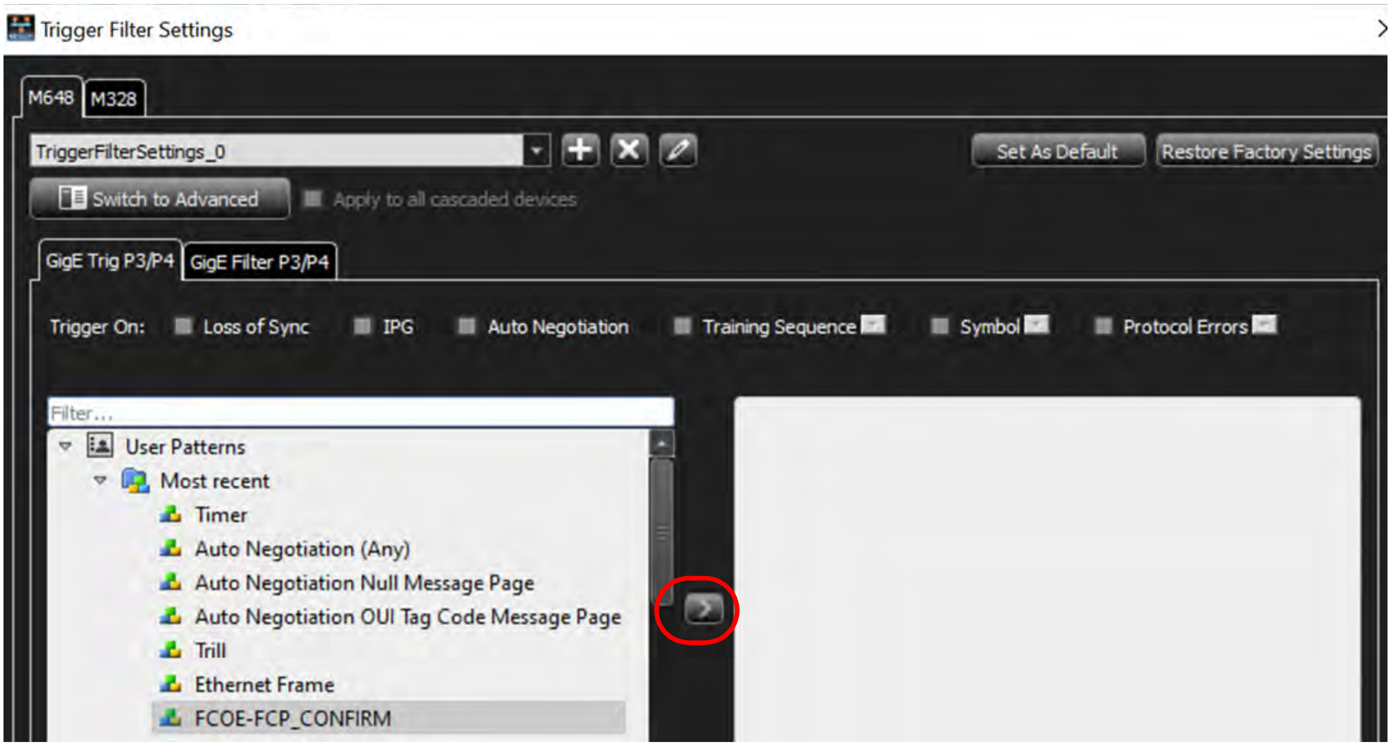


Figure 4.99: User Pattern FCOE-FCP_CONFIRM

The FCOE-FCP_CONFIRM window displays (Figure 4.100).

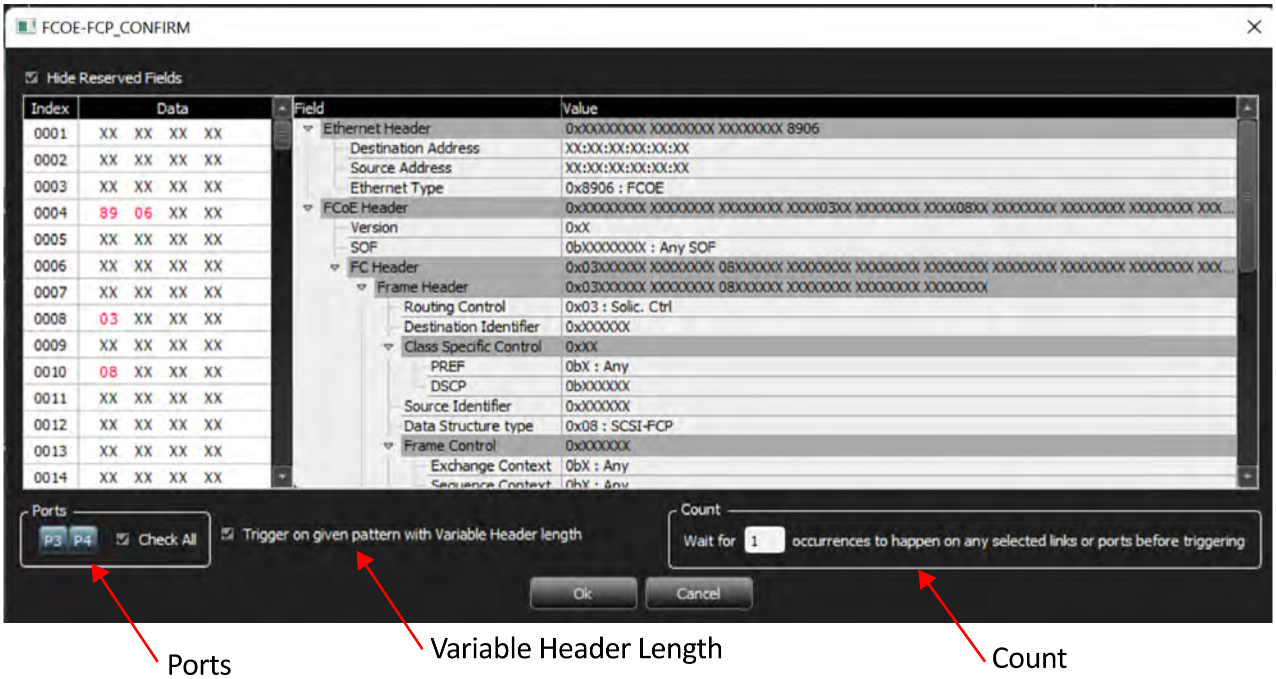


Figure 4.100: FCOE-FCP-CONFIRM Window

Select the following:

- Ports: Select which ports (links) to trigger on (or click Check All for all ports)
- Variable Header Length: Trigger on given pattern with Variable Header length
- Count: Set the analyzer to Trigger on the number of occurrences on each link. This specifies the number of times that the pattern must occur before triggering. The Events on each link are counted independently, causing a trigger whenever the number of occurrences on any link equals the specified value.

Once complete, click the **OK** button to return to the Triggering Filter Settings window. Notice that the FCOE-FCP-CONFIRM pattern now displays in the Active Pane.

4.2.1.4 Filter Tab

Drag and drop patterns from the Filter Library pane into the Active Pane. Select the pattern and use the Add and Remove arrows to move patterns between the Patterns Library and the Active pane (see Figure 4.101).

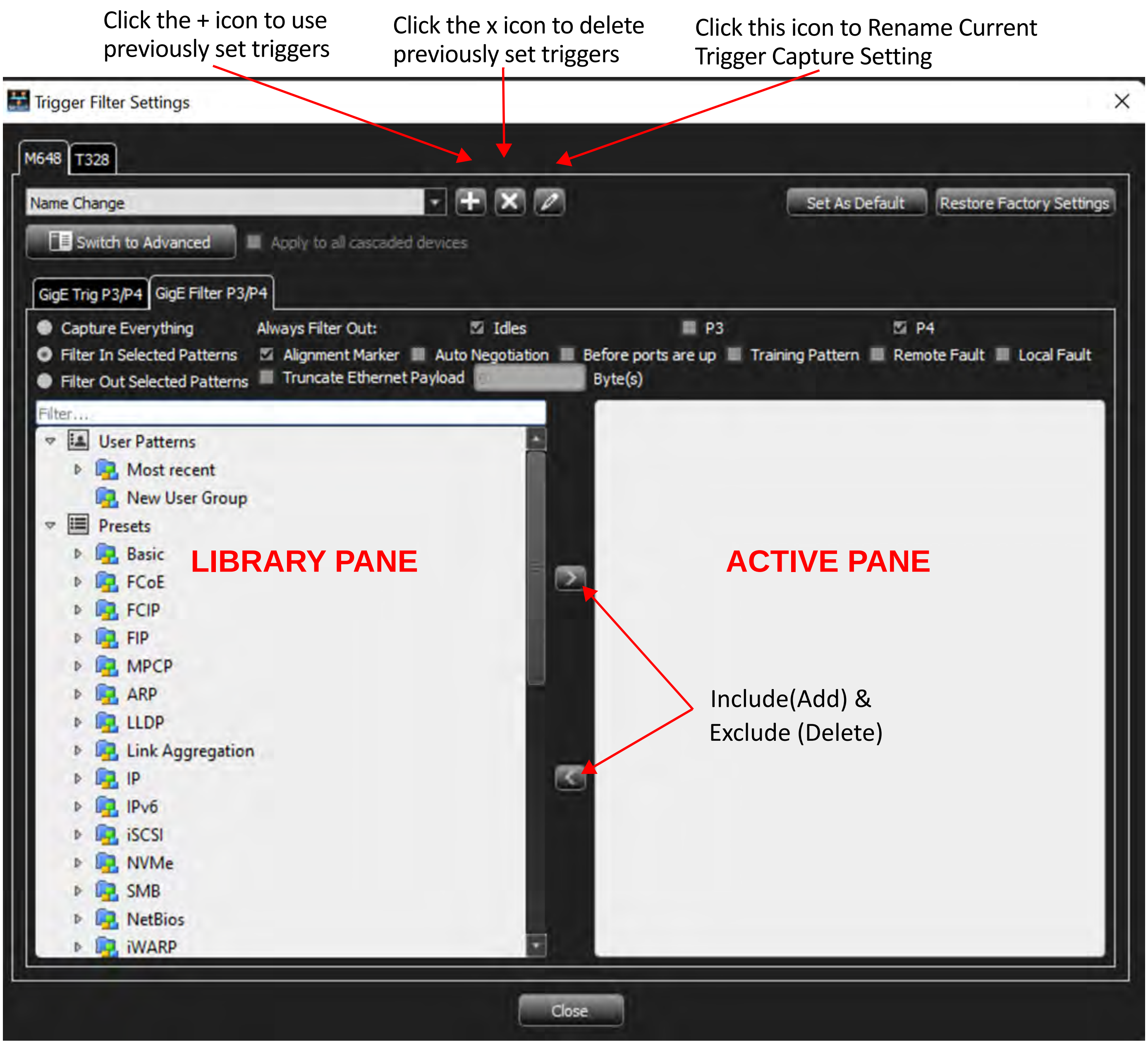


Figure 4.101: Filter Window

The following filtering shortcuts are available:

Capture Everything

Checking this option captures everything on the bus and the disables the Pattern Library.

Filter in Selected Patterns

Checking this option includes the selected patterns in the trace capture.

Filter Out Selected Patterns

Checking this option excludes the selected patterns in the trace capture.

Always Filter Out

Check one or more option to exclude Idles and or specific channels in the trace capture.

NOTE: Capturing a full buffer requires capturing the traffic with all ports. Using four ports captures only half the system memory. Note that the size of the system memory is based upon the purchased license.

Auto Negotiation

Check this box to always filter out Auto Speed Negotiation traffic. (see Figure 4.101).

Truncate Fibre Channel Over Ethernet (FCoE) Payload

Check this option to truncate FCoE payloads after x-number of DWORD(s) (see Figure 4.101).

NOTE:

- For iSCSI events, payload truncation may not truncate at the specified value as some events could come out of sequence.
- For Ethernet frames, the CRC and Termination will also be truncated, but for FC frames, the CRC and Termination will be kept.

4.2.1.5 Patterns and Data Capture Setup

Refine data capturing by choosing **Pattern** and then selecting specific patterns for capture. Additionally, define a different set of patterns to capture after trigger. See Figure 4.102.

The Trigger and Filter settings window allows you to set the parameters for triggering on selected triggers and filtering in (including) or filtering out (excluding) selected patterns. Refer to 4.102, *Trigger and Filter Preset Patterns (RDMA and NVMe)*.

4.2.1.6 Trigger and Filter Preset Patterns (RDMA and NVMe)

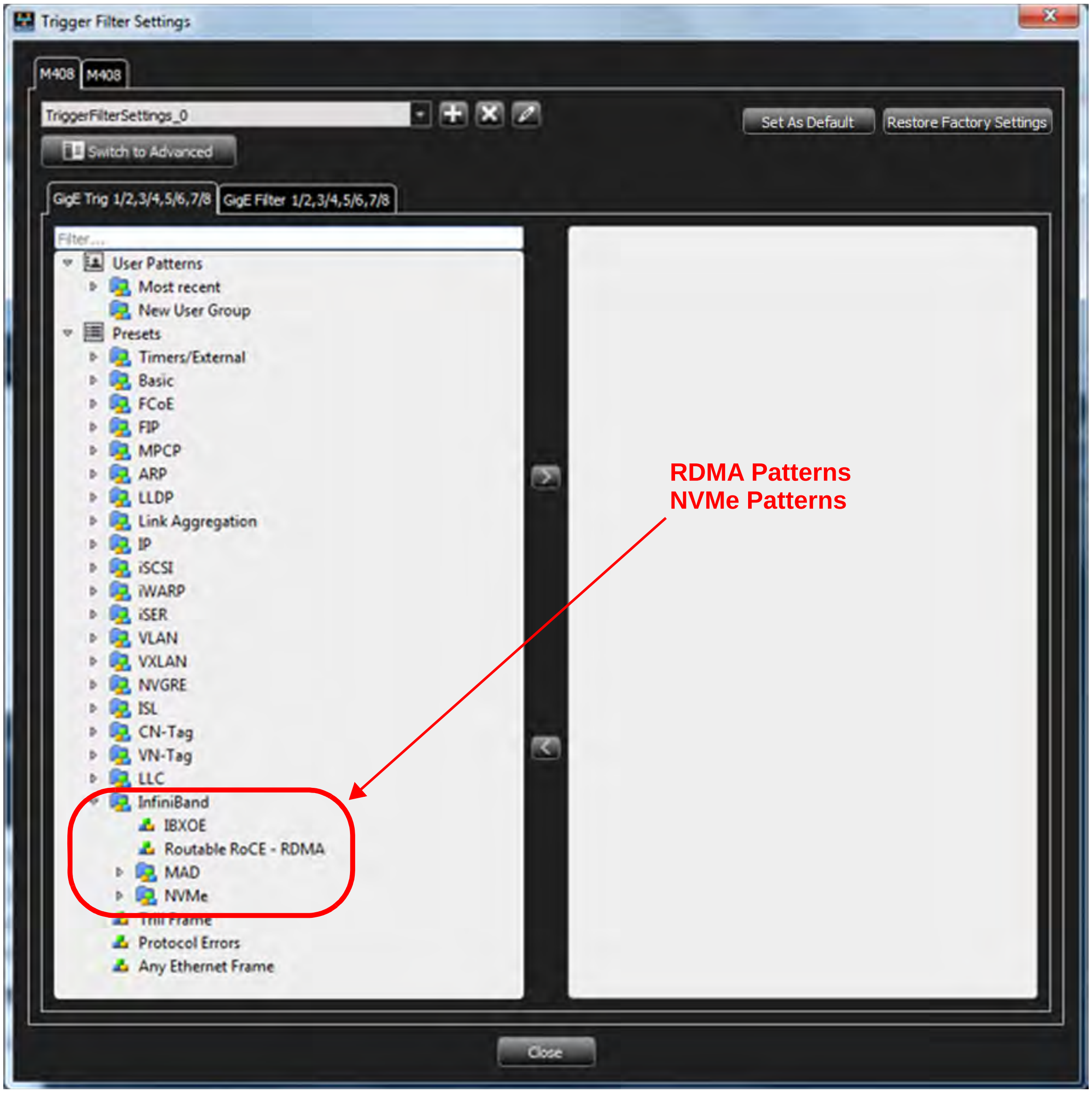


Figure 4.102: Trigger and Filter Preset Patterns (RDMA and NVMe)

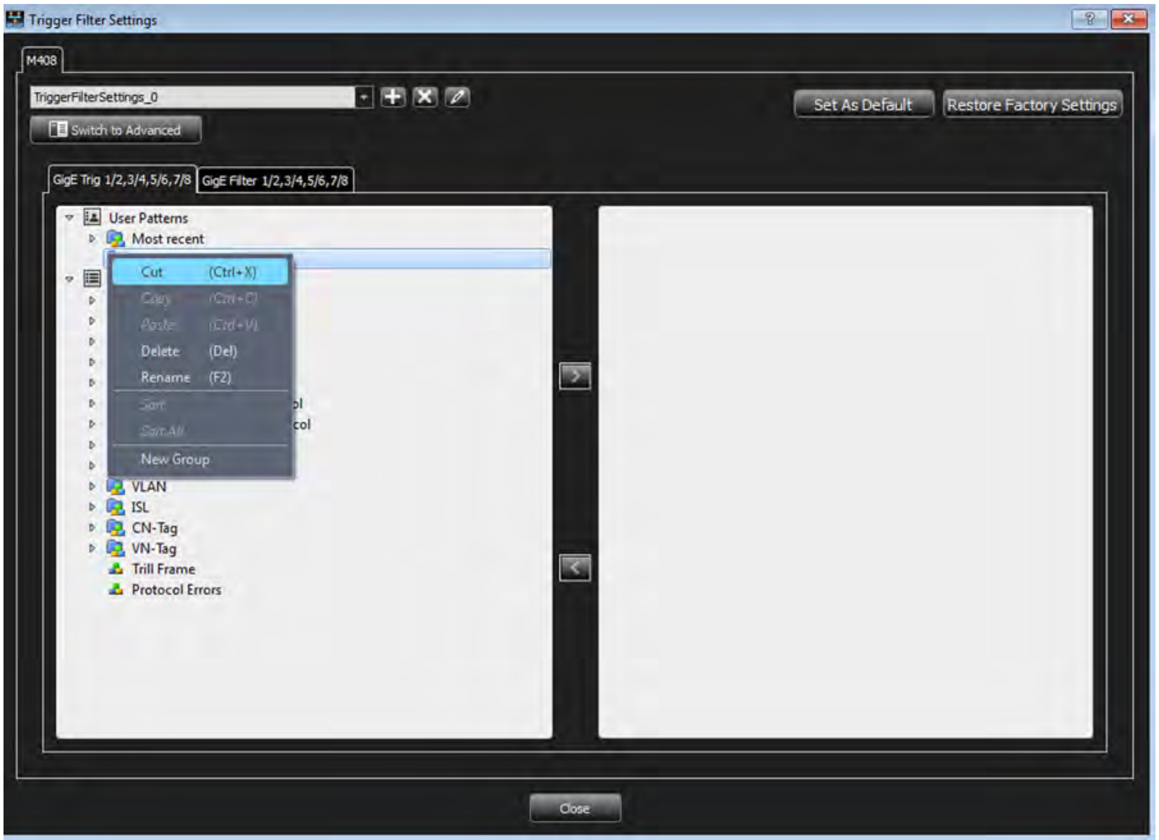


Figure 4.103: Creating a New User Group

4.2.2 Timers/External

4.2.2.1 Timer

You can set a timer independently of any other trigger selection, to cause an unconditional trigger after a set time.

Double-click **Timer** in the Pattern window to open the Add Timer Pattern window.

Check a Time Unit, enter the Timer Value, and click **OK**.

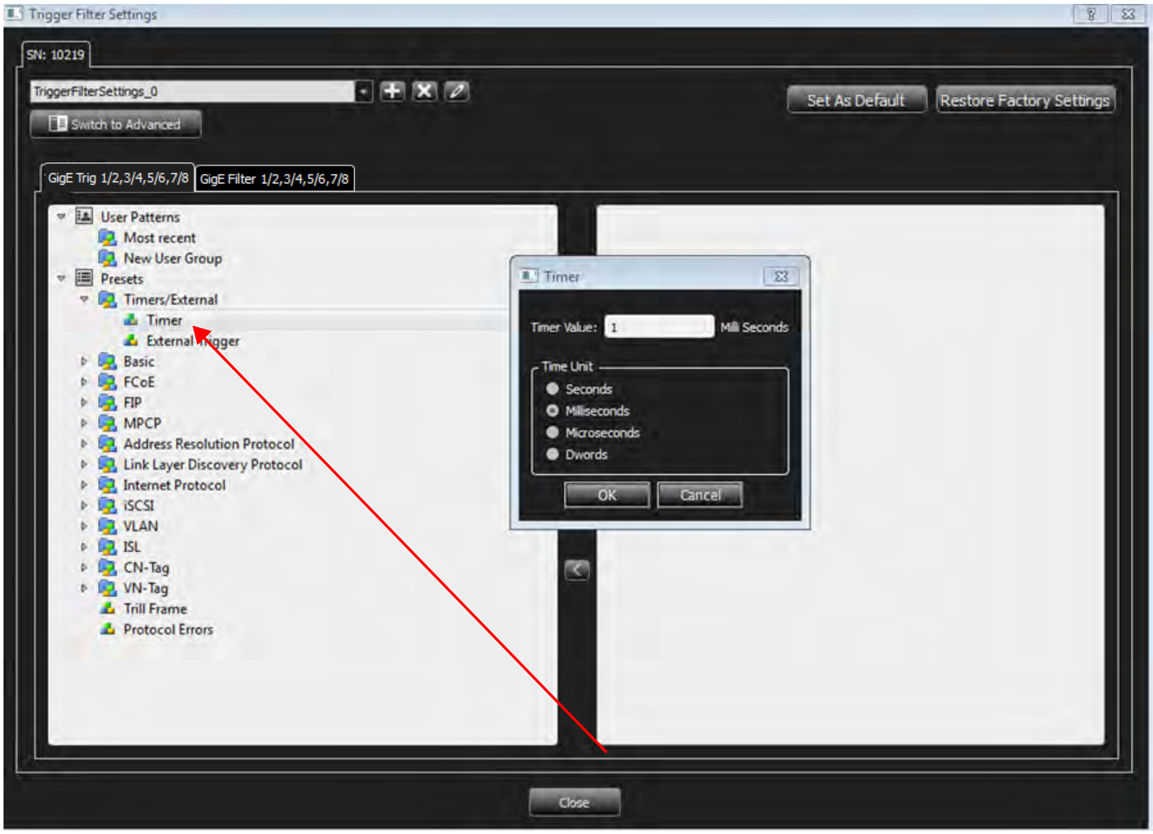


Figure 4.104: Timer Pattern Window

NOTE: The timer resolution is limited to one DWORD. The minimum value is 12-13 DWORD.

4.2.2.2 External Trigger

Use this event to wait for a signal on the analyzer's external trigger input. Refer to 4.1.2.6, *External Trigger* for details on configuring the external trigger input.

4.2.3 Pattern Editing Conventions

When entering values in patterns the following conventions apply:

In Binary, 'X' means one bit which is "don't care" and the value can be either 1 or 0. Below are some examples in binary and their meanings:

"X10": The value length is 3 bits and from right to left, the first and second bits have specific values and the third one is "don't care".

"XXXXXXX1": The value length is 8 bits and from right to left, the first bit has a specific value and the rest are "don't care".

In Hexadecimal 'X' means 4 bits in which all four are “don't care”. In hexadecimal '?' means either one of the bits 1, 2, 3 or 4 bits is “don't care” and it is not clear which bit is “don't care” and which ones have specific value. Some examples are given in the Table 4.5 below.

TABLE 4.5: Example Hexadecimal Values

Hexadecimal Value	Length in bits	Equivalent Value in Binary
“X1”	8 bits	“XXXX0001”
“X?”	8 bits	“XXXXXX10”
“?X”	8 bits	“110XXXXX”
“?”	2 bits	“XX”
“?”	3 bits	“11X”
“7”	3 bits	“111”
“7?”	8 bits	“01110XX1”

If VI_READ_RQST is selected, the value for the “Device HDR” field will be “10” in binary format as this field is a two-bits field. This field is the last field in the “DF_CTL” field which is an 8 bits field. For this specific frame, the value of “DF_CTL” will be “XXXXXX10” in binary format and “X?” in hexadecimal format according to the conventions above.

NOTE: In some protocols, certain fields determine the encoding for some of the following fields. A common example is the ‘Payload Length’ field. If fields deeper in the packet are set and the Payload Length field is changed, all following fields are reset to their defaults, and the previously set values are removed.

4.2.4 Ethernet User Patterns – Presets

This section describes the *Presets* Ethernet patterns for SierraNet T328, SierraNet M328, SierraNet M408, and SierraNet M168.

NOTE: The example images used in this section are for M168, Ports P3/P4, GigE 10.

4.2.4.1 Basic

Loss of Sync

1. Double-click **Loss of Sync** to open the Loss of Sync dialog box (Figure 4.105).

   This event detects loss of sync on the Ethernet physical layer receiver.

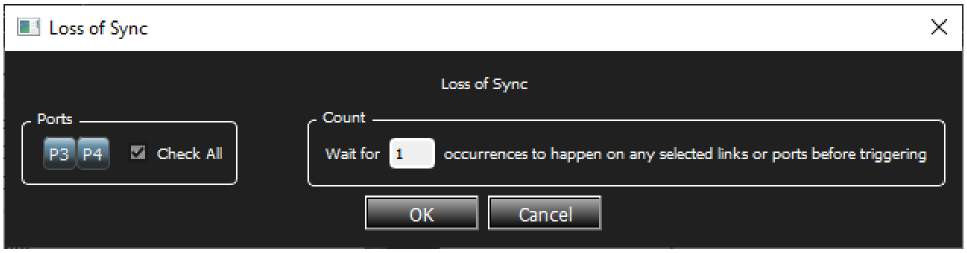


Figure 4.105: Loss of Sync Pattern Dialog Box

2. Click inside the **Check All** box to select all available ports.
3. In the **Count** area, enter the expected number of occurrences.

Symbols

1. Click the arrow next to **Symbols** to expand the list of Symbols patterns.
2. Double-click on the pattern you need.

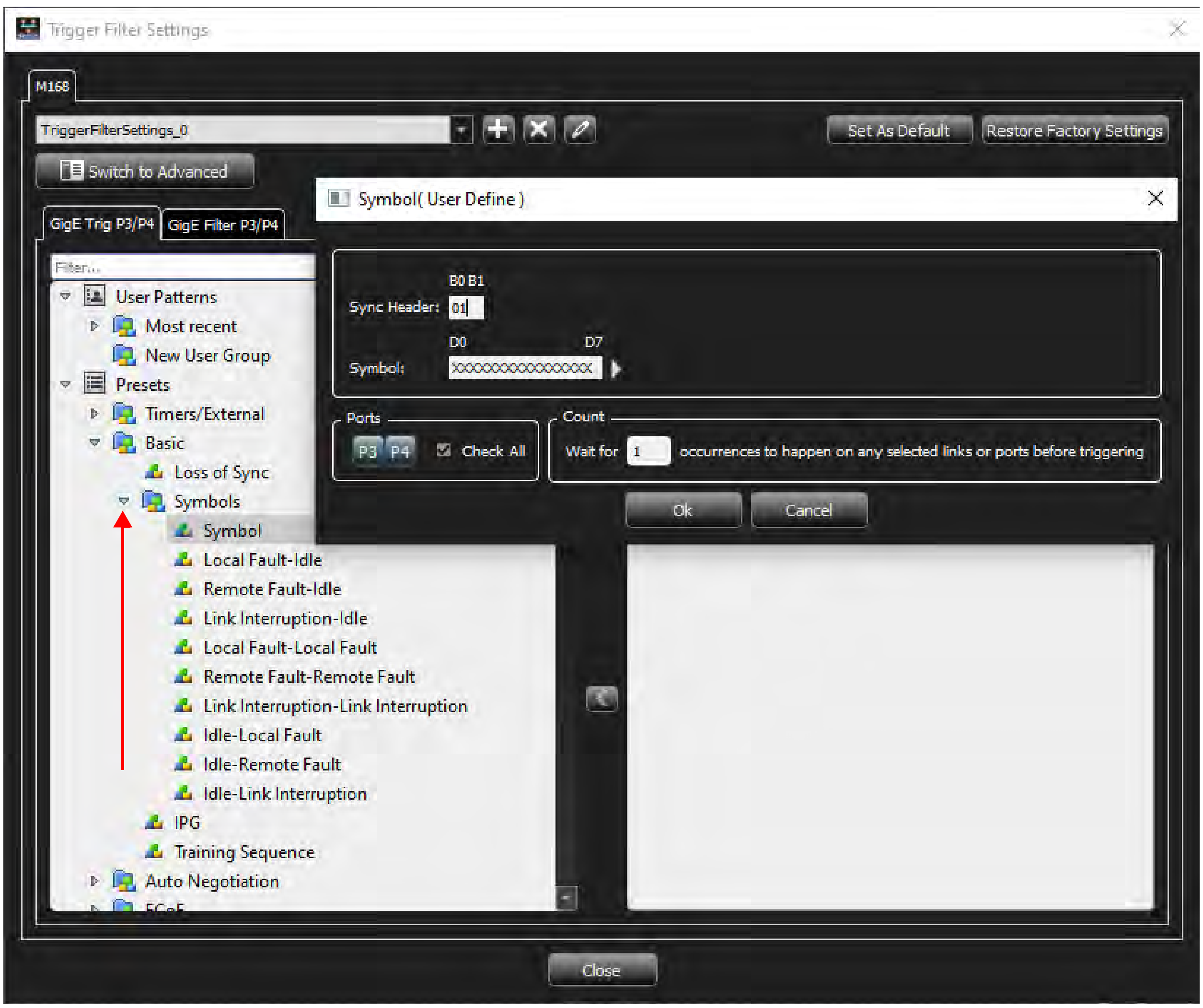


Figure 4.106: Symbols Patterns — Symbol

3. Enter the values for the **Sync Header** and **Symbol**.

4. In the **Ports** area, click inside the box for **Check All** to select all available ports, or use default.
5. Enter the expected number of occurrences in the **Count** field.
6. Click **OK** to add the Pattern.

Two different order sets can exist in one 64 bits payload of a 66 bits block. The six examples of a remote and local fault given below demonstrate how to manually enter ordered set triggers.

- 0x0100000001000055 → local fault-local fault
- 0x000000000100004b → local fault-idle
- 0x010000000000002D → idle-local fault
- 0x0200000002000055 → remote fault-remote fault
- 0x000000000200004b → remote fault-idle
- 0x020000000000002D → idle-remote fault

IPG

1. Double-click **IPG** to open the IPG dialog box.

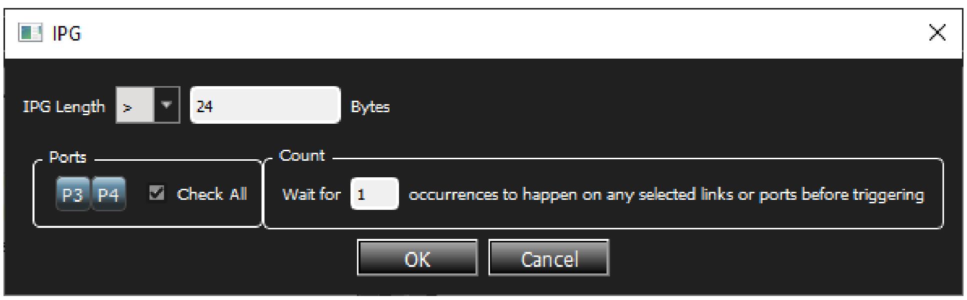


Figure 4.107: IPG Pattern Dialog Box

2. Enter the IPG Length from the drop-down list, Bytes values, and the count of the expected number of occurrences.
3. Check the **Check All** box to select all available ports, or you can individually select ports.

Training Sequence

1. Double-click **Training Sequence** to open the Training Sequence window (Figure 4.108).

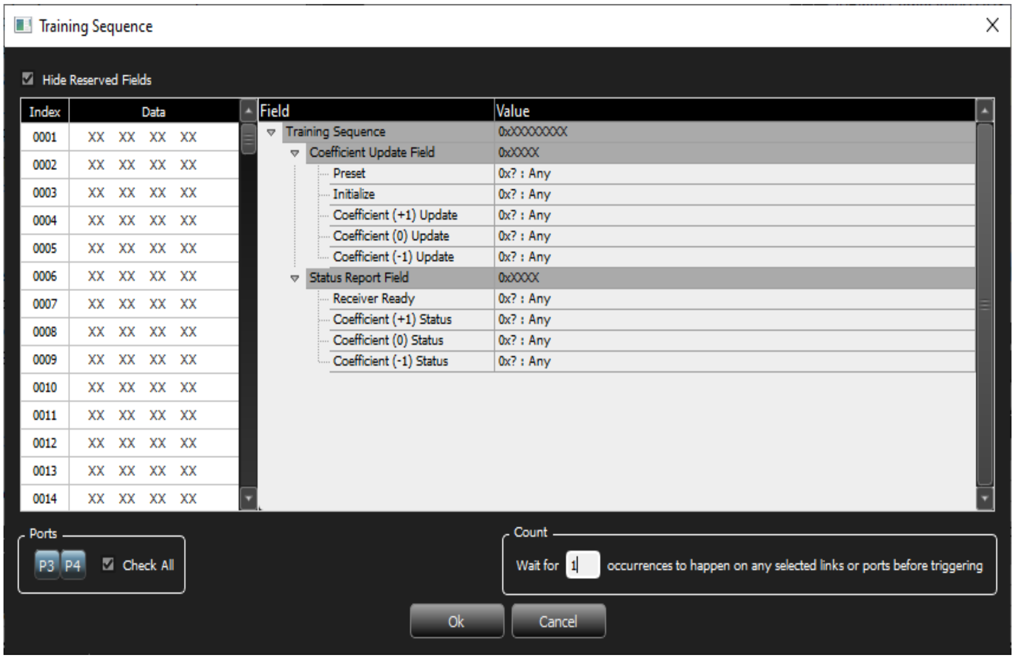


Figure 4.108: Training Sequence Window

2. Enter the values for **Control Field** and **Status Field**, then enter the count for the expected number of occurrences.

3. Click inside the **Check All** box to select all available ports, or individually select ports.

4.2.4.2 Auto Negotiation

1. Click the arrow next to **Auto Negotiation** to expand the list of Auto Negotiation patterns.

2. Double click on the pattern you need (Figure 4.109).

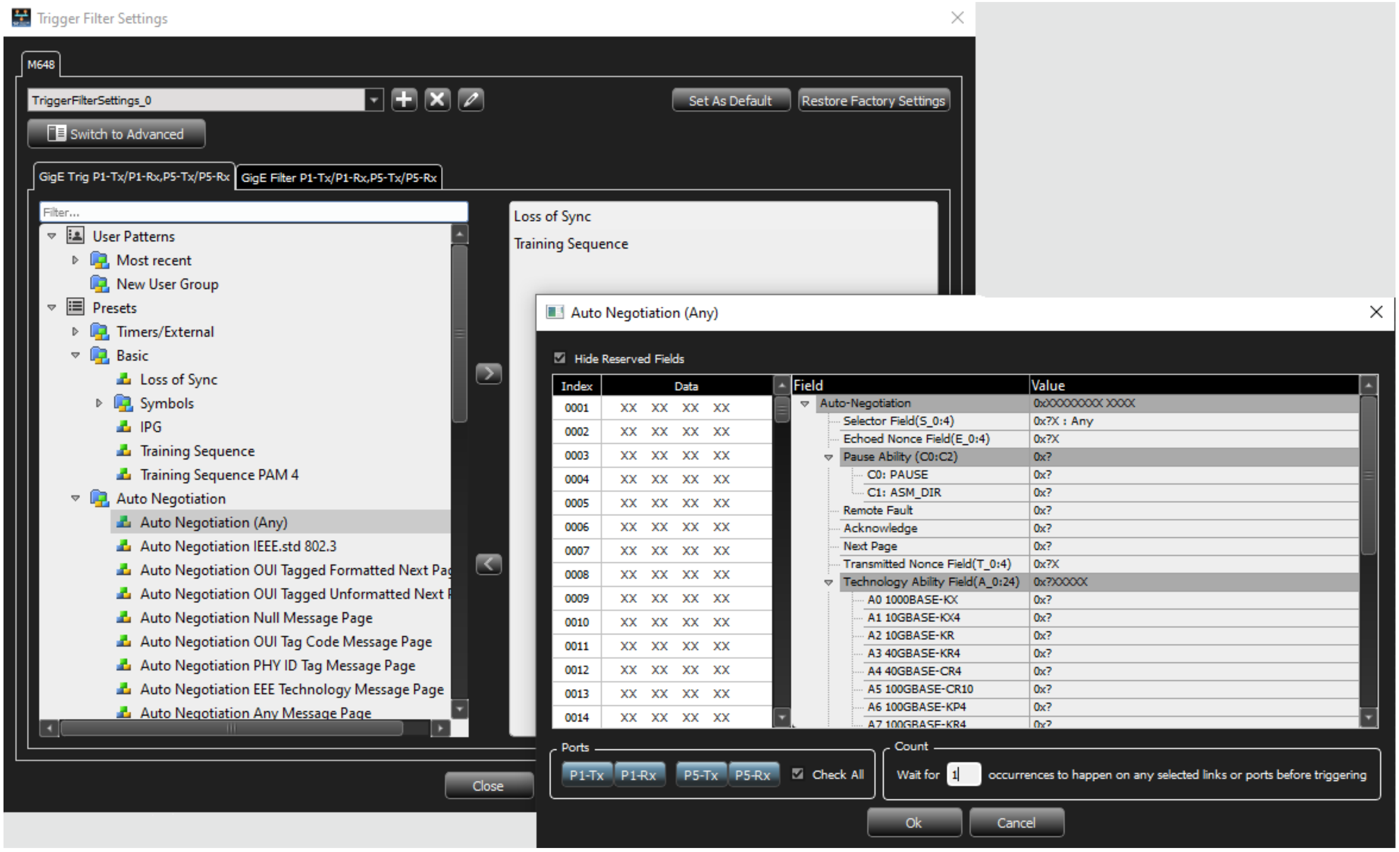


Figure 4.109: Example Auto Negotiation Patterns with Auto Negotiation (Any) Selected

3. Enter the values for the fields as appropriate.
4. Enter the expected number of occurrences.
5. Click inside the **Check All** box to select all available ports, or individually select ports.

4.2.4.3 FCoE Patterns

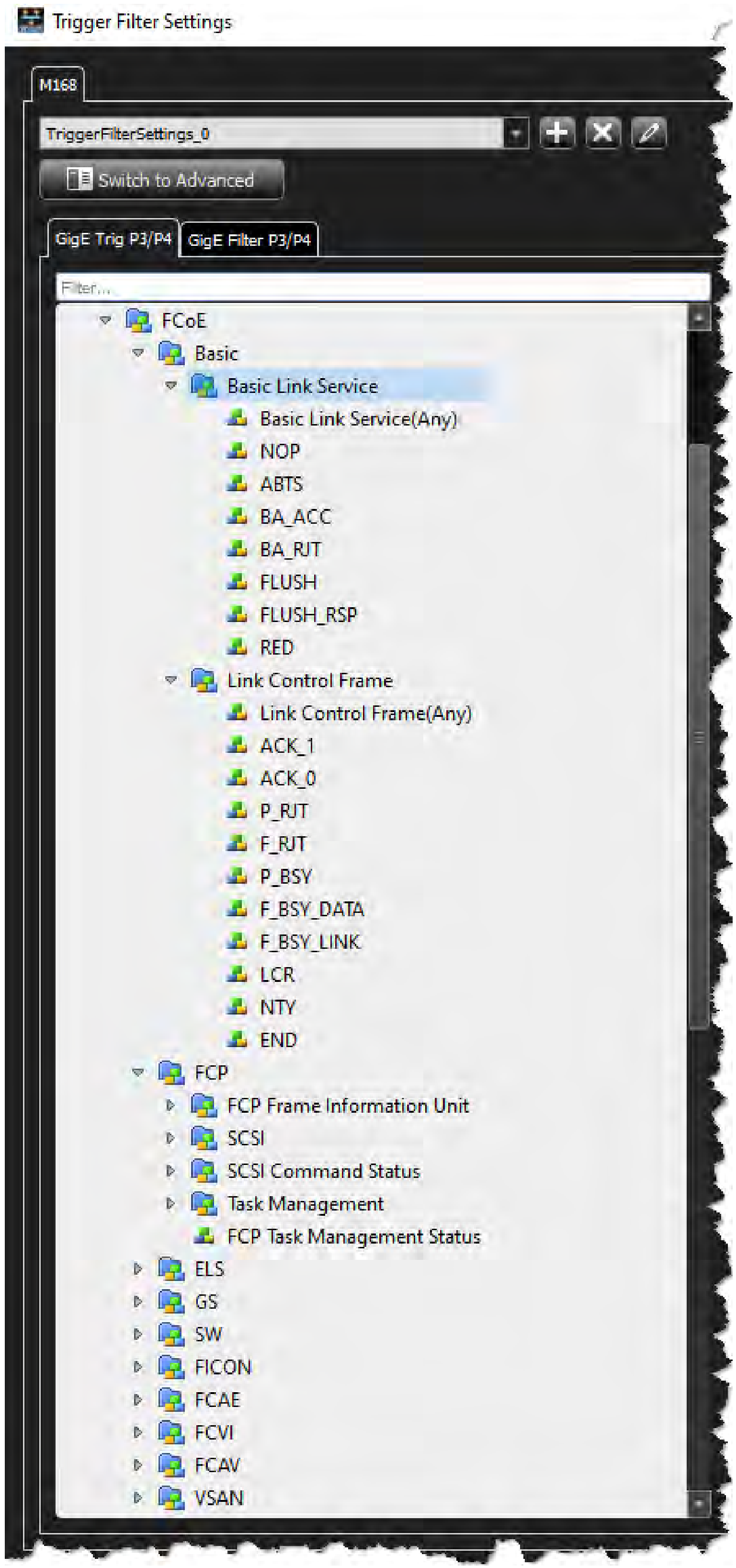


Figure 4.110: FCoE Trigger Filter Patterns

Basic

Basic Link Service

For any Ethernet pattern, double-click the pattern name.

Click the arrow next to **Basic Link Service** to expand the list of patterns.

NOTE: Some screen captures for the Ethernet patterns are similar to the screen capture shown below.

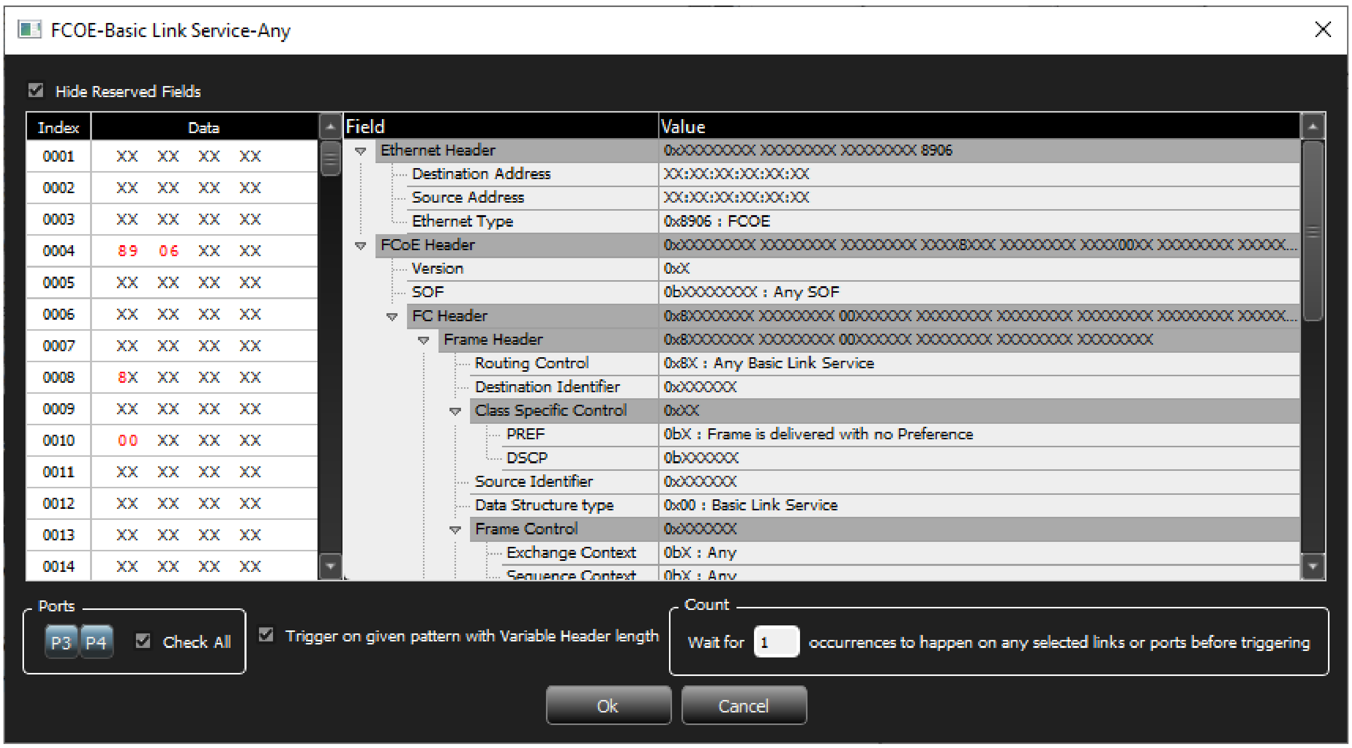


Figure 4.111: Basic Link Service Pattern Window

Enter the values for the Ethernet header, FCoE header, Frame header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Check the **Trigger on given pattern with variable header length** box to automatically adjust the offset, if optional headers like VLAN tag, VNTag, etc. are present. Uncheck it, to trigger for a pattern at a specific offset from the start of the frame.

NOTE: Some patterns have additional options to select from drop-drown lists as shown in the figure above.

Link Control Frame

For any FCoE pattern, double-click the pattern name; for example, double-click **Basic Link Service** to open the Basic Link Service Pattern window.

NOTE: Some screen captures for the FCoE patterns are similar to the screen capture shown below.

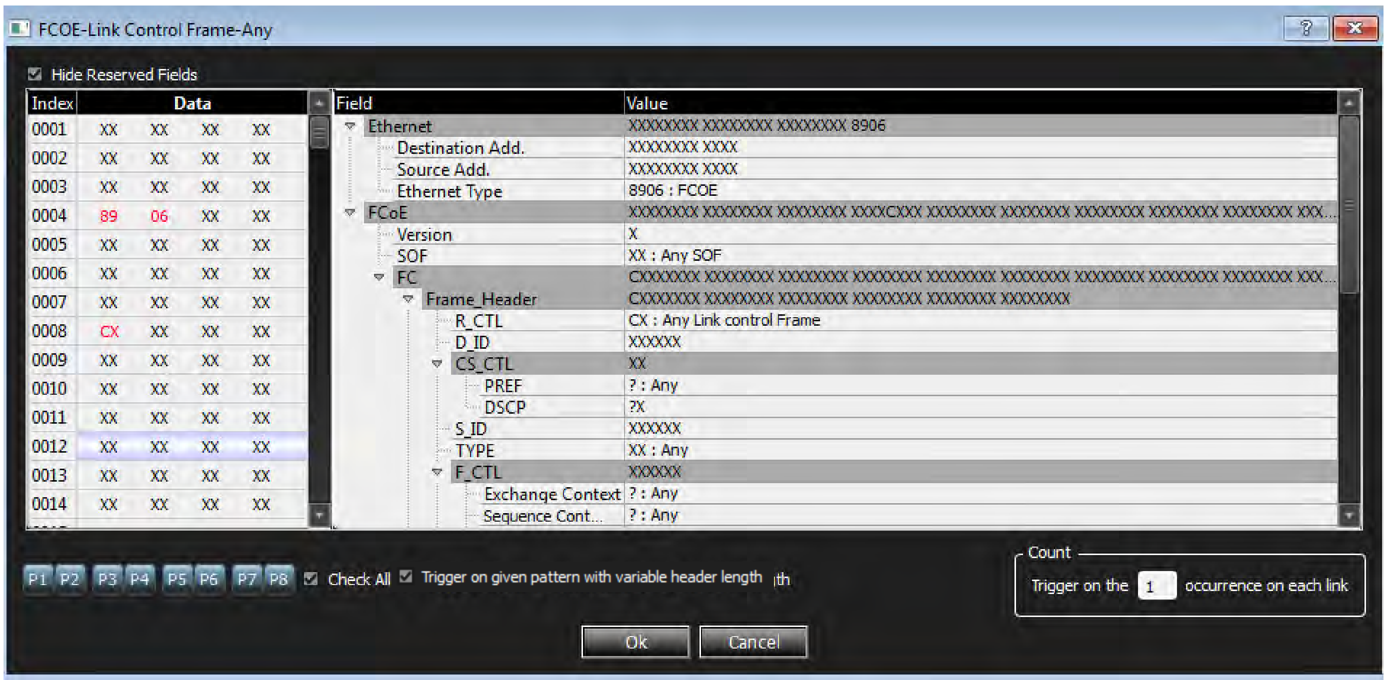


Figure 4.112: Link Control Frame Pattern Window

Enter the values for the Ethernet header, FCoE header, Frame header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Check the **Trigger on given pattern with variable header length** box to automatically adjust the offset, if optional headers like VLAN tag, VNTag, etc. are present. Uncheck it, to trigger for a pattern at a specific offset from the start of the frame.

The following additional Ethernet patterns are available:

FCP Patterns

Frame Information Unit

SCSI

Any SCSI Command

- 6-Byte Any SCSI Cmd
- 10-Byte Any SCSI Cmd
- 12-Byte Any SCSI Cmd
- 16-Byte Any SCSI Cmd

- Long LBA 16-Byte Any SCSI Cmd
- Variable Length Any SCSI Cmd
- Variable Length for Long LBA 32-Byte Any SCSI Cmd
  - SPC4
  - SBC3
  - MMC6
  - SMC2
  - SSC (see Table 4.5 for latest version of SSC supported)
  - OSD2
  - ADC3

FCP Task Management

ELS Patterns

ELS Request

ELS Reply

GS Patterns

Generic Link Service-Request

GS Reply

- GS_RJT
- GS Accept
  - FC-SW-5
  - Event Service
  - Key Distribution Service
  - Alias Service
  - Management Service
    - Fabric Configuration Service
    - Unzoned Name Server
    - Fabric Zone Server
    - Reserved for Performance Server
    - Security Policy Server
    - Security Information Server
    - Fabric Device Management Server
  - Time Service
  - Directory Service
    - Name Server
    - Directory Service - FC-4 Specific Servers

SW Patterns

SW Request

SW Reply

FICON Patterns

FCAE Patterns

FCAE_ASM

FCAE-1553

FCVI Patterns

FCAV Patterns

VSAN Patterns

(all FC patterns listed above are available under VSAN as well)

4.2.4.4 FIP Patterns

For any FIP pattern, double-click the pattern name, for example, double-click **Discovery Solicitation from ENode** to open the window.

> **NOTE:** All the screen captures for the FIP patterns are similar to the screen capture shown below.

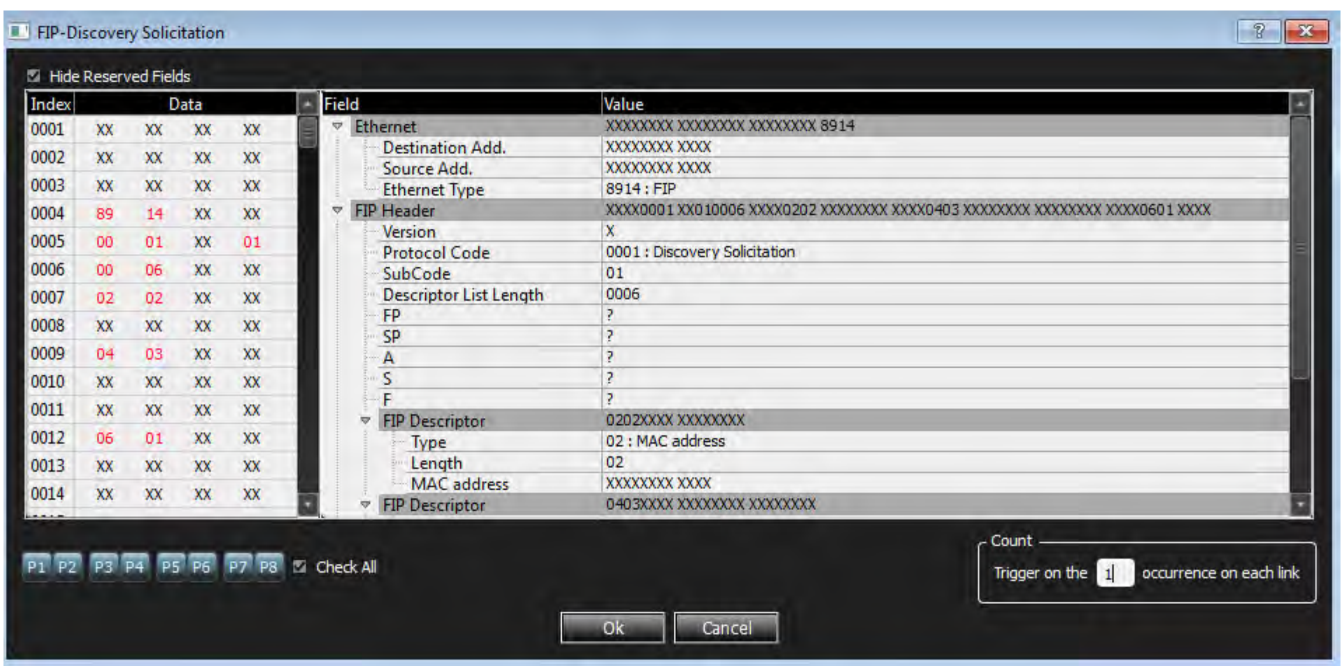


Figure 4.113: FIP Discovery Solicitation from ENode Pattern Window

Enter the values for the Ether header, FIP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

The following FIP patterns are available:

- Discovery Solicitation from ENode

- Discovery Solicitation from FCF
- Discovery Advertisement
- FIP FLOGI Request
- FIP FLOGI LS_ACC
- FIP FLOGI LS_RJT
- FIP NPIV FDISC Request
- FIP NPIV FDISC LS_ACC
- FIP NPIV FDISC LS_RJT
- FIP Fabric LOGO
- FIP Fabric LOGO LS_ACC
- FIP Fabric LOGO LS_RJT
- FIP ELP Request
- FIP ELP SW_ACC
- FIP ELP SW_RJT
- FIP Keep Alive
- FIP Clear Virtual Links-5DWORD Descriptor
- FIP VLAN Request-2DWORD Descriptor
- FIP VLAN Notification

4.2.4.5 MPCP Pattern

Double-click **Multi control Protocol Frame** to open the window.

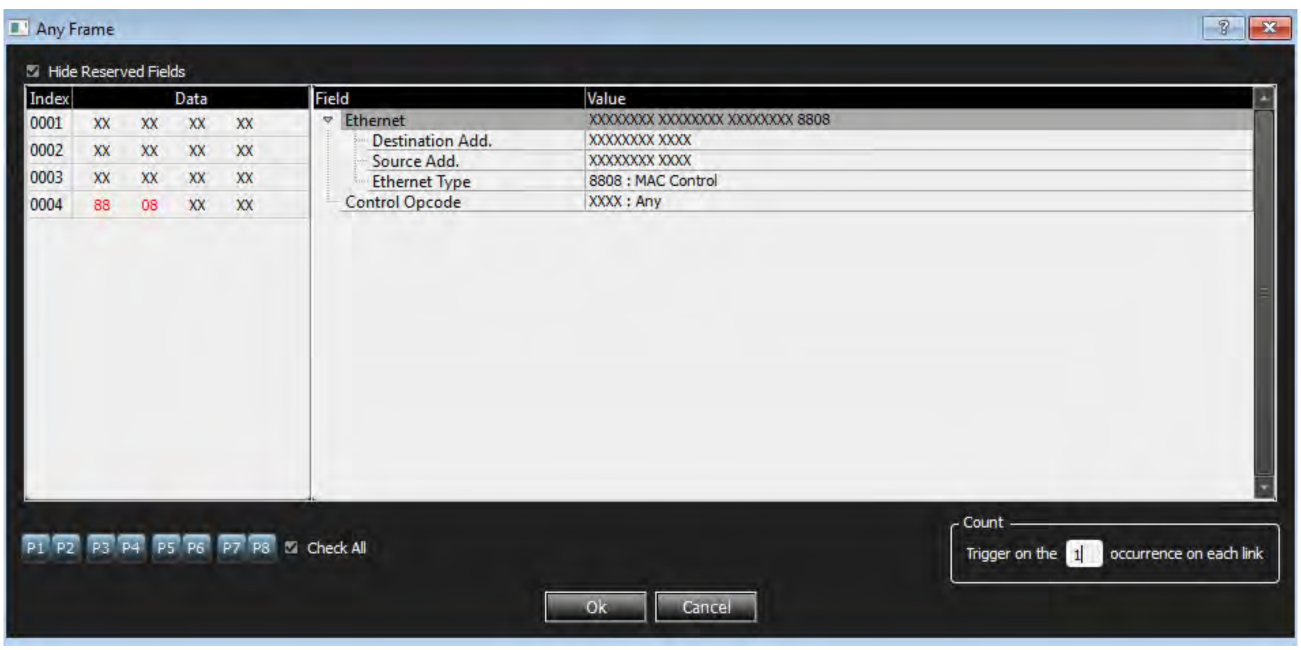


Figure 4.114: Multi control Protocol Frame Pattern Window

Enter the values for the Ether header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.4.6 Address Resolution Protocol Pattern

Double-click **Address Resolution Protocol** to open the window.

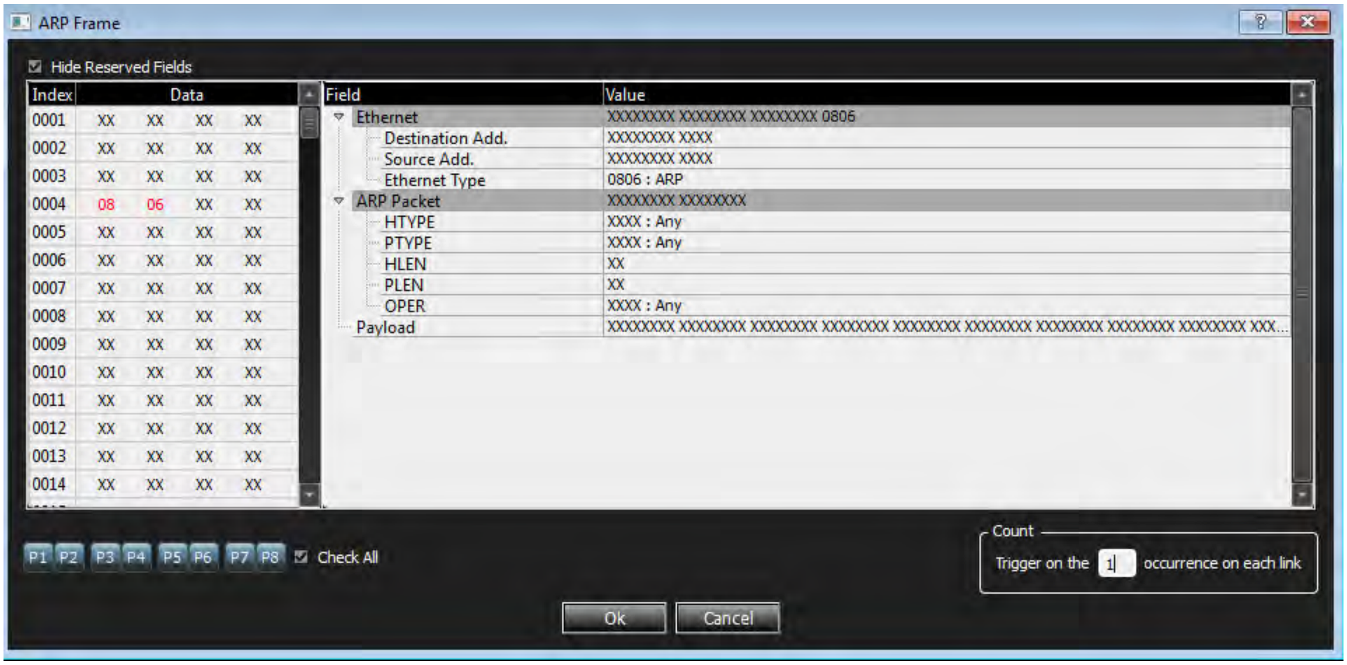


Figure 4.115: ARP Frame Window

Enter the values for the Ether header, ARP Event and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.4.7 Link Layer Discovery Protocol Pattern

Double-click **LLDP Frame** to open the window.

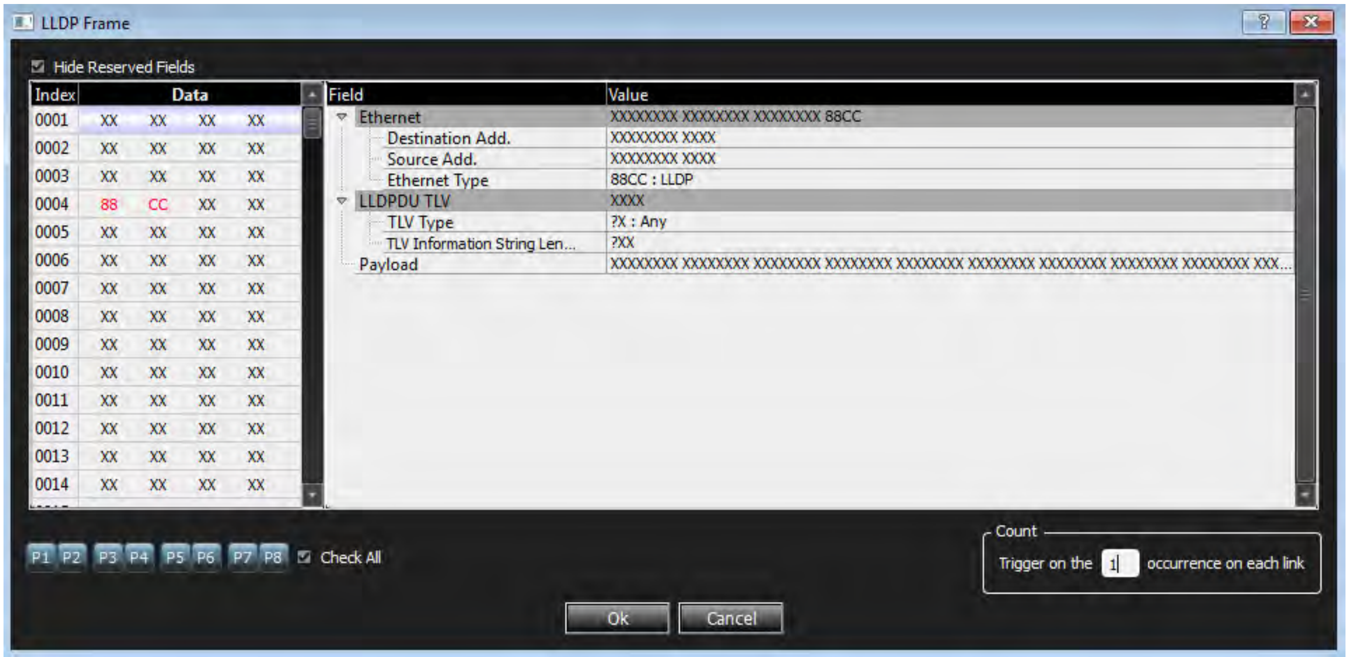


Figure 4.116: LLDP Frame Window

Enter the values for the Ether header, LLDPDU TLV and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.4.8 Internet Protocol Pattern

Double-click **Any IP Frame** to open the window.

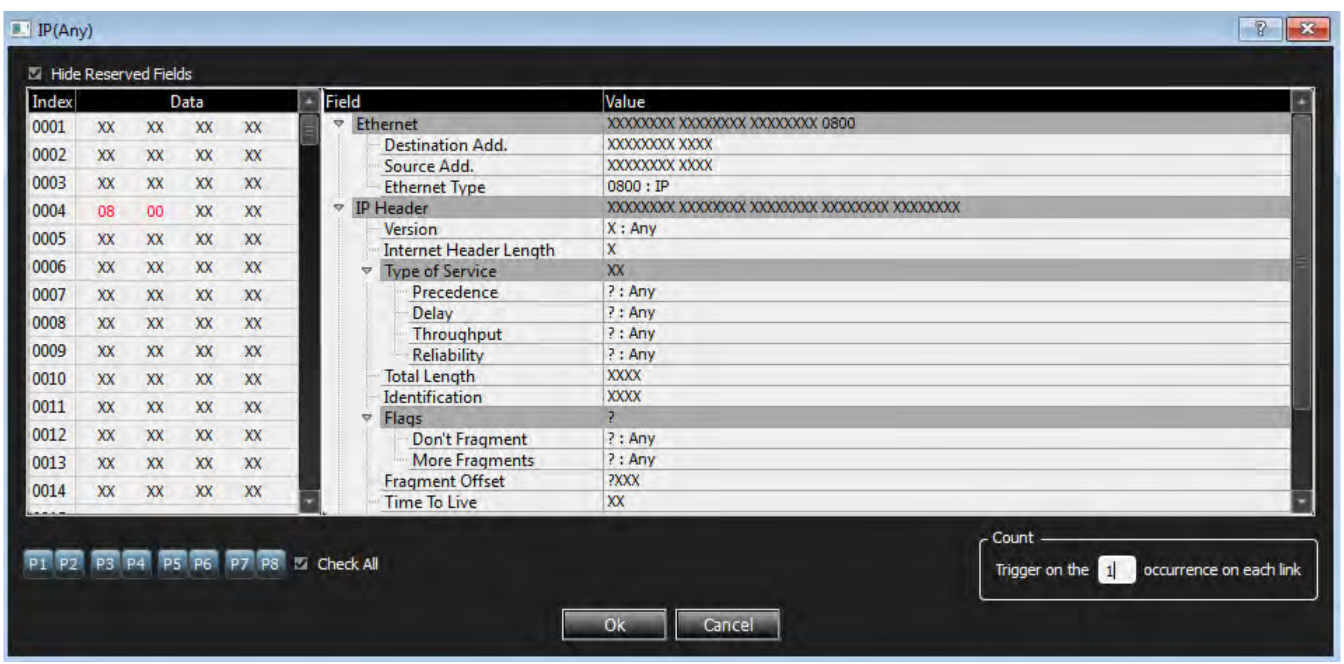


Figure 4.117: IP Frame Window

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other Internet Protocol patterns available are:

- IP Frame (ICMP)
- IP Frame (IGMP)
- IP Frame (IPV6)
- IP Frame (OSPF)
- IP Frame (AH)
- IP Frame (ESP)
- IP Frame (PIM)
- IP Frame (UDP)
- IP Frame (TCP)

4.2.4.9 iSCSI Pattern

Initiator PDU

Double-click **iSCSI Data-Out** to open the window.

Figure 4.118: iSCSI Data-Out Window

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other ISCSI patterns available are:

- iSCSI Login Request
- iSCSI Logout Request

- iSCSI NOP-Out
- iSCSI SNACK Request
- iSCSI Task Mgmt Request
- iSCSI Text Request

Target PDU

The dialogs are similar to the Initiator PDU above. The patterns available are:

- iSCSI Asynchronous Message
- iSCSI Response
- iSCSI Data-In
- iSCSI Login Response
- iSCSI Logout Response
- iSCSI Nop-In
- iSCSI Ready to Transfer
- iSCSI Reject
- iSCSI Task Mgmt Request
- iSCSI Text Request

ISCSI Cmd

Any SCSI Command

Double-click **6-Byte Any SCSI Cmd** to open the window.

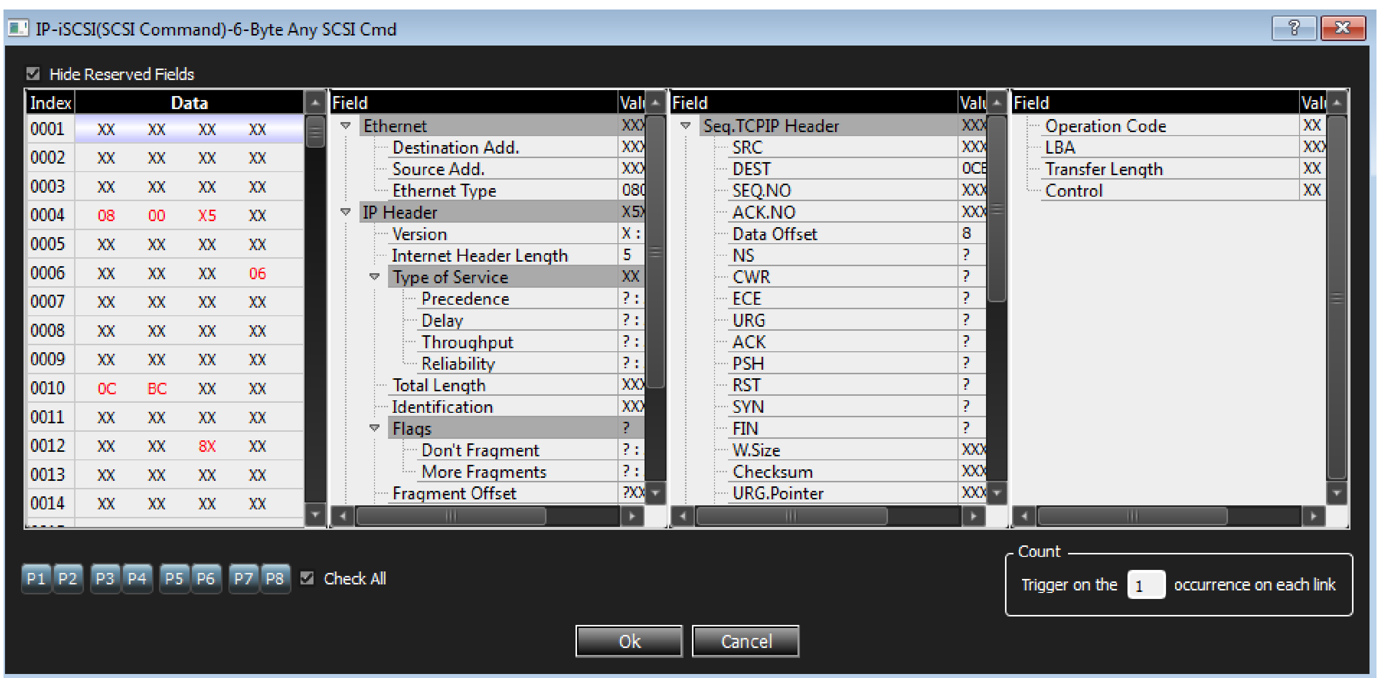


Figure 4.119: 6-Byte Any SCSI Cmd Window

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other ISCSI patterns available are:

- 10-Byte Any SCSI Cmd
- 12-Byte Any SCSI Cmd
- 16-Byte Any SCSI Cmd
- Long LBA16-Byte Any SCSI Cmd
- Variable Length Any SCSI Cmd
- Variable Length For Long LBA 32-Byte Any SCSI Cmd
  - SPC4
  - SBC3
  - MMC6
  - SMC2
  - SSC (see Table D.1 for latest version of SSC supported)
  - OSD2
  - ADC3

4.2.4.10 iWARP Patterns

You may set patterns for the following iWARP RDMA operations:

- Write
- Read Request
- Read Response
- Send
- Send with Invalidate
- Send with SE
- Send with SE and Invalidate
- Terminate

4.2.4.11 VLAN Patterns

All Ethernet Patterns are available as VLAN Patterns as well. The only difference is that the Ethernet Type of the Ethernet header will be preset to “VLAN”, and you should specify the VLAN id value in the VLAN Tag header.

4.2.4.12 VXLAN Patterns

All Ethernet Patterns are available as VXLAN Patterns as well. The only difference is that the frame will be preset as an IP/UDP frame with the UDP destination port set to “VXLAN”, and you should specify the VXLAN Network Id in the VXLAN header.

4.2.4.13 NVGRE Patterns

All Ethernet Patterns are available as NVGRE Patterns as well. The only difference is that the frame will be preset as an IP frame with “GRE” protocol, and a GRE Header will be added set to “NVGRE” protocol type.

4.2.4.14 ISL Patterns

FCoE

All the ISL FCoE patterns are similar to Ethernet patterns. Refer to 4.2.4.3, *FCoE Patterns*.

FIP

All the ISL FIP patterns are similar to FIP patterns. Refer to 4.2.4.4, *FIP Patterns*.

MPCP

All the ISL MPCP patterns are similar to MPCP patterns. Refer to 4.2.4.5, *MPCP Pattern*.

Address Resolution Protocol

The ISL Address Resolution Protocol pattern is similar to Address Resolution Protocol pattern. Refer to 4.2.4.6, *Address Resolution Protocol Pattern*.

Link Layer Discovery Protocol

The ISL Link Layer Discovery Protocol pattern is similar to Link Layer Discovery Protocol pattern. Refer to 4.2.4.7, *Link Layer Discovery Protocol Pattern*.

ISL Internet Protocol

All the ISL Internet Protocol patterns are similar to Internet Protocol patterns. Refer to 4.2.4.8, *Internet Protocol Pattern*.

iSCSI Pattern

All the ISL ISCSI patterns are similar to ISCSI patterns. Refer to 4.2.4.9, *iSCSI Pattern*.

Initiator PDU

See *Initiator PDU*.

Target PDU

See *Target PDU*.

iSCSI Cmd

See *ISCSI Cmd*.

NOTE: For all ISL patterns enter a value for the ISL Header.

InfiniBand Over Ethernet (IBXoE)

See 4.2.4.18, *InfiniBand Over Ethernet (IBXoE)*.

4.2.4.15 CN Tag Patterns

All the CN Tag patterns are similar to Ethernet patterns. Refer to 4.2.4.3, *FCoE Patterns*.

NOTE: For all CN Tag patterns enter a value for CN Tag.

4.2.4.16 VN Tag Patterns

All the VN Tag patterns are similar to Ethernet patterns. Refer to 4.2.4.3, *FCoE Patterns*.

NOTE: For all VN Tag patterns enter a value for VN Tag.

4.2.4.17 LLC

LLC-IEEE802.1D Frame

Double-click **LLC-IEEE802.1D** Frame to open the window.

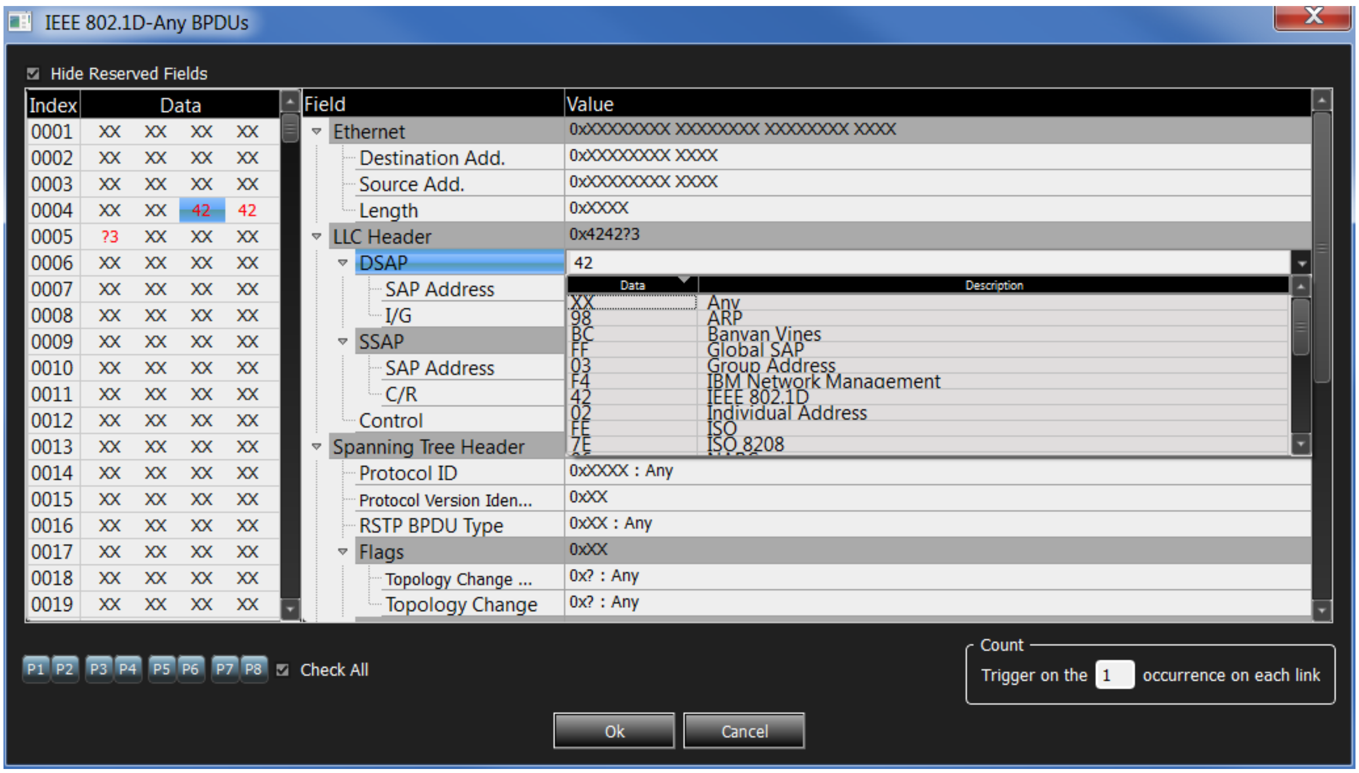


Figure 4.120: LLC-IEEE802.1D Window

Enter the values for the Ethernet, LLC Header, Spanning Tree Header, GARP Header and select an option from the DSAP and SSAP pull -down menus. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other LLC-IEEE802.1D patterns available are:

- Bridge Protocol Data Unit (BPDU)
- Configuration BPDUs
- Multiple Spanning Tree BPDUs (MSTP)
- Rapid Spanning Tree BPDUs (RSTP)
- Topology Change Notification BPDU (TCNP)
- GARP Multicast Registration Protocol (GMRP)
- GARP VLAN Registration Protocol (GVRP)
- Generic Attribute Registration Protocol (GARP)

4.2.4.18 InfiniBand Over Ethernet (IBXoE)

Double-click **InfiniBand Over Ethernet (IBXoE)** to open the IBXoE Frame window.

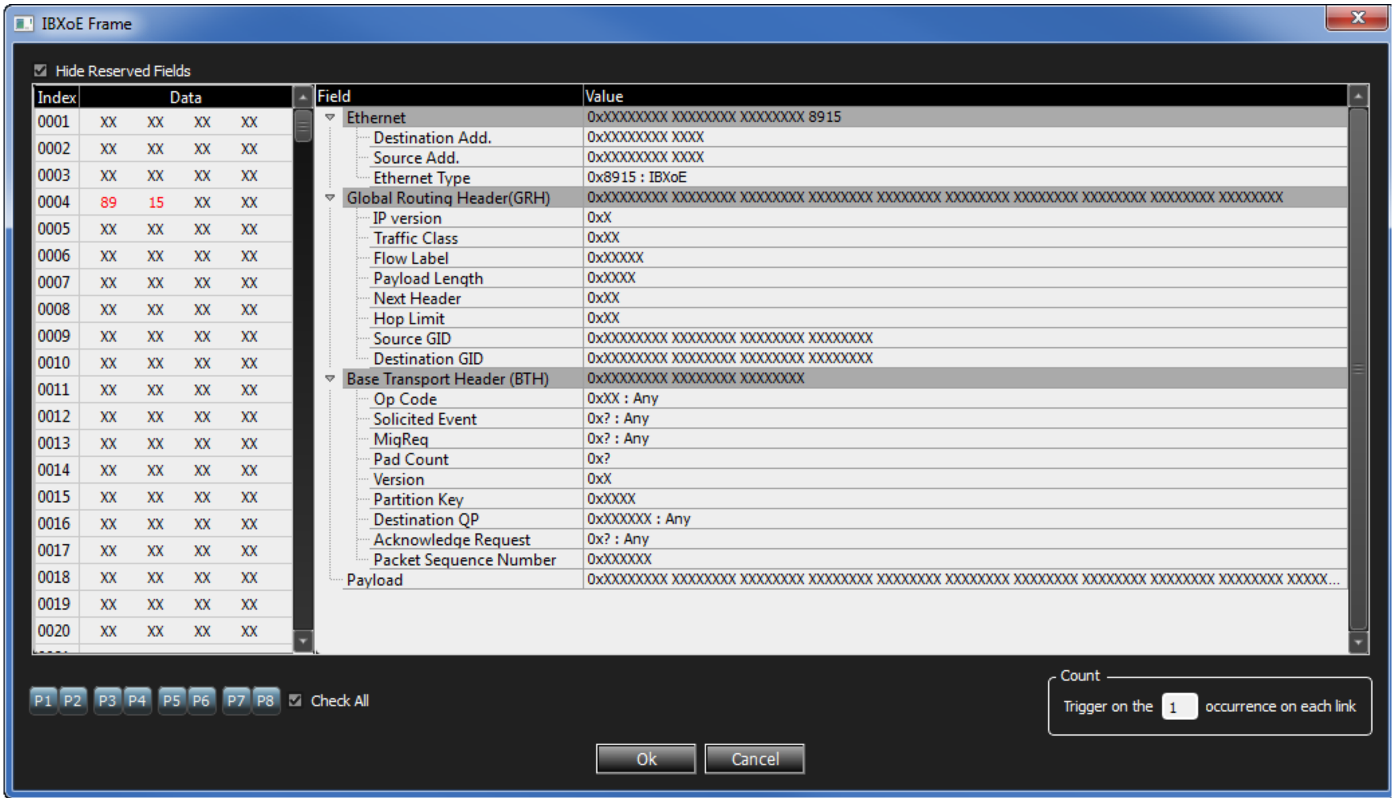


Figure 4.121: IBXoE Frame Window

Enter the values for the Ethernet header, Global Routing Header (GRH), Base transport header (BTH) and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

InfiniBand Over Ethernet: RDMA and NVMe Triggers

RDMA and NVMe events can also be set as triggers. See Figure 4.122.

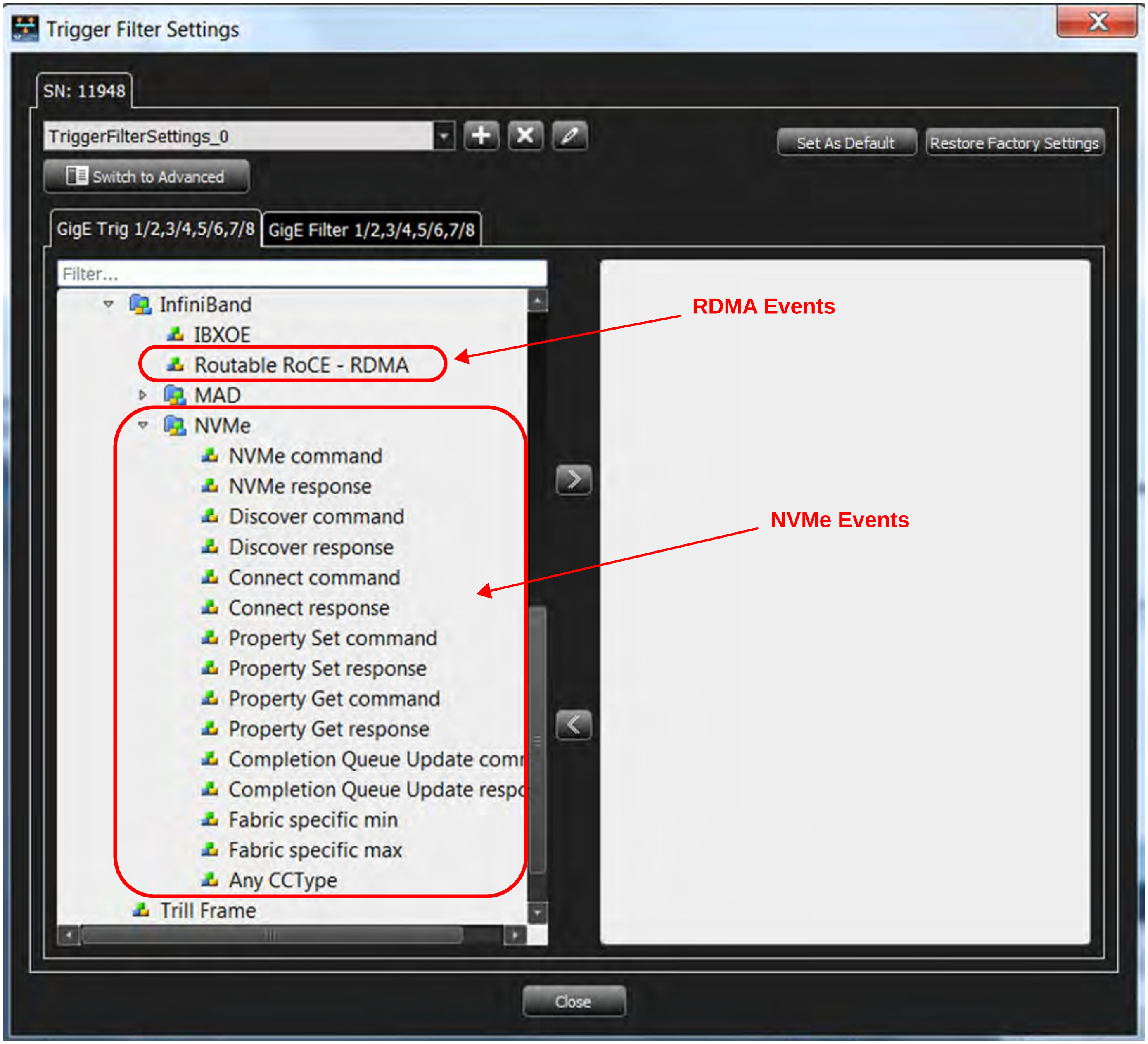


Figure 4.122: Triggering on RDMA or NVMe Events

The Routable RoCE – RDMA triggering menu is shown in Figure 4.123. A typical NVMe event triggering menu for commands is shown in Figure 4.124.

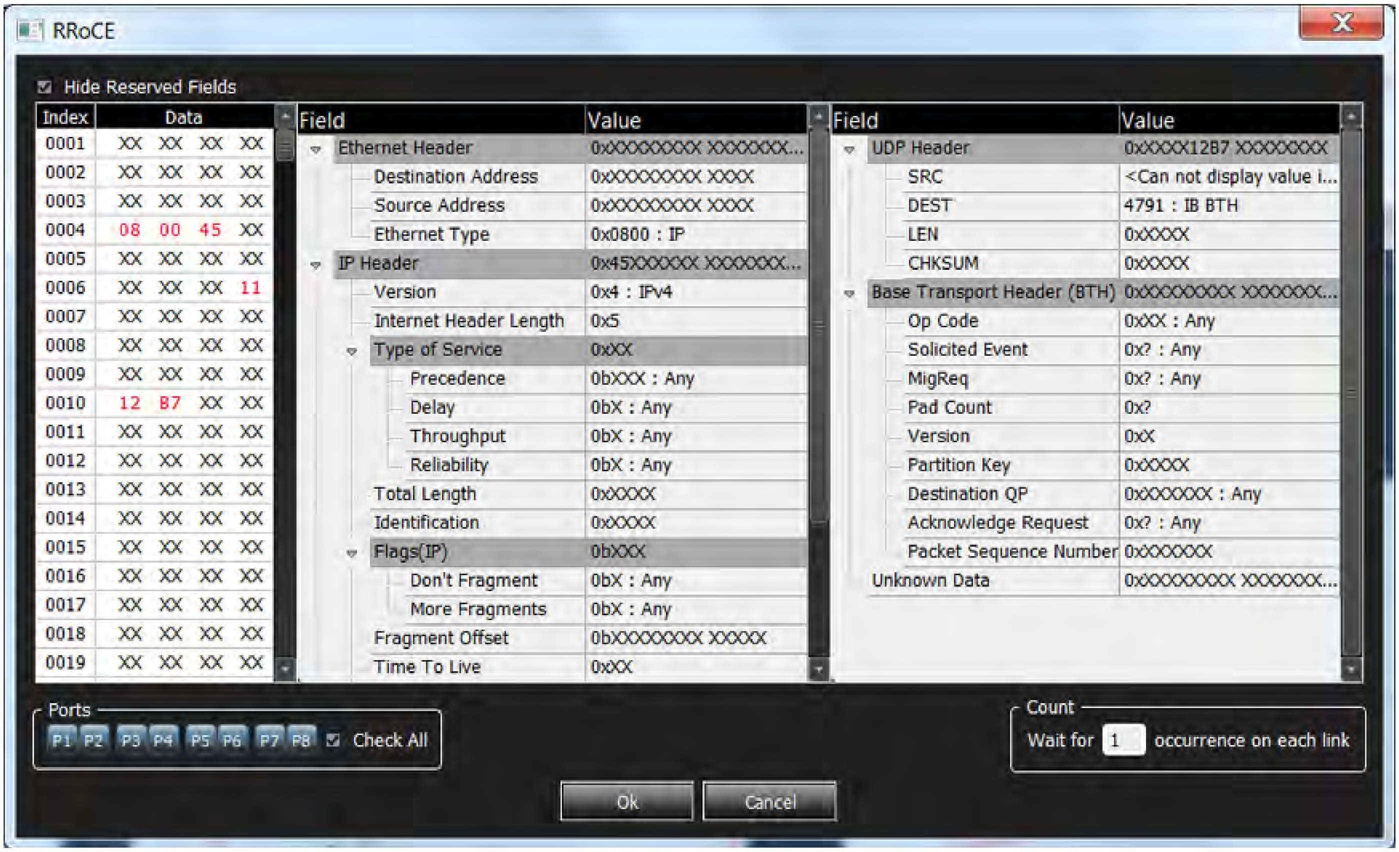


Figure 4.123: Routable RoCE – RDMA Triggering Menu

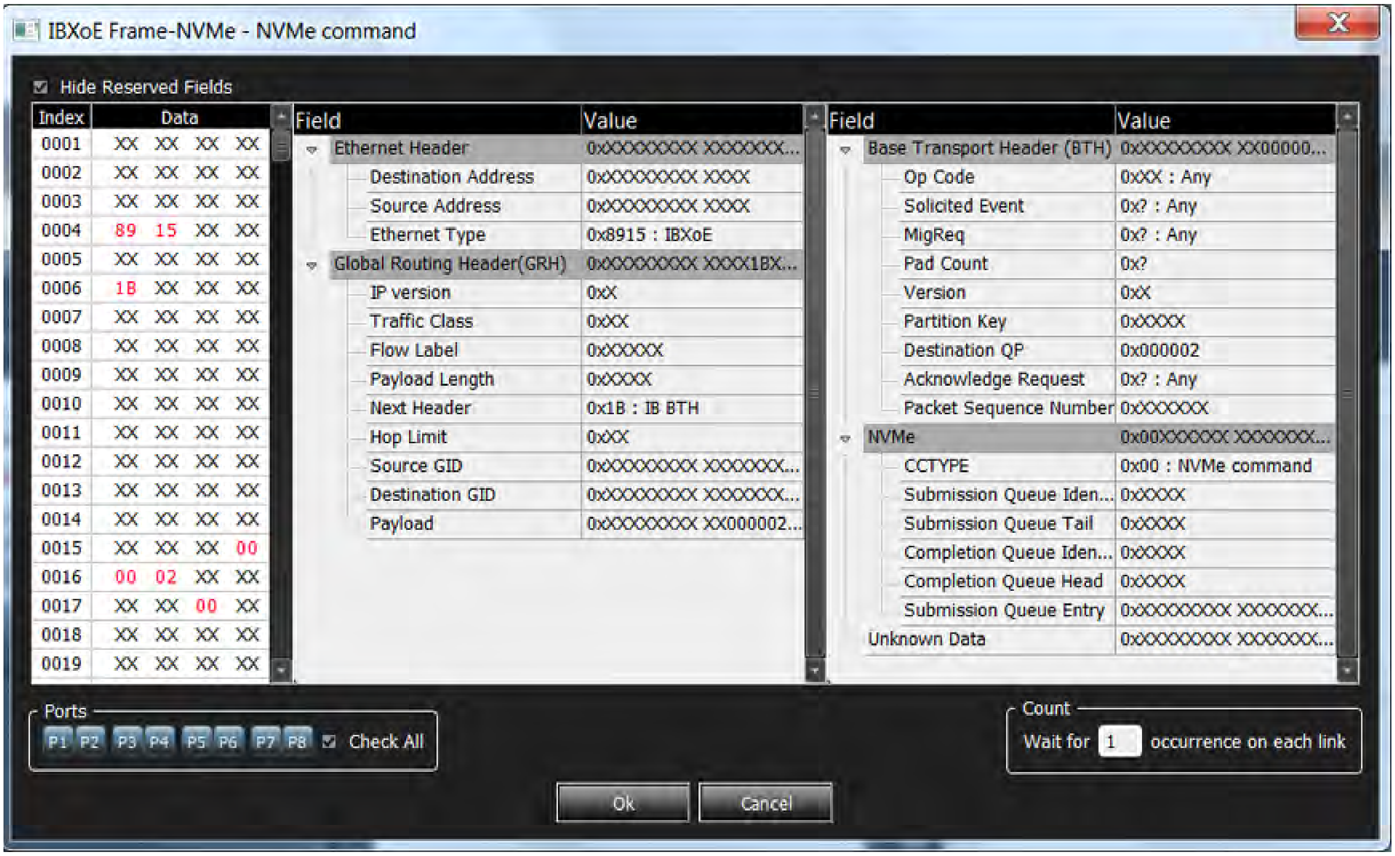


Figure 4.124: NVMe Trigger Menu

4.2.4.19 Trill Frame

Double-click **Trill Frame** to open the window.

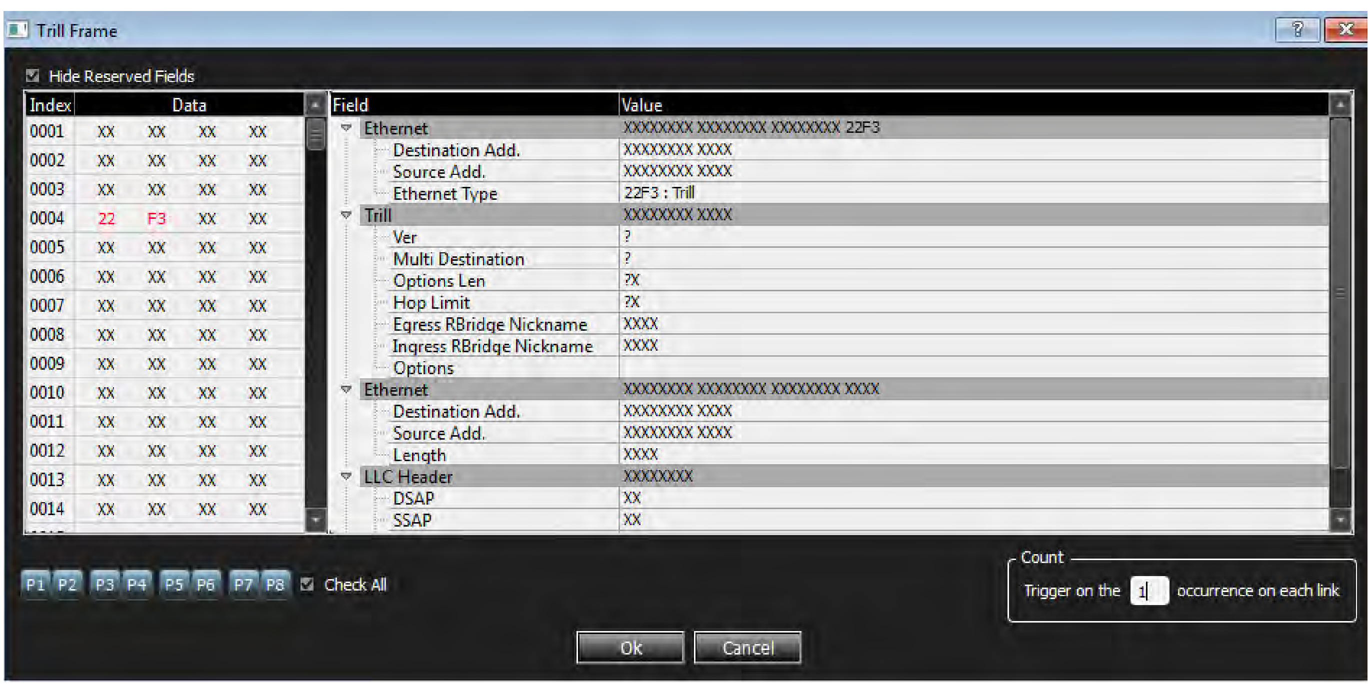


Figure 4.125: Trill Frame Window

Enter the values for the Ethernet header, Trill and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.4.20 Protocol Errors

Double-click **Protocol Errors** to open the window.

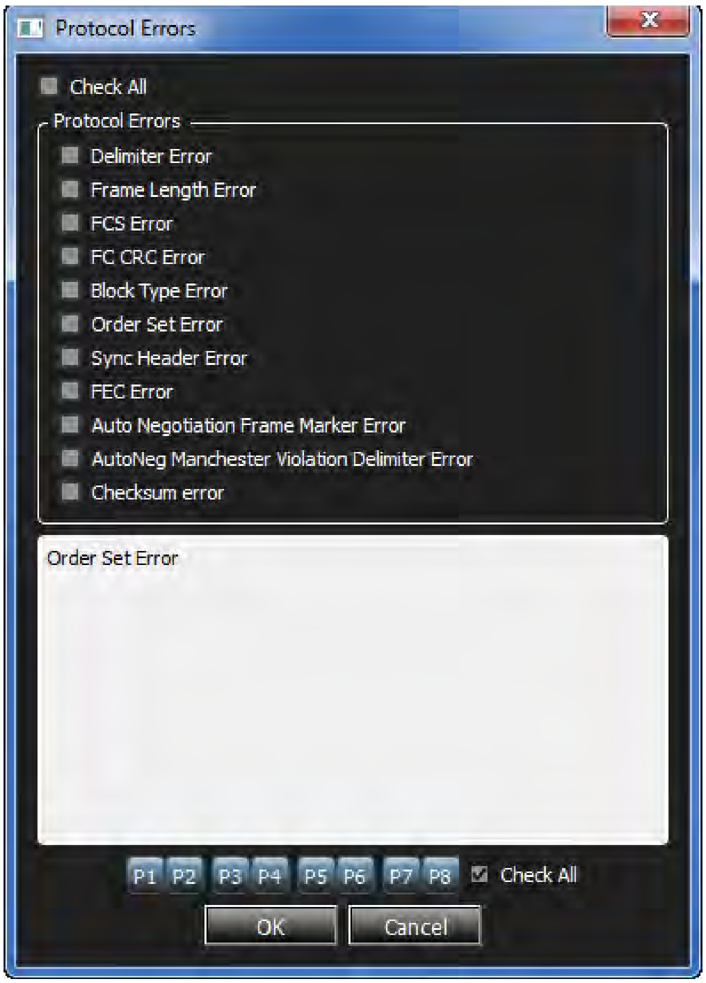


Figure 4.126: Protocol Errors Window

Select the protocol errors or click on the **Check All** box to select all. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.4.21 Any Ethernet Frame

Double-click **Any Ethernet Frame** to open the window.

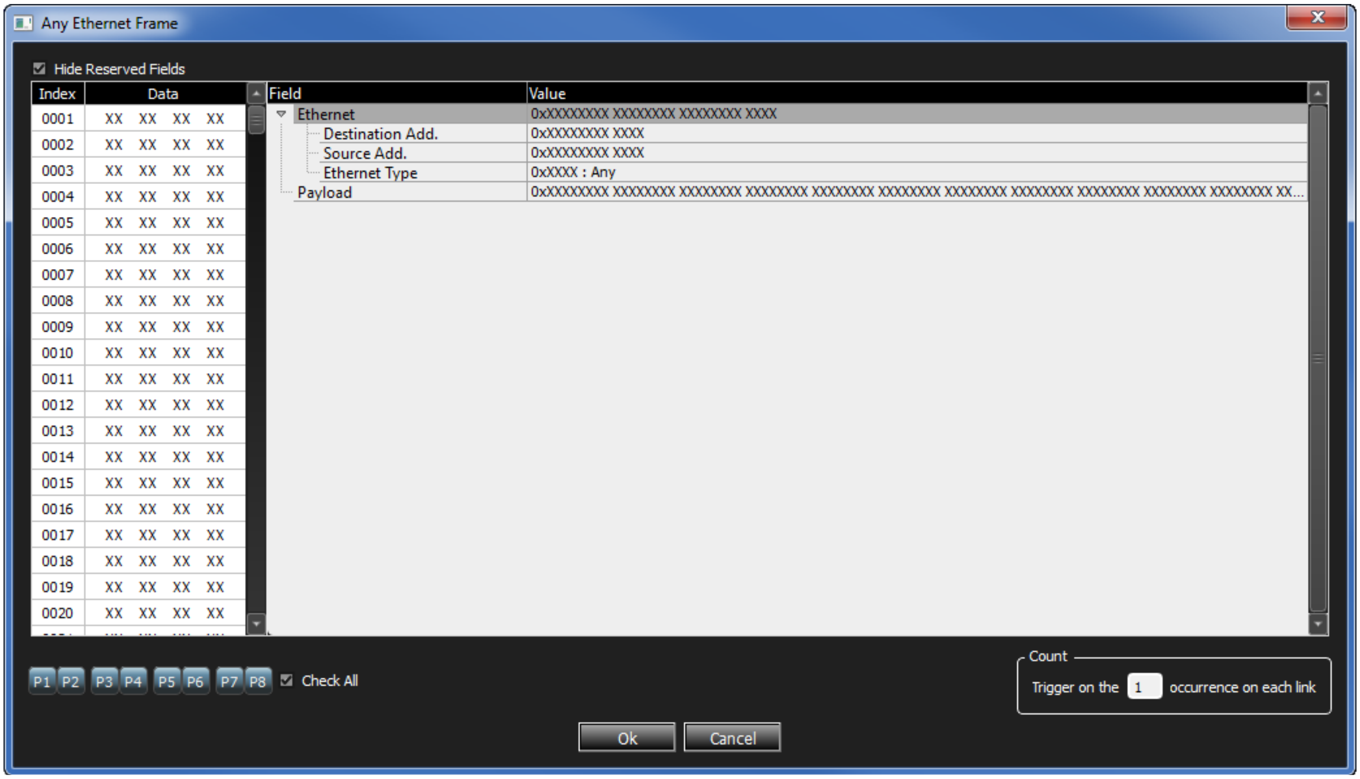


Figure 4.127: Any Ethernet Frame Window

Enter the values for the Ether header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.2.5 FC Patterns (Easy Mode)

4.2.5.1 Basic Patterns

Connect/Disconnect

1. Double-click **Connect/Disconnect** to open the **Connect/Disconnect** dialog box (Figure 4.128).

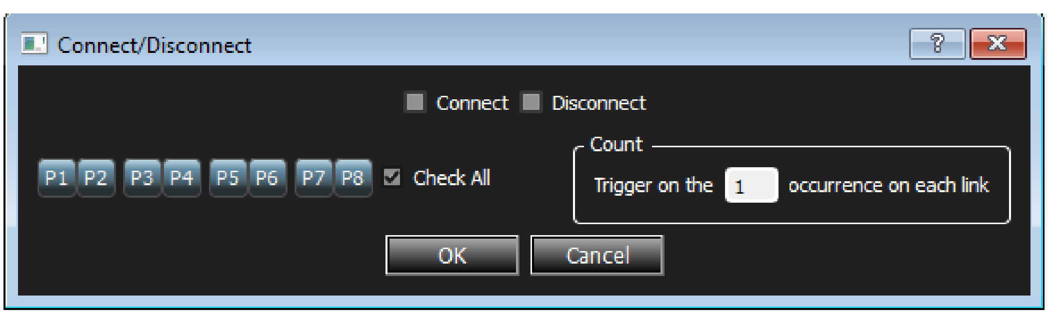


Figure 4.128: Connect/Disconnect Dialog Box

2. Select **Connect/Disconnect** and the count of the expected number of occurrences.
3. Select the **Check All** box to select ports P1 through P8 or individually select ports.
4. Click **OK**.

Ordered Set

1. From the *Trigger Filter Settings* window, double-click **Ordered Set**. This opens the **Order Set** dialog box.

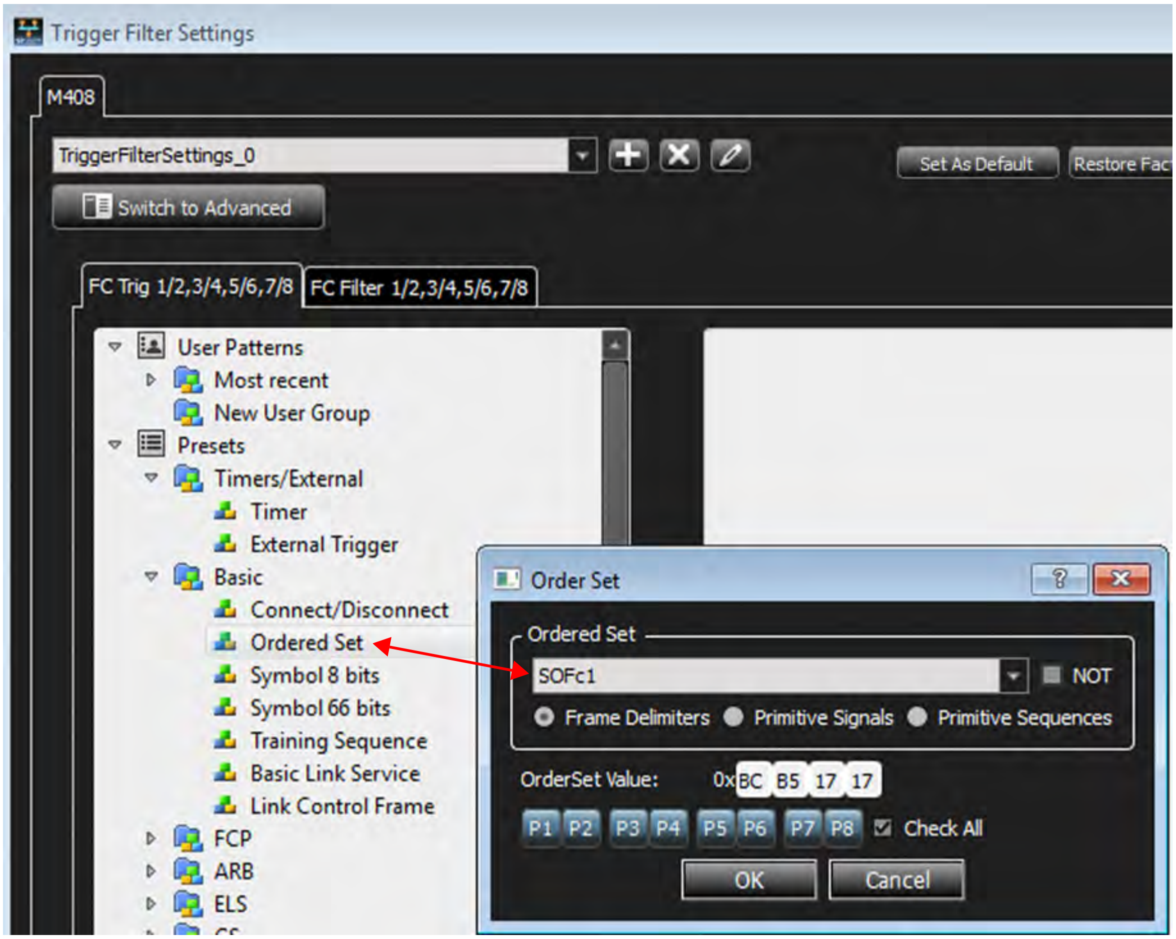


Figure 4.129: Order Set Pattern Dialog Box

Select the values for the Ordered Set from the drop-down list. Select Frame Delimiters, Primitive Signals and Primitive Sequences as applicable. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Symbol 8 Bits

Double-click **Symbol 8 bits** to open the Symbol 8G Pattern dialog box (Figure 4.130).

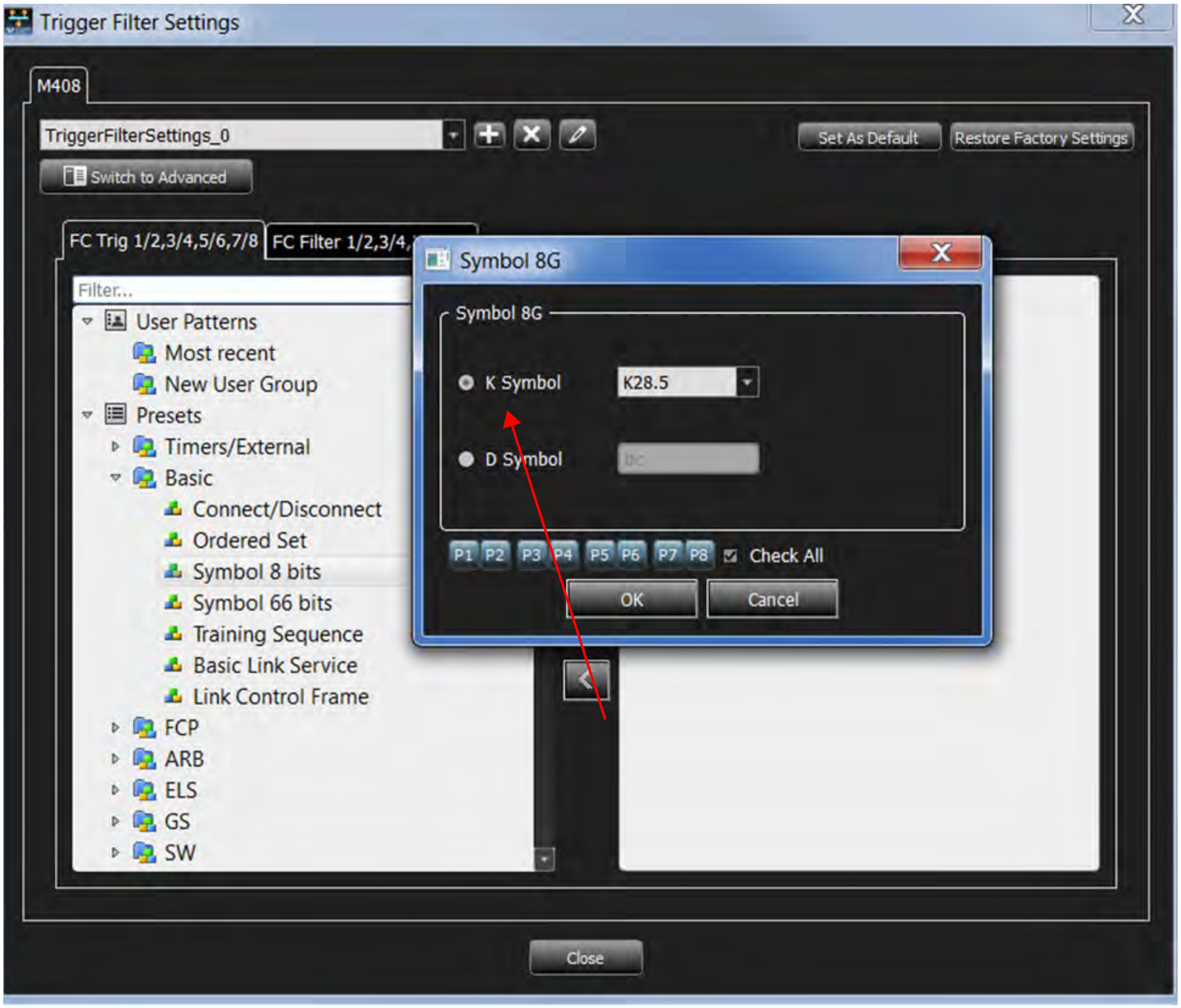


Figure 4.130: Symbol 8G Dialog Box

Check **K Symbol** or **D Symbol**, as applicable. Select the value for K Symbol from the drop-down list or enter the value for D Symbol. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Symbol 66 Bits

Double-click **Symbol 66 bits** to open the Symbol 66 Bits Pattern dialog box.

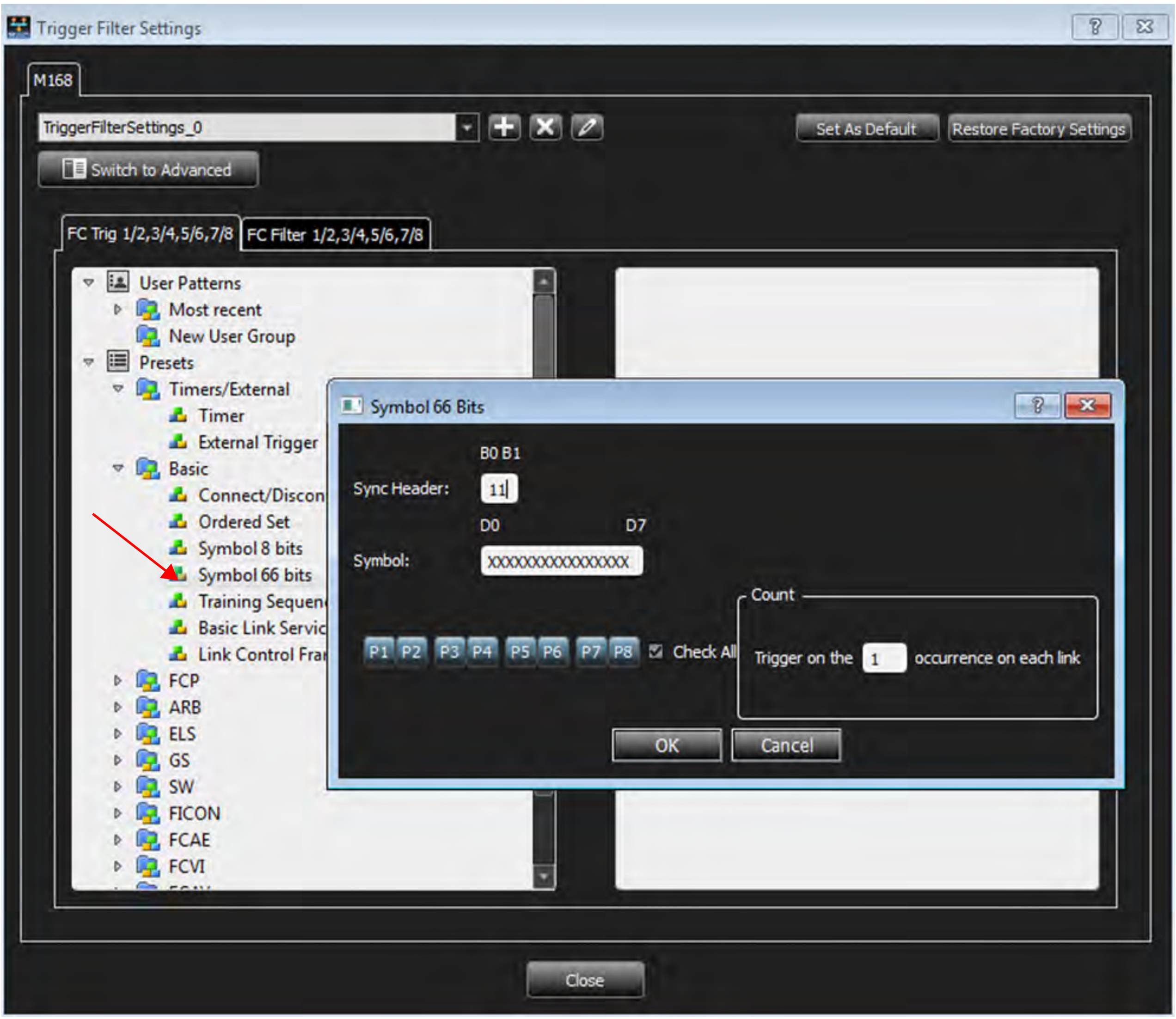


Figure 4.131: Symbol 66 Bits Dialog Box

Enter the values for the Sync Header, Symbol and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Two different order sets can exist in one 64 bits payload of a 66 bits block. The six examples of a remote and local fault given below demonstrate how to manually enter ordered set triggers.

- 0x0100000001000055 → local fault-local fault
- 0x000000000100004b → local fault-idle
- 0x010000000000002D → idle-local fault
- 0x0200000002000055 → remote fault-remote fault
- 0x000000000200004b → remote fault-idle
- 0x020000000000002D → idle-remote fault

4.2.5.2 Basic Link Service

Double-click **Basic Link Service** to open the Basic Link Service Pattern dialog box.

For any FC pattern, double-click the pattern name, for example, double-click **Basic Link Service** to open the Basic Link Service Pattern dialog box.

NOTE: Some screen captures for the FC patterns are similar to the screen capture shown below.

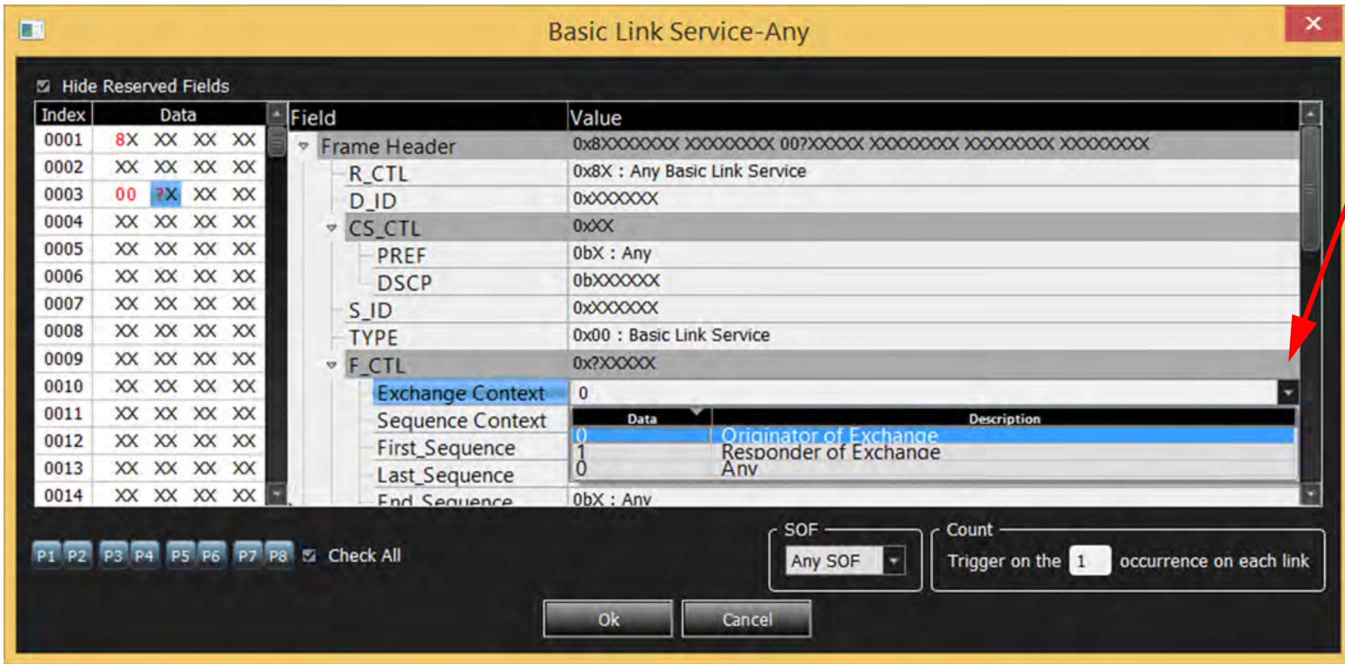


Figure 4.132: Basic Link Service Pattern Window

Enter the values for the Frame Header, CS_CTL, F_CTL and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports. You can specify the type of SOF to match on for the frame by selecting it from the SOF drop-down list.

NOTE: Some patterns have additional options to select from drop-drown lists as shown in the figure above.

Link Control Frame

Double-click **Link Control Frame** in the Pattern window to open the Add Link Control Frame Pattern dialog box.

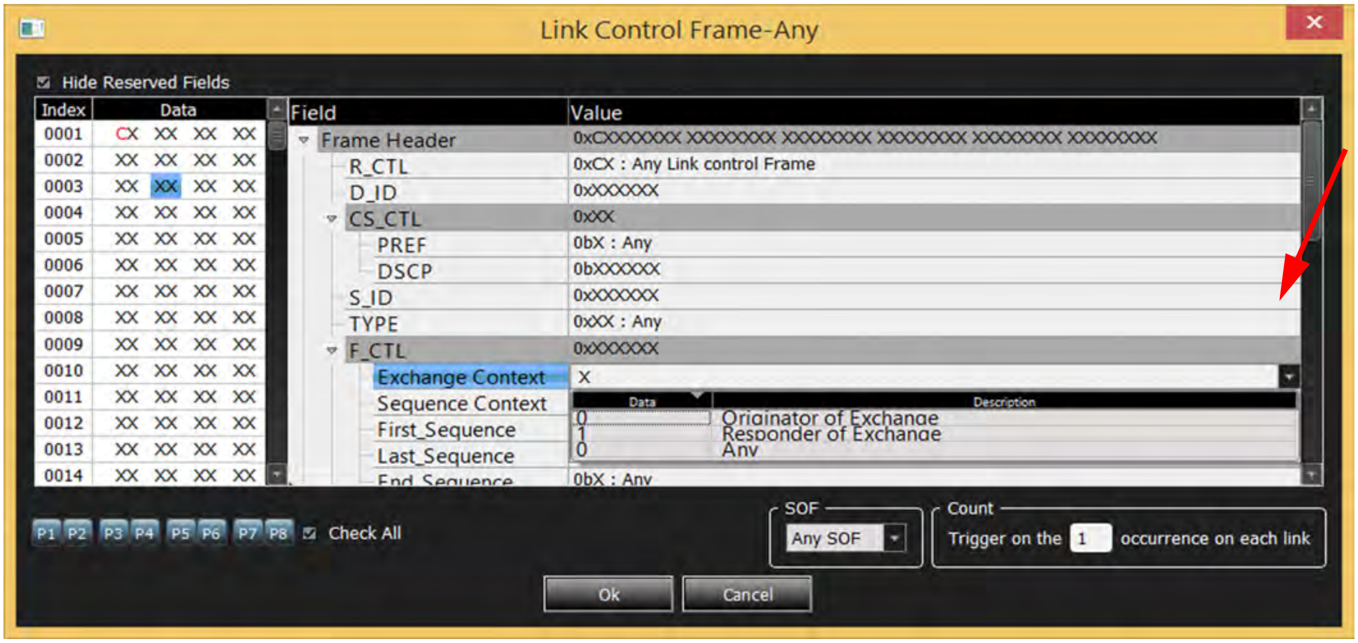


Figure 4.133: Link Control Frame Pattern Window

Enter the values for the Frame Header, CS_CTL, F_CTL and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P4 or individually select ports. You can specify the type of SOF to match on for the frame by selecting it from the SOF drop-down list.

The following additional FC patterns are available:

4.2.5.3 Other FC Patterns

The same pattern types listed for FCoE are also available for native FC as well. Refer to *4.2.4.3, FCoE Patterns* above.

4.2.5.4 FC Protocol Errors

Double-click **Protocol Errors** to open the dialog box.

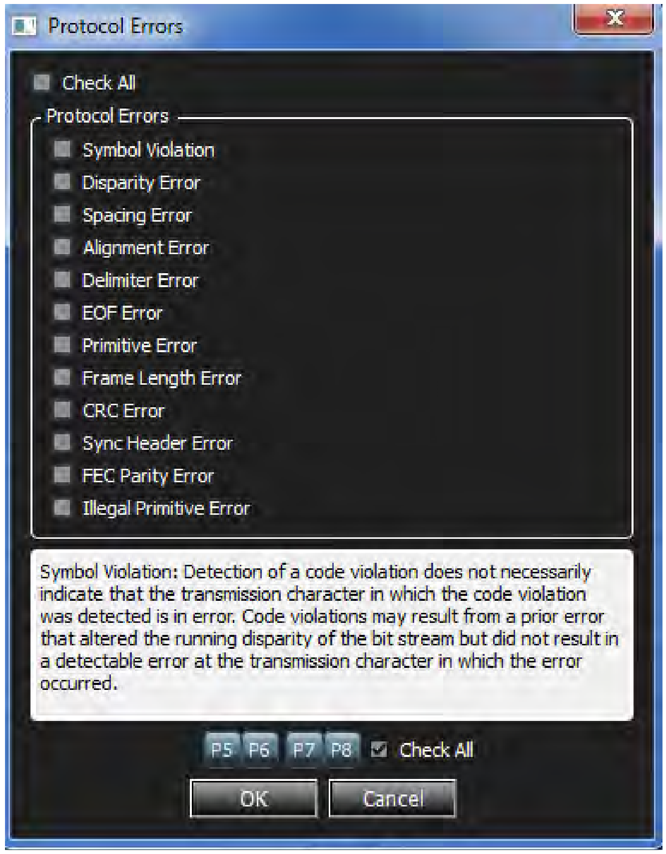


Figure 4.134: Protocol Errors Dialog Box

Select the desired protocol errors or click on the **Check All** box to select all the errors. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

4.3 Advanced Mode (User-Defined)

Advanced Mode expands Analysis capability by allowing you to program complex triggering and data capture projects.

The Advanced Mode is a state machine. You can program each state individually to:

- Trigger on a different Event or trigger unconditionally.
- Capture Everything, Nothing, or a user-defined pattern.
- Include up to three ELSE IF statements, allowing a jump to any other state based on a user definition.
- Use up to three timers, which you can set to a maximum value of 4294900 ms or over one hour.
  - If you enter a value larger than 42494900ms a warning pop-up displays: **Invalid value! Please enter a value between 0 and 4294900**.
  - You can set a timer in the state or continue the timer set in the previous state.
- Output an external trigger High or Low.

4.3.1 Working in Advanced Mode

NOTE: Some Analyzers will have different options in Advanced Mode.

To start working in the Advanced Mode, click **Switch to Advanced** mode in the Trigger Filter Settings as shown in Figure 4.135.

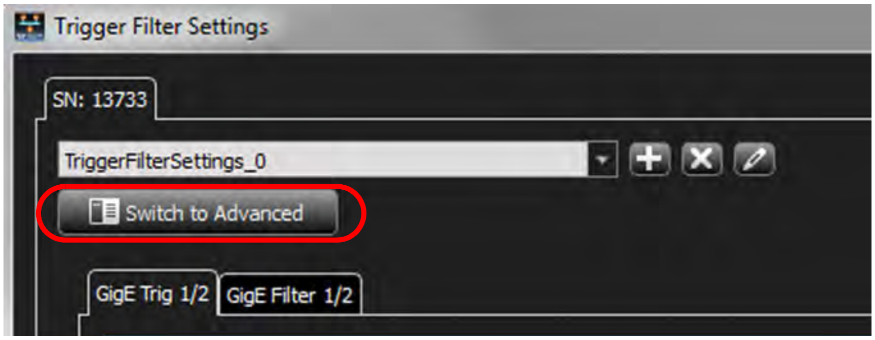


Figure 4.135: Switching to Advanced Mode Triggering

You can:

- Display the state definition
- Set Output Trigger level
- Select up to three timers
- Define the If condition and up to three Else If conditions
- Set number of occurrences before trigger
- Set captured data
- Set excluded data
- Go to next state
- Add state
- Choose link for Sequencer setup

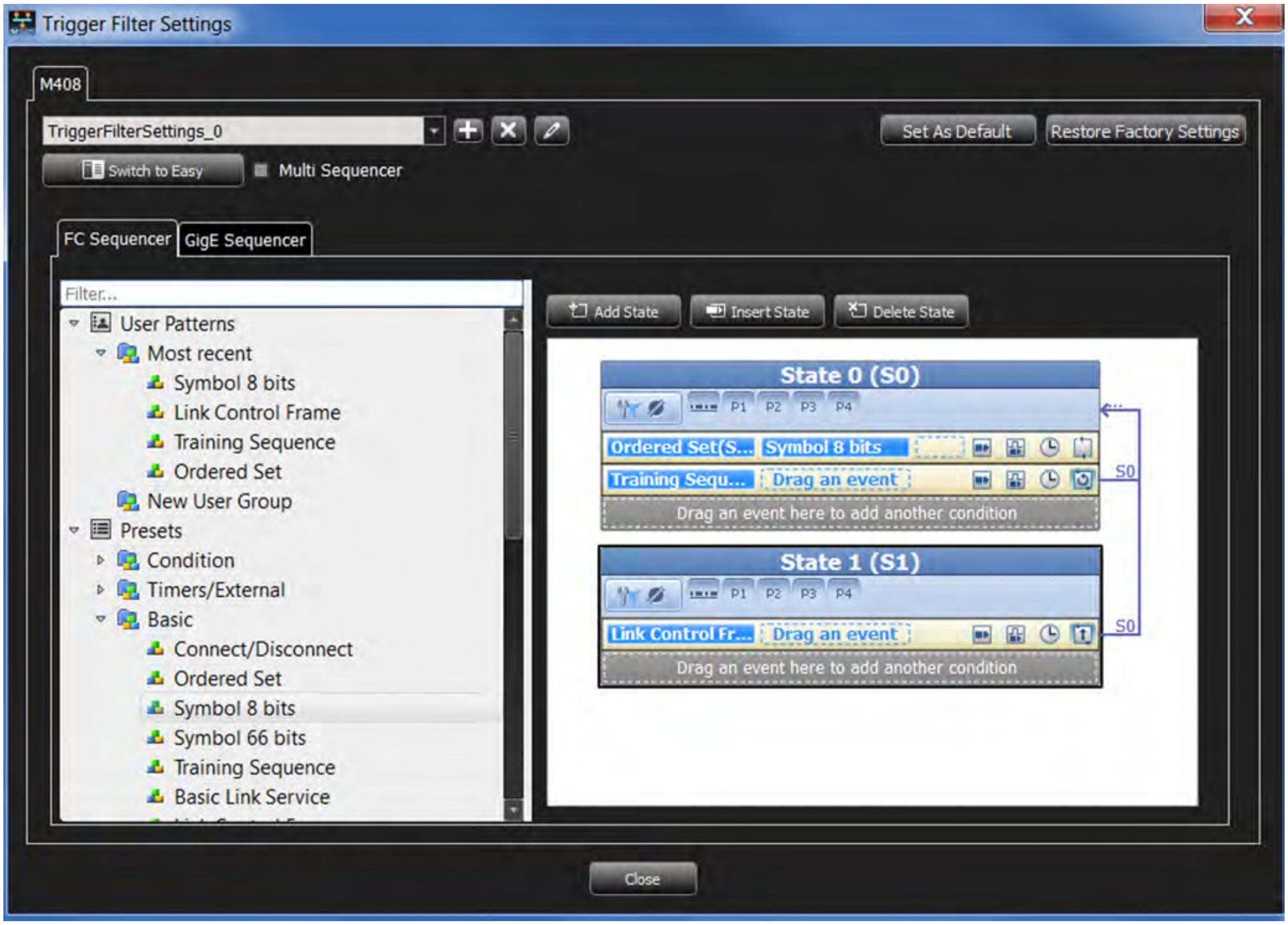


Figure 4.136: State Programming Window

4.3.1.1 Add State

Click on the Add State  button to add a State to the Sequencer. A State will be added below the last State.

4.3.1.2 Insert State

Select a State and click on the Insert State  button to insert a State. A State will be inserted after a selected State.

4.3.1.3 Delete State

Select a State and click on the Delete State  button to delete a State.

4.3.1.4 Copy/Cut and Paste States

You can copy and paste states within a Sequence.

1. Right-click in the blue title area of the State you want to copy and select Copy State (or Cut State if applicable).

2. Right-click in the white workspace of the desired target Sequence and select Paste State.

4.3.1.5 Copy/Cut and Paste Conditions

You can copy and paste Conditions within and between States.

1. Right-click in the empty yellow space of the Condition you want to copy and select Copy Condition (or Cut Condition if applicable).
2. Right-click in the gray placeholder area (i.e. in the area that says “Drag an event here....”) of the desired target State and select Paste.

4.3.1.6 Copy/Cut and Paste Events

You can copy and paste Events within and between States.

1. Right-click on the Event you want to copy and select Copy (or Cut if applicable).
2. Right-click in the empty yellow space of the desired target Condition or in the gray placeholder area (i.e. in the area that says “Drag an event here....”) of the desired target State and select Paste.

4.3.1.7 Adding Patterns to a State

1. Drag a pattern from the list of patterns displayed in the left panel and drop it in the State to add it. The application displays **Drag an event** or **Drag an event here to add another condition**, to indicate the location to drop events in a State. **Drag/Drop events** between states will copy/paste the event.
2. Define each selected pattern in the same way as in Easy Mode, as described in 4.102, *Trigger and Filter Preset Patterns (RDMA and NVMe)*. To use a timer, define it first.

NOTE:
- You can copy a frame from the spreadsheet view and paste it for triggering.
- You can set a timer for any If or Else If condition.

3. Enter a value for the number of occurrences before trigger in the **Count** field, up to a maximum of 65535 occurrences.

4.3.1.8 Setting Triggers

The trigger icon toggles between a blue outline and no outline, activating and deactivating it.

Click the Trigger icon  to activate the trigger. Once the trigger is activated the trigger icon turns  to blue outline.

NOTE: When the Timer is in “Advanced Trigger” mode, it does not work in single state. When the Timer elapses, you must branch to a new state that performs the Trigger.

4.3.1.9 External Output Trigger

The external output trigger icon toggles between a blue outline and no outline, activating and deactivating it. The External Output Trigger icon (no outline) indicates there is no change. Click to activate the trigger. Once the trigger is activated the icon has a blue outline indicating it is active.

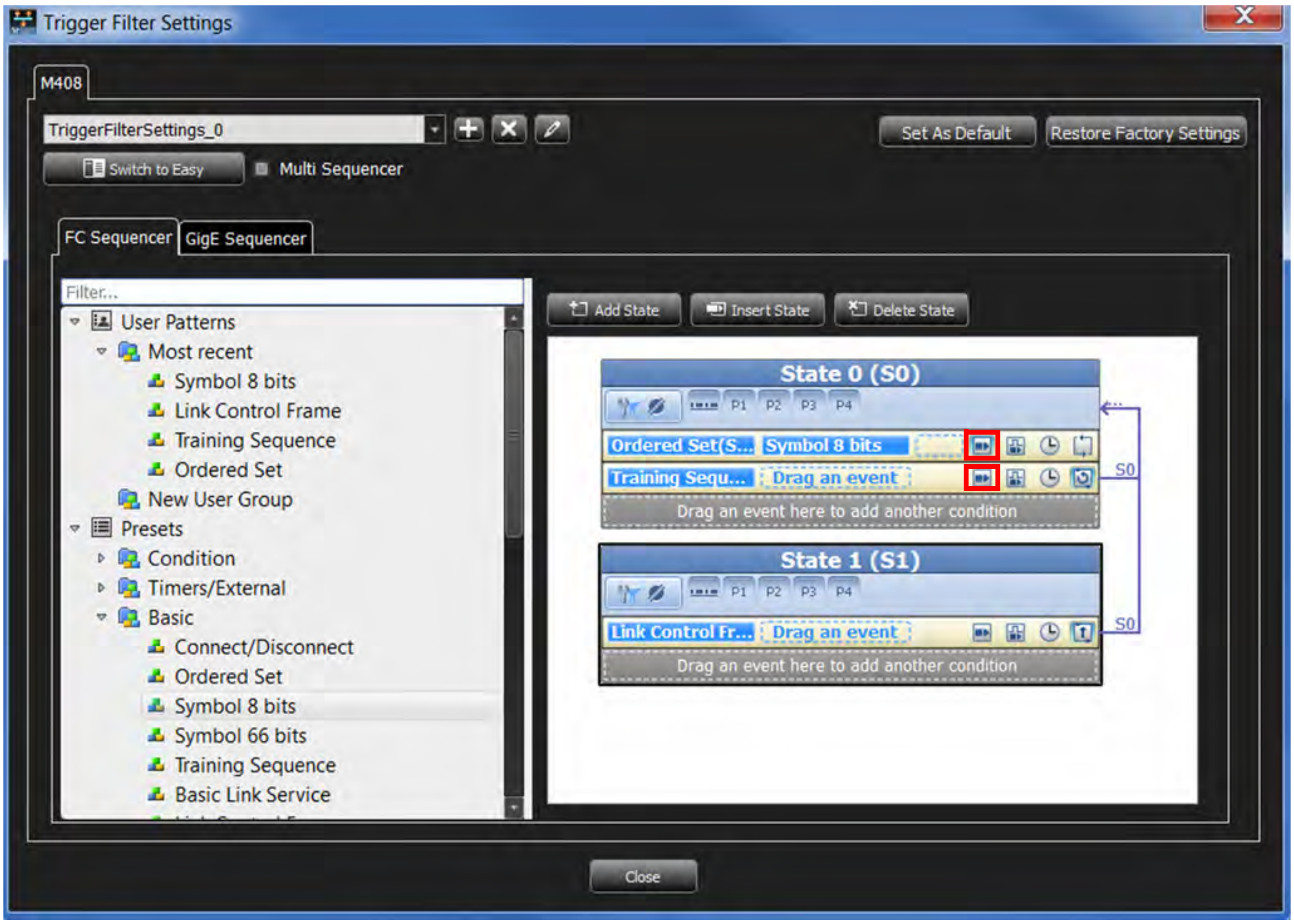


Figure 4.137: Setting Triggers

4.3.1.10 Setting State Transitions

Click on the State Transition icon to change the state to transition to. Left-click for menu options to display as shown in the following screen capture and select the state to transition to. To remove the state transition select **No Jump.**

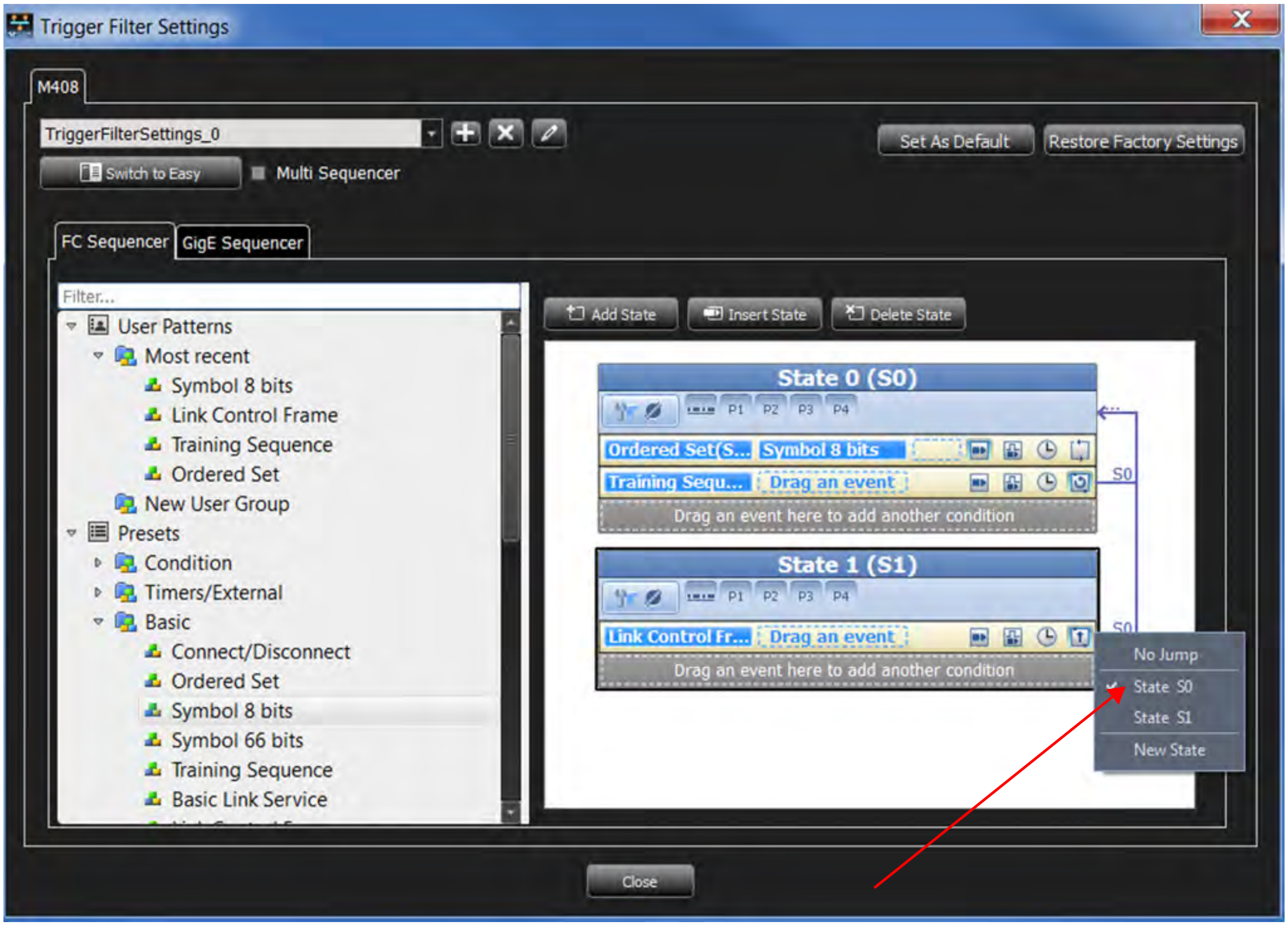


Figure 4.138: State Transition

4.3.1.11 Settings Capture Filters

- Choose a capture option by clicking on the Capture Everything  icon shown in the figure below. The Filter Settings window displays (Figure 4.139).

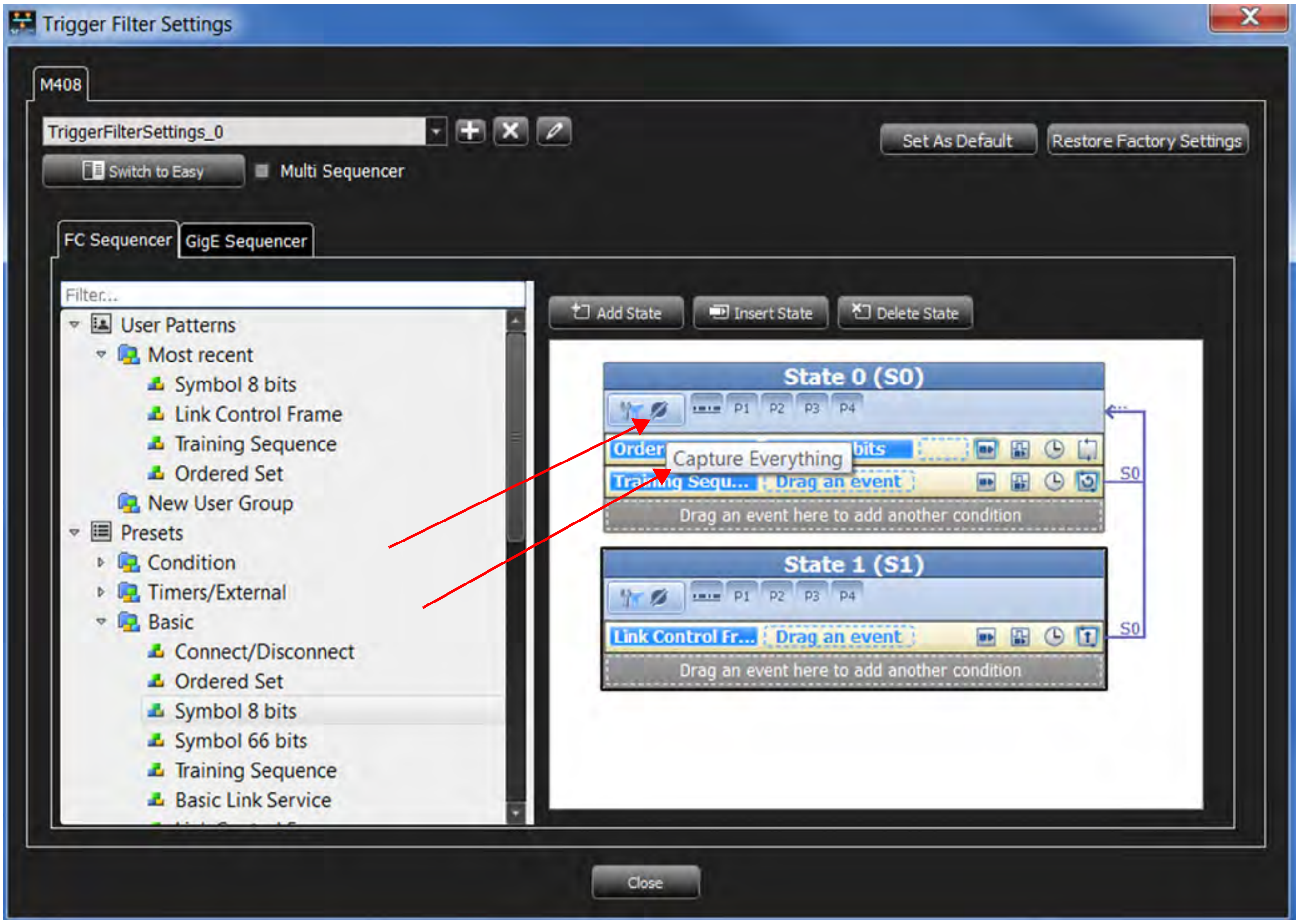


Figure 4.139: Capture Everything

- If you choose Capture Everything, you can select options for exclusion. See Figure 4.140.

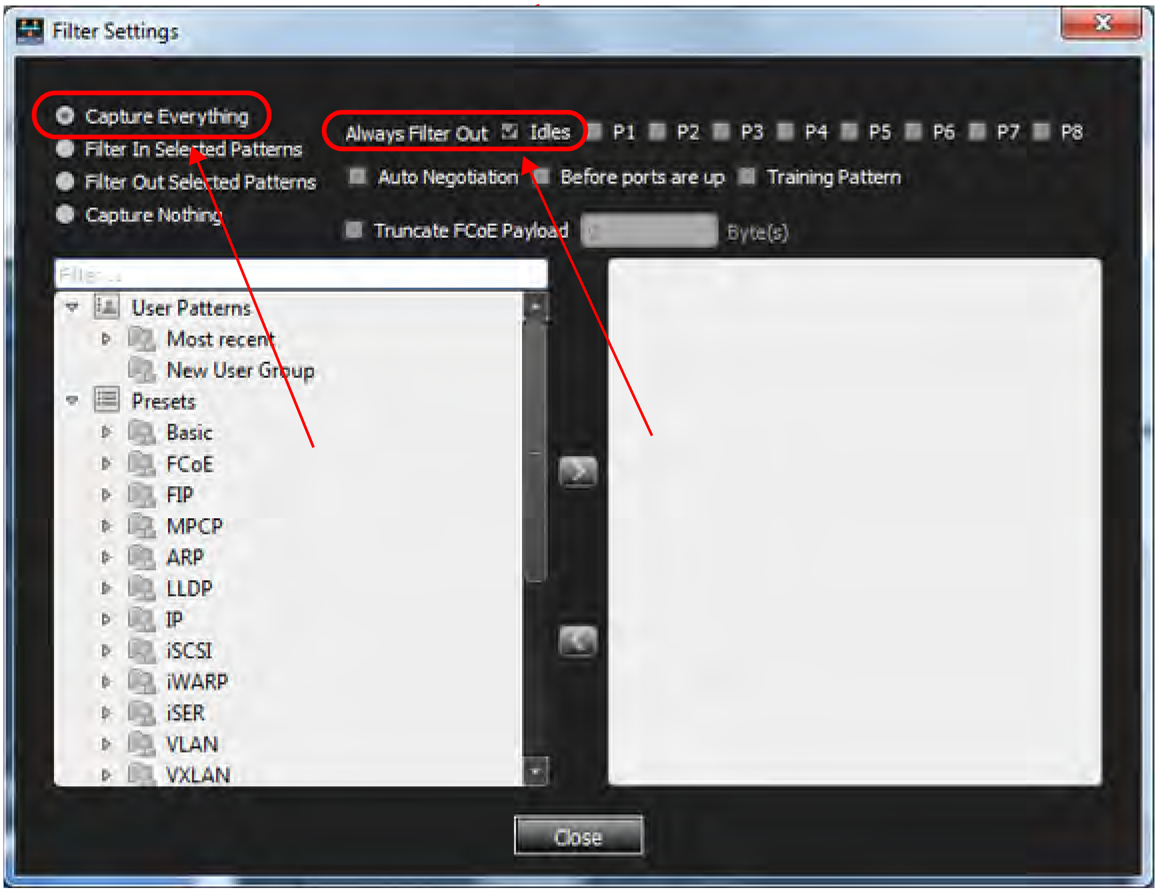


Figure 4.140: Filter Settings Window: Capture Everything, Exclude Idles

- ❑ Select Filter In Selected Patterns or Filter Out Selected Patterns to select patterns for inclusion or exclusion (Figure 4.141). See 4.102, *Trigger and Filter Preset Patterns (RDMA and NVMe)*.

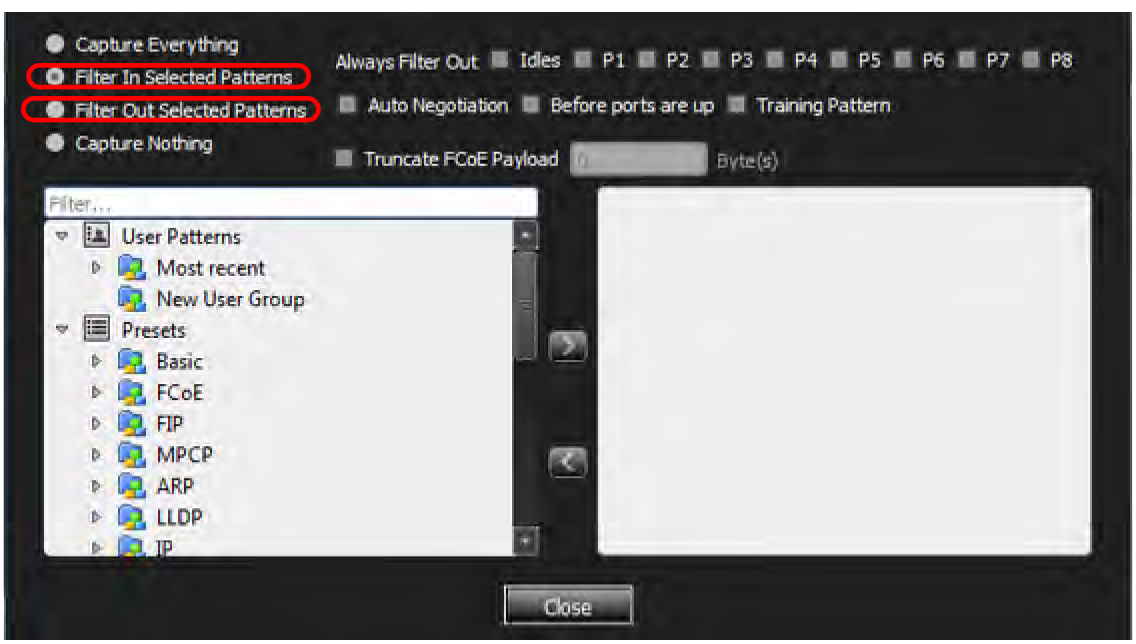


Figure 4.141: Filter In Selected Patterns or Filter Out Selected Patterns

- Choose pattern(s) and click the → button to add them for capture or exclusion. You define each pattern the same way as in Easy mode (4.102, *Trigger and Filter Preset Patterns (RDMA and NVMe)*).
- Click Capture Nothing to run the state without capturing anything.
- Click on the checkboxes to Capture Everything, Always Filter Out specified options. See Figure 4.142 and Figure 4.143.

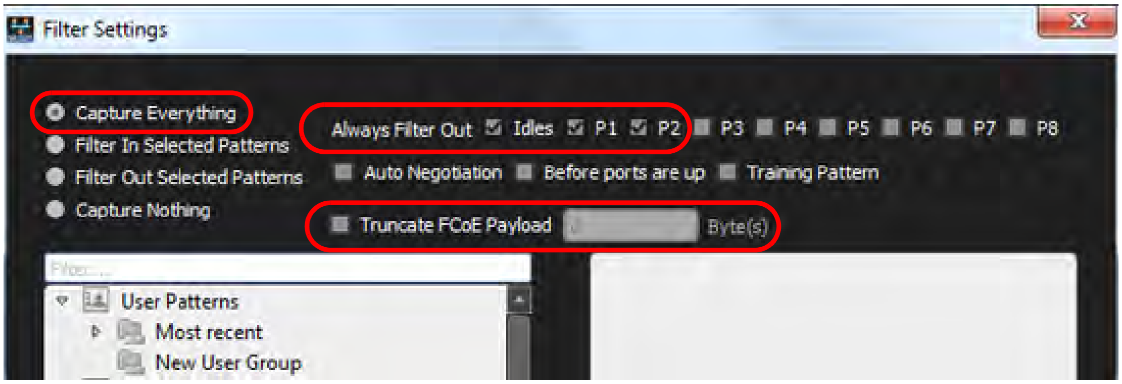


Figure 4.142: Advanced Triggering: Filter Settings

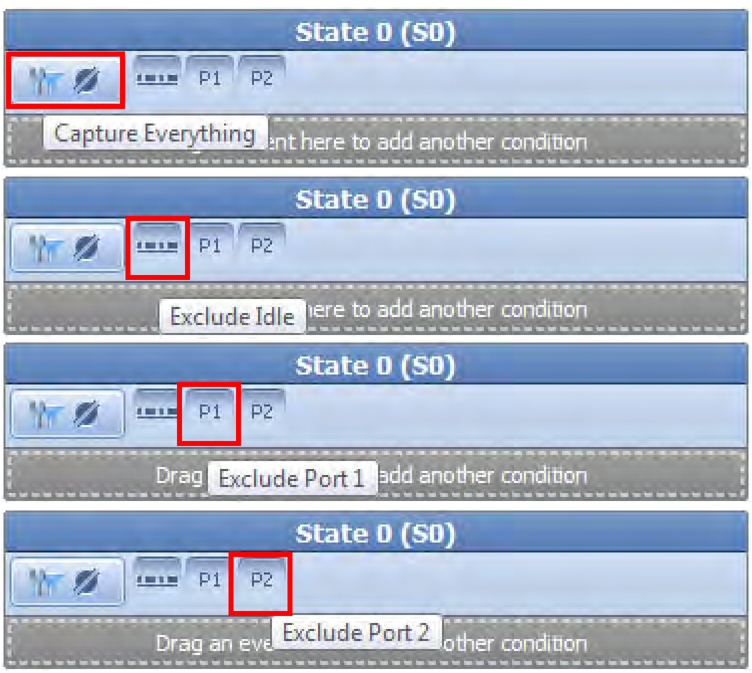


Figure 4.143: Advanced Mode – Capture All, Exclude Idles, Ports 1 & 2

- Select ARBFF, NOS, VC_RDY, Before ports are up, or Training Pattern. ARBff, NOS and VC_RDY are ordered sets that show up frequently and are of little use in most cases, and selecting allows you to specifically filter them out. Before ports are up will filter everything before the ports are up, to save buffer space and allow to concentrate on the parts important to the user. Training Pattern will similarly filter out all Training Patterns

- Check the Truncate Payload option to truncate payload after x-number of Dword(s) 0 bytes. (see Figure 4.140).

4.3.1.12 Multi-Link Triggering

NOTE: This applies only to the SierraNet M408 and SierraNet M168 Analyzers.

You can set different triggering for each link. To set different trigger conditions for a link, check the **Multi Sequencer** check box and select the link for setup from the Port tabs. When you select this option, you can define a sequencer per link (pair port). These sequencers are independent from each other and will be run separately on each link.

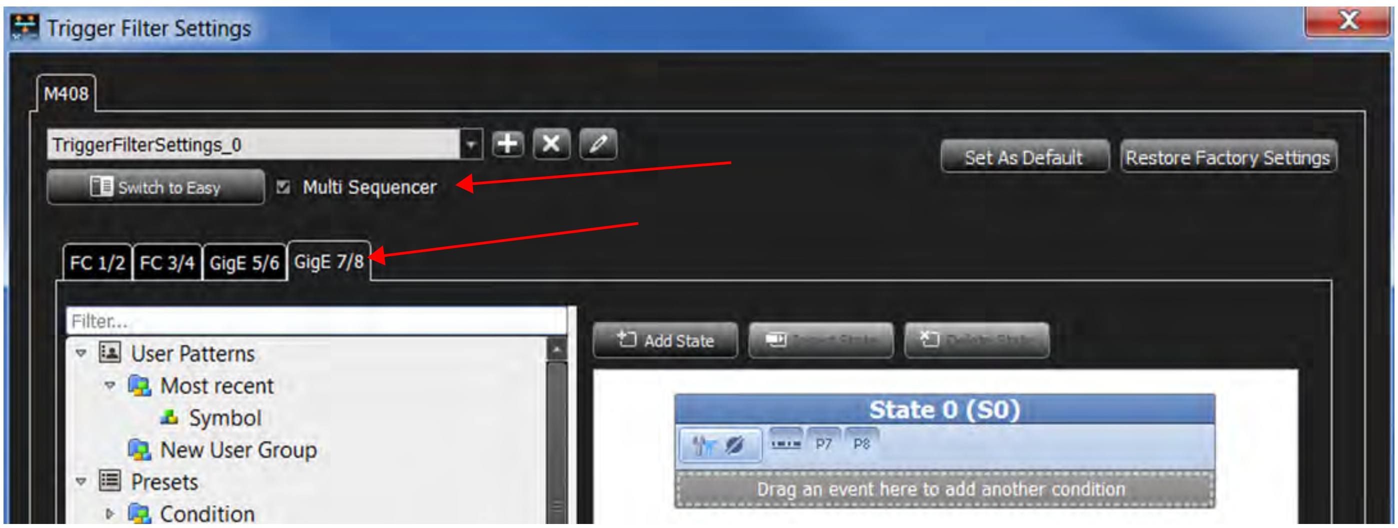


Figure 4.144: Multi-Link Triggering Setup

4.3.1.13 Set Timers

You can set and use up to three Timers for triggering. You can set each Timer for each state, or continue from a Timer set in the previous state. The Timer defined for a particular state starts when entering that state. To set Timers:

1. Click the **Timer**  icon for a state.
2. Define timer in the Timer Setting window.
3. Repeat the above steps for each state.

NOTE: Each Timer action must reside in a separate state (Set and Start).

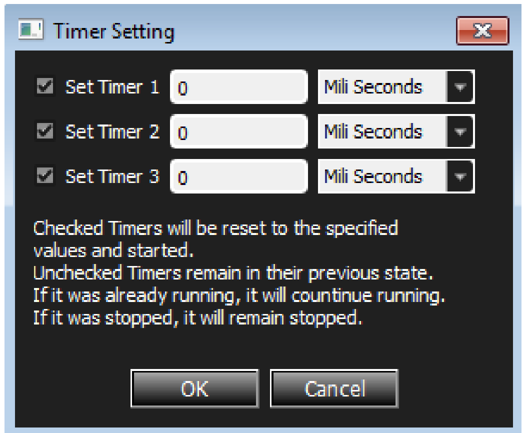


Figure 4.145: Timer Settings Dialog Box

You must set and start each timer before continuing to the next timer. For example, start Timer 1, continue it, then set Timer 2 in order to continue it. It will not allow you to continue Timer 2 until you first set it.

4.3.1.14 Enable Fast State Switching

Prior to 4.80, Fast State Switching was disabled and not available in Advanced Trigger mode. Because the M648 analyzer needs around 3.5 us between Sequencer State transitions, if the next several consecutive jumps happen faster than this time period, the Analyzer forces a trigger without waiting for the set trigger point. This resulted in an Internal Error.

The new option, *Enable Fast State Switching*, will counter the timing limitations. When this option is checked, the minimal back-to-back events (Sequencer transitions) duration is reduced to 100 ns.

The trade-off and the reason this is not the default setting is that, if the events are less than 100 ns apart, the second event will be missed, which will result in a malfunction of the Sequencer state machine as programmed.

To summarize, you must be aware of the advantages and the disadvantages of using this feature.

- When *Enable Fast State Switching* is unchecked (default):
  - **Advantage**: All events will be detected and transitioned correctly, even if less than 100 ns apart.
  - **Disadvantage**: If a few events in a row happen less than 3.5 ns apart, the Analyzer will force a trigger and report an Internal Error.
- When *Enable Fast State Switching* is checked:
  - **Advantage**: If state switching happens less often than every 100 ns, state switches can happen infinitely.
  - **Disadvantage**: When the time difference between the event(s) in back-to-back states is less than 100 ns, the second event in the 100 ns window will not be registered, leading to an incorrect final trigger.

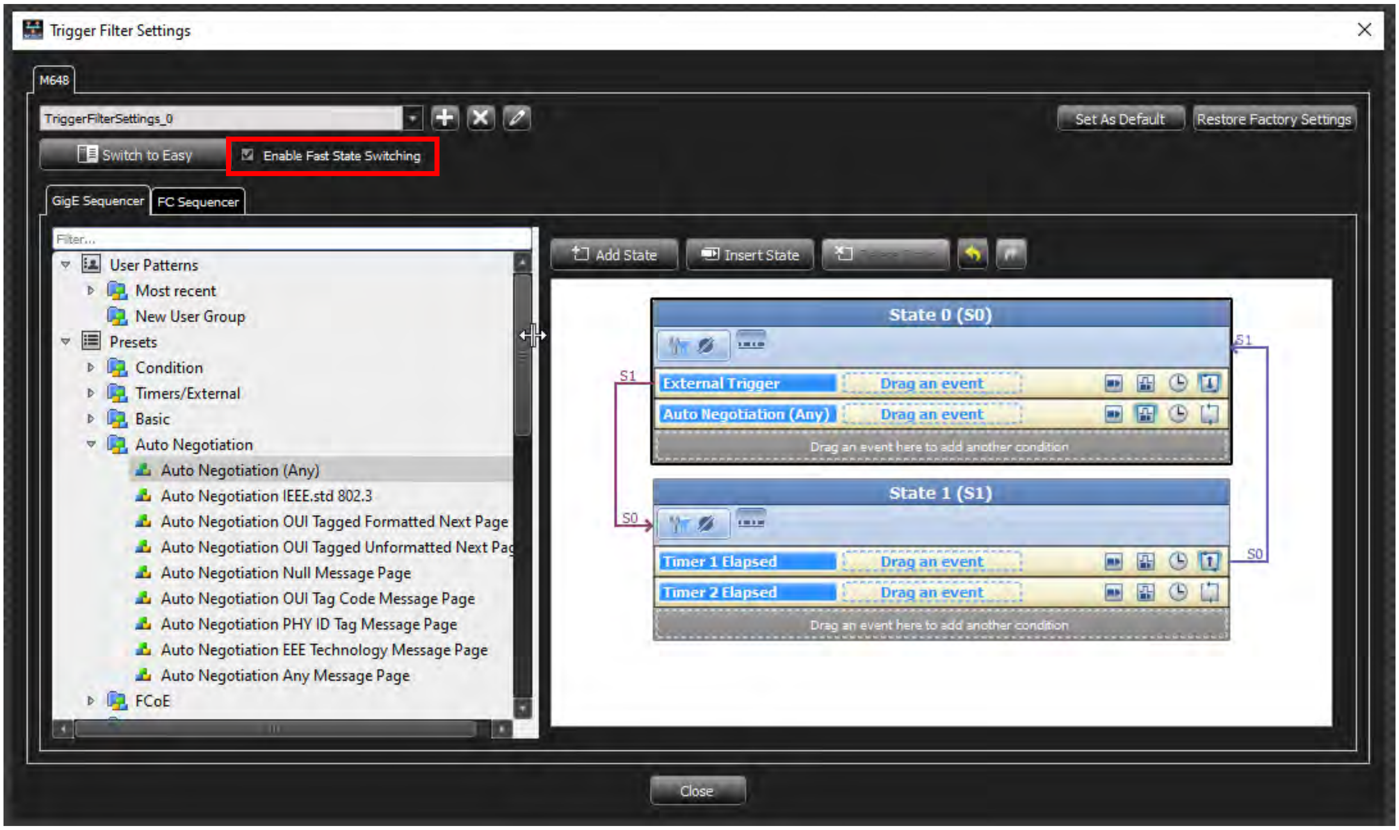


Figure 4.146: M648 Trigger Filter Settings – Enable Fast State Switching

To enable the *Fast State Switching* feature, follow the instructions below.

NOTE: This assumes you have already configured State 0 and State 1.

1. Click the  to the right of *Trigger Filter Settings* to open the settings window.
2. Click the **Switch to Advanced** tab.
3. Check **Enable Fast State Switching** (Figure 4.146).
4. Start Recording as usual.

4.4 Real Time Traffic Profile

Real Time Traffic Profile is a graphical tool, which allows the user to monitor a wide variety of traffic on the bus and manipulate the display of that information.

To start up a Real Time Traffic Profile:

1. Open a new Project: From the Main Menu, select **File** → **New Project**. See Figure 4.147 and Figure 4.148.

Figure 4.147: Net Protocol Suite – Main Menu

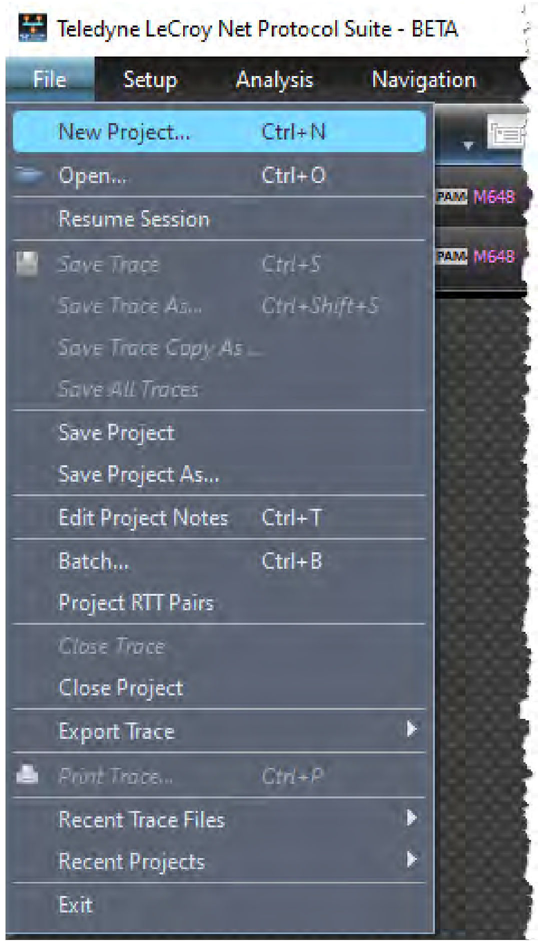


Figure 4.148: New Project

The Add Device To Project window appears (Figure 4.149). In this example, an M408 Analyzer is available to add to the Project.

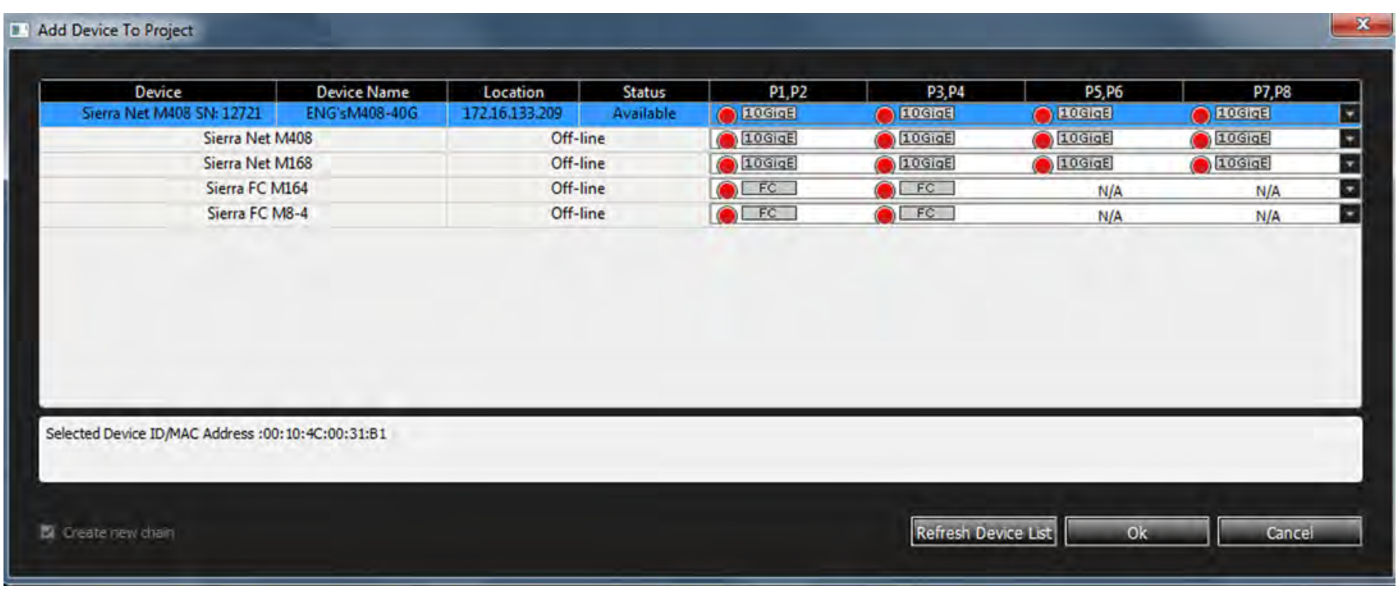


Figure 4.149: Add Device to Project

2. Click the small arrow at the far right of the screen to select Port assignments. Select Jammer/Analyzer 40GigE. See Figure 4.150

Figure 4.150: M408 Analyzer is Added to the Project

The Main Menu will update to show the M408 is connected. See Figure 4.151.

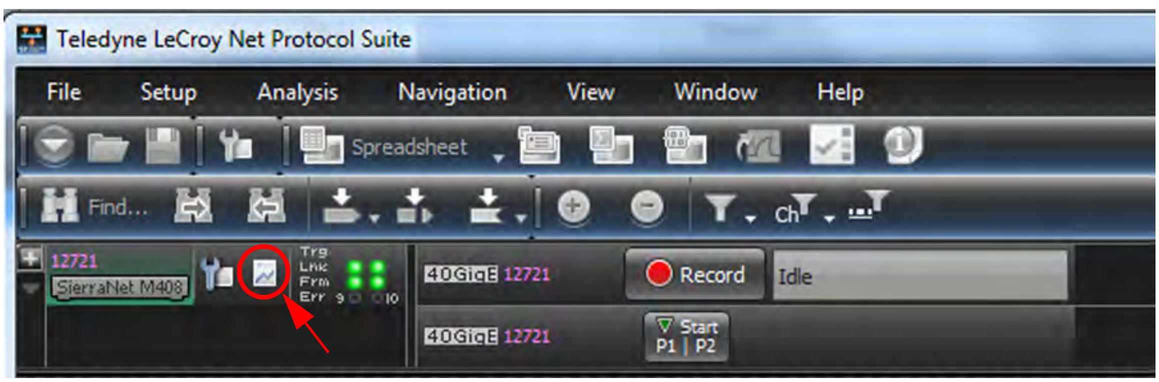


Figure 4.151: M408 is Connected to Project

4.4.1 Real Time Statistics

Select the Real Time Statistics icon to bring up the GUI (Figure 4.152).

Figure 4.152: Real Time Statistics – Traffic Profile

By default seven windows are displayed:

- Frames Rate
- Payload Rate
- IO Command Write
- Error Count
- Average Frame Size
- Link Utilization
- IO Command Read

In this case, we have data being generated and sent to the analyzer. The controls for the Real Time Statistics -- Traffic Profile are shown in Figure 4.153.

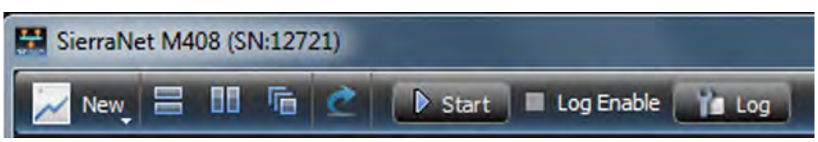


Figure 4.153: Real Time Statistics – Traffic Profile

The controls are:

- New Window (see Figure 4.154)
- Tile Windows (Tile Vertically, Tile Horizontally, Tile Grid)
- Reset All
- Start/Stop Displaying Data
- Log Enable (On/Off)
- Log (Set location of Log file, see Figure 4.172)

The New Window function allows you to add more of each type of window.

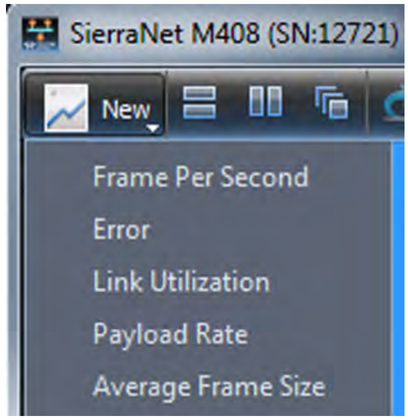


Figure 4.154: Real Time Statistics – Traffic Profile, New Window

4.4.2 Start Real Time Traffic Display

To start the analyzer collecting data: Select the Start icon and each of the windows in the grid display will show filtered activity. In this case we've set the Filter to Any Ethernet Frame, so we see a lot of activity and no Errors were detected.

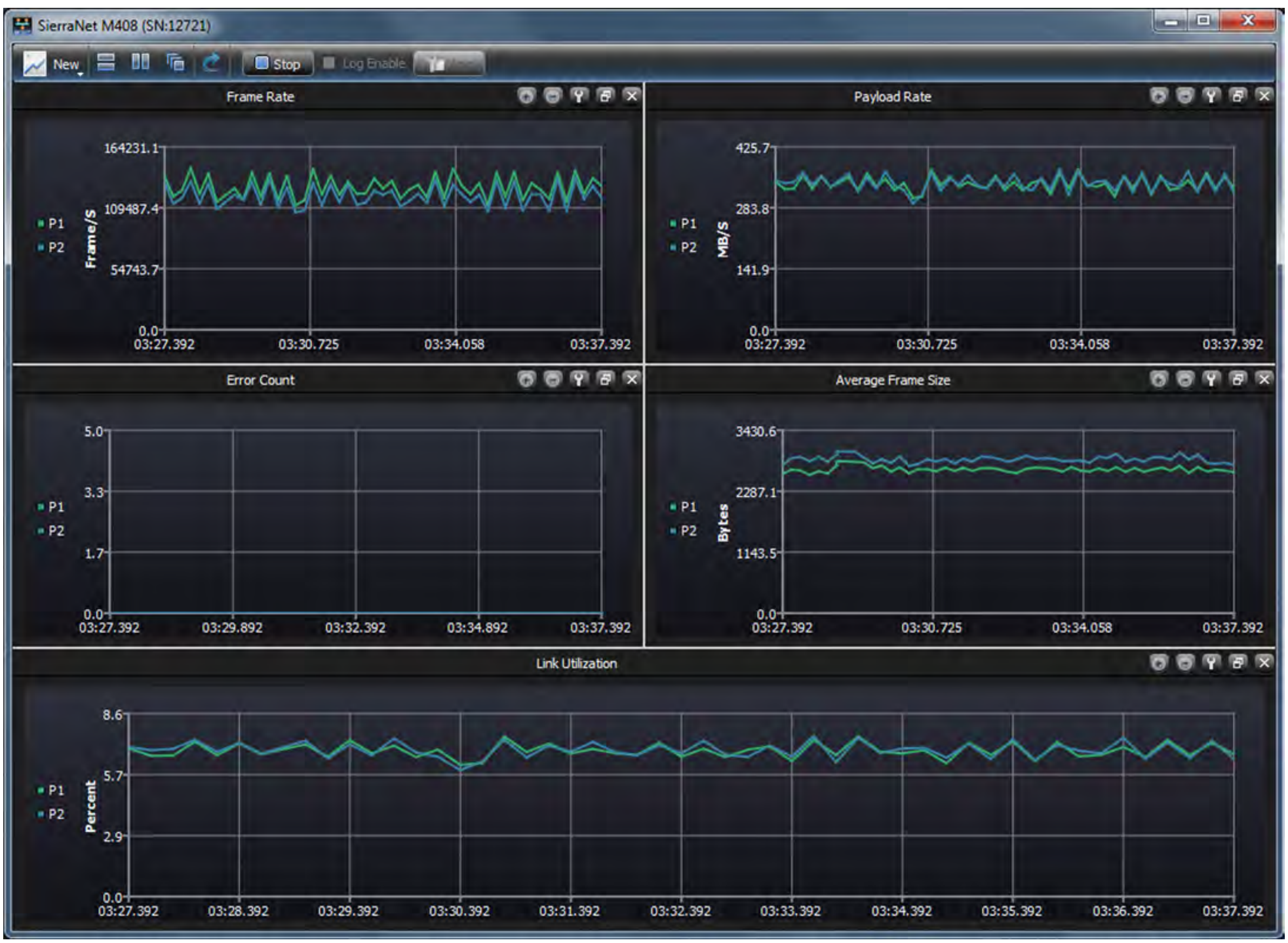


Figure 4.155: Real Time Traffic in Grid Display Mode

4.4.2.1 Manipulating Individual Windows

Each window can be docked or undocked from the display. Each window can also be duplicated or deleted. By deleting some graphs and adding others, you can graph individual ports to compare specific parameters. See Figure 4.156.

Figure 4.156: Compare Frame Rates and Average Frames Sizes on Port 1 vs. Port 2

This is just one example of the flexibility of the windows being displayed. You can manipulate the types of traffic being displayed to suit your individual preferences.

4.4.2.2 Individual Window Controls

Each window has five control icons:

- Zoom In
- Zoom Out
- Settings
- Pop Window Out of Current Display
- Close Current Display

As an example, the controls for Payload Rate are shown in Figure 4.157.

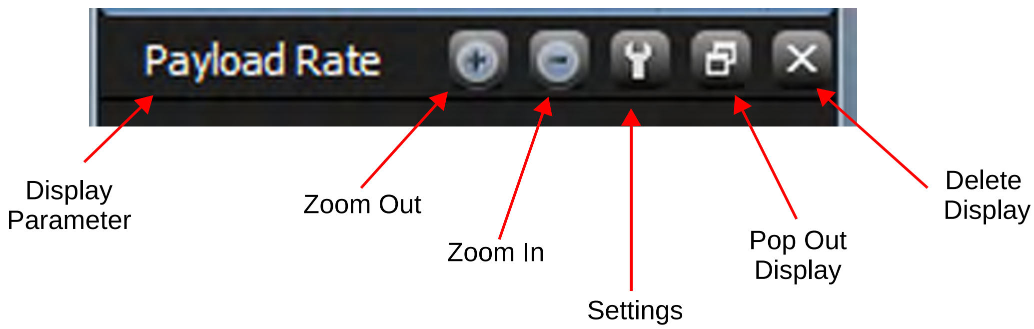


Figure 4.157: Typical Display Controls

4.4.2.3 Settings - Filter

Settings allows you to set up filters for the traffic you want to see, as well as detect a wide variety of protocol errors. In the display above (Figure 4.155) we can now see that the only Filter Setting is Any Ethernet Frame.

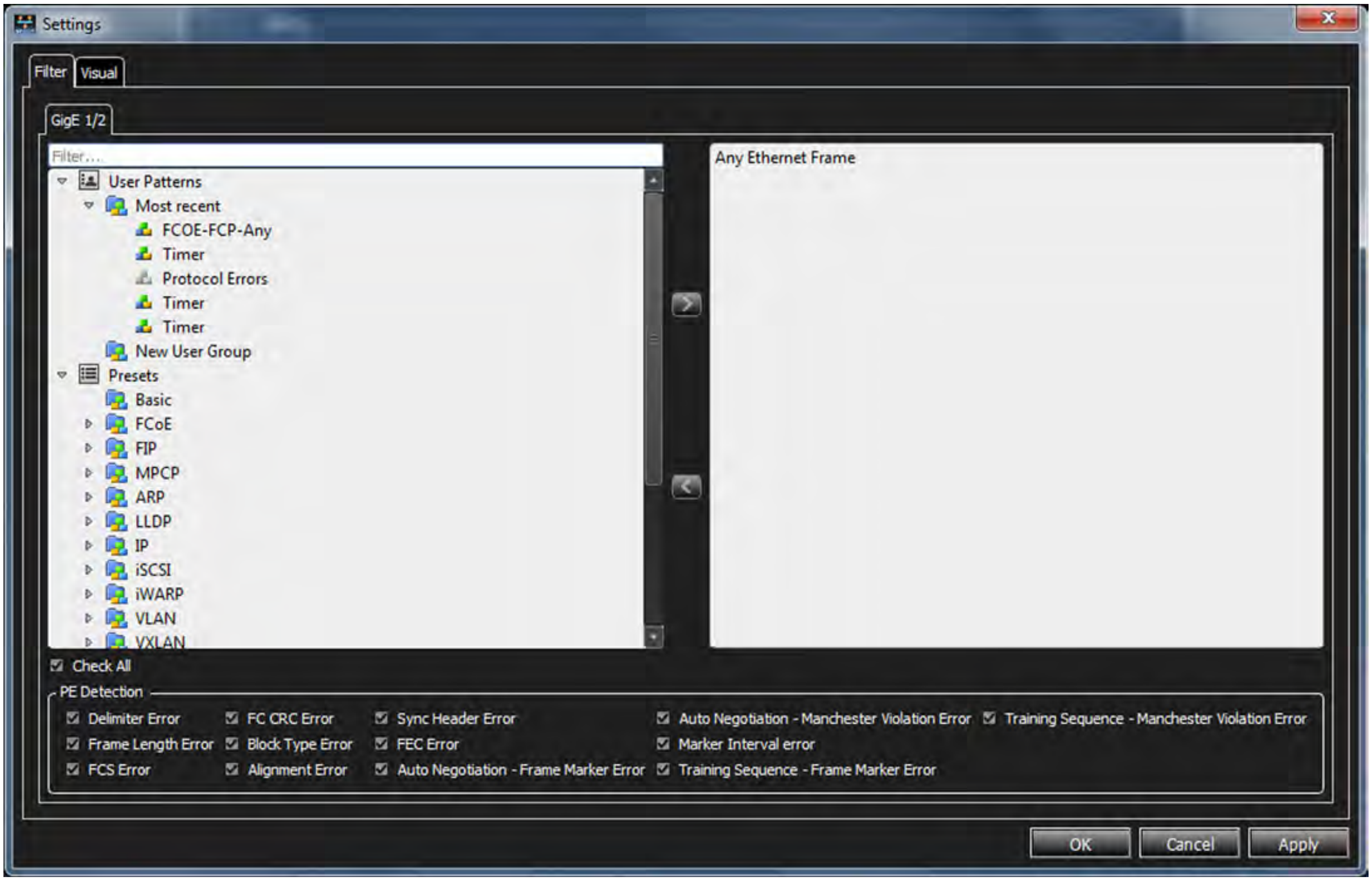
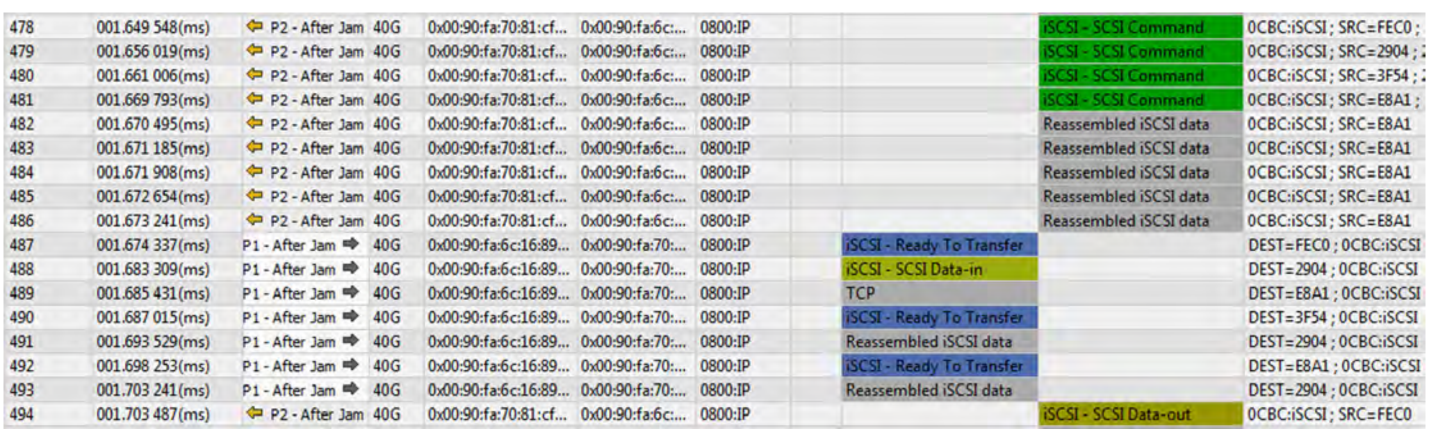


Figure 4.158: Display Settings: Filter Patterns and Protocol Errors

If you don't know exactly what you want to filter out of the traffic, one method would be to Record a Snapshot of the traffic you're interested in and use it as a guide for defining your filter.

For example, if you were running SCSI traffic into the analyzer and took a Snapshot (see Figure 4.159).



478	001.649 548(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			iSCSI - SCSI Command	0CBC:iSCSI ; SRC=FEC0 ;
479	001.656 019(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			iSCSI - SCSI Command	0CBC:iSCSI ; SRC=2904 ;
480	001.661 006(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			iSCSI - SCSI Command	0CBC:iSCSI ; SRC=3F54 ;
481	001.669 793(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			iSCSI - SCSI Command	0CBC:iSCSI ; SRC=E8A1 ;
482	001.670 495(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			Reassembled iSCSI data	0CBC:iSCSI ; SRC=E8A1
483	001.671 185(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			Reassembled iSCSI data	0CBC:iSCSI ; SRC=E8A1
484	001.671 908(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			Reassembled iSCSI data	0CBC:iSCSI ; SRC=E8A1
485	001.672 654(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			Reassembled iSCSI data	0CBC:iSCSI ; SRC=E8A1
486	001.673 241(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			Reassembled iSCSI data	0CBC:iSCSI ; SRC=E8A1
487	001.674 337(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		iSCSI - Ready To Transfer		DEST=FEC0 ; 0CBC:iSCSI
488	001.683 309(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		iSCSI - SCSI Data-in		DEST=2904 ; 0CBC:iSCSI
489	001.685 431(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		TCP		DEST=E8A1 ; 0CBC:iSCSI
490	001.687 015(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		iSCSI - Ready To Transfer		DEST=3F54 ; 0CBC:iSCSI
491	001.693 529(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		Reassembled iSCSI data		DEST=2904 ; 0CBC:iSCSI
492	001.698 253(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		iSCSI - Ready To Transfer		DEST=E8A1 ; 0CBC:iSCSI
493	001.703 241(ms)	P1 - After Jam	40G	0x00:90:fa:6c:16:89...	0x00:90:fa:70:...	0800:IP		Reassembled iSCSI data		DEST=2904 ; 0CBC:iSCSI
494	001.703 487(ms)	P2 - After Jam	40G	0x00:90:fa:70:81:cf...	0x00:90:fa:6c:...	0800:IP			iSCSI - SCSI Data-out	0CBC:iSCSI ; SRC=FEC0

Figure 4.159: Snapshot of Traffic

Notice that the traffic is mainly SCSI commands and data on Ports 1 and 2. In the filter window, choose the following filters. See Figure 4.160.

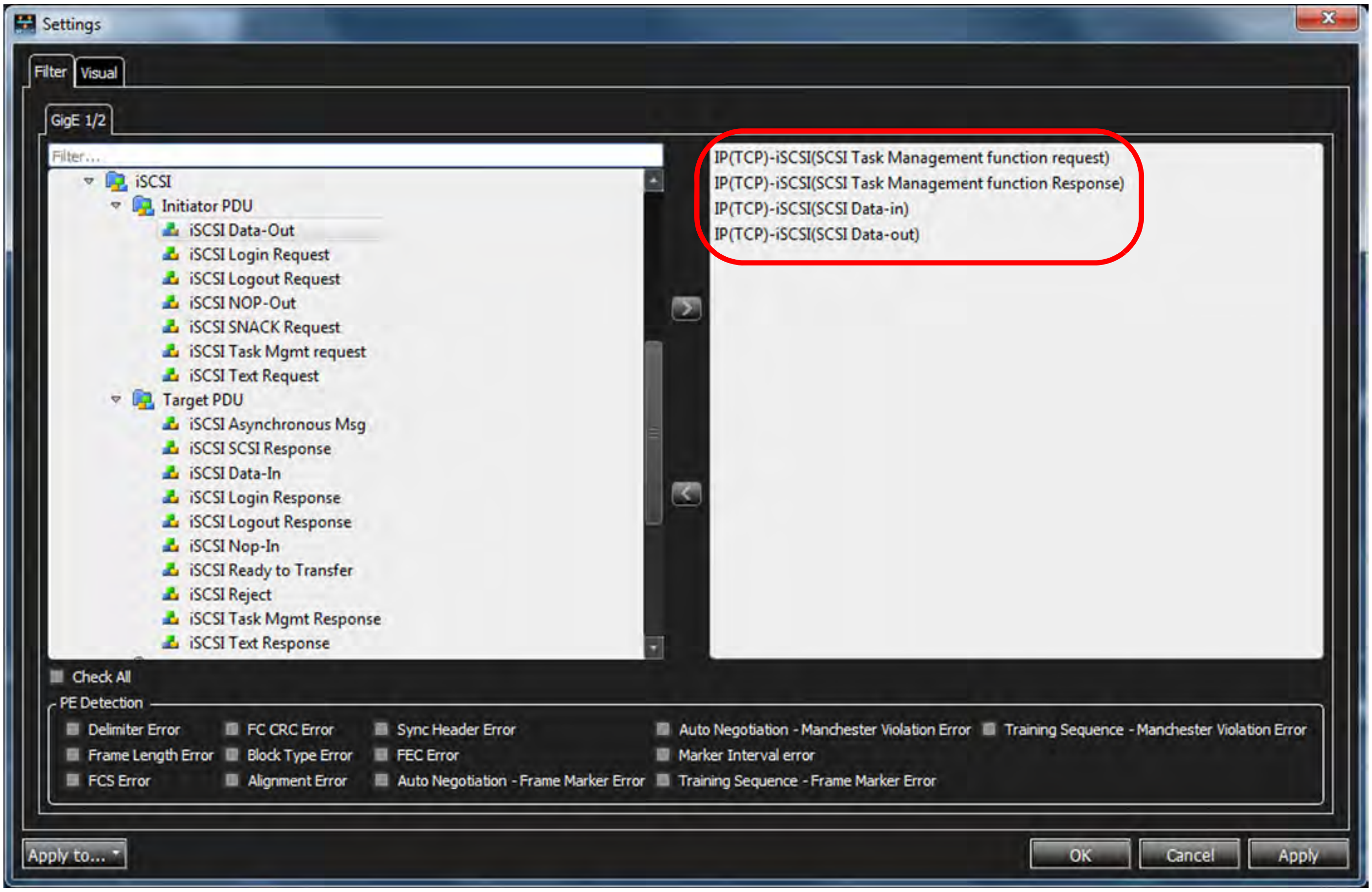


Figure 4.160: Filter for SCSI Commands and Data

Any time you change either Filter or Visual Settings this Warning message will pop up:

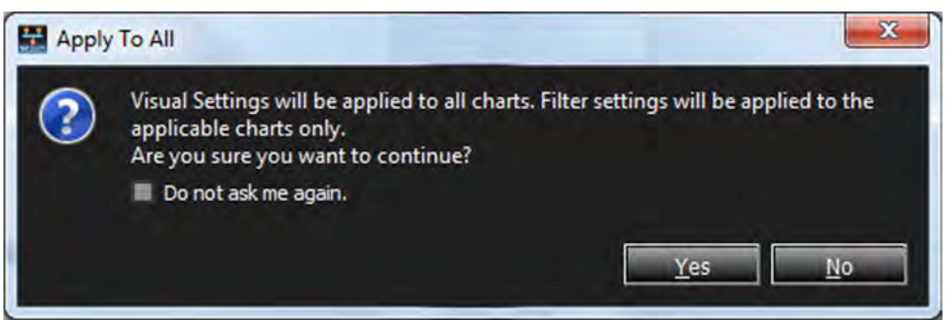


Figure 4.161: Warning Message

4.4.2.4 Settings - Visual

You can also choose Settings – Visual to change the way the traffic is displayed (see Figure 4.162).

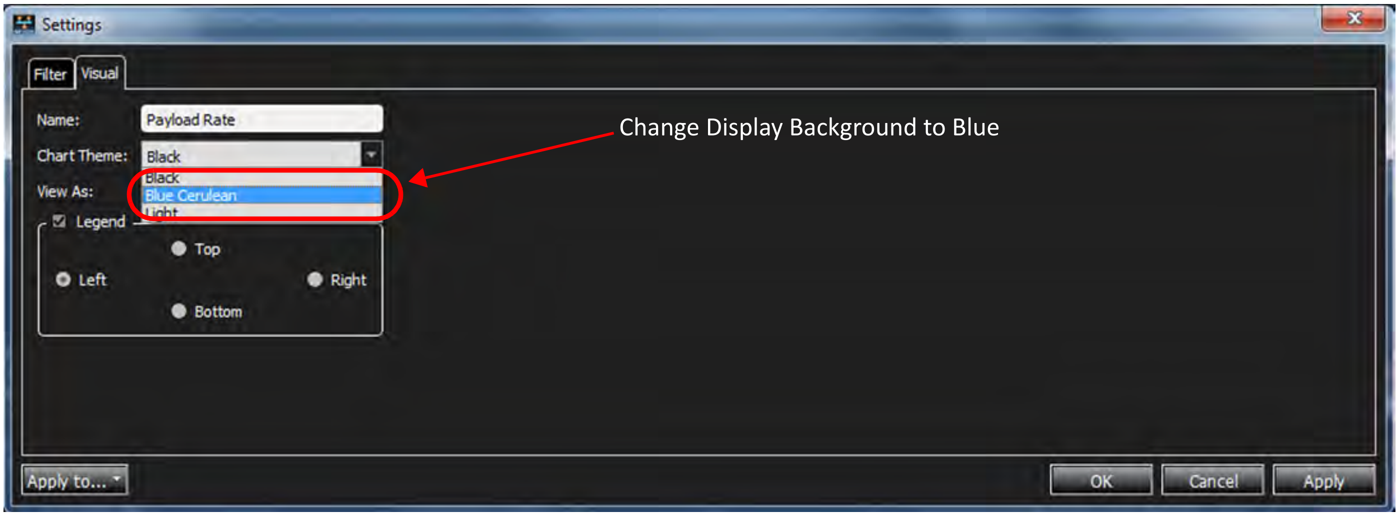


Figure 4.162: Options to Change Visual Displays of Traffic

Changing the background to blue is shown in Figure 4.163.

Figure 4.163: Traffic Display Background: Blue

If you compare these graphs with the ones from Figure 4.155, you'll see the reduced amount of traffic because of the filters added.

Selecting "Light" will generate a light colored background on the displays. See Figure 4.164.

Figure 4.164: Background of Graphs Changed to Light

You can also display the traffic in Area Charts or Tables. See Figure 4.165.

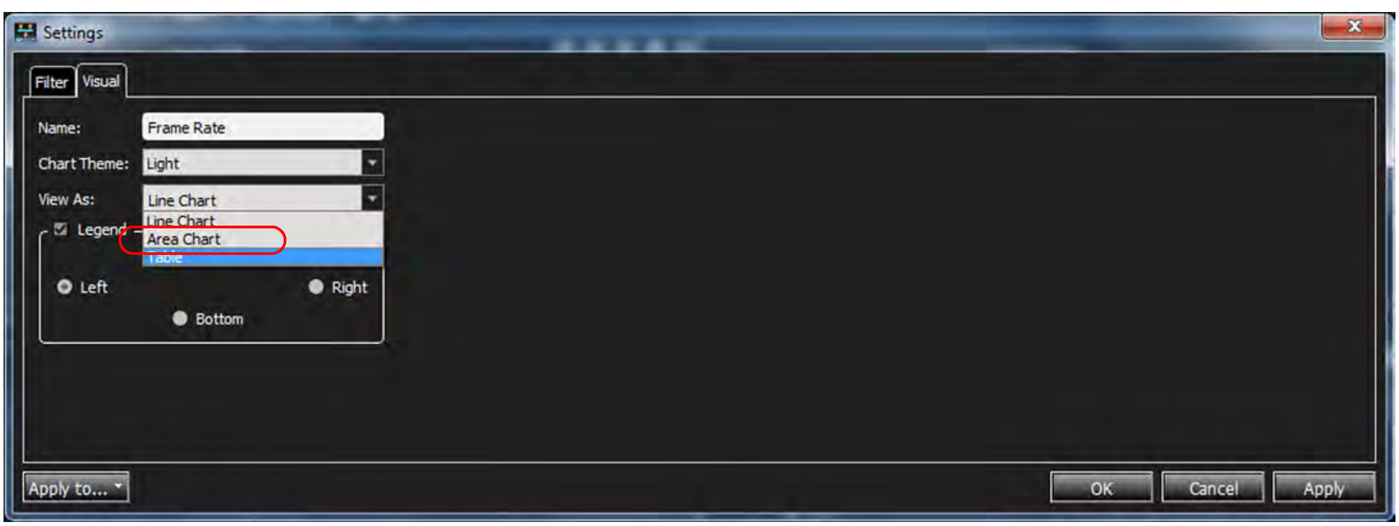


Figure 4.165: Select Area Chart or Table to Display Traffic

See Figure 4.166 for Area Chart displays and Figure 4.167 for Table displays.

Figure 4.166: Traffic Displayed as Area Graphs

Frame Rate

Port	Frame/S
P1	25830.08
P2	32729.68
P3	25814.75
P4	32709.77
P5	0.00
P6	0.00
P7	0.00
P8	0.00

Frame Rate

Port	Frame/S
P1	25830.08
P2	32729.68
P3	25814.75
P4	32709.77
P5	0.00
P6	0.00
P7	0.00
P8	0.00

Error Count

Port	Count
P1	0.00
P2	0.00
P3	0.00
P4	0.00
P5	0.00
P6	0.00
P7	0.00

Average Frame Size

Port	Bytes
P1	2424.31
P2	2299.93
P3	2423.62
P4	2300.61
P5	0.00
P6	0.00
P7	0.00

Figure 4.167: Traffic Displayed in Table Format

Another option is to change the location of the Legend within each display. In this case, the Legend is the Port Numbers. They can be moved to the Left, Top, Right or Bottom of the display. See Figure 4.168.

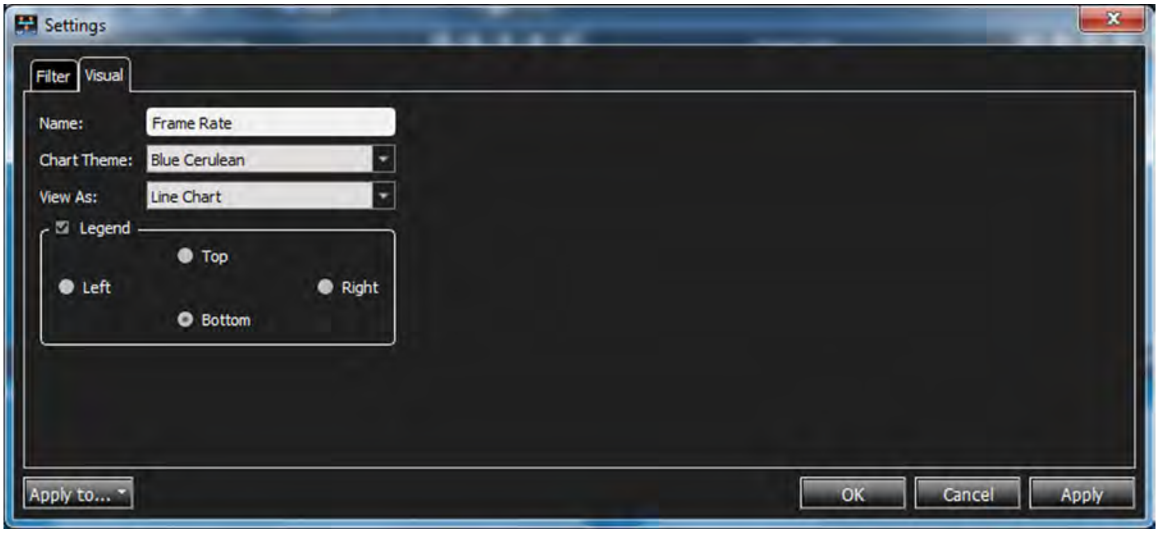


Figure 4.168: Location of Legend on Displays

The Legends displayed on the Bottom of the Graphs is shown in Figure 4.169.

Figure 4.169: Legends Displayed at Bottom of Graphs

4.4.3 Log Files

Log File Enable

To record the traffic in a log file in CSV format, select the Log Enable button on the Main Toolbar, see Figure 4.170.

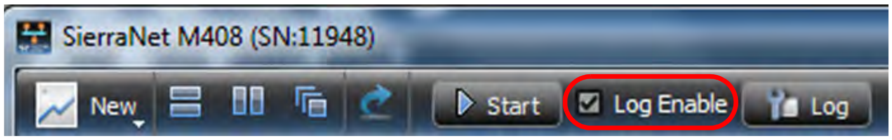


Figure 4.170: Log File Enable

Log File Settings

The log file Settings can be changed by selecting the “Wrench” icon, see Figure 4.171.

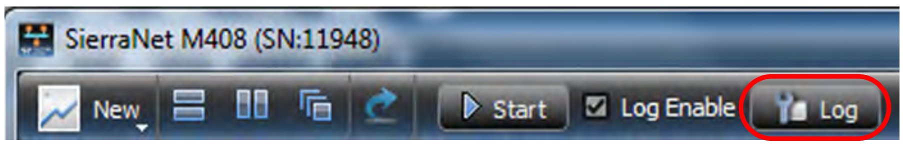


Figure 4.171: Log File Settings

Log File Location

The Location of the default Log File is shown below, see Figure 4.172:

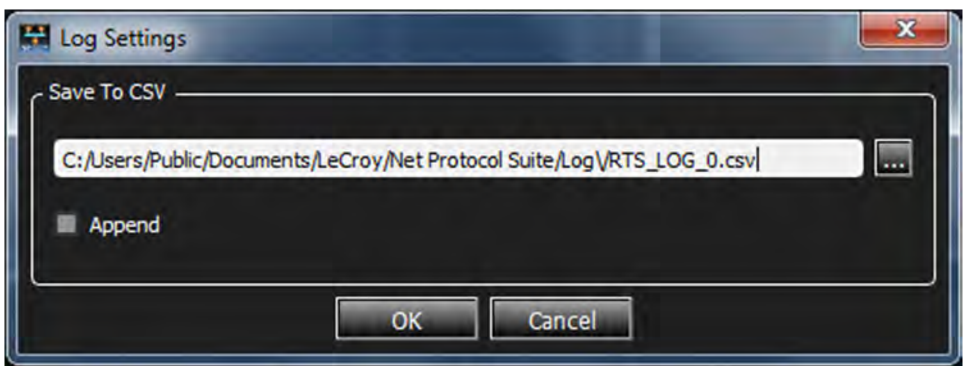


Figure 4.172: Location of Log File

If you click on the “...” icon, the contents of the log file folder will pop up (Figure 4.173).

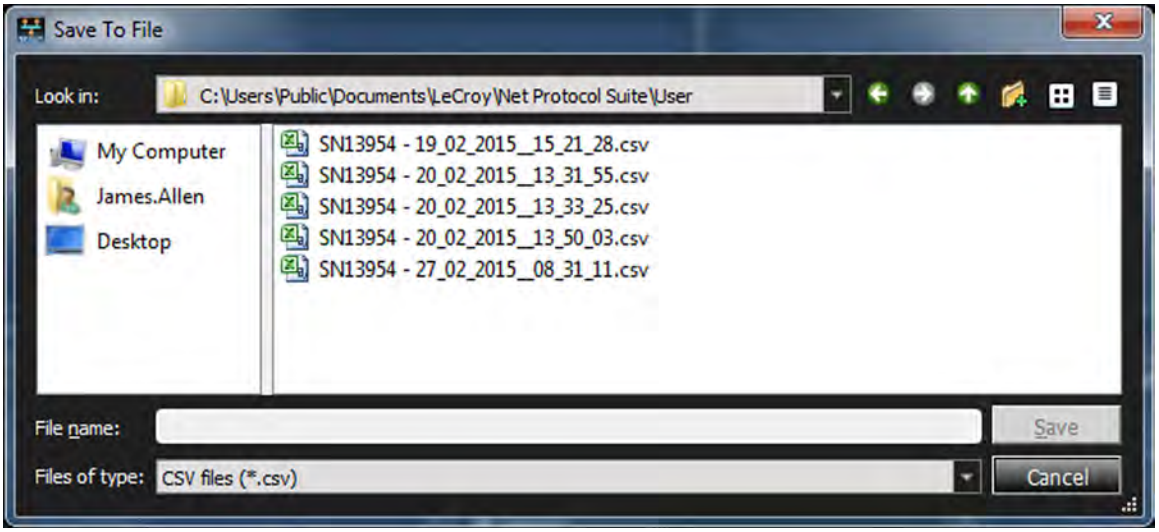


Figure 4.173: Log File Folder

Click on the "Start" icon to display traffic in the various windows and generate a log file.

The log file for the current scenario is named SN11948_1June_2015. See Figure 4.174.

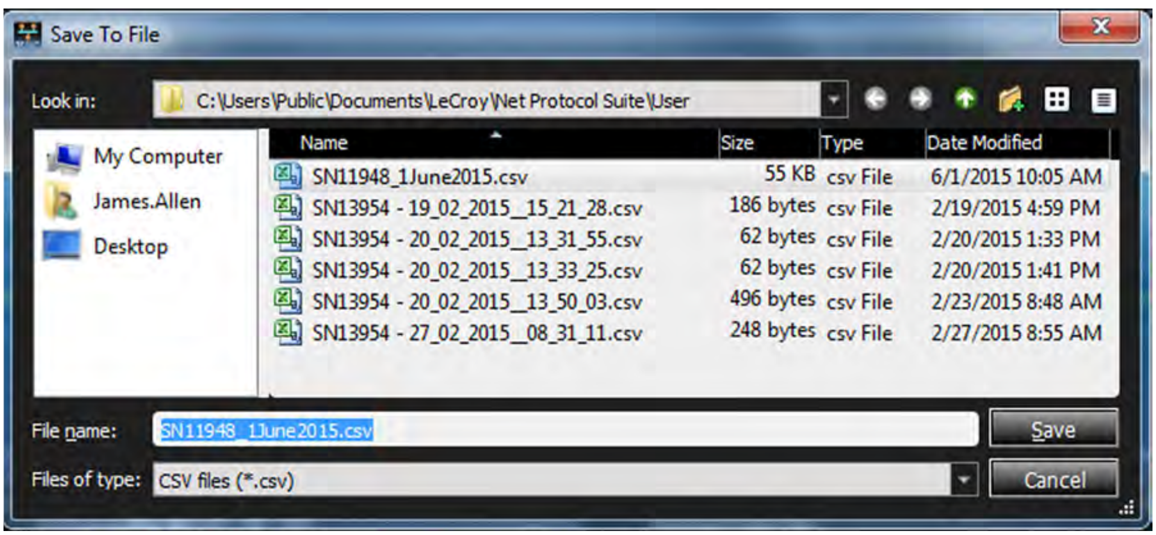


Figure 4.174: New Log File

If you open the file from the location shown in Figure 4.175, you will see a spreadsheet similar to Figure 4.176. This log file has been manually edited to remove ports that are not being used.

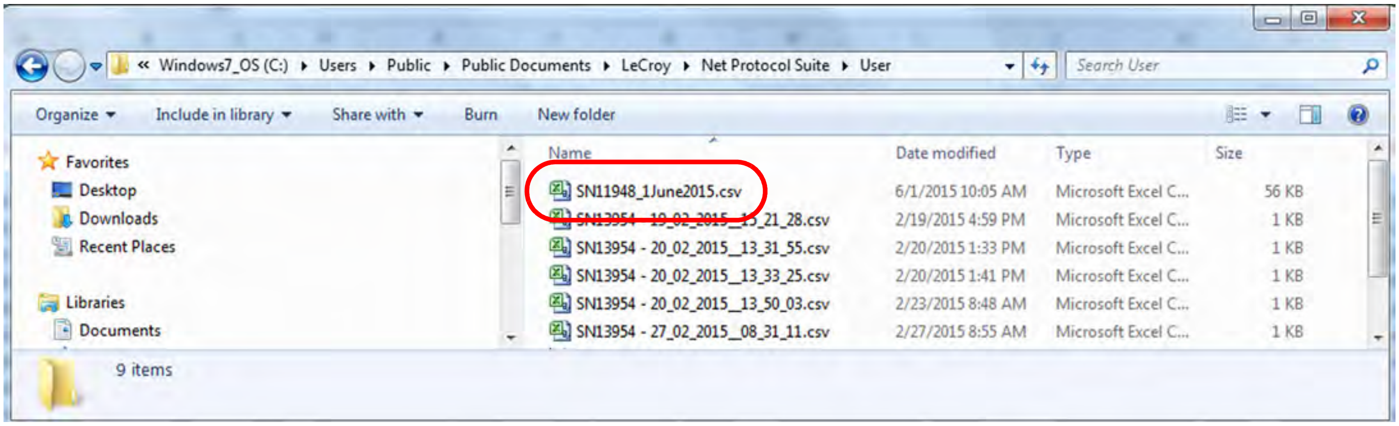


Figure 4.175: Location of Log File

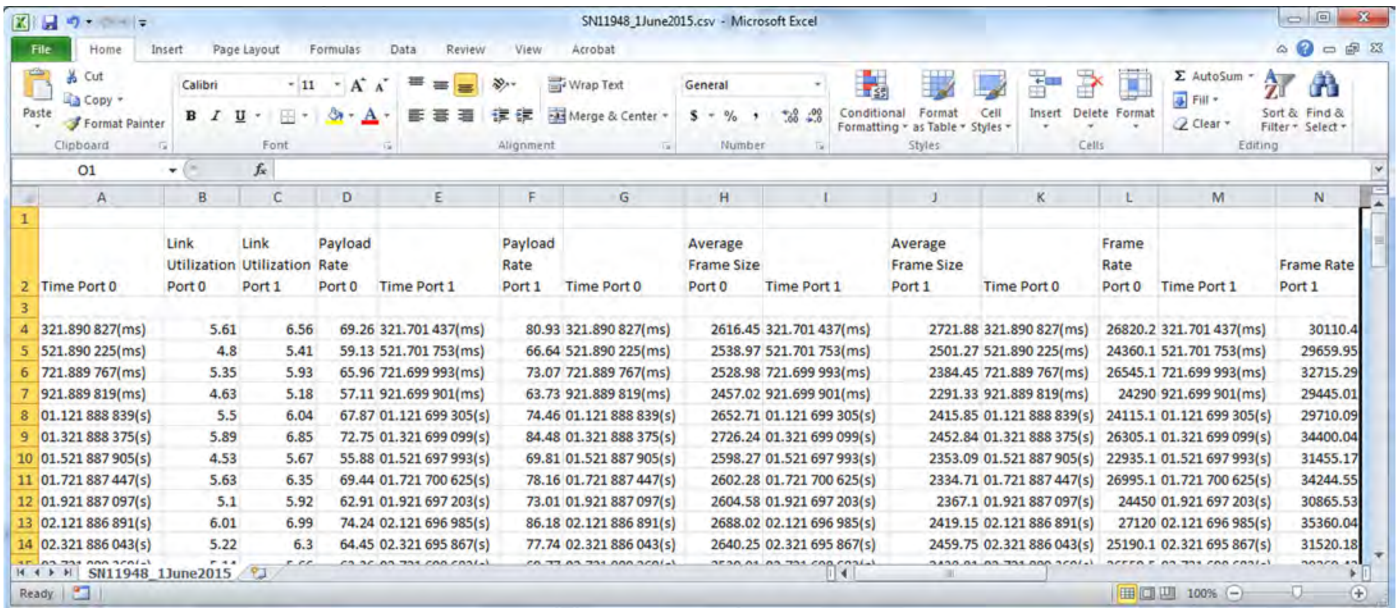


Figure 4.176: Log File Contents – Current Trace

4.5 Link Status Viewer

The Link Status Viewer allows you see if your link is up and if so the health of the link. The two most important things shown are described below.

NOTE: This section only applies to the SierraNet M648 and SierraNet M1288 models and only to PAM4 port configurations.

4.5.1 Overview of PAM4 Link Signaling

50G PAM4 Ethernet (50GE) signaling is done with two logical lanes transmitted over one physical lane. Each logical lane has a unique marker value transmitted on it. The physical media can be electrical backplane, twinaxial copper or fiber.

64G PAM4 Fibre Channel (64GFC) is done with one logical lane over one physical lane and only has one alignment marker as opposed to two markers for 50GE. The physical media is typically optical fiber.

In order for a 50GE link to come up, the physical coding sublayer must first achieve alignment marker lock (AM lock) on both logical lanes. After marker lock on all lanes is achieved the logical lanes are deskewed and reordered.

For 64GFC the M648 protocol analyzer physical coding sublayer splits the incoming signal into two bit streams and individually locks onto the two halves of the single 64GFC alignment marker.

Lock to only half of the markers may indicate that Gray coding, polarity or other settings are not consistent.

After the logical lanes are locked, deskewed and reordered, the bit error rate (BER) of the logical lanes and of the entire link can be found by counting the bit errors in correctable FEC blocks.

An RS(544,514) FEC block is a 5440-bit block of link data. This 5440-bit block consists of 544 10-bit symbols. An RS(544,514) FEC can correct up to 15 symbols in a single 544 symbol FEC block.

4.5.2 Using the Link Status Viewer

To open the Link Status Viewer:

1. Click the wrench icon to the right of the device (Figure 4.177). The Device Settings window opens (Figure 4.178).

Figure 4.177: Open Status Viewer

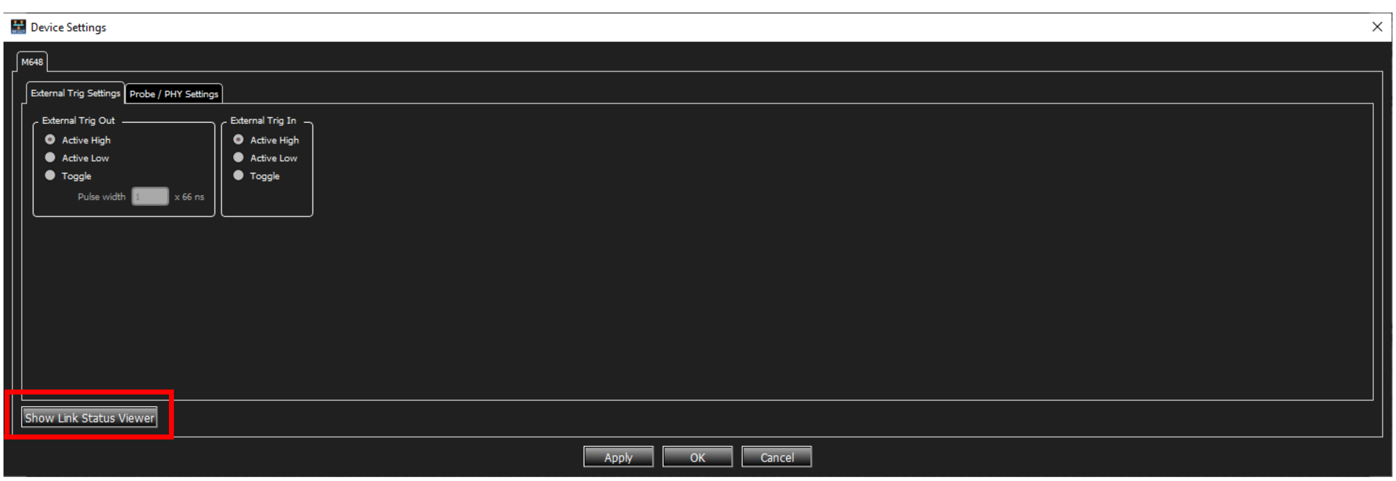


Figure 4.178: Device Settings Window

2. Click the Show Link Status Viewer. The Link Status Pane displays: Figure 4.179 for the M648 and Figure 4.180 for the M1288.

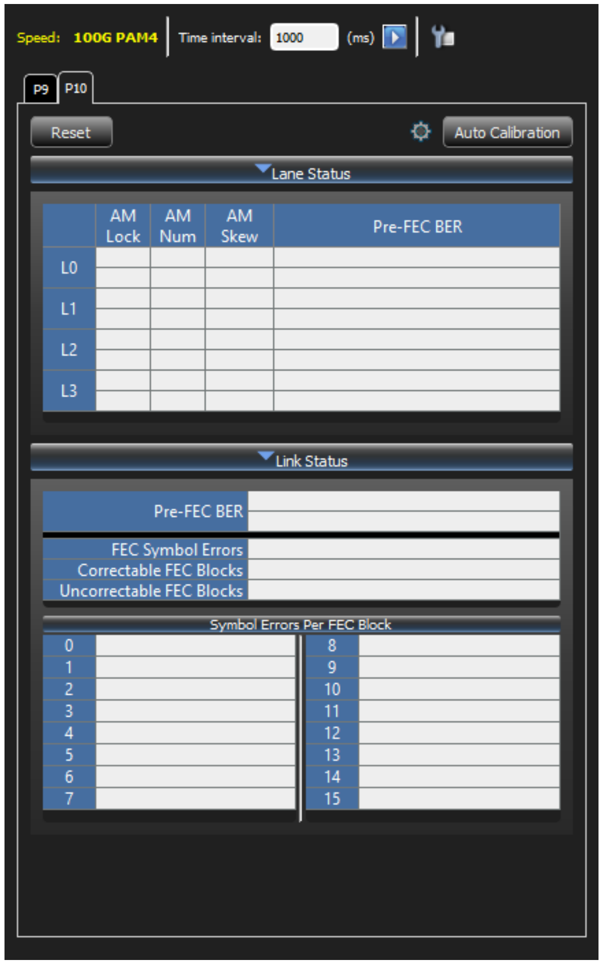


Figure 4.179: Link Status Viewer (for M648)

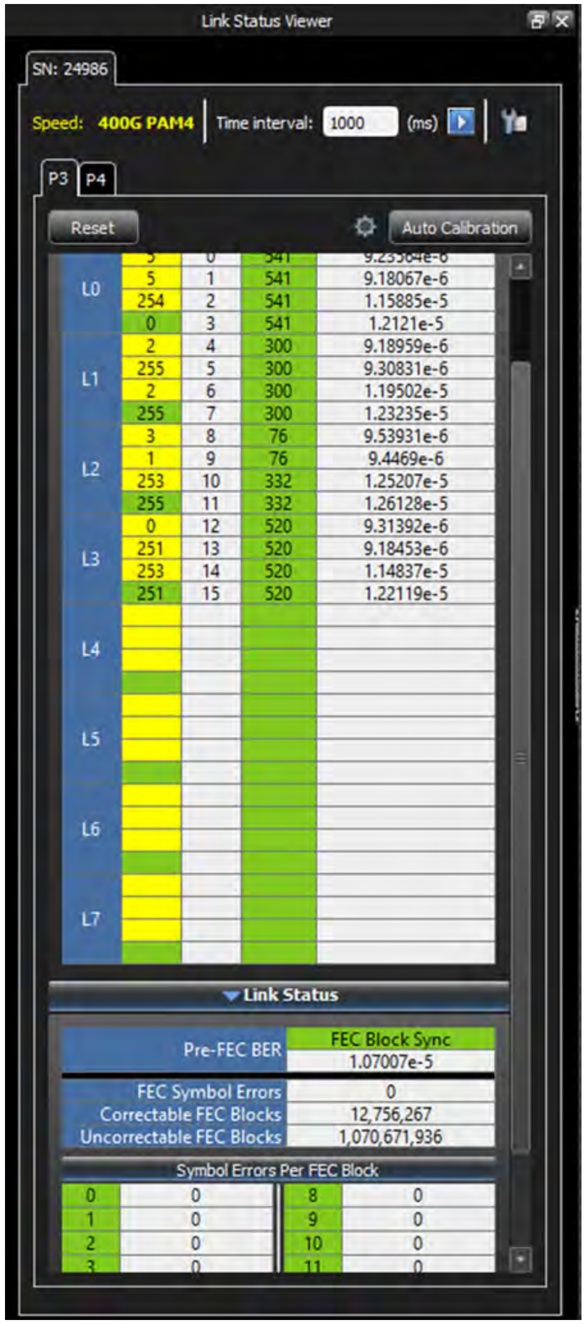


Figure 4.180: Link Status Viewer (for M1288)

The Link Status Viewer contains the following information:

Lane Status

- AM Lock (Alignment Marker Lock)
  - A healthy link shows the AM Lock column green for both marker lockers 0 and 1.
  - If either marker lock 0 or 1 bounces out of lock and then relocks the color for that AM lock is yellow.

- If either marker lock 0 or 1 is currently unlocked the color for that AM Lock is red.

- AM Num (Alignment Marker Number)
  - Each logical lane has a unique marker value. The marker value found is shown.
  - No color for AM Num.
- AM Skew (Alignment Marker Skew)
  - The logical lanes may be skewed in time. The AM Skew column indicates the number of bits the logical lanes are skewed relative to each other.
  - The 50GE spec (802.3cd) maximum skew spec is 4781 bits.
- Lane Status Pre-FEC BER (pre-FEC bit error rate)
  - The number of bits errors are counted for each logical lane and the bit error rate (BER) is shown.
  - At 50GE each logical lane is 26.5625 Gbps. Five bit errors on one logical lane in one second would result in a lane BER of 1.88e-10
  - If marker lock is not achieved this value is blank.

Link Status

- FEC Block Sync
  - If the FEC decoder receives three consecutive FEC blocks that have no errors or are correctable then FEC block sync is achieved and the field is highlighted green.
  - If FEC block sync is lost and regained the field is highlighted yellow.
  - If the FEC decoder receives three consecutive FEC blocks that are uncorrectable then FEC block sync is lost and the field is highlighted red.
- Link Status Pre-FEC BER (pre-FEC bit error rate)
  - The number of bits errors are counted for all logical lanes and the bit error rate (BER) is shown.
  - At 50GE the link is 53.125 Gbps. A total of twelve bit errors across all logical lanes in one second would result in a link BER of 2.26e-10.
  - No color.
- FEC Symbol Errors
  - The total number of symbol errors counted since counter reset.
  - Uncorrectable FEC blocks 16 of this count since the number of symbol errors is unknown in this case.
  - No color.
- Correctable FEC Blocks
  - The total number of correctable FEC blocks counted since counter reset
  - No color
- Uncorrectable FEC Blocks

- The total number of uncorrectable FEC blocks counted since counter reset.
- If zero and FEC block sync, the field is highlighted green.
- If non-zero and FEC block sync, the field is highlighted orange.

❑ Symbol Errors per FEC Block

- This is a bucket counter of symbol errors per FEC block. The number of symbol errors in a correctable RS(544,514) FEC block is known and can range from 0 to 15 symbol errors. For example if a correctable FEC block with three symbols errors occurs then Symbol Errors Per FEC Block[3] would increment by 1.
- These symbol error counters are an indicator of the link health. Symbol errors per FEC block [0-9] are always highlighted green.
- If symbol errors per FEC block [10-15] are non-zero this indicates a link with a high BER and is likely to have uncorrectable FEC blocks. Non-zero values are highlighted yellow.

Link and Lane Status per Port

Both Link and Lane status are available per port.

Time Interval

Time interval for reading all the above information can be selected.

Reset

The content of counters per port can be reset.

Probe/Phy Settings

1. Open Link Status and probe settings in real-time to see how any change in probe/ phy settings impacts link status.
   - There are two tab pages for ports, and each tab page shows the link status for one port.
   - The time interval timer value is 1000ms by default. The minimum allowed value is 200ms.
2. To change the interval, open link status view and change the value, then press the **Start** icon next to the time interval timer. The session restarts with the new value.

   There are two expandable sections in the view (Lane Status and Link Status). Both sections can be expanded or collapsed.

Chapter 5

Trace File Analysis

5.1 Viewer Display

After data is captured (Recorded), the Viewer displays the captured data and saves it as a trace file with a **.get** file extension.

Statistics are available only after the whole trace has uploaded. The data is available for analysis in various views, which are explained in this section.

Click on **Analysis** in the Analyzer main menu options to enable and disable different trace views.

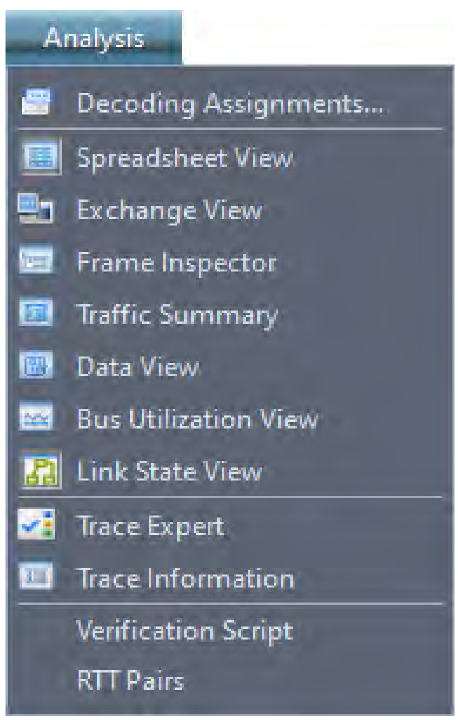


Figure 5.1: Analysis Menu

5.1.1 Decoding Assignments

The **Analysis → Decoding Assignments...** menu controls the decoding settings for the opened trace file. The default set of Decoding Assignments are set in the **Setup → Preferences → Decoding Assignment** menu (see 3.2.2.2, *Preferences*). The decoded ports and types of traffic can be seen by selecting **Analysis → Decoding Assignments** in the Main Menu. If there is traffic in the trace that needs special decoding you can add port assignments and traffic types in the same window on a trace by trace basis. After the new assignments are made and the window is closed, the trace file decoding will automatically be updated to apply the new assignments.

The first option in the Analysis menu allows you to set decoding assignments by selecting **Analysis → Decoding Assignments....** When **Decoding Assignments** is selected the default Port Assignments and SCSI assignments will be displayed. You can also see the default SCSI traffic types that were decoded. You can also see the default SCSI decoding assignments. In this case all SCSI traffic used the SBC3 Command Set. See Figure 5.2.

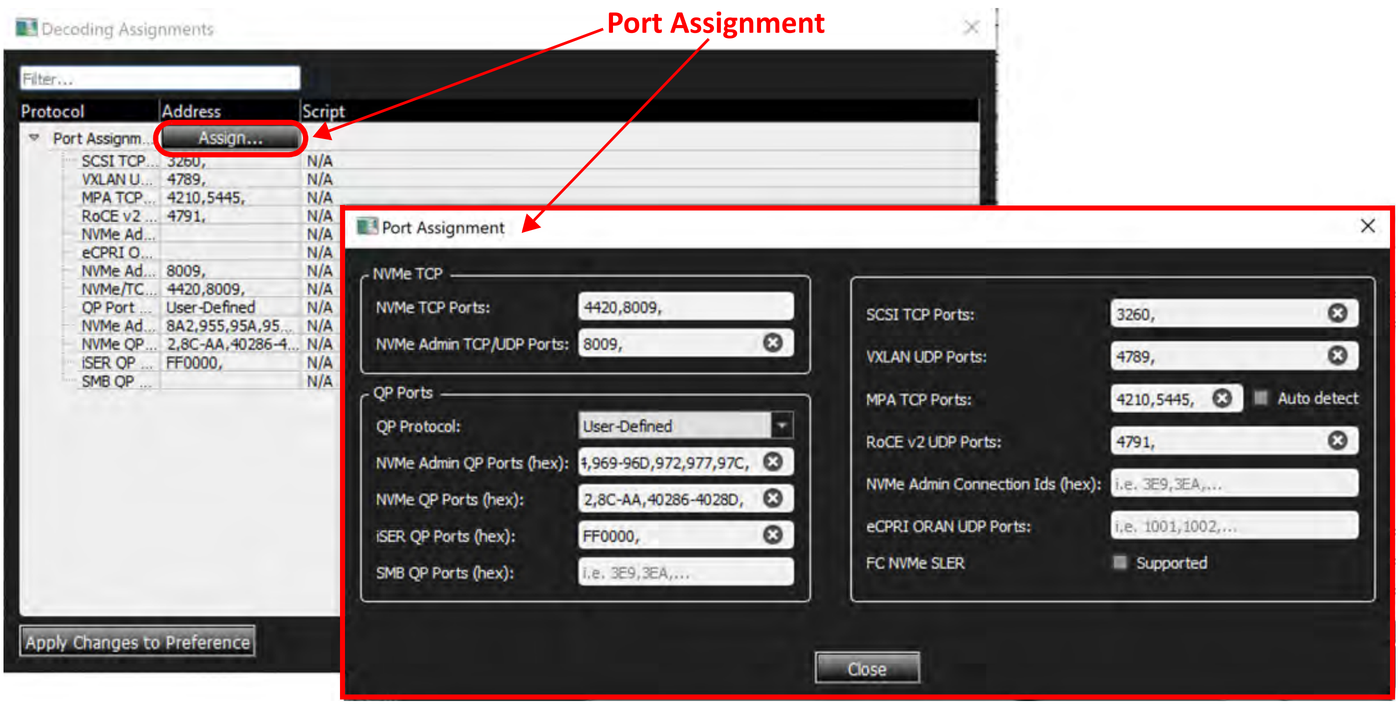


Figure 5.2: Port Assignments

eCPRI ORAN UDP Ports: Specifies UDP port numbers for ORAN over IP/UDP.

QP Ports: Gives user the option to choose any of the following:

- User defined: Means if the software captures the connection phase, it extracts the QP port and uses it for the desired protocol, otherwise the user can add QP ports manually to “NVMe QP port” or “iSER QP Port” or “iSER QP Port”.
- NVMe: Means software considers any QP port as NVMe.
- iSER: Means software considers any QP port as iSER.
- SMB: Means software considers any QP port as SMB

There are two types of data traffic that can be associated with different Decoding Assignments:

- Port Assignments: See 5.1.1.1, *Port Assignments (Default Set from Preferences)*.
- Small Computer System Interface (SCSI) Assignments: See 5.1.1.2, *Default SCSI Decoding Assignments Found in Trace*.

5.1.1.1 Port Assignments (Default Set from Preferences)

Initially the Net Protocol Suite software will decode all of the default port assignments set in the Preferences (see 3.2.2.2, *Preferences*) and display them when you select **Analysis → Decoding Assignments**. In the captured trace the following Port Assignments and data traffic were decoded:

- SCSI TCP Ports
- VXLAN UDP Ports
- MPA TCP Ports (with Auto Detect)
- IB BTY UDP Ports
- NVMe QP Ports
- iSER QP Ports

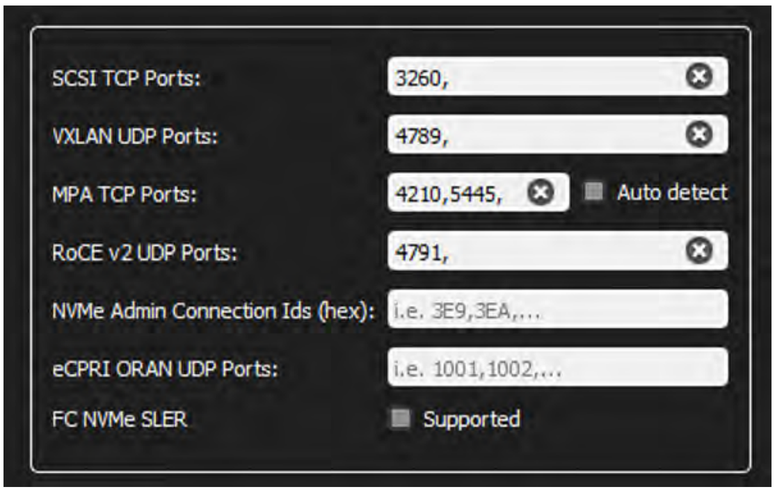


Figure 5.3: Port Assignment Window

If you know there are more ports in the system that were not decoded, you can add port numbers by typing into the appropriate Port type. See Figure 5.4.

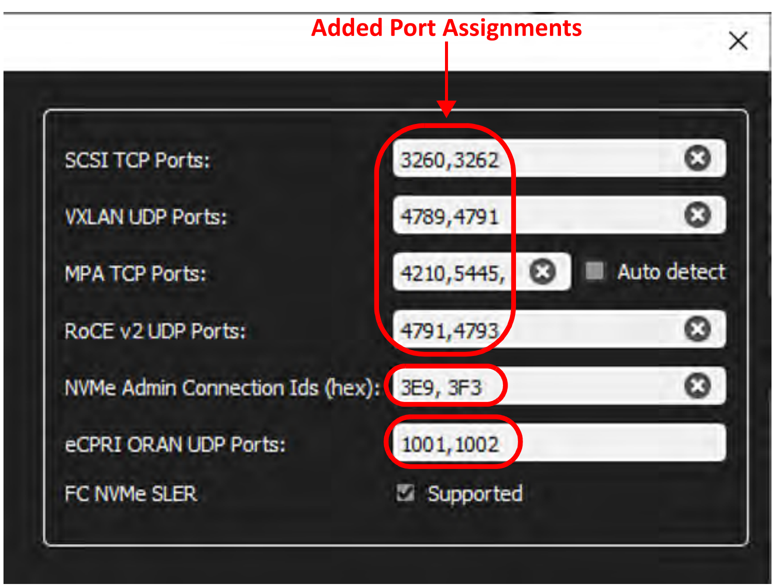


Figure 5.4: Ports Added to Defaults

Select **Analysis → Decoding Assignments** to see the updated Port Number assignments (Figure 5.5).

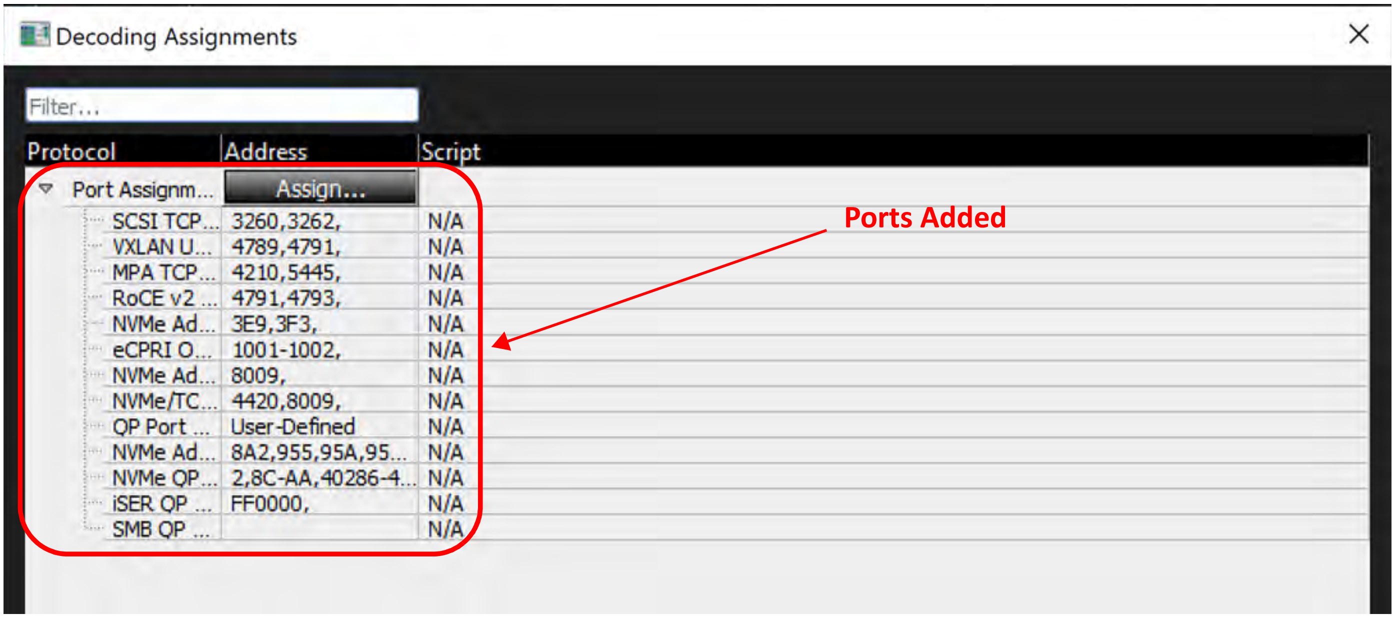


Figure 5.5: Ports Added to the Default Set

5.1.1.2 Default SCSI Decoding Assignments Found in Trace

Initially, only SBC3 SCSI data traffic was detected. See Figure 5.6.

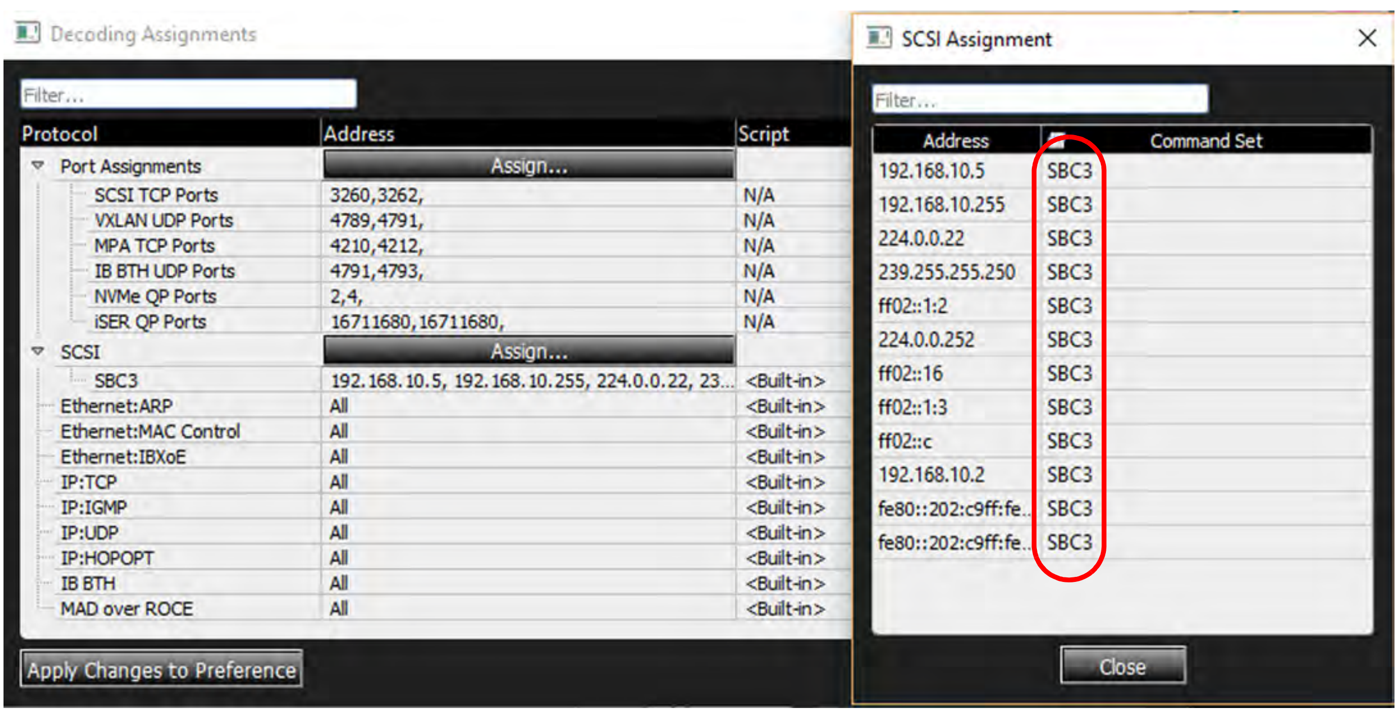


Figure 5.6: SCSI Traffic Types Added to Default Set

If other types of SCSI traffic should have been decoded at specific address, you can update the types of traffic and addresses with the following decoding assignments:

- MMC—Multi-Media Commands
- SBC—Block Commands
- SMC—Medium Changer Commands
- SSC
- SCC—Controller Commands
- OSD—Object -Based Storage Devices Commands
- ADC—Automation/Drive Interface Commands

See Figure 5.7.

NOTE: The latest supported protocols and specifications are listed in Table D.1, Appendix D, *Supported Protocol Decoders*.

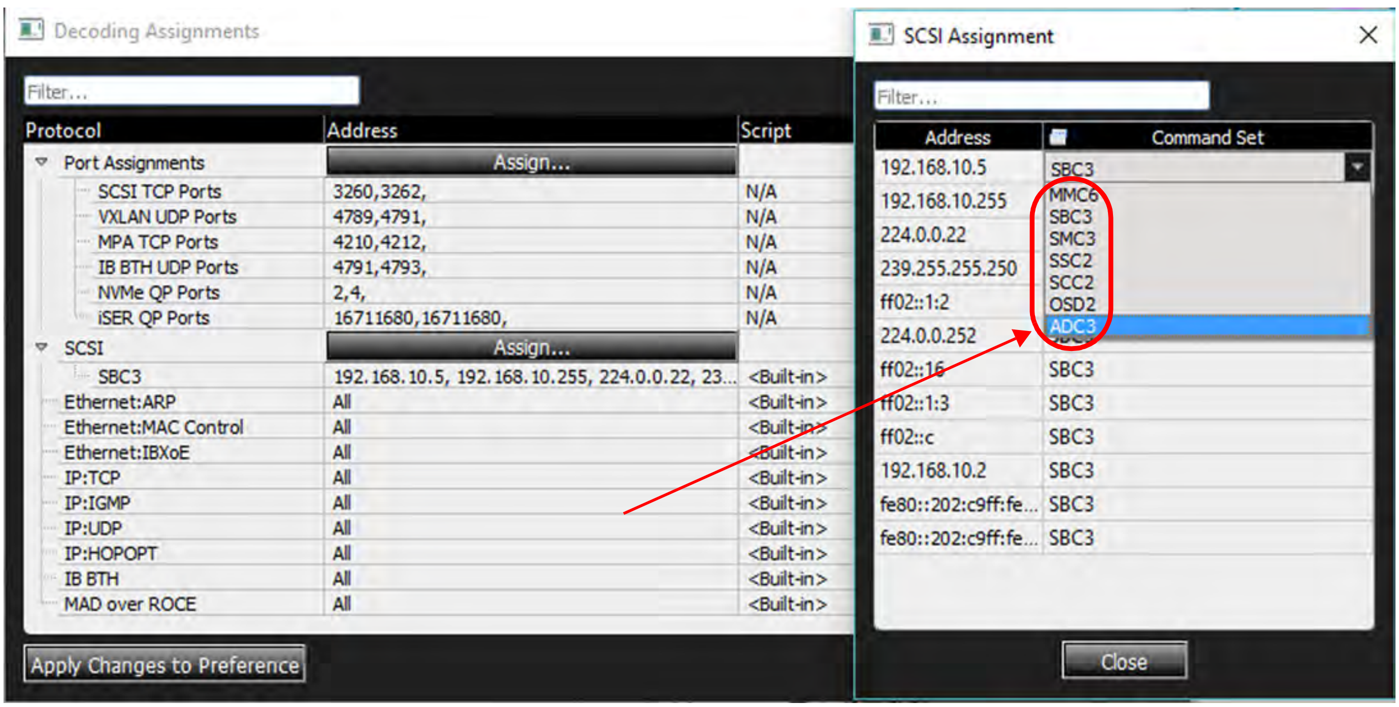


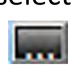
Figure 5.7: Additional Types of SCSI Decodes Available

5.1.1.3 Script Column

The Script column identifies the script that will be used to decode the protocol. **<Built-in>** means that a built-in decoder will be used.

- Double-click in the cell to specify the path to a user-defined script (.udd).

  See the Net Protocol Suite User-DeMMC: Multi-Media Commandsfined Decoding manual for details on how to write a decoding script.

- To select traffic types and apply a custom decoding script, double-click the far right tab  (Figure 5.9), then select the script you have written.

  An example has been placed in the directory shown in Figure 5.8.

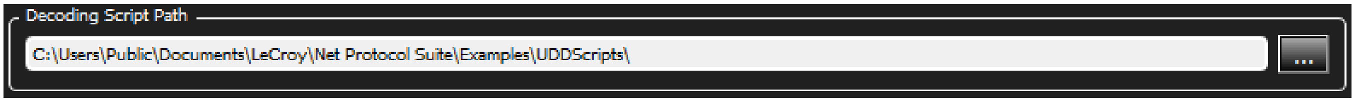


Figure 5.8: Decoding Script Path

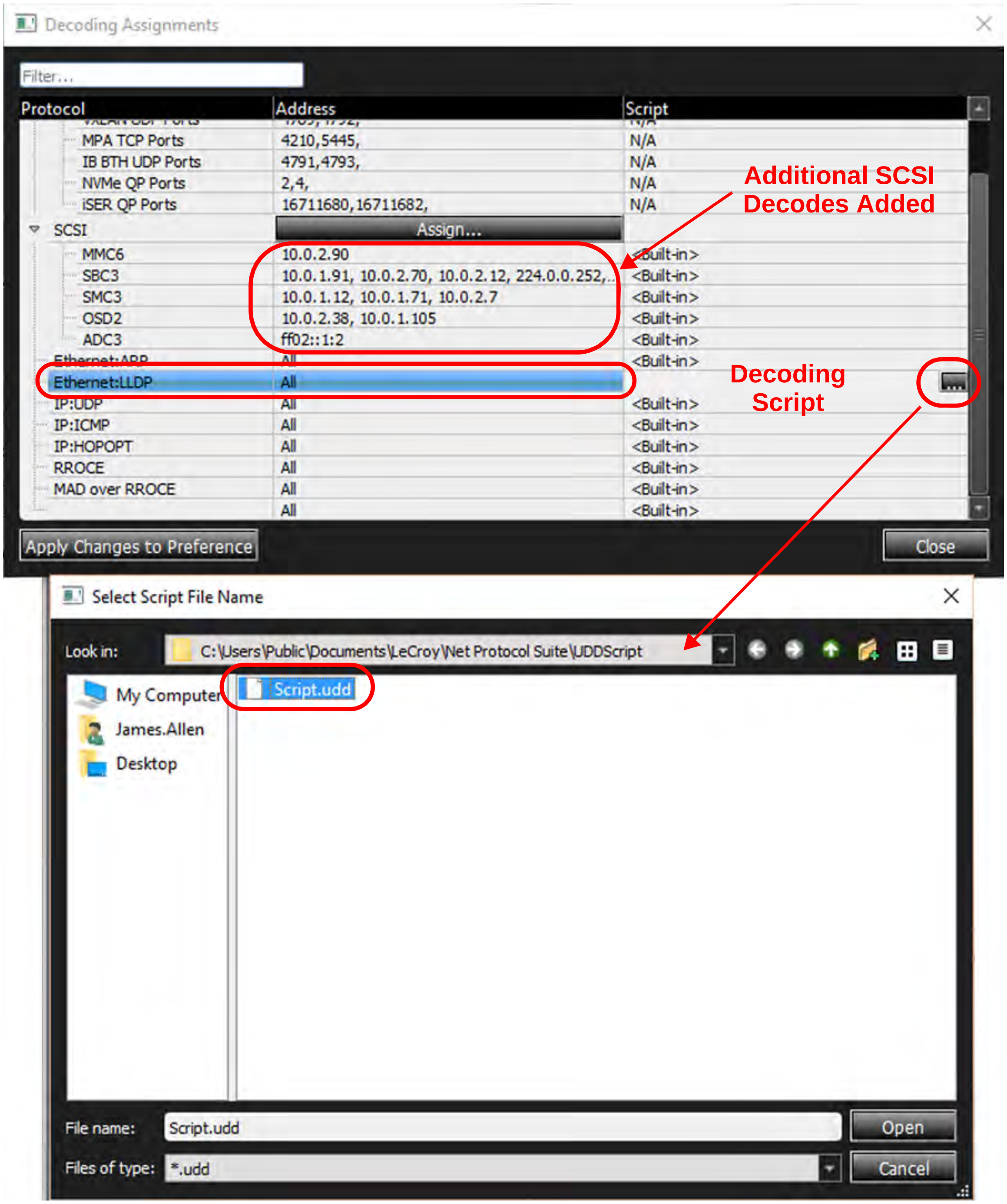


Figure 5.9: Custom Decoding Script Applied

5.2 Switching Analysis Views

- To enable and disable views, use the Analysis menu item or the Analysis toolbar.

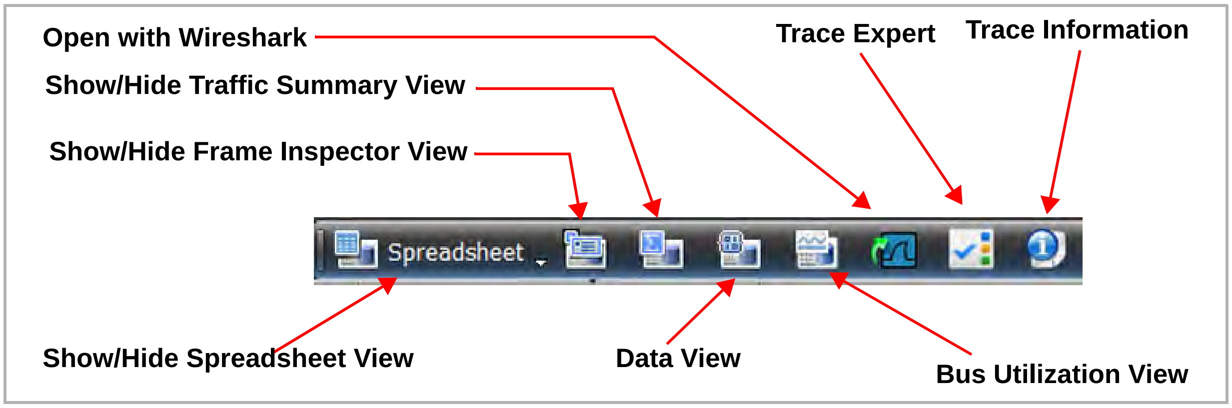


Figure 5.10: Analysis Toolbar

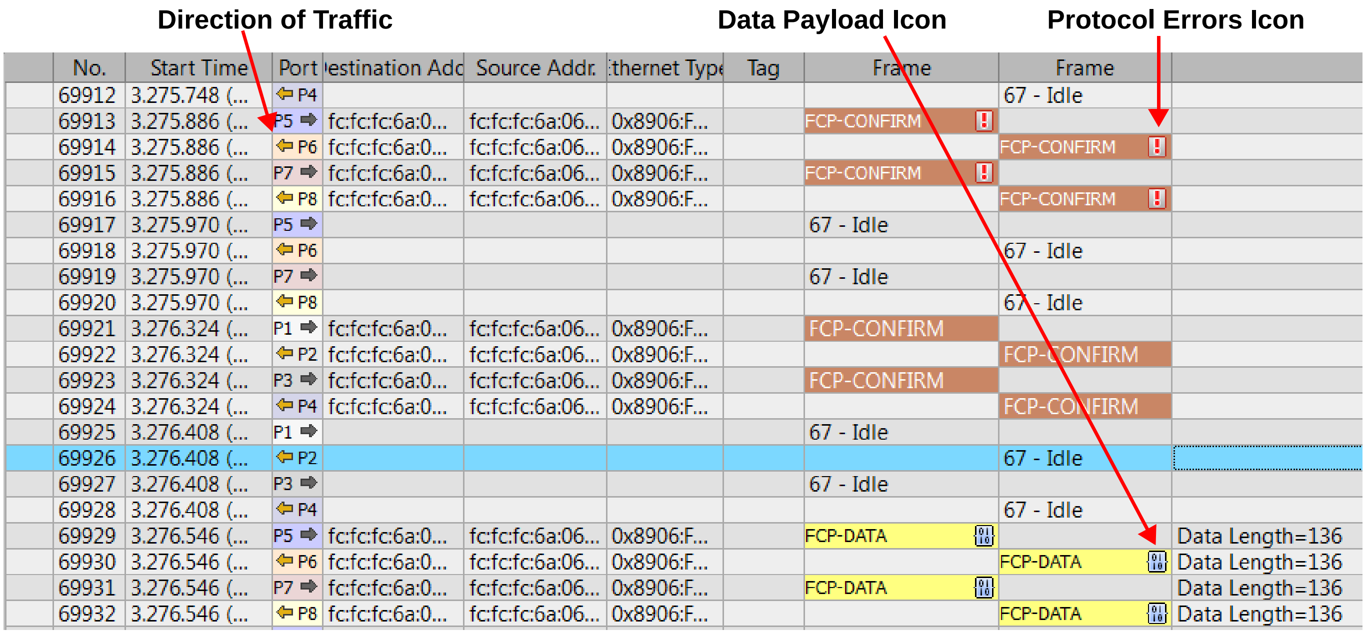
- After you select a view, it appears in a separate window.
- To increase the new window display size, use Zoom in and Zoom out from the View menu item or the buttons from the View Toolbar.
- To rearrange the tiling, select the **Window** menu and choose **Window Cascade** or **Window Tile.**

5.2.1 Spreadsheet View

The Spreadsheet View displays captured events sequentially, one per line. The events are decoded and event fields are displayed column by column.

To display the Spreadsheet View of the current capture, click **Analysis** → **Spreadsheet View** or click the 

button on the View toolbar.



No.	Start Time	Port	estination Add	Source Addr.	thernet Type	Tag	Frame	Frame	
69912	3.275.748 (...	⇦ P4						67 - Idle	
69913	3.275.886 (...	P5 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
69914	3.275.886 (...	⇦ P6	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
69915	3.275.886 (...	P7 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
69916	3.275.886 (...	⇦ P8	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
69917	3.275.970 (...	P5 ⇨					67 - Idle		
69918	3.275.970 (...	⇦ P6						67 - Idle	
69919	3.275.970 (...	P7 ⇨					67 - Idle		
69920	3.275.970 (...	⇦ P8						67 - Idle	
69921	3.276.324 (...	P1 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
69922	3.276.324 (...	⇦ P2	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
69923	3.276.324 (...	P3 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
69924	3.276.324 (...	⇦ P4	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
69925	3.276.408 (...	P1 ⇨					67 - Idle		
69926	3.276.408 (...	⇦ P2						67 - Idle	
69927	3.276.408 (...	P3 ⇨					67 - Idle		
69928	3.276.408 (...	⇦ P4						67 - Idle	
69929	3.276.546 (...	P5 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-DATA		Data Length=136
69930	3.276.546 (...	⇦ P6	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-DATA	Data Length=136
69931	3.276.546 (...	P7 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-DATA		Data Length=136
69932	3.276.546 (...	⇦ P8	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-DATA	Data Length=136

Figure 5.11: Spreadsheet View

5.2.1.1 Data Payload

1. Click the icon to display the Data Payload window (Figure 5.12).
2. Click the **Export** button to export the data payload to a text file.
3. Enter a value and click the **Next** or **Previous** button to search the data payload in Hexadecimal or ASCII format.

   The application looks for byte boundaries while searching. Hence, searching for '1A' will not result in a match because it spans two bytes, whereas searching for '01AC' will result in a match (Figure 5.13).
4. Click the **Columns in Row** and **Bytes in Column** drop-down menu lists in the View pane to configure the display.
5. Click **Hex** or **ASCII** to specify the search criteria.

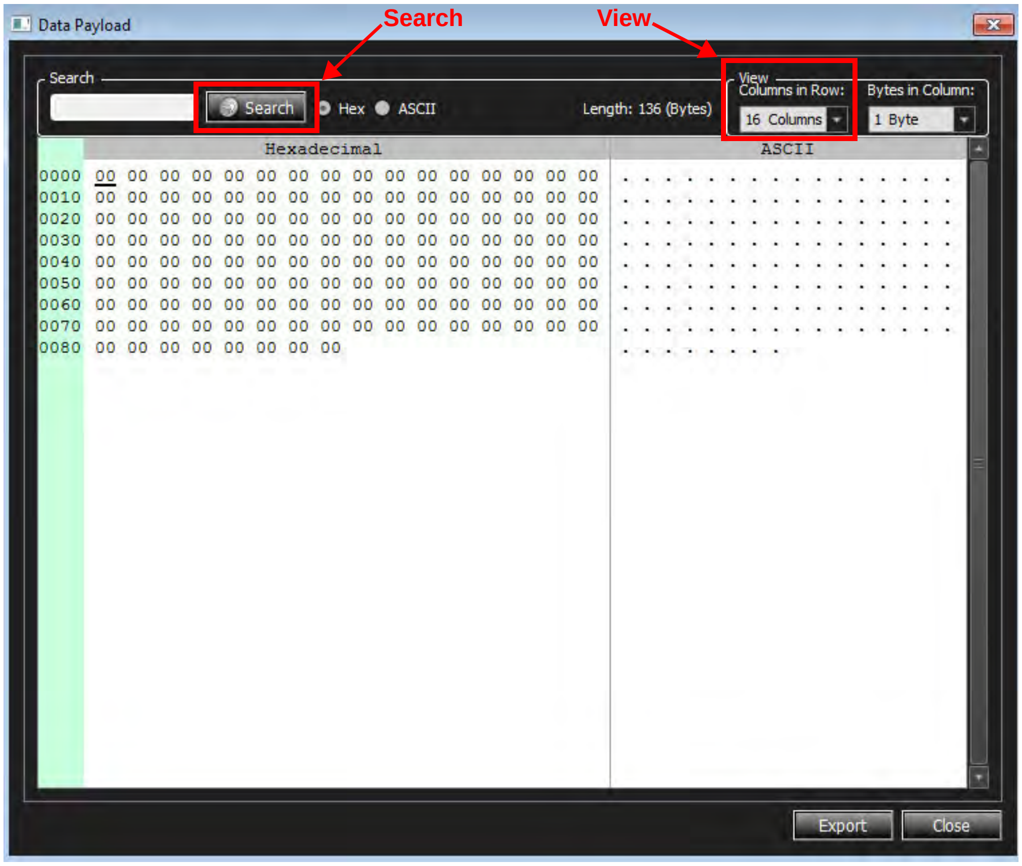


Figure 5.12: Data Payload Window

6. To configure the display, click the **Columns in Row** and **Bytes in Column** drop-down lists in the View pane.

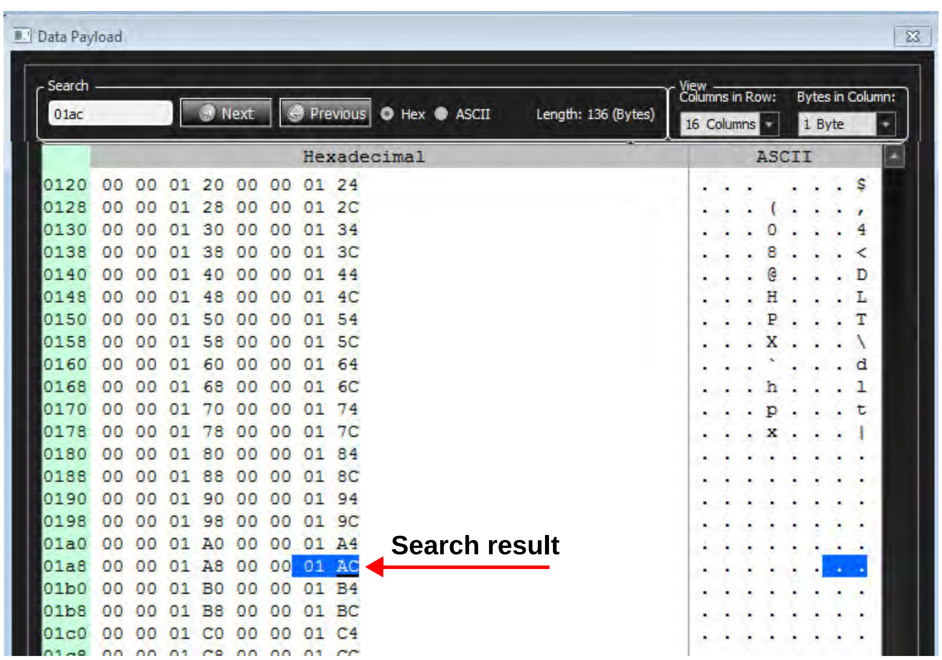


Figure 5.13: Data Payload Search Result.

5.2.1.2 Protocol Errors

Click the icon to display the Protocol Errors window (see Figure 5.14). The Code and Name are displayed.

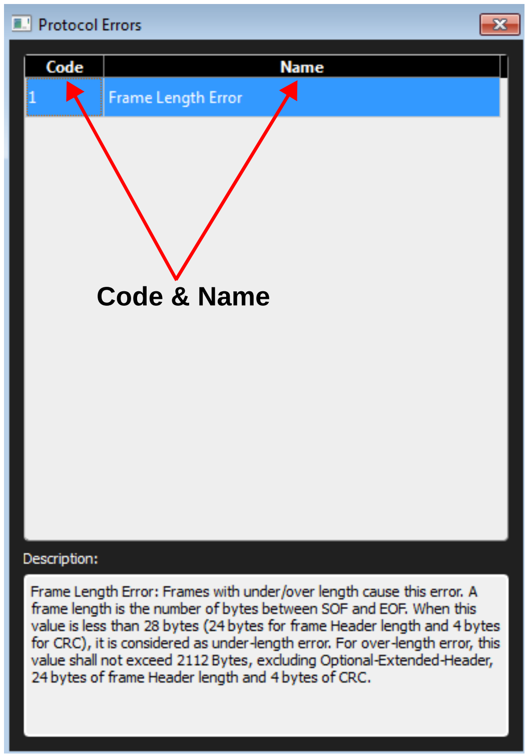
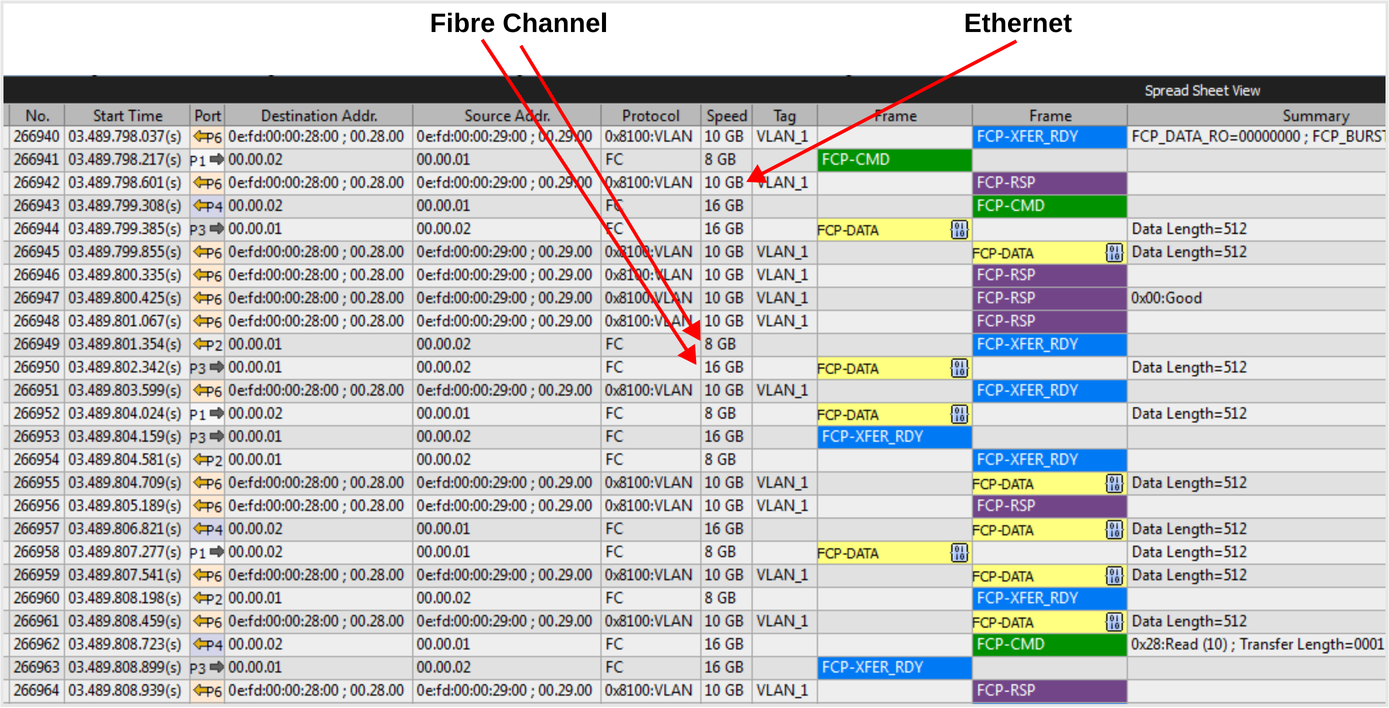


Figure 5.14: Protocol Error Window

5.2.1.3 Viewing Ethernet and Fibre Channel Traces

The application captures and displays both Ethernet and Fibre Channel data.



No.	Start Time	Port	Destination Addr.	Source Addr.	Protocol	Speed	Tag	Frame	Frame	Summary
266940	03.489.798.037(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-XFER_RDY	FCP_DATA_RO=00000000 ; FCP_BURST
266941	03.489.798.217(s)	P1	00.00.02	00.00.01	FC	8 GB		FCP-CMD		
266942	03.489.798.601(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266943	03.489.799.308(s)	P4	00.00.02	00.00.01	FC	16 GB			FCP-CMD	
266944	03.489.799.385(s)	P3	00.00.01	00.00.02	FC	16 GB		FCP-DATA		Data Length=512
266945	03.489.799.855(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266946	03.489.800.335(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266947	03.489.800.425(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	0x00:Good
266948	03.489.801.067(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266949	03.489.801.354(s)	P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266950	03.489.802.342(s)	P3	00.00.01	00.00.02	FC	16 GB		FCP-DATA		Data Length=512
266951	03.489.803.599(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-XFER_RDY	
266952	03.489.804.024(s)	P1	00.00.02	00.00.01	FC	8 GB		FCP-DATA		Data Length=512
266953	03.489.804.159(s)	P3	00.00.01	00.00.02	FC	16 GB		FCP-XFER_RDY		
266954	03.489.804.581(s)	P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266955	03.489.804.709(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266956	03.489.805.189(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266957	03.489.806.821(s)	P4	00.00.02	00.00.01	FC	16 GB			FCP-DATA	Data Length=512
266958	03.489.807.277(s)	P1	00.00.02	00.00.01	FC	8 GB		FCP-DATA		Data Length=512
266959	03.489.807.541(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266960	03.489.808.198(s)	P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266961	03.489.808.459(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266962	03.489.808.723(s)	P4	00.00.02	00.00.01	FC	16 GB			FCP-CMD	0x28:Read (10) ; Transfer Length=0001
266963	03.489.808.899(s)	P3	00.00.01	00.00.02	FC	16 GB		FCP-XFER_RDY		
266964	03.489.808.939(s)	P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	

Figure 5.15: Merged FC and Ethernet Traces in Spreadsheet View

5.2.1.4 Spreadsheet View Options

Right click in any row of the Spreadsheet View to display the context menu (Figure 5.16). Byte Oder is displayed for destination and source columns only.

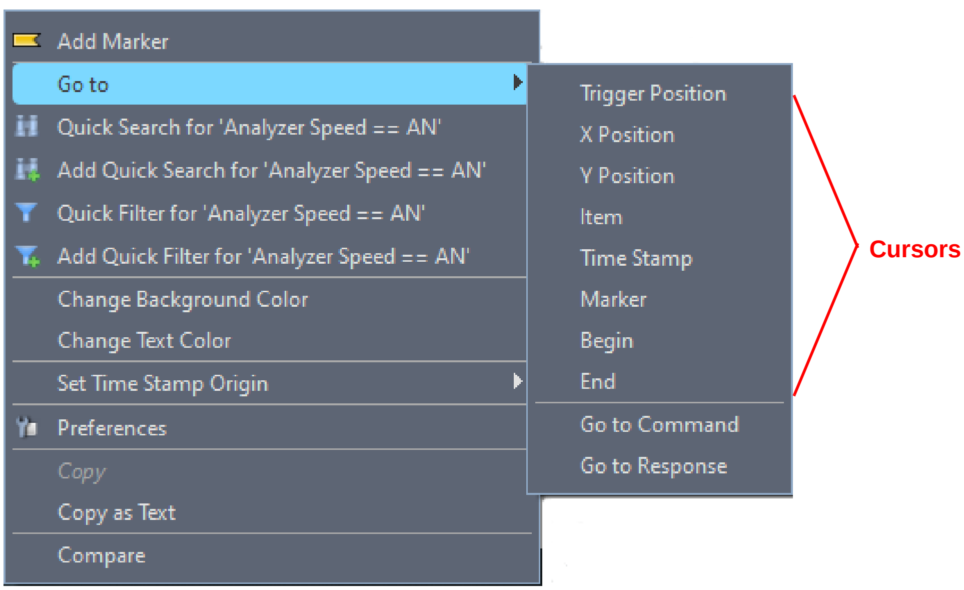


Figure 5.16: Locate Cursor

TABLE 5.1: Spreadsheet View Options

Menu Option	Description
Add Marker	Opens the Marker List dialog. You can add and delete markers (see 5.2.1.7, *Markers*.)
Byte Order	This option is context sensitive. This option allows a you left/ right align the data display in each cell.
Go to	The Go to option jumps to a related frame in the viewer. It displays the following sub-menu options to Go to Trigger, X or Y Position, Event, Time Stamp, Marker, Begin and End, which are all Cursors. See 5.2.1.8, *Cursors*.
Quick Search	Pops up the Quick Search Dialog.
Quick Filter	Pops up the Quick Filter Dialog.
Change Background Color	Displays colors to change the background.
Change Text Color	Displays colors to change the text.
Set Time Stamp Origin	There are four options to set time stamp origin. See *Set Time Stamp Origin*
Absolute	Sets the time stamp to zero when the recording starts. The first frame in the trace might have the time stamp larger than zero due to filtering, hiding or other reasons such as recording started in the middle of a frame.
Trigger	Sets time to when the trace was triggered.
Current Position	Sets time to the current position.
Based on System Time	Sets time based on the system time.
Preferences	Displays the Preferences window
Copy	Copies the frame to allow you to paste it in the Trigger settings and/or InFusion Scenario events.
Copy as Text	Copies the information from the frame and allows you to paste it into any text editor. See Figure 5.17 and Figure 5.18.
Compare	Compare data payload from two different transactions. See 5.2.1.6, *Compare (Data Payloads)*.

5.2.1.5 Copy as Text

Allows you to select a frame from the Spreadsheet View. Then you can copy and paste the information into any text editor (example: in Note Pad see Figure 5.18).

Figure 5.17: Example: Spreadsheet View of Copy Frame as Text

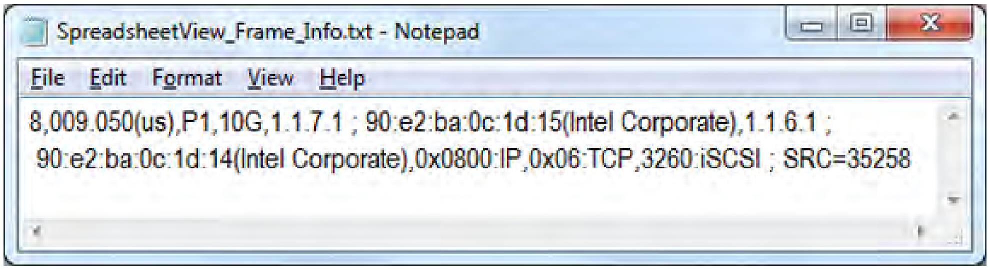


Figure 5.18: Example Information from Spreadsheet View Pasted into Text Editor

5.2.1.6 Compare (Data Payloads)

The *Compare* function allows you to select two different transactions and compare their data payloads. After loading a trace and selecting the Spreadsheet View, right click in the Spreadsheet View to bring up the context menu. See Figure 5.19.

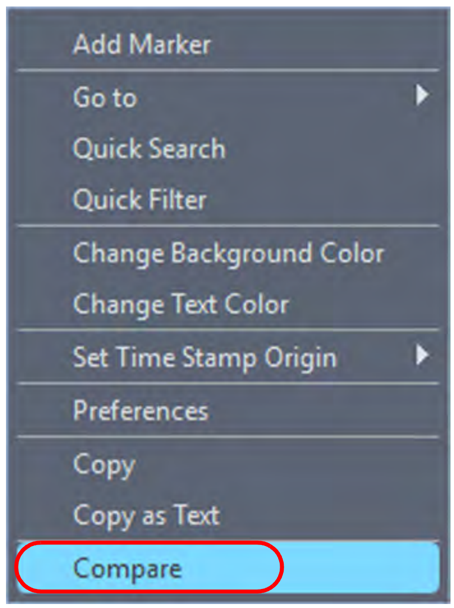


Figure 5.19: Context Menu – Compare Option

Click the **Compare** tab and the Data View will show data from two items. See Figure 5.20.

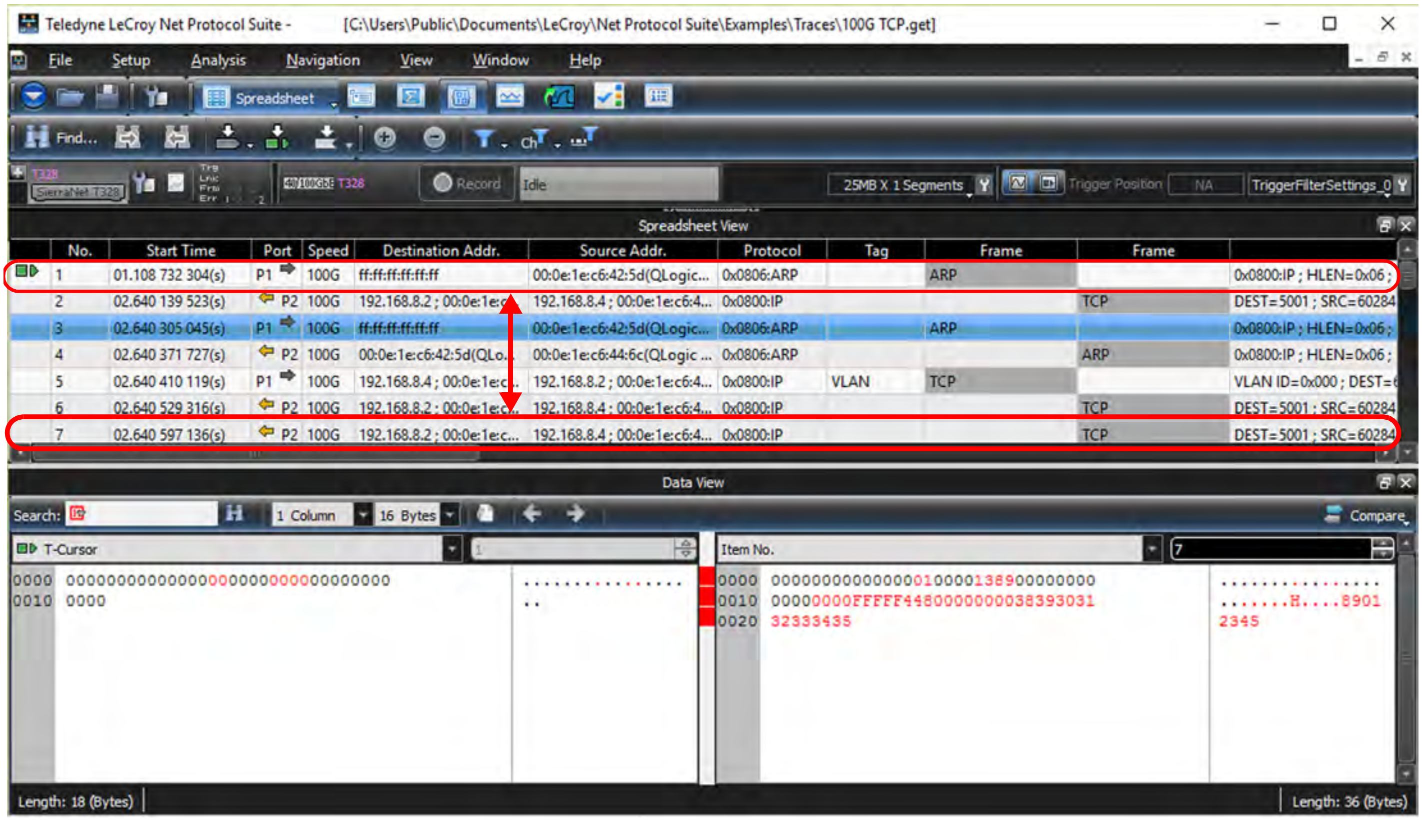


Figure 5.20: Spreadsheet View with Compare Data View

The Compare Data View shows you the payloads of two different transaction so you can explore their differences. In the case shown above transaction #1 is compared to transaction #7.

The differences in their respective payloads are highlighted in red. Data that is the same is displayed in black. See Figure 5.21.

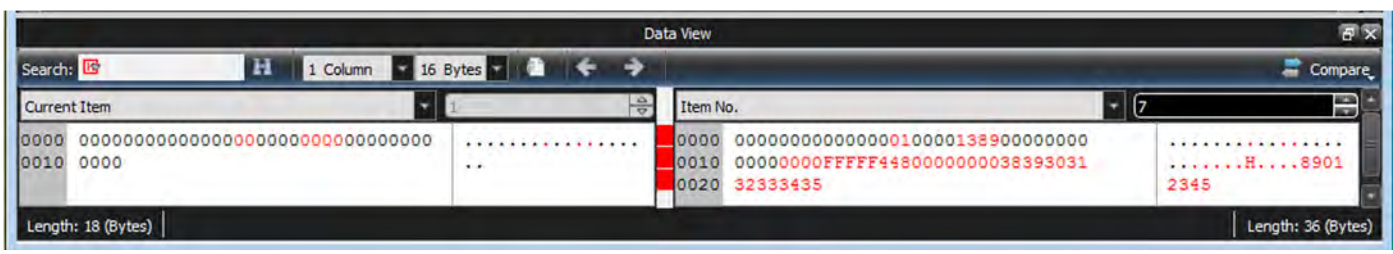


Figure 5.21: Compare Data View Only – Transaction #1 vs. Transaction #7

Data View ToolBar

The Data View toolbar has the following features:

- Search (Entry window: HEX or ASCII), Search Next, Search Previous (Figure 5.22)
- # Columns in Row (Figure 5.23)
- # Bytes in Column (Figure 5.23)
- Item No. (Current Item, Item No., Y-Cursor, T-Cursor, X-Cursor) (Figure 5.24)
- Display HEX and ASCII. See Figure 5.25.
- Exit Compare (Figure 5.24)

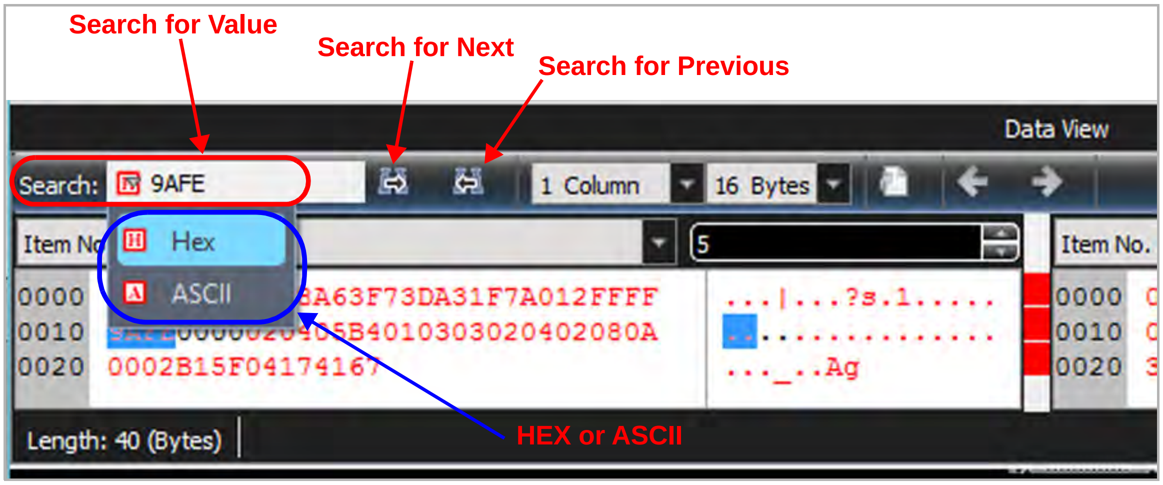


Figure 5.22: Data View Toolbar – Search ➔ HEX or ASCII

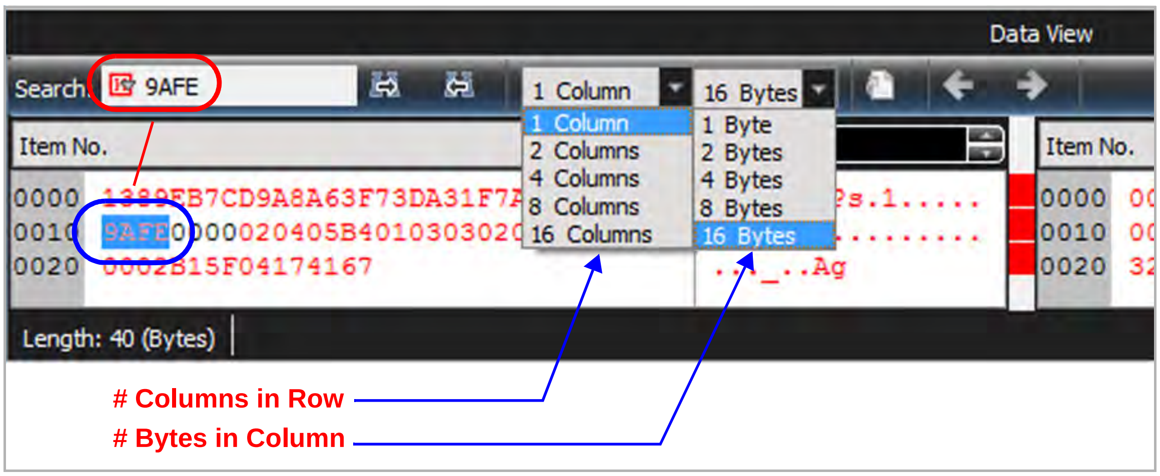


Figure 5.23: # Columns in Row, # Bytes in Column

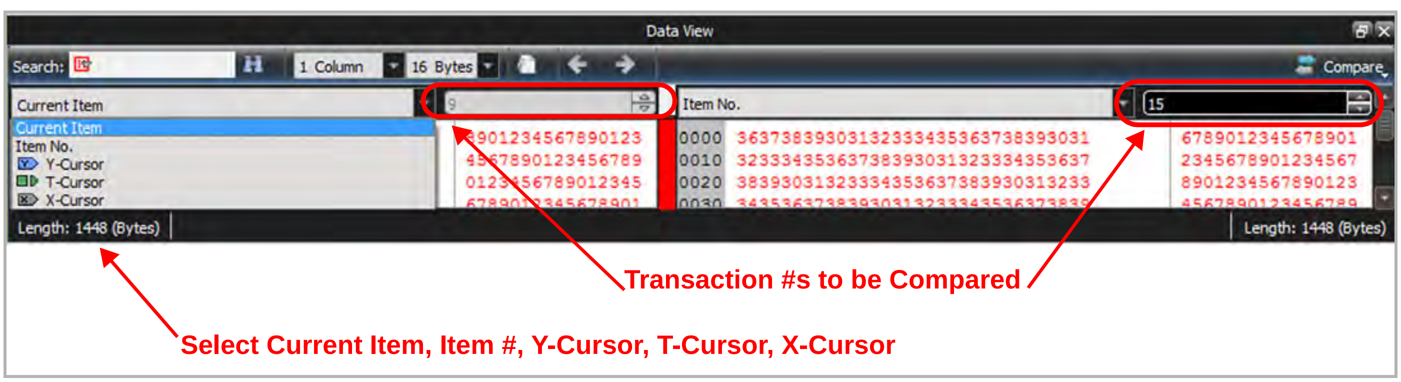


Figure 5.24: Select Transactions to be Compared

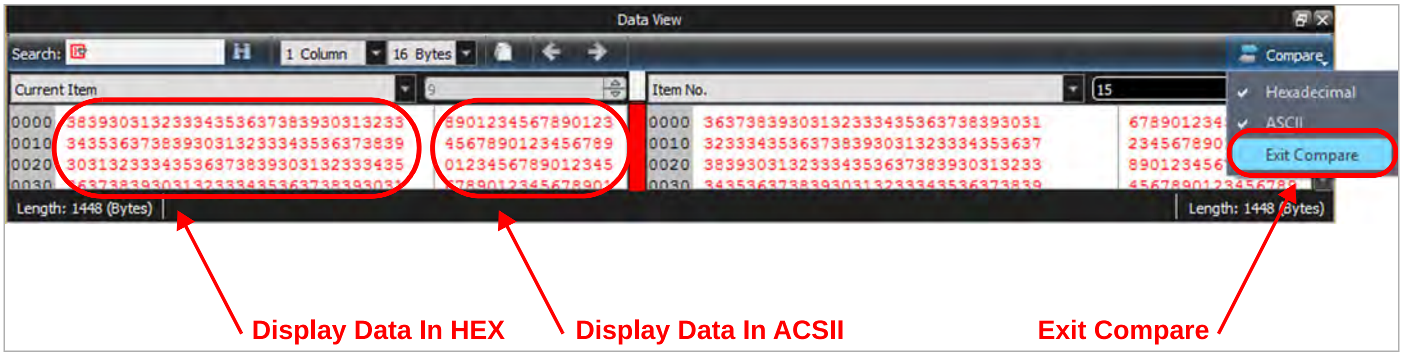


Figure 5.25: Display Data in HEX or ASCII or Exit Compare

If you select “Exit Compare” the display will return to Data Display for a single item. See Figure 5.26.

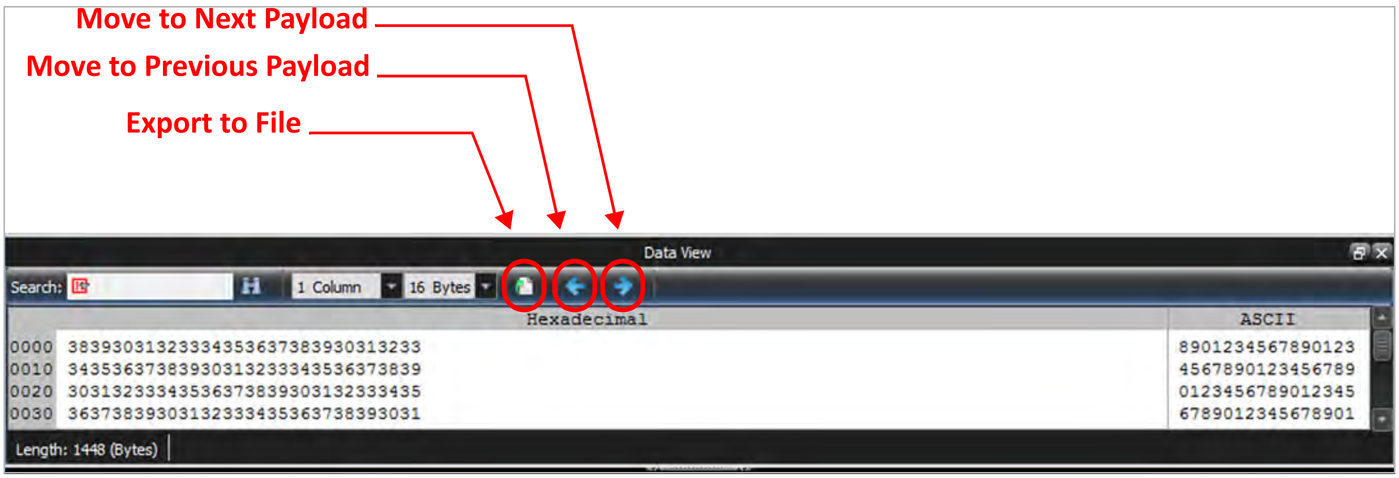


Figure 5.26: Default Data Display – Single Item

5.2.1.7 Markers

Markers are a convenient way to mark a point in the trace with your own label, so that you can rapidly return to that point. To create markers for your data:

1. Right-click anywhere in the data in Spreadsheet view and select **Add Marker** (see Figure 5.27).
2. Enter a **Name** and **description** for the Marker, then click **Add**.

   Once you have a list of Markers (Figure 5.31), you can delete, edit or go to a specific marker.

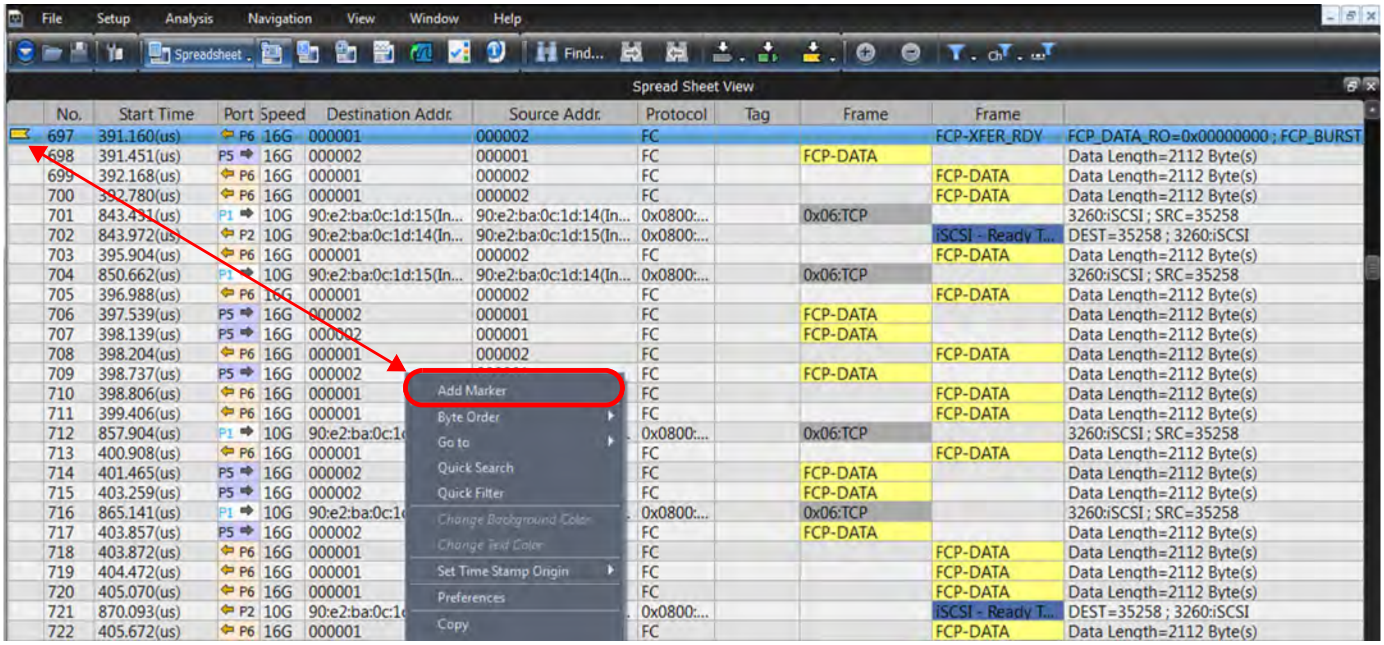


Figure 5.27: Adding a Marker Window

3. Right-click on a frame in the Spreadsheet view, then click **Add Marker** from the drop-down menu.

   A dialog box appears, which can be populated with a name and description (Figure 5.28).

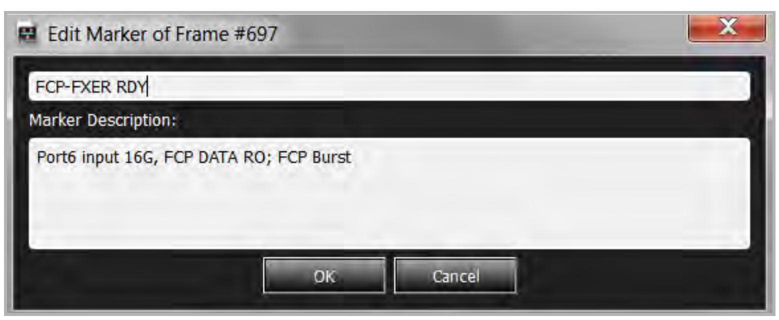


Figure 5.28: Marker Name and Description

   Once markers are created, they are displayed in the left column of the rows as shown below (Figure 5.29).

4. Hover the mouse over these markers to quickly see their name and description.

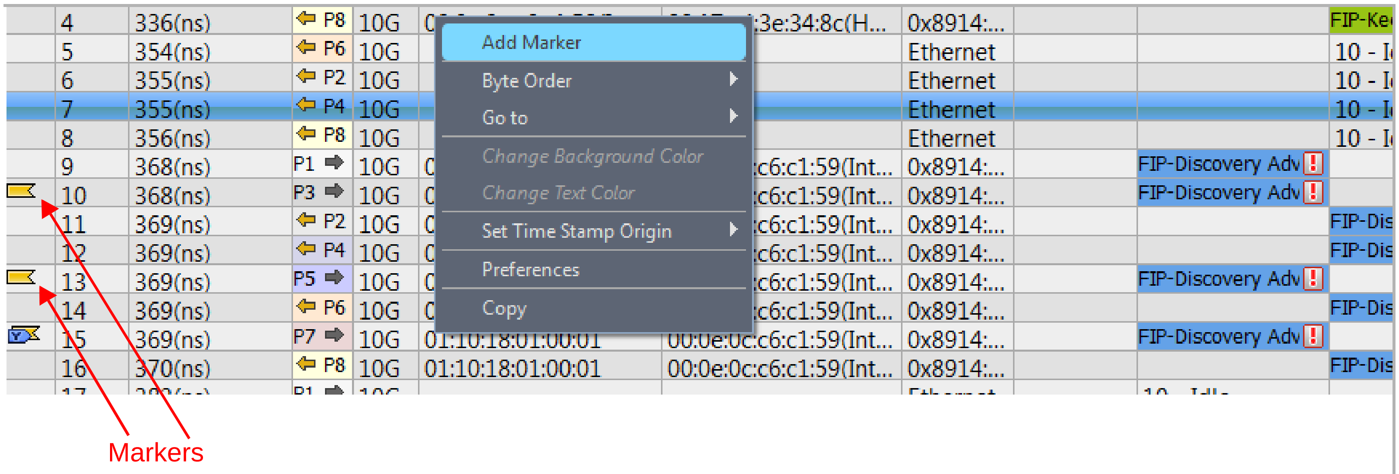


Figure 5.29: Markers in Spreadsheet View

Finding a Marker

To find a marker in the Trace:

1. Right-click the mouse in the trace viewer and select **Go to → Marker** (Figure 5.30).

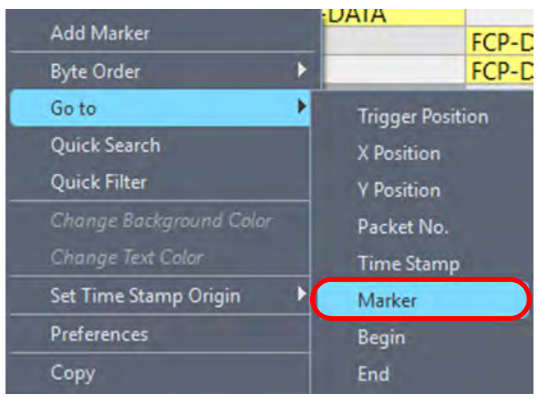


Figure 5.30: Go to Marker Window

A window appears that contains all of the Markers in the Trace (Figure 5.31).

2. Use the Scroll Bar to quickly view Markers that have been added for this Trace.

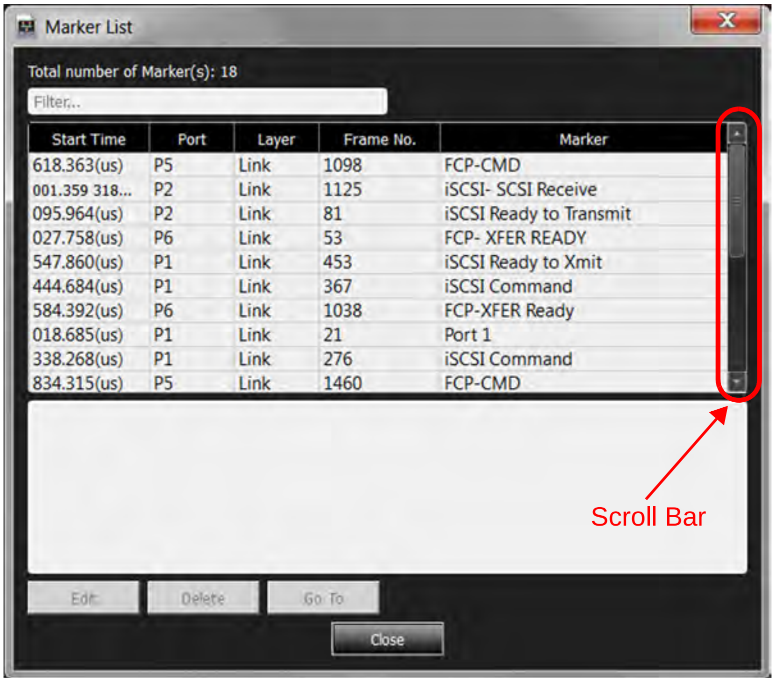


Figure 5.31: Complete Marker List

Sorting the Marker List

There are several ways of sorting the Marker List. One is by using the Filter Box at the top of the Marker List window. In this case, all Markers of type FCP are displayed. See Figure 5.32 below.

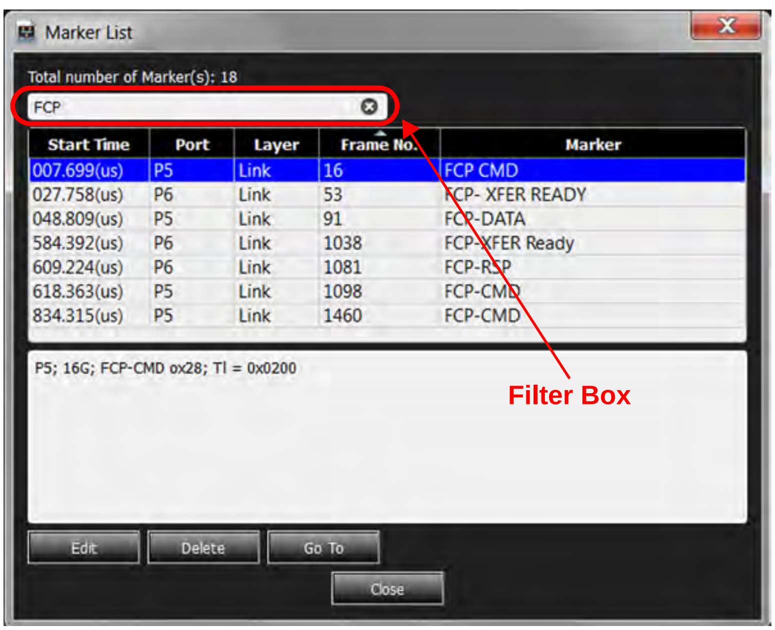


Figure 5.32: Sort Markers by Using Filter Box

You can also sort by each column header of the list (Start Time, Port, Layer Type, Frame #, or Marker text in the last column) can be used to sort the list by that column header in ascending or descending order. See Figures 5.33 and 5.34.

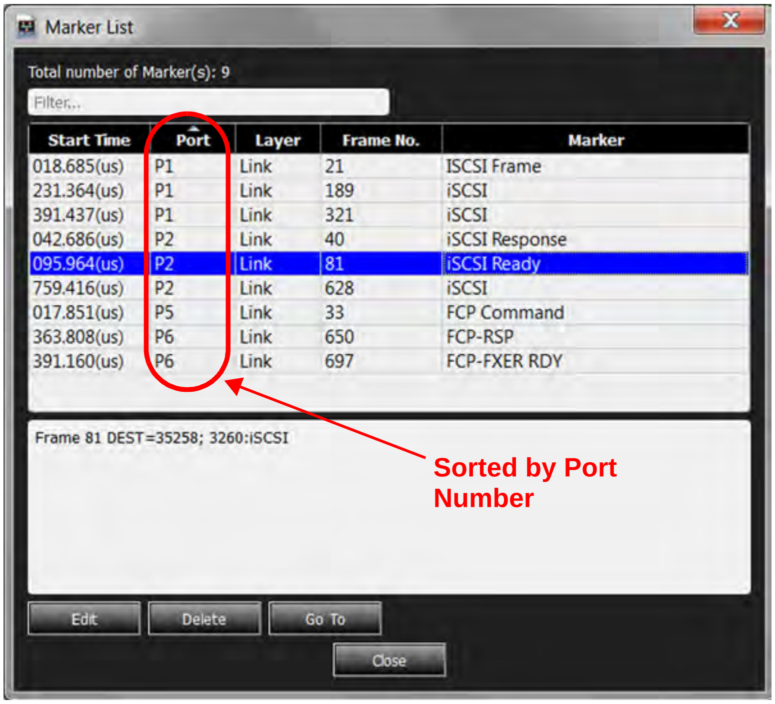


Figure 5.33: Markers Sorted by Port Number

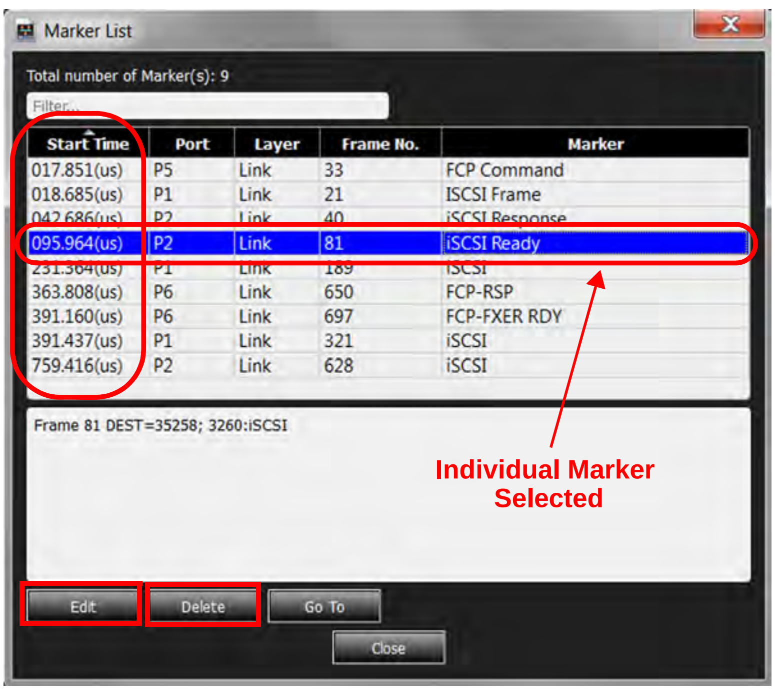


Figure 5.34: Markers Sorted by Start Time

Selecting/Go To a Marker

In Figure 5.34 the Marker in Frame 81 has been Selected. After being Selected, a Marker can be Edited or Deleted by clicking on the appropriate button.

Another option is to use the **Go To** button (highlighted in Figure 5.35 below), which moves the Spreadsheet view to the specific frame selected by clicking the **Go To** button. In this case, Frame 81 was selected and is shown at the top of the Spreadsheet view. See Figure 5.35 below.

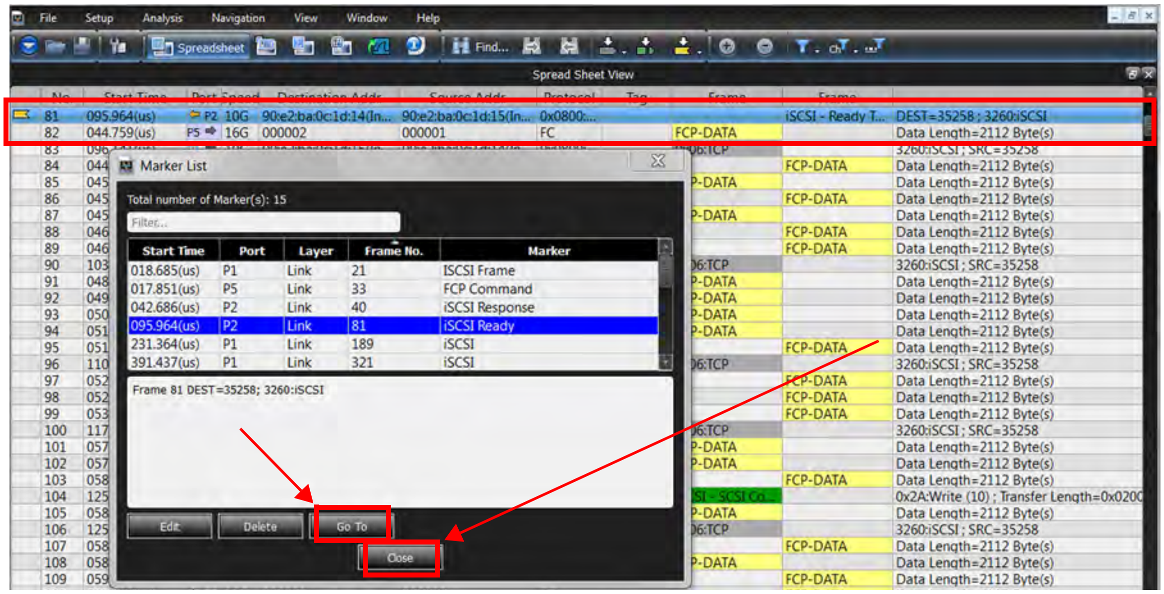


Figure 5.35: Frame 81 Selected and Moved

After working with the Markers, click the **Close** button to close the window.

5.2.1.8 Cursors

The spreadsheet view display incorporates three cursors labeled **X, Y,** and **T.** All cursors are initially overlaid and positioned at location 0, which is the trigger position of the display. The Trigger, or **T**, cursor is the measurement reference and is always at location 0 in the display.

Positioning the X Cursor

To position the X-Cursor within the viewer data display, click the left mouse button in the gray bar on the left side of the trace viewer next to the line in which to place the cursor.

Positioning the Y Cursor

To position the Y-cursor within the viewer data display, click the right mouse button in the gray bar on the left side of the trace viewer next to the line in which to place the cursor.

Locate Cursors

To quickly locate any cursor within the data viewer display, right-click and select the **Go To X** or **Go To Y** option and choose the cursor to locate (see Figure 5.16). You can also locate a cursor by selecting **Go To** from the Navigation menu and choosing the cursor to locate.

5.2.1.9 Spreadsheet Context Menu

To access the Spreadsheet context menu, right click anywhere in the Spreadsheet View. The menu shown in Figure 5.36 appears.

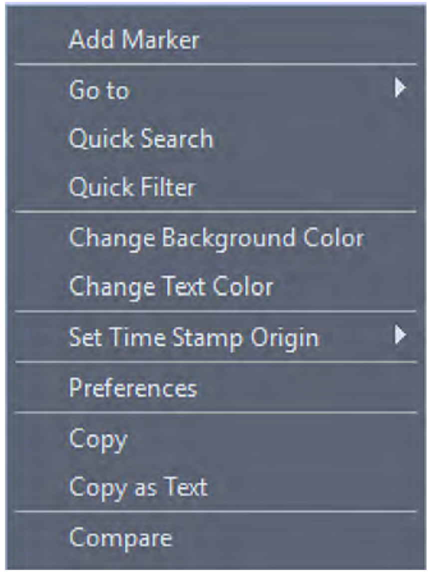


Figure 5.36: Spreadsheet View Context Menu

Add Marker Option

See 5.2.1.7, *Markers* for information on adding Markers.

Go To Options

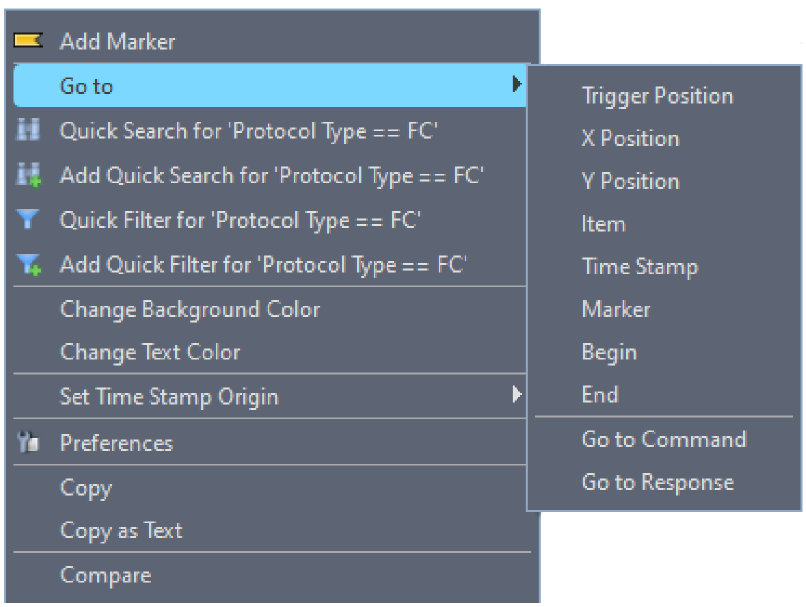


Figure 5.37: Spreadsheet Context Menu – Go to Options

The following options are available (Figure 5.37):

- Trigger Position
- X Position
- Y Position
- Item
- Time Stamp
- Marker

- Begin
- End
- Go to Command
- Go to Response

Go to Trigger Position

To go to the Trigger Position of a trace, click the **Go To** button and choose **Trigger Position**.

Go to X Position

To go to the X Position of a trace, click the **Go To** button and choose **X Position**.

Go to Y Position

To go to the Y Position of a trace, click the **Go To** button and choose **Y Position**.

Go to Item

1. To locate an Item, select **Go To Item** or click the down arrow ▼ to select **Links** or **Sequences**.
2. Enter the Type and Number of Items you need in the Go To dialog box and click **OK**.

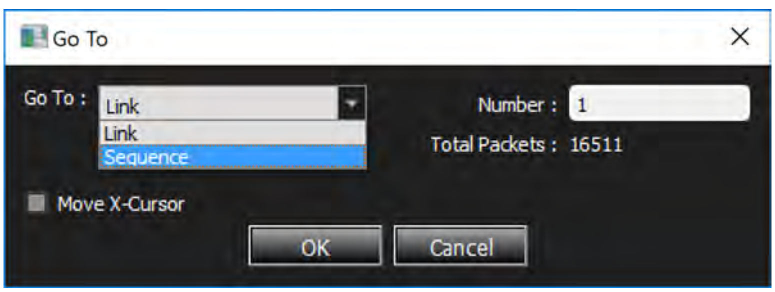


Figure 5.38: Go to Item Dialog Box

Go to Time Stamp

To go to a specific Time Stamp of a trace, click the **Go To** button and choose **Time Stamp**.

Go to Marker

To go to a specific marker of a trace, click the **Go To** button and choose **Marker** (see 5.2.1.7, *Markers*).

Go to Begin

To go to the beginning of a trace, click the **Go To** button and choose **Begin**.

Go to End

To go to the end of a trace, click the **Go To** button and choose **End**.

Go to Command

Go to Response

Set Time Stamp Origin

Right-click and choose **Set Time Stamp Origin** (see Figure 5.39) and 5.2.1.4, *Spreadsheet View Options* for explanations about these options.

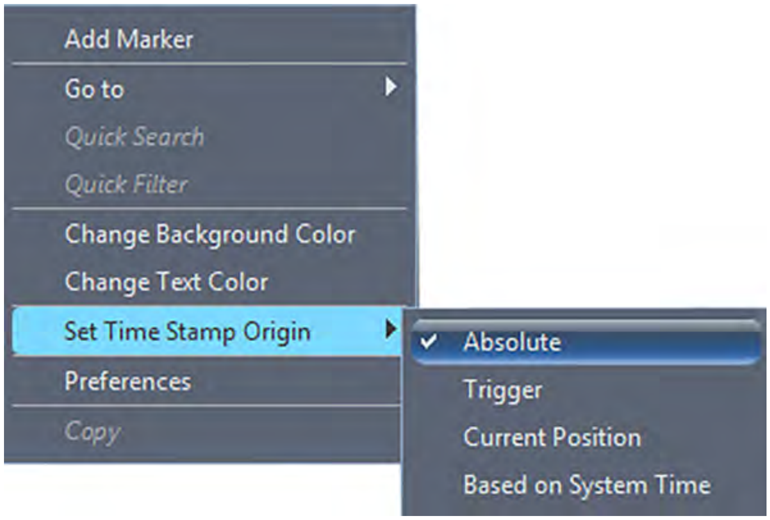


Figure 5.39: Set Time Stamp Origin – Menu

5.2.1.10 Cursor/Marker Timing Calculations Display Bar

A Timing Calculator Display Bar is located at the bottom of the Net Protocol Suite Main Menu, after a Trace is recorded or loaded. See Figure 5.40.

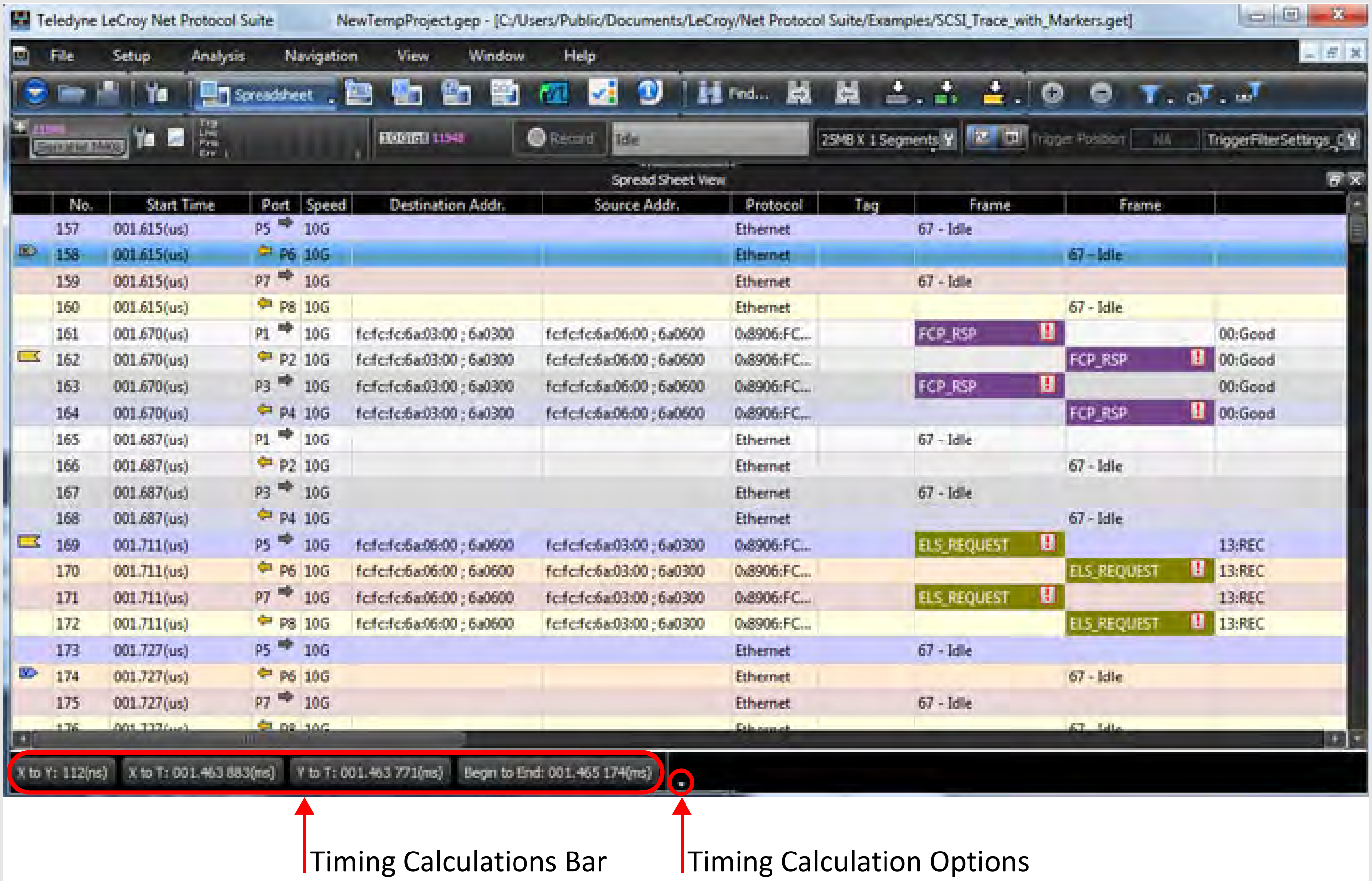


Figure 5.40: Loaded Trace with Timing Calculations Bar

Default Timing Calculations

The default times displayed are:

- X to Y
- X to T
- Y to T
- Begin to End

Each of the Default Timing Display Options can be seen more detail in Figure 5.41.

- Show
- Hide
- Show Entire Timing Display
- Copy

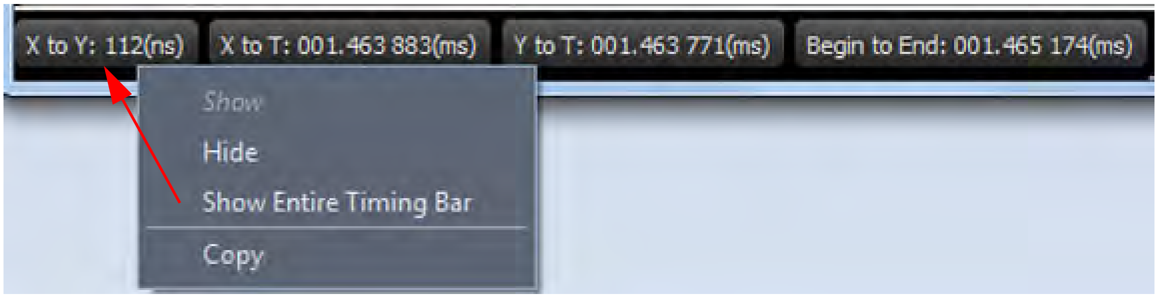


Figure 5.41: Default Timing Bar Options

Customize Timing Calculations Bar

There is also a Customize option – click on the small white triangle to the right of the Timing Bar (see Figures 5.40 and 5.42).

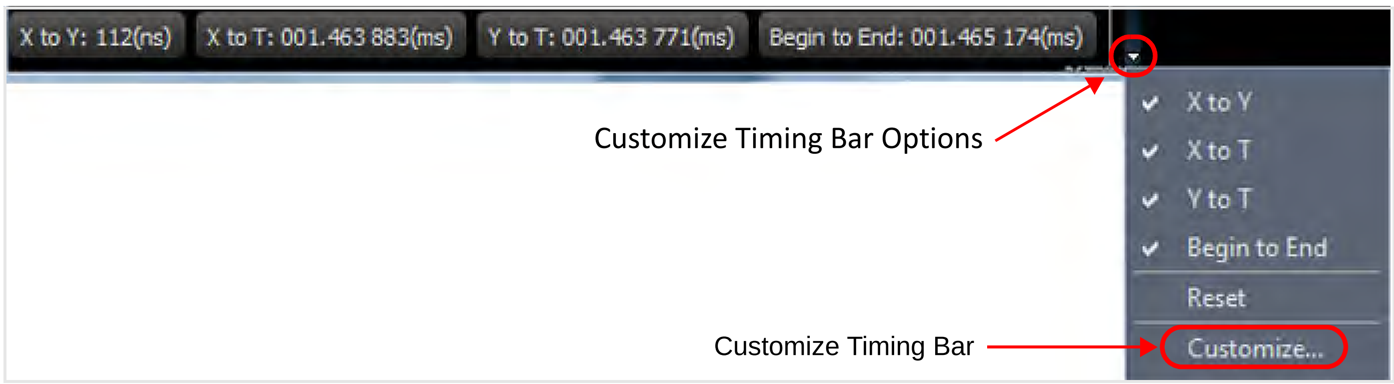


Figure 5.42: Timing Bar with Options Displayed

Timing Bar Customization

The Customize option allows you to specify Markers, enabling you to find the exact time between any two Markers,

1. Click the **Customize Option** and the Timing Bar Customize window appears (Figure 5.43).

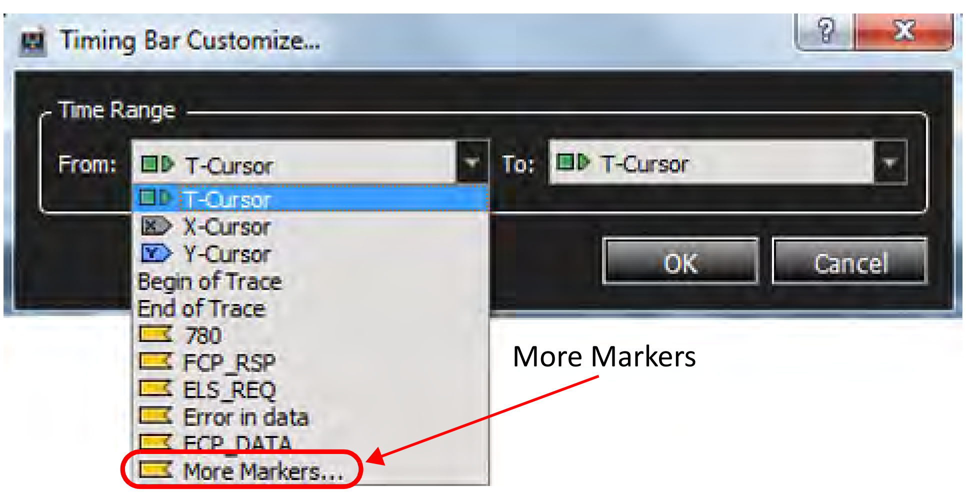


Figure 5.43: Customize Cursors for Timing Calculations

2. To choose a range, select **More Markers**. The Marker List window containing All Markers appears.

3. Choose any Marker for **From** and any Marker for **To** (Figure 5.44).

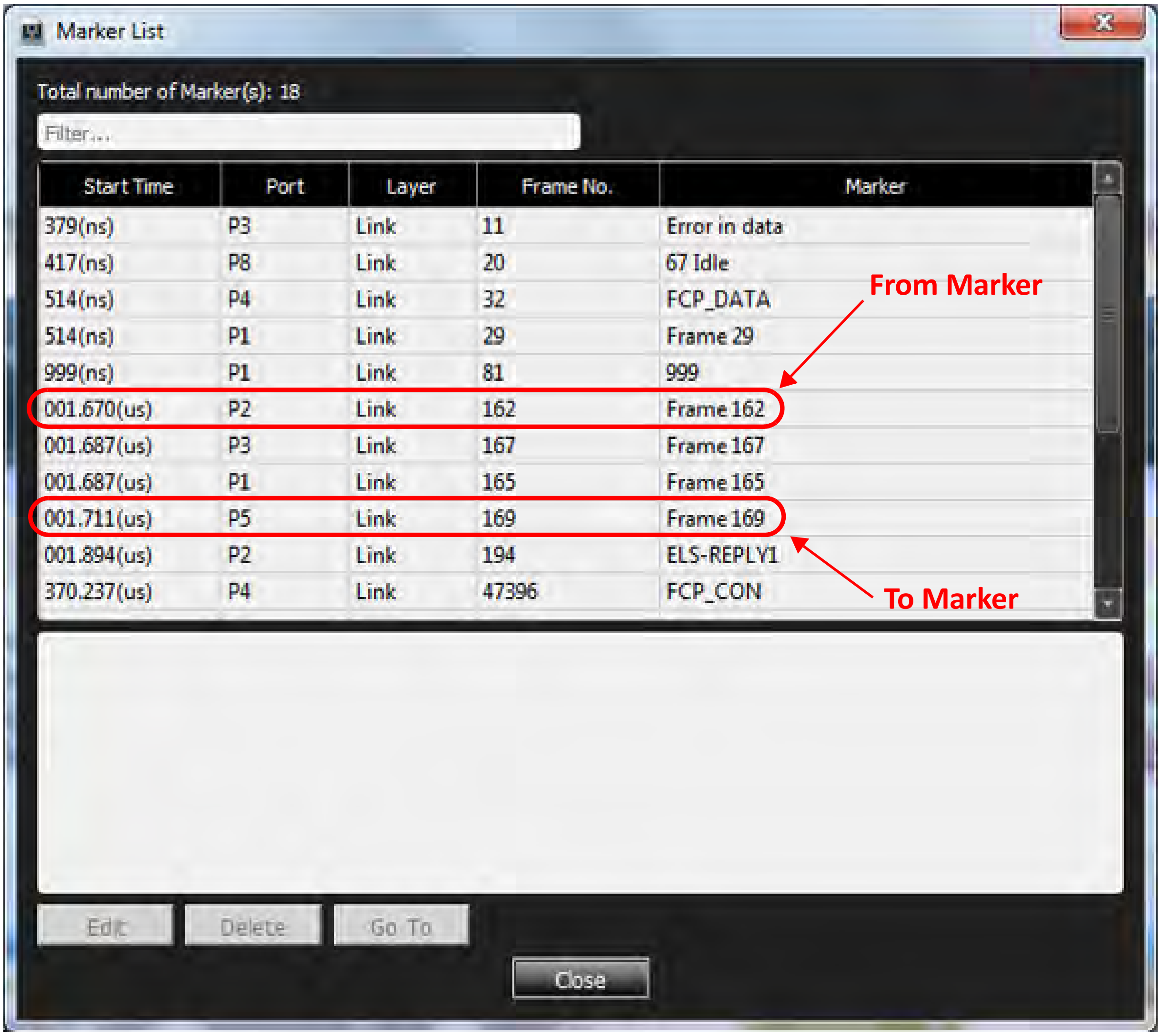


Figure 5.44: Marker Dialog

For example:

1. Frame 162 is selected for the **From** Marker and Frame 169 is selected for the **To** Marker. The Timing Bar Customize dialog box displays the two Markers of interest (Figure 5.45).

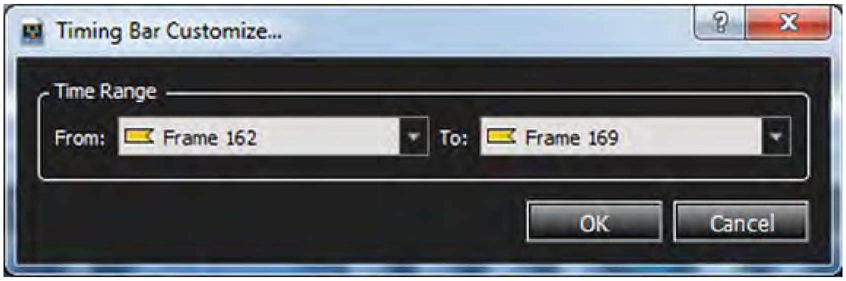


Figure 5.45: Timing Bar Customize

2. Click **OK** to show the time between the two markers in the updated Timing Bar (Figure 5.46).

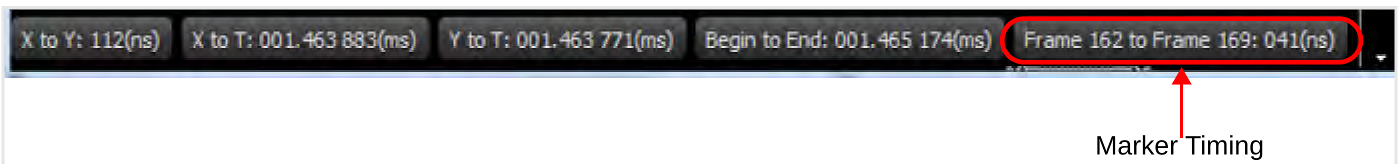


Figure 5.46: Timing between Selected Markers

Options for Customized Timing Bar

The options available for a Customized Timing Bar are shown in Figure 5.47.

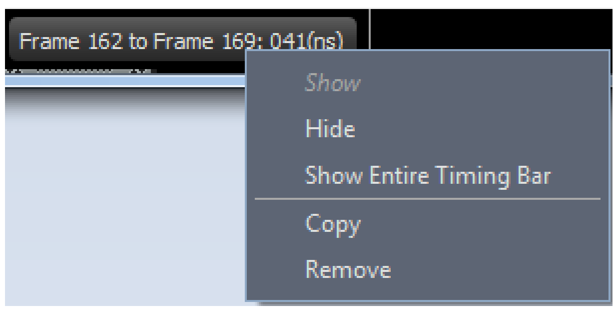


Figure 5.47: Customized Timing Bar Options

5.2.1.11 Column Display Options

You can customize the columns display by showing/hiding, adding, editing or deleting columns. Right-click in the column header and select an option as shown in Figure 5.48.

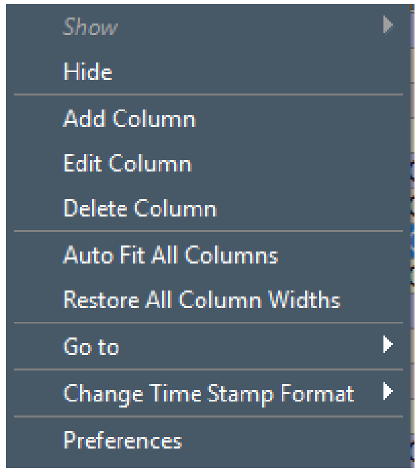


Figure 5.48: Menu Options for Columns in Spreadsheet View

TABLE 5.2: Spreadsheet Column View Options

Menu Option	Description
Show	Displays a hidden column.
Hide	Hides a column.
Add Column	Allows you to add a column (see 5.2.1.12, *Adding Columns to the Spreadsheet View*). Select Field, Column Name, Source Direction, foreground and back ground Colors, choose And/OR, display Data Payload Protocol Error icons, apply Frame and Port color, enable Time Format, display Field name, set column Alignment and Width and Add to Pre-defined Columns. Columns can also be added to the Pre-defined columns list. This list is a flat list where you can keep columns you might want to toggle on/off.
Edit Column	Allows you to edit column properties. It has the same functionality as Add Column above (see 5.2.1.16, *Editing Items in a Column*).
Delete Column	Allows you to delete the selected column.
Auto Fit All Columns	Adjusts the column widths to fit the text.
Restore All Columns Widths	Restores the column widths to the previous size.
Go to:	Displays options to go to Trigger, X or Y Position, event No., Time Stamp, Marker, Begin and End.
Change Time Stamp Format:	Displays options to select the time stamp format.
Preferences	Displays the Preferences window

5.2.1.12 Adding Columns to the Spreadsheet View

Selecting **Add Column** displays the following dialog.

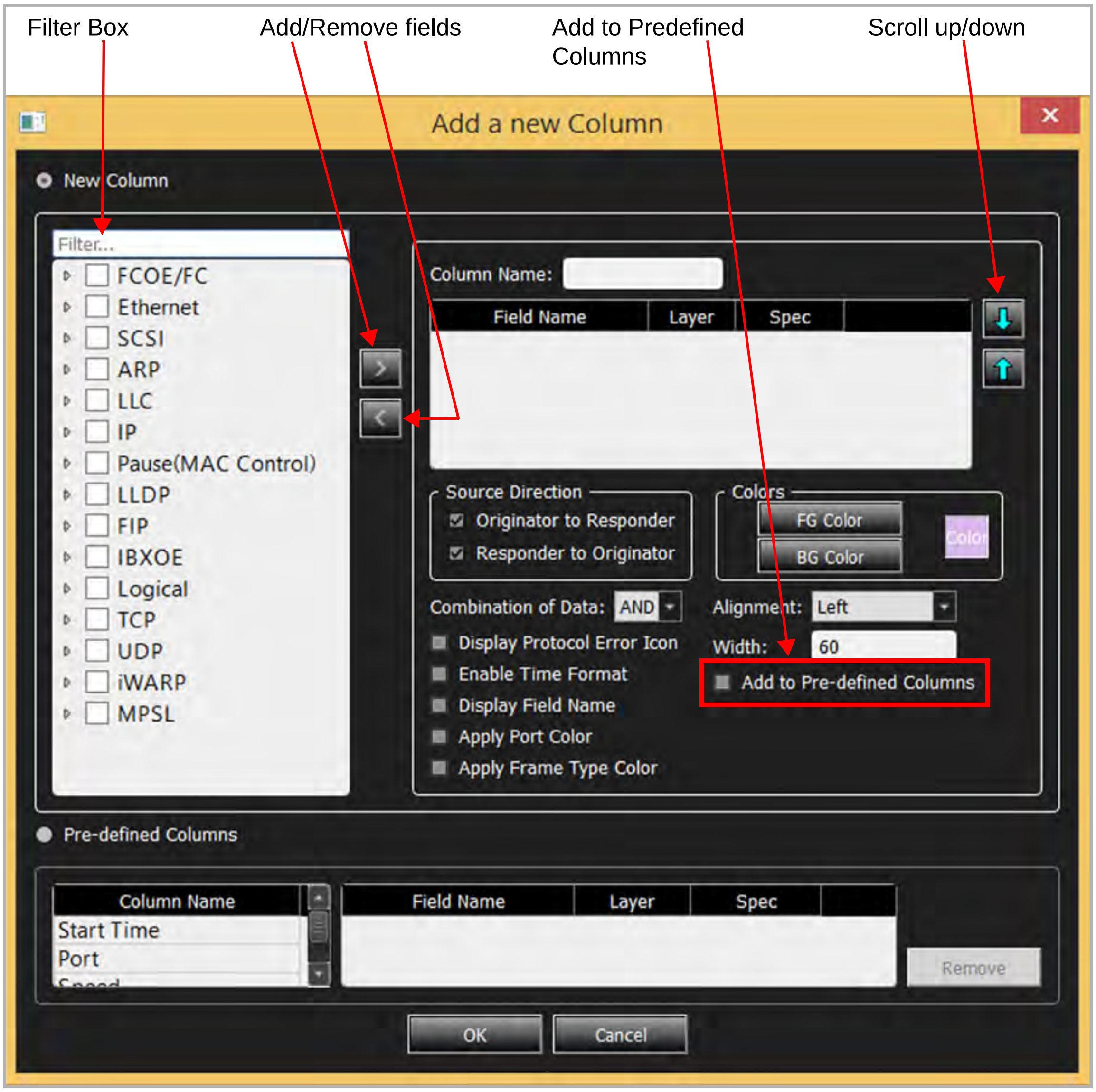


Figure 5.49: Add a New Column Dialog

You can select any combination of fields to fill the content of the column. Use the Filter text box above the Fields tree list to more easily find the fields you're interested in. In case you select multiple fields, the up/down buttons enable you to specify in which order they should be displayed in the column. Desired columns can also be added to the pre-defined columns. Pre-defined columns are ones that contain metadata (such as timestamp, port number, etc.) or custom ones that have been added by checking the "Add to Predefined Column" checkbox.

Selecting **Edit Column** displays the following dialog.

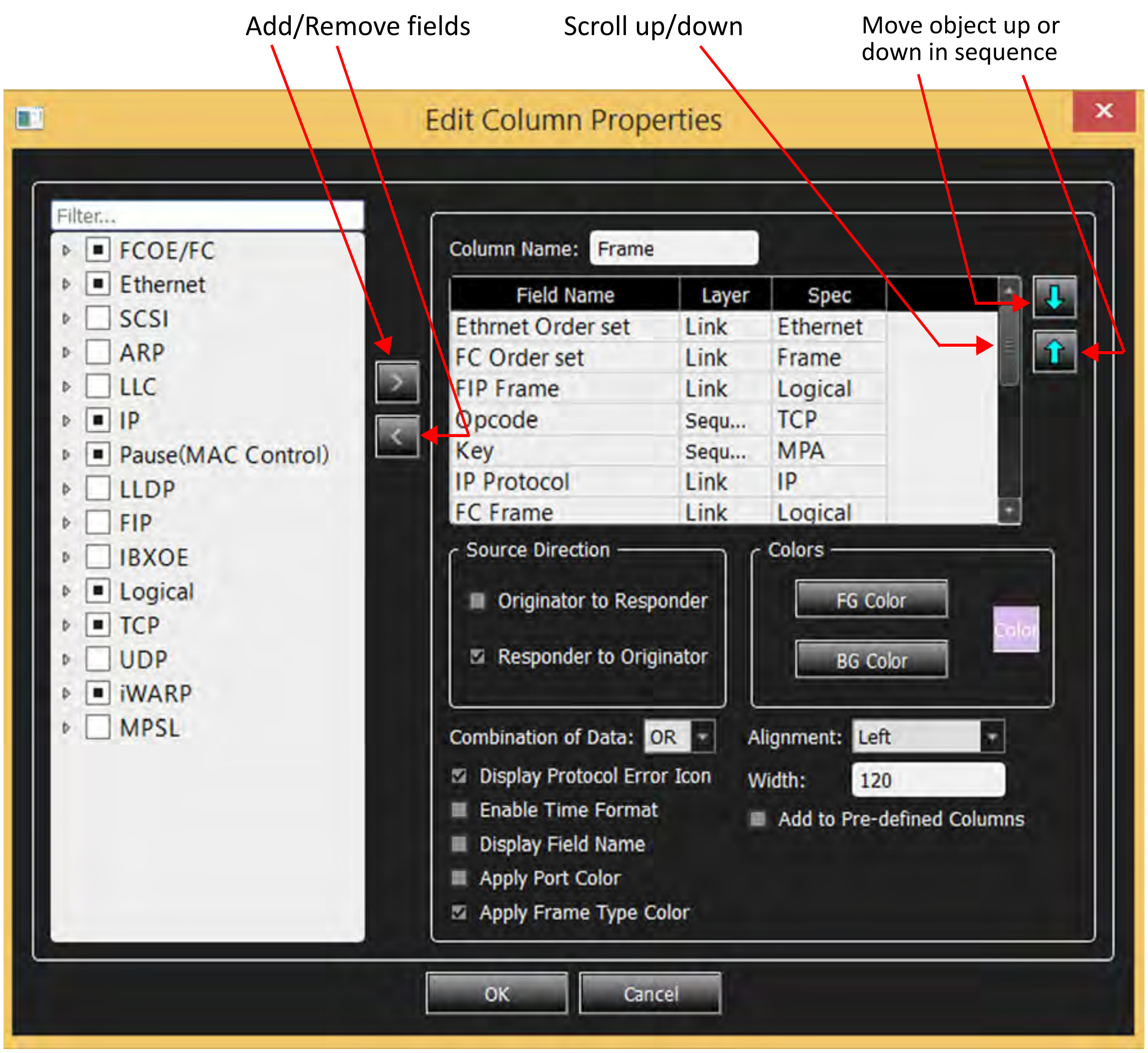
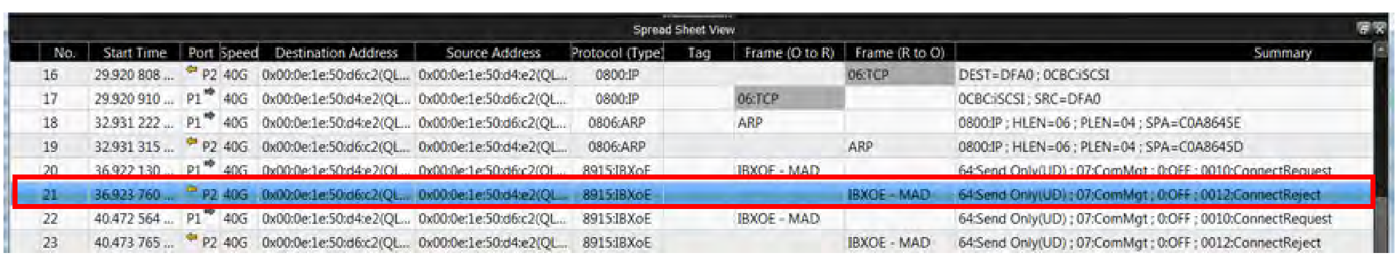


Figure 5.50: Edit Column Properties Dialog

5.2.1.13 MAD Header Decoded

MAD Headers can be decoded and located in a Trace, see Figure 5.51.



Spread Sheet View

No.	Start Time	Port	Speed	Destination Address	Source Address	Protocol (Type)	Tag	Frame (O to R)	Frame (R to O)	Summary
16	29.920 808 ...	P2	40G	0x00:0e:1e:50:d6:c2(QL...	0x00:0e:1e:50:d4:e2(QL...	0800:IP			06:TCP	DEST=DFA0 ; 0CBC:iSCSI
17	29.920 910 ...	P1	40G	0x00:0e:1e:50:d4:e2(QL...	0x00:0e:1e:50:d6:c2(QL...	0800:IP		06:TCP		0CBC:iSCSI ; SRC=DFA0
18	32.931 222 ...	P1	40G	0x00:0e:1e:50:d4:e2(QL...	0x00:0e:1e:50:d6:c2(QL...	0806:ARP		ARP		0800:IP ; HLEN=06 ; PLEN=04 ; SPA=C0A8645E
19	32.931 315 ...	P2	40G	0x00:0e:1e:50:d6:c2(QL...	0x00:0e:1e:50:d4:e2(QL...	0806:ARP			ARP	0800:IP ; HLEN=06 ; PLEN=04 ; SPA=C0A8645D
20	36.922 130 ...	P1	40G	0x00:0e:1e:50:d4:e2(QL...	0x00:0e:1e:50:d6:c2(QL...	8915:IBXoE		IBXOE - MAD		64:Send Only(UD) ; 07:ComMgt ; 0:OFF ; 0010:ConnectRequest
21	36.923 760 ...	P2	40G	0x00:0e:1e:50:d6:c2(QL...	0x00:0e:1e:50:d4:e2(QL...	8915:IBXoE			IBXOE - MAD	64:Send Only(UD) ; 07:ComMgt ; 0:OFF ; 0012:ConnectReject
22	40.472 564 ...	P1	40G	0x00:0e:1e:50:d4:e2(QL...	0x00:0e:1e:50:d6:c2(QL...	8915:IBXoE		IBXOE - MAD		64:Send Only(UD) ; 07:ComMgt ; 0:OFF ; 0010:ConnectRequest
23	40.473 765 ...	P2	40G	0x00:0e:1e:50:d6:c2(QL...	0x00:0e:1e:50:d4:e2(QL...	8915:IBXoE			IBXOE - MAD	64:Send Only(UD) ; 07:ComMgt ; 0:OFF ; 0012:ConnectReject

Figure 5.51: MAD Header Decoded in Spreadsheet View

5.2.1.14 iSER Header Decoded

iSER Headers can be decoded and located in a Trace, see Figure 5.52.

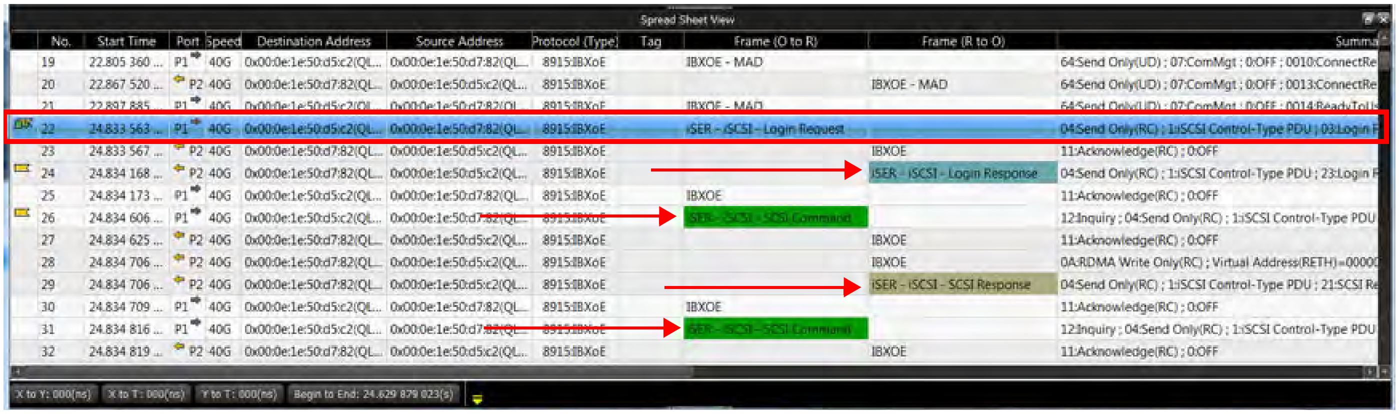


Figure 5.52: iSER Decoded in Spreadsheet View

5.2.1.15 Decoding NVMe Transactions

NVMe transactions can be decoded and displayed in Spreadsheet Mode (Figure 5.53).

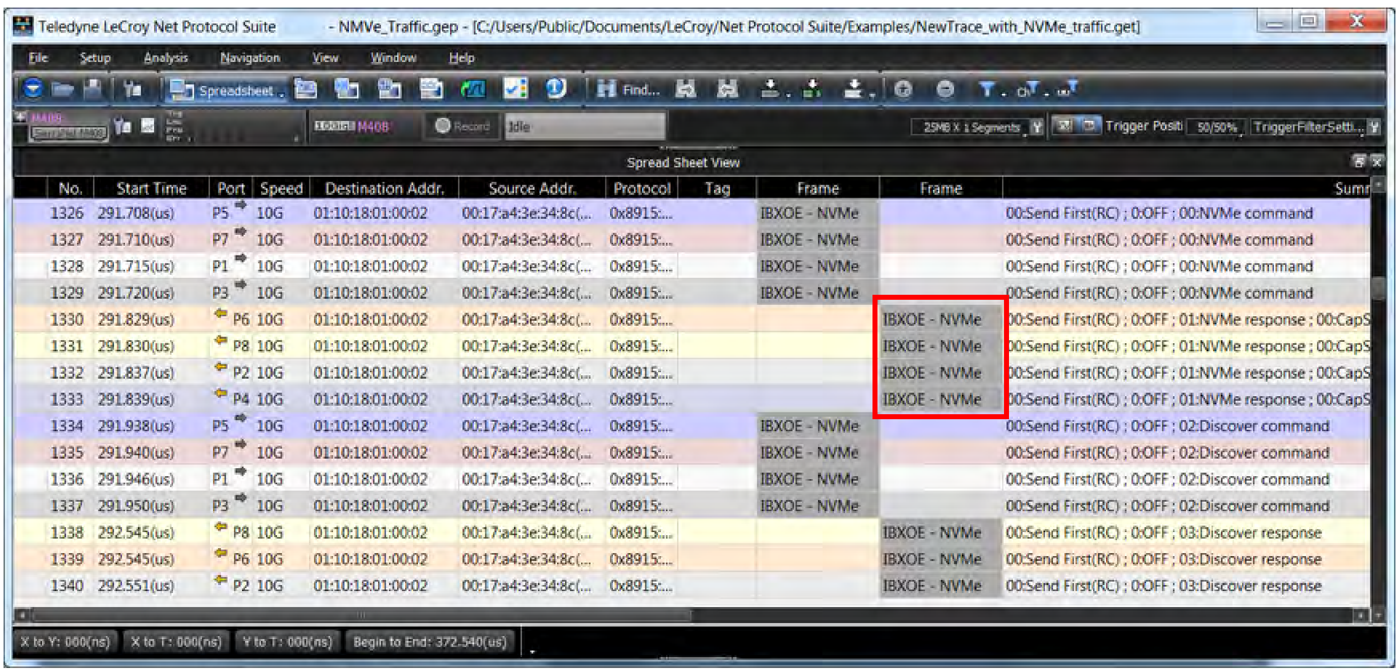


Figure 5.53: NVMe Traffic with Commands Decoded

5.2.1.16 Editing Items in a Column

You can choose any information available and add it to a column. In this example the Summary column has been selected for editing. A sample Summary column is shown in Figure 5.54.

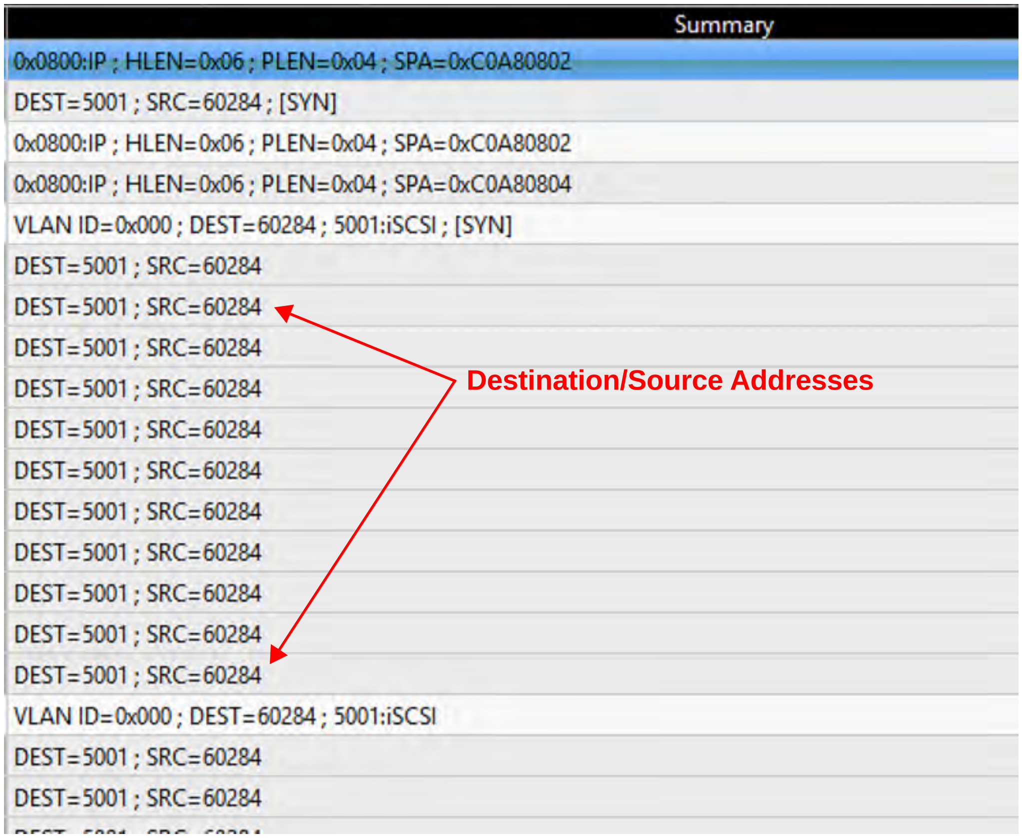


Figure 5.54: Typical Summary Column

To edit items in a column:

1. Move the cursor to the top of the Summary column you want to edit, then right-click in column title area. The menu shown in Figure 5.55 appears.

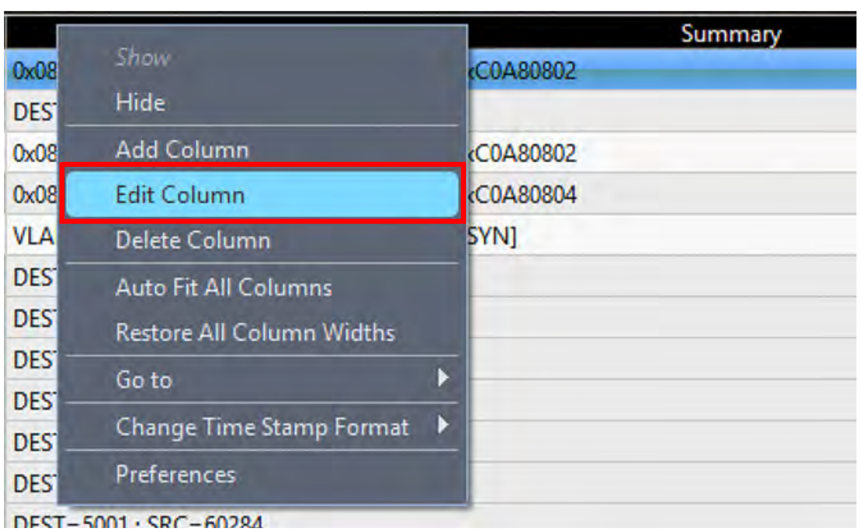


Figure 5.55: Editing a Column

2. Select **Edit Column**. The *Edit Table View Column* window appears in which you can manipulate the data in the Summary column (Figure 5.56).

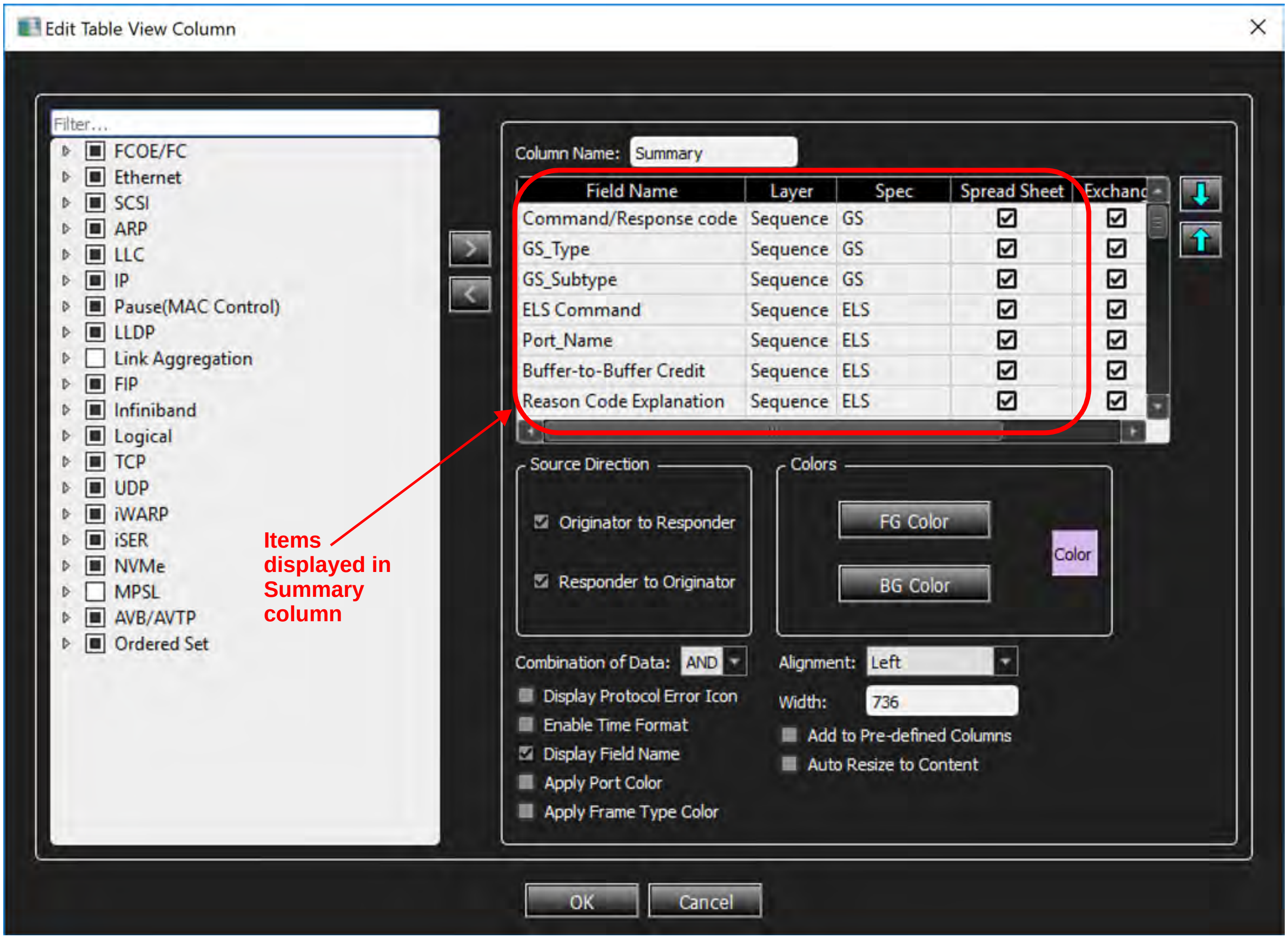


Figure 5.56: Edit Column

3. Scroll down to see all of the items that will be displayed in the Summary column.

Example: Add ACK and ACK.NO to Summary Column

1. Scroll down to the bottom of the item list.

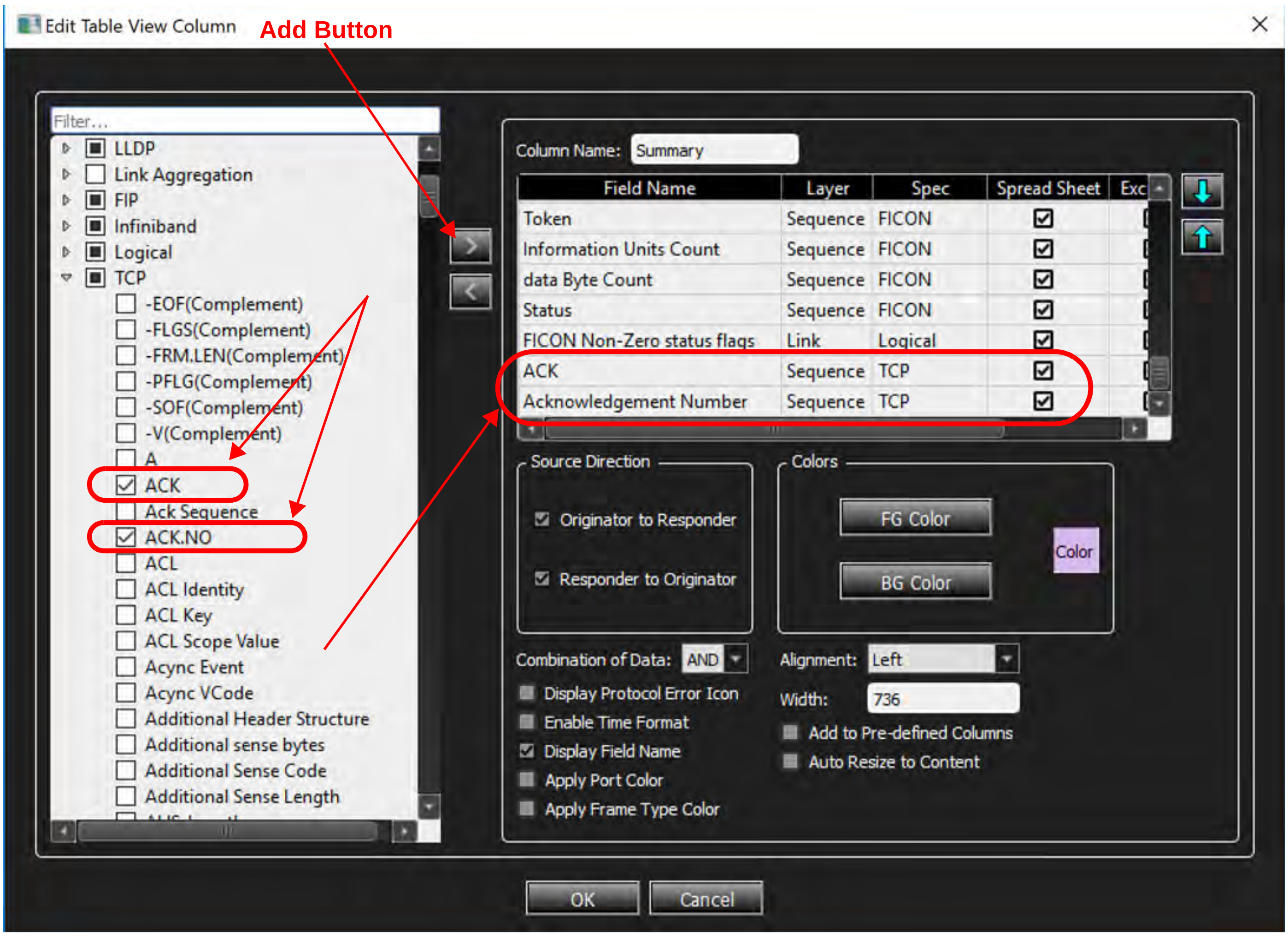
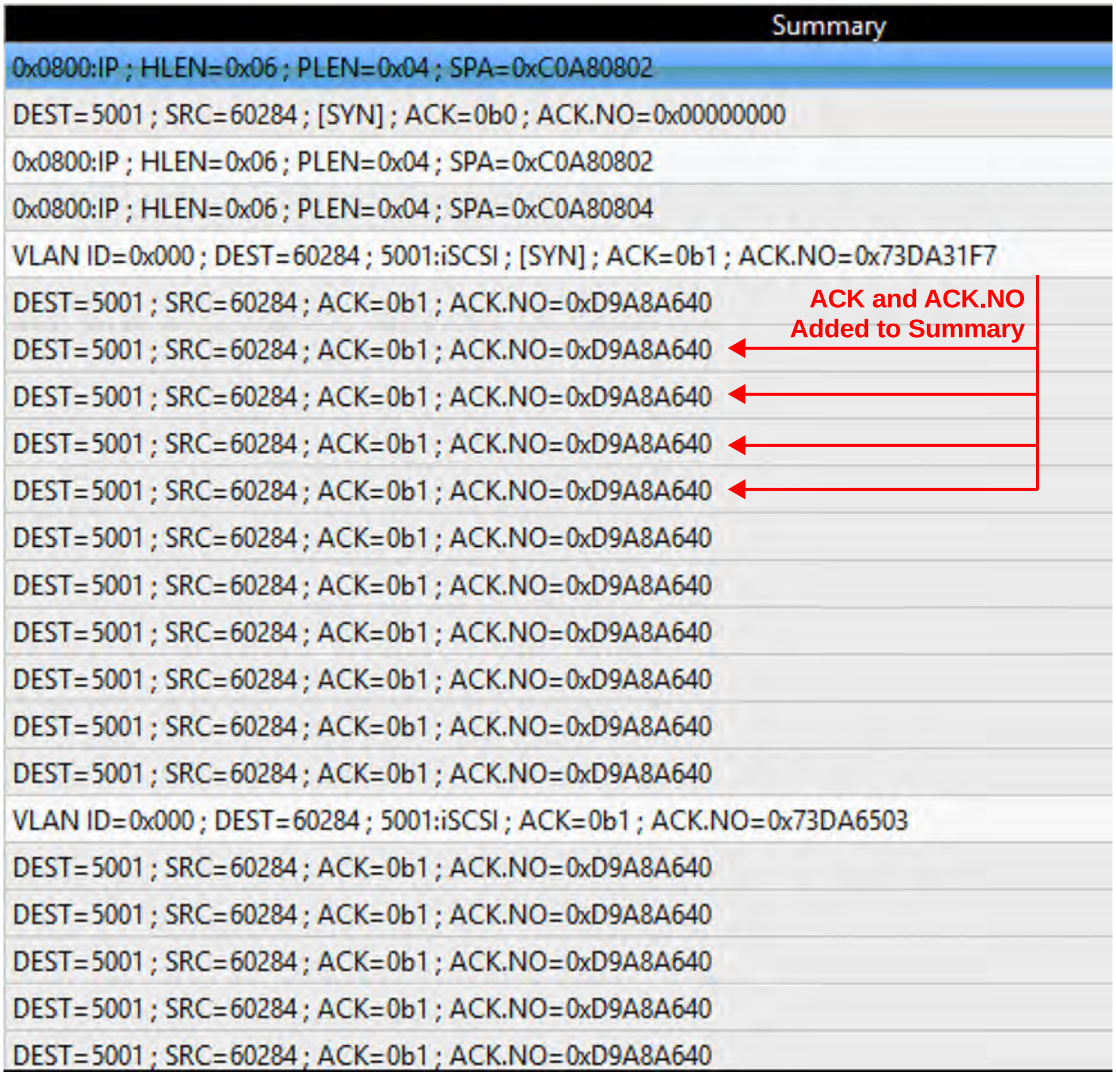


Figure 5.57: Add Payload Size to Summary Column

2. In the left pane, click the down arrow next to TCP to display its items.

3. Check the boxes for **ACK** and **ACK.NO**, then click **OK**. ACK and ACK.NO are added to the Summary Column. See Figure 5.58.



Summary
0x0800:IP ; HLEN=0x06 ; PLEN=0x04 ; SPA=0xC0A80802
DEST=5001 ; SRC=60284 ; [SYN] ; ACK=0b0 ; ACK.NO=0x00000000
0x0800:IP ; HLEN=0x06 ; PLEN=0x04 ; SPA=0xC0A80802
0x0800:IP ; HLEN=0x06 ; PLEN=0x04 ; SPA=0xC0A80804
VLAN ID=0x000 ; DEST=60284 ; 5001:iSCSI ; [SYN] ; ACK=0b1 ; ACK.NO=0x73DA31F7
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
VLAN ID=0x000 ; DEST=60284 ; 5001:iSCSI ; ACK=0b1 ; ACK.NO=0x73DA6503
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640
DEST=5001 ; SRC=60284 ; ACK=0b1 ; ACK.NO=0xD9A8A640

Figure 5.58: ACK and ACK.NO Added to Summary Column

5.2.2 Exchange View

In a typical trace shown in Spreadsheet view (see Figure 5.59), which displays captured events sequentially, one event per line. In the example below you can see that in the first 34 events there are commands and data going back and forth from Ports 1 and 3 combined with commands and data on Ports 2 and 4.

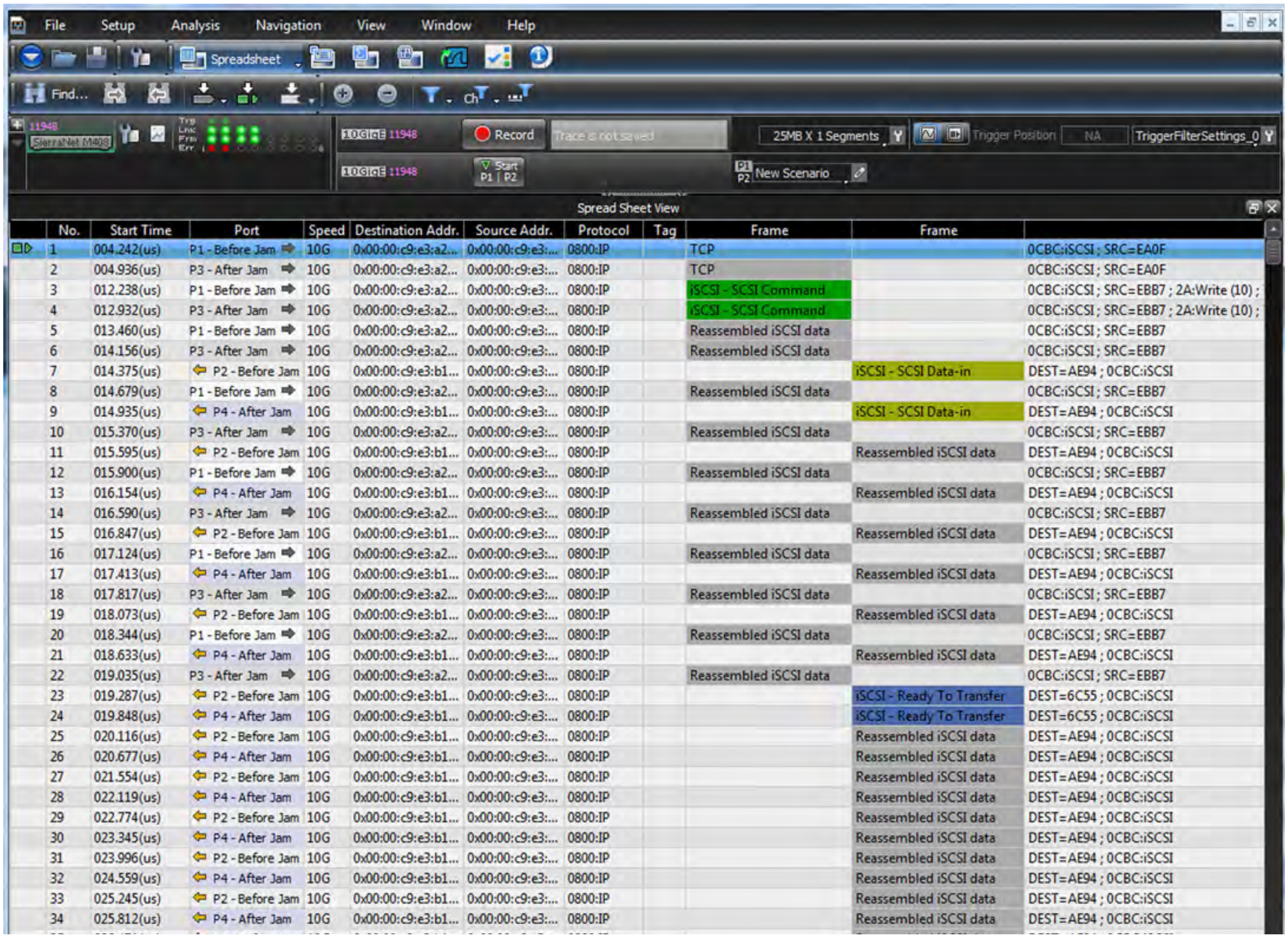


Figure 5.59: Typical Trace in Spreadsheet View

NOTE: Exchange View only works when both sides of a link are captured on a single port pair.

In Exchange View (see Figure 5.60) events are arraigned logically, so that all the events that are a part of SCSI command #1 are grouped together (see Figure 5.61) and all the events that are part of SCSI command #2 are grouped together (see Figure 5.62).

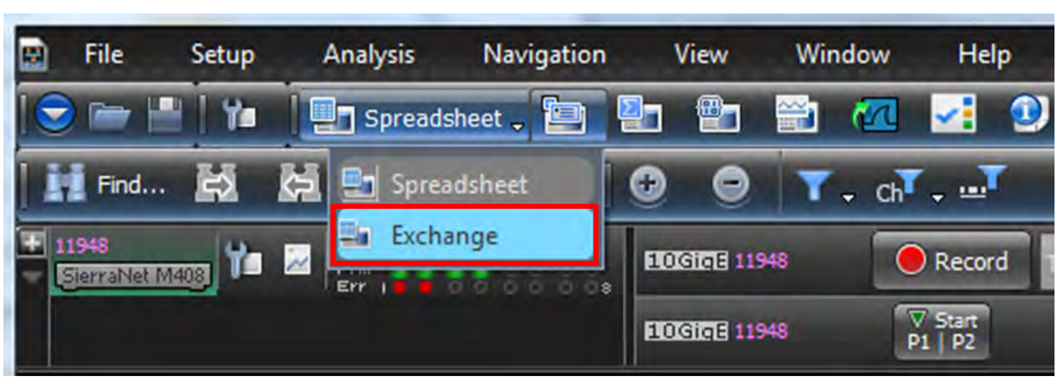


Figure 5.60: Exchange View

In Exchange View the elements of a event are grouped together hierarchically rather than sequentially. See Figure 5.61.

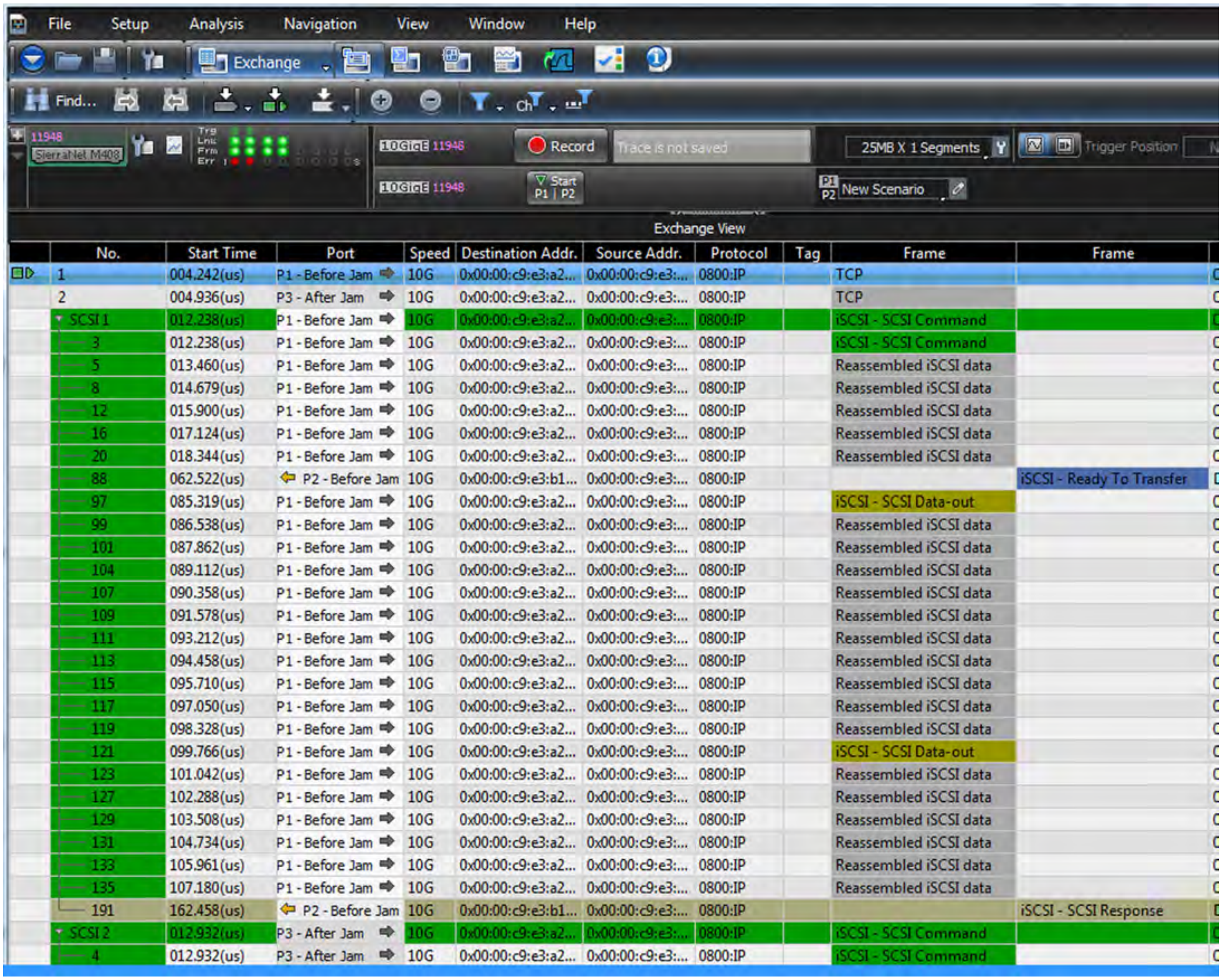
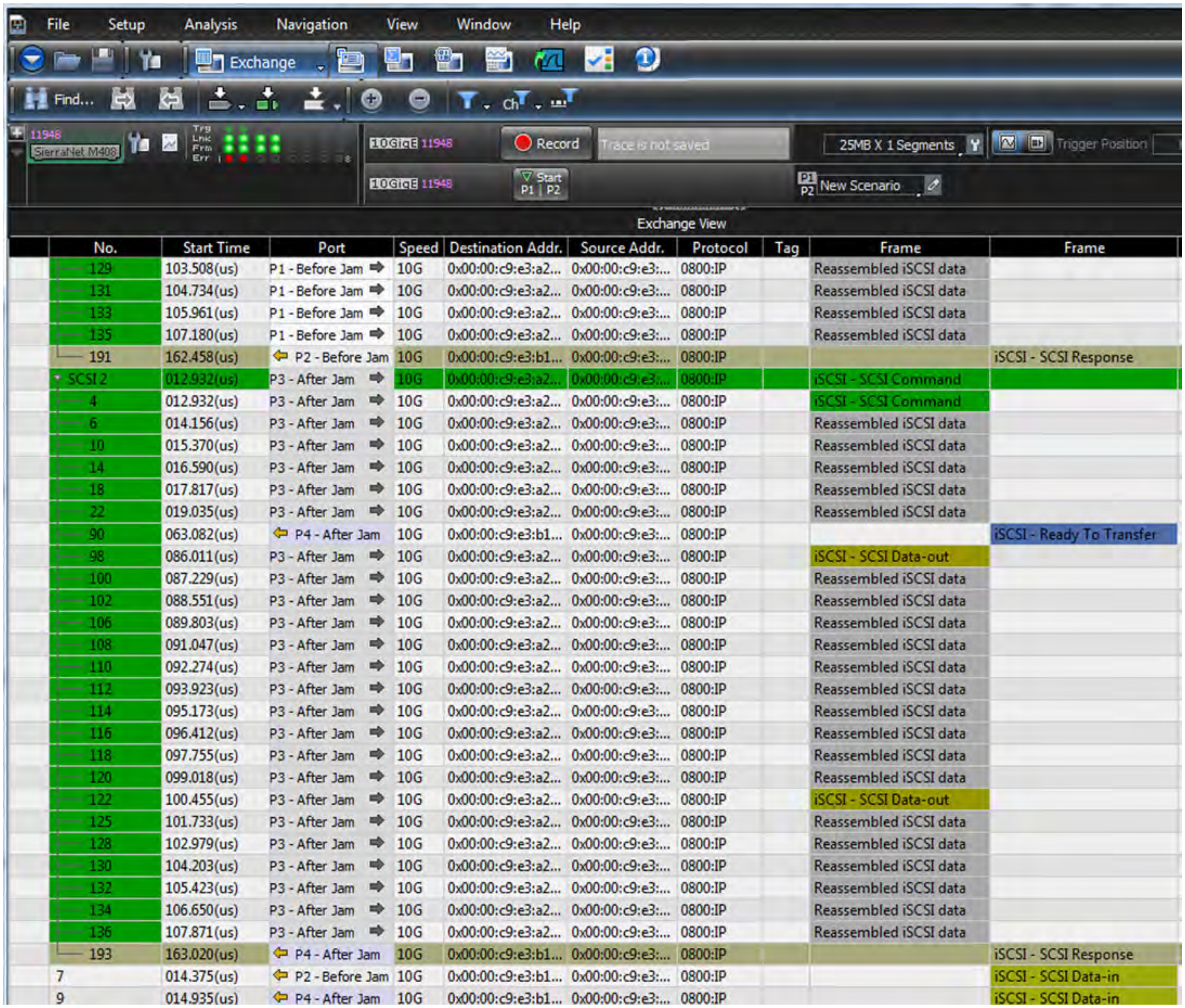


Figure 5.61: Exchange View – Events Arranged Hierarchically vs. Sequentially SCSI CMMD #1

The first SCSI Command that starts with event 3, but the elements of that command are not sequential. As seen in the Frame column, data on the bus includes information from other SCSI commands. In the Exchange view, you can see that the first SCSI command has reassembled iSCSI data and iSCSI commands in events 3, 5, 8, 12, 16, 20, 88, 97, 99, 101, 104, 107, 109, 111, 113,115, 117, 119, 121, 123, 127, 129, 131, 133 and 135 before a final SCSI Response is returned in event 191.

SCSI command 2 start with event 4, but elements of that command are interspersed with commands and data from events 6, 10, 14, 18, 22, 90, 98, 100, 102, 106, 108, 110, 112, 114, 116, 118, 120, 122, 125, 128, 130, 132, 134, 136 before a final SCSI Response is returned in event 193. See Figure 5.62.

As you can see from this simple example, SCSI commands and data are interspersed with events from a variety of other commands, but in the Exchange View you can see which events should be arraigned logically to form a single transaction.



No.	Start Time	Port	Speed	Destination Addr.	Source Addr.	Protocol	Tag	Frame	Frame
129	103.508(us)	P1 - Before Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
131	104.734(us)	P1 - Before Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
133	105.961(us)	P1 - Before Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
135	107.180(us)	P1 - Before Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
191	162.458(us)	P2 - Before Jam	10G	0x00:00:c9:e3:b1...	0x00:00:c9:e3:...	0800:IP			iSCSI - SCSI Response
SCSI 2	012.932(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		iSCSI - SCSI Command	
4	012.932(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		iSCSI - SCSI Command	
6	014.156(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
10	015.370(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
14	016.590(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
18	017.817(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
22	019.035(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
90	063.082(us)	P4 - After Jam	10G	0x00:00:c9:e3:b1...	0x00:00:c9:e3:...	0800:IP			iSCSI - Ready To Transfer
98	086.011(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		iSCSI - SCSI Data-out	
100	087.229(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
102	088.551(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
106	089.803(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
108	091.047(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
110	092.274(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
112	093.923(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
114	095.173(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
116	096.412(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
118	097.755(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
120	099.018(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
122	100.455(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		iSCSI - SCSI Data-out	
125	101.733(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
128	102.979(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
130	104.203(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
132	105.423(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
134	106.650(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
136	107.871(us)	P3 - After Jam	10G	0x00:00:c9:e3:a2...	0x00:00:c9:e3:...	0800:IP		Reassembled iSCSI data	
193	163.020(us)	P4 - After Jam	10G	0x00:00:c9:e3:b1...	0x00:00:c9:e3:...	0800:IP			iSCSI - SCSI Response
7	014.375(us)	P2 - Before Jam	10G	0x00:00:c9:e3:b1...	0x00:00:c9:e3:...	0800:IP			iSCSI - SCSI Data-in
9	014.935(us)	P4 - After Jam	10G	0x00:00:c9:e3:b1...	0x00:00:c9:e3:...	0800:IP			iSCSI - SCSI Data-in

Figure 5.62: Exchange View of SCSI Command #2

Exchange View offers you a powerful debugging capability by grouping events together hierarchically.

NVMe Transactions

For NVMe transactions the start and end of the transaction are clearly displayed in the Exchange View. See Figure 5.63.

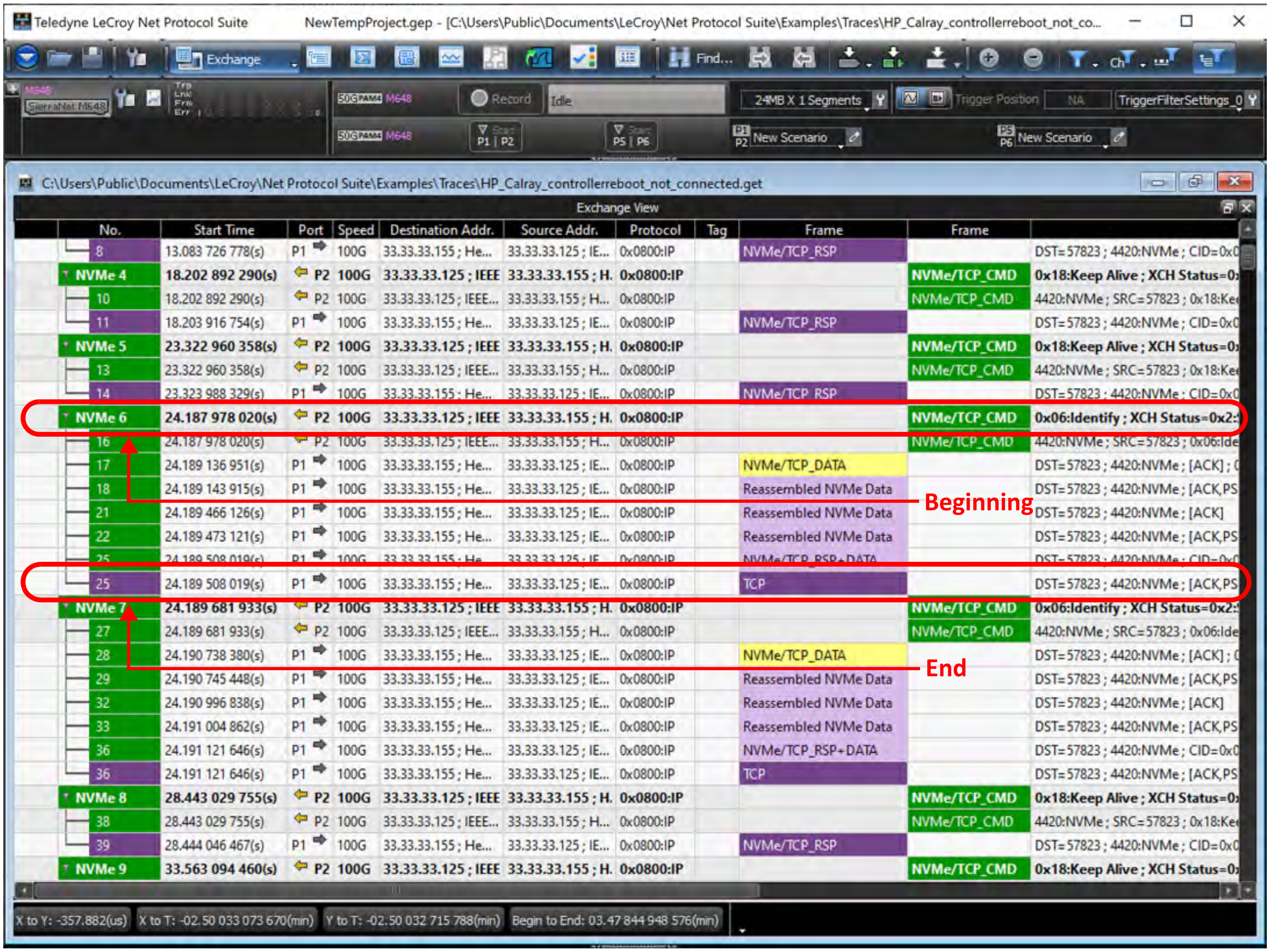


Figure 5.63: Exchange View – NVMe Transactions Highlighted

Thresholds: Errors and Warnings

You can also set Error and Warning thresholds for the following Logical Fields:

- Duration
- Data Length
- Packet length
- TCP Payload length
- Latency
- Response time
- Pending commands

To set the Threshold values go to the Preferences icon  in the Main Toolbar and select Preferences/Display settings/Types/Field Attributes/ Logical and select one of the Logical Fields (see Figure 5.64).

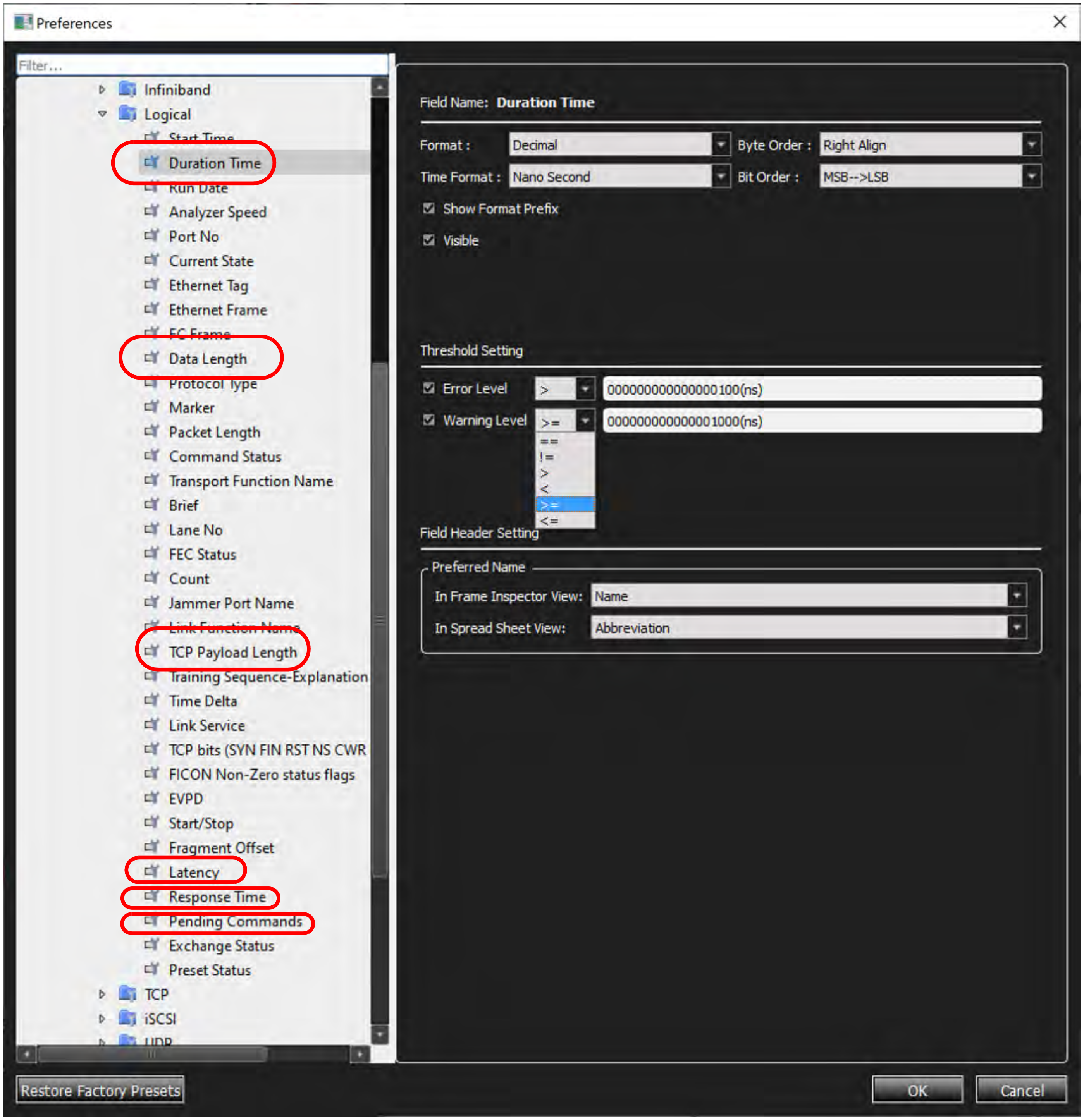


Figure 5.64: Logical Fields with Thresholds for Errors and Warnings

After you set up the Thresholds, if they are exceeded they will show up in the recorded trace. You can see typical results of setting Thresholds in Figure 5.65.

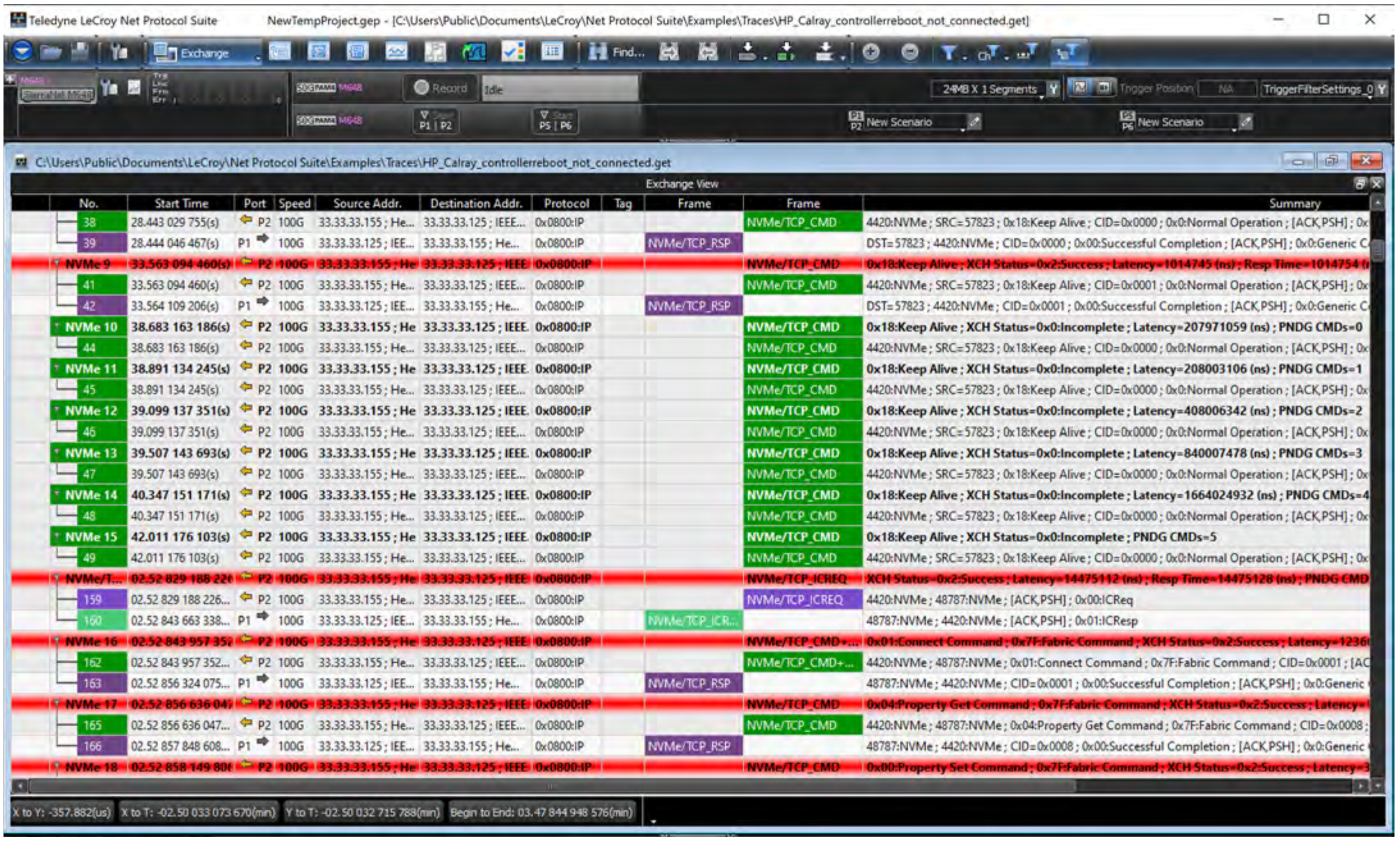


Figure 5.65: Exchange View with Errors/Warnings Shown

5.2.3 Frame Inspector View

Frame Inspector View has lots of information that is available in event View, but not Spreadsheet View, so it is most useful in conjunction with the Spreadsheet View.

To open a Frame Inspector View of the current capture, select **Analysis → Frame Inspector View** or click the  button on the View Type toolbar.

This Frame Inspector View has the following three tabs:

5.2.3.1 Spec View

This view shows the Frame as it would appear in the spec, with the field names and values spelled out clearly. Fields that are too short to clearly contain the description can be viewed as tooltips by hovering the mouse over them. Some fields might have a a lowercase ‘e’ button at the top right corner. Pressing this button displays an ‘expanded’ view of the sub-fields in this field.

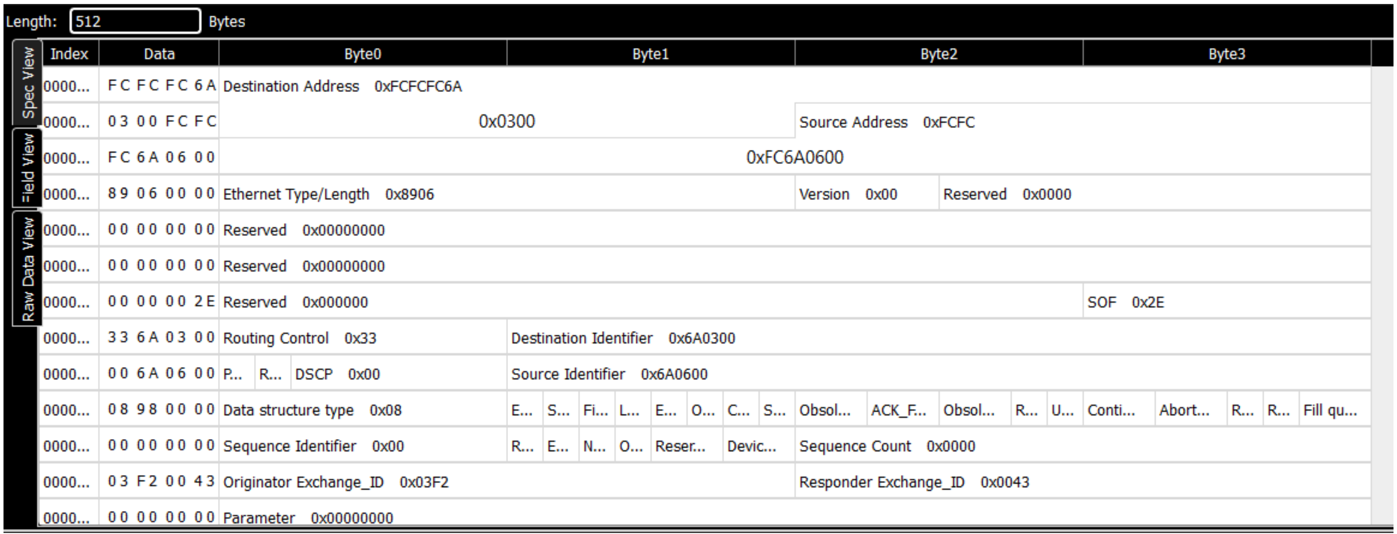


Figure 5.66: Frame Inspector-Spec View

5.2.3.2 Field View

This view shows, when applicable, a hierarchical display of the selected event, with the relevant fields in each level.

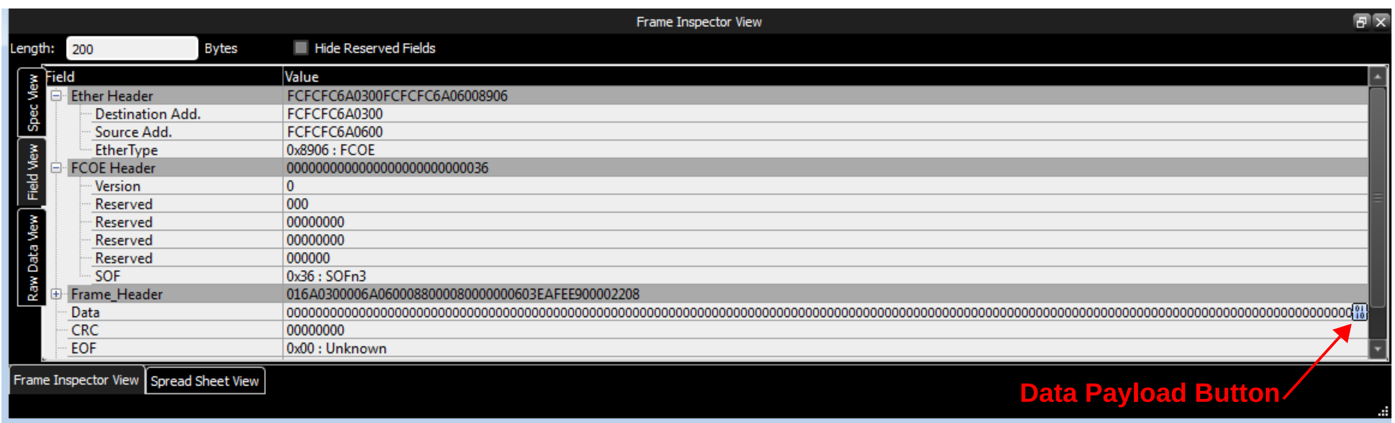


Figure 5.67: Frame Inspector-Field View

Click the Data Payload button to display the Data Payload window (see Figure 5.68).

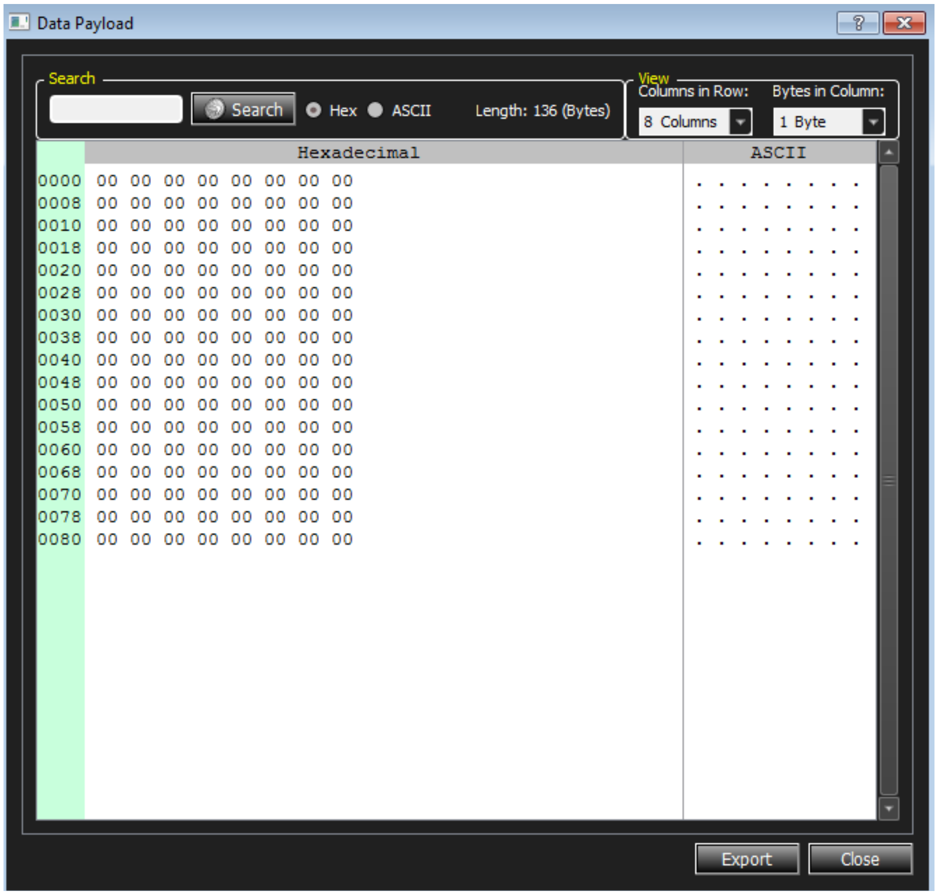


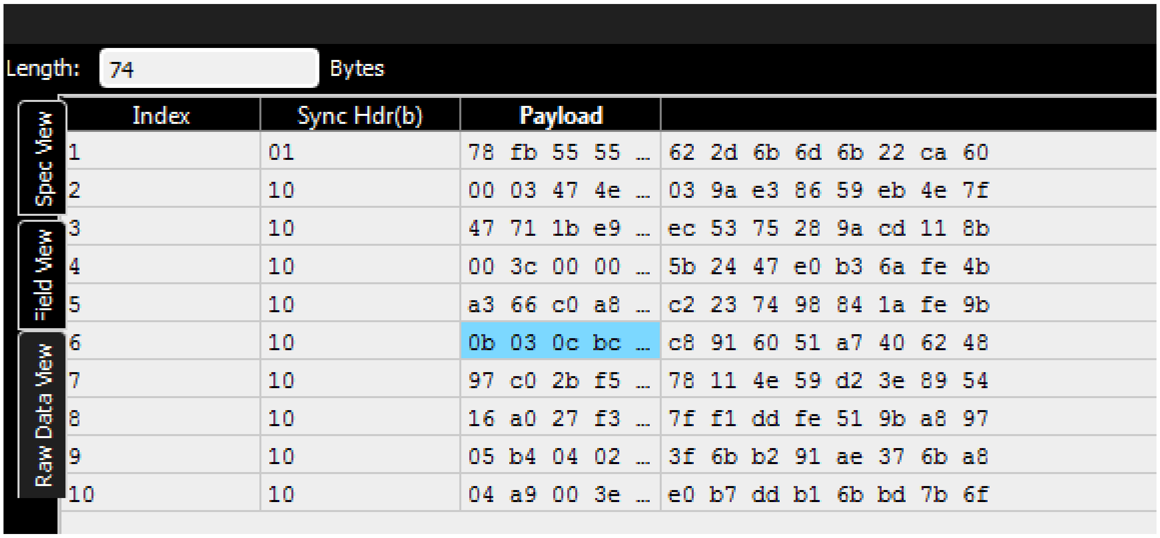
Figure 5.68: Data Payload Dialog Window

Any ASCII non-printable characters are depicted as black dots as shown above.

5.2.3.3 Raw Data View – Frame Inspector View for 64b/66b Decoding

Raw Data View in the **Frame Inspector View** window shows the exact bit stream in 66b format (see Figure 5.69). This view shows Hex, 10-bit and Running Disparity views of each dword in the selected event. In this view, a 66 bits block is reconstructed similar to the received data (see the screen capture below). The following columns are displayed in the **Raw Data View**:

- **Index**: This column demonstrates the index of the 66-bits symbol in current blocks.
- **Sync Header**: This column shows the Sync Header bits of a symbol.
- **Payload**: This column shows the 8 payload bytes in each symbol before scrambling.
- **Scrambled**: This column shows the 8 payload bytes in each symbol after scrambling.



Length: 74 Bytes

Index	Sync Hdr(b)	Payload	
1	01	78 fb 55 55 ...	62 2d 6b 6d 6b 22 ca 60
2	10	00 03 47 4e ...	03 9a e3 86 59 eb 4e 7f
3	10	47 71 1b e9 ...	ec 53 75 28 9a cd 11 8b
4	10	00 3c 00 00 ...	5b 24 47 e0 b3 6a fe 4b
5	10	a3 66 c0 a8 ...	c2 23 74 98 84 1a fe 9b
6	10	0b 03 0c bc ...	c8 91 60 51 a7 40 62 48
7	10	97 c0 2b f5 ...	78 11 4e 59 d2 3e 89 54
8	10	16 a0 27 f3 ...	7f f1 dd fe 51 9b a8 97
9	10	05 b4 04 02 ...	3f 6b b2 91 ae 37 6b a8
10	10	04 a9 00 3e ...	e0 b7 dd b1 6b bd 7b 6f

Figure 5.69: Raw Data View without FEC

5.2.3.4 MAD Header Decode in Frame Inspector View

Another example of the link between Spreadsheet View and Frame Inspector View can be seen below (Figure 5.70) in a MAD Header decode.

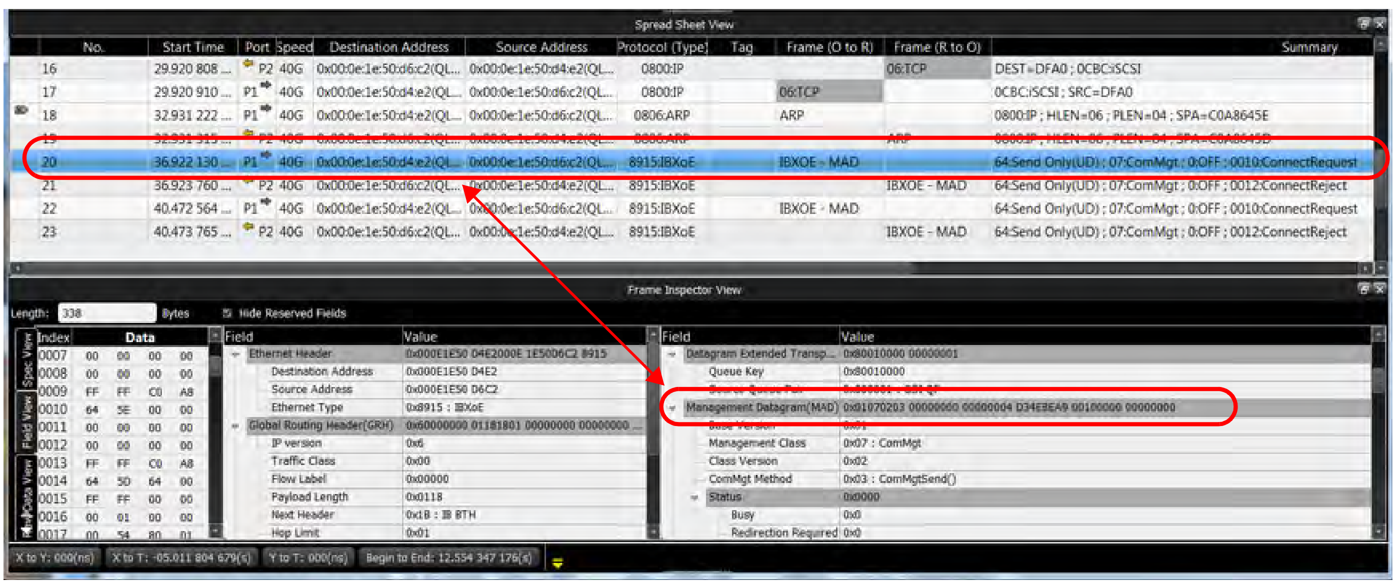


Figure 5.70: MAD Header Decoded in Spreadsheet and Frame Inspector Views

5.2.3.5 iSER Header Decode in Frame Inspector View

Another example of the link between Spreadsheet View and Frame Inspector View can be seen below in an iSER Header decode, see Figure 5.71.

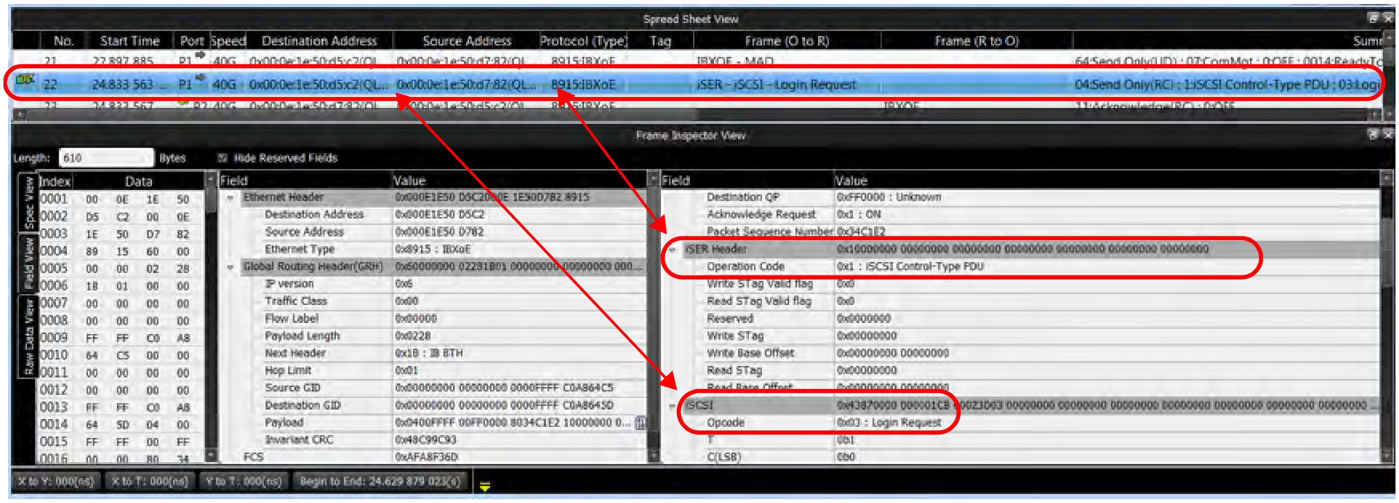


Figure 5.71: iSER Header Decoded in Spreadsheet and Frame Inspector Views

5.2.3.6 Adding a New Column from Frame Inspector View to Spreadsheet View

You can add new columns to the Spreadsheet View from Frame Inspector by selecting a field of interest and performing a right click. A context menu will popup with a "Create new column" tab and asking After which current column you want the new column added. See Figure 5.72.

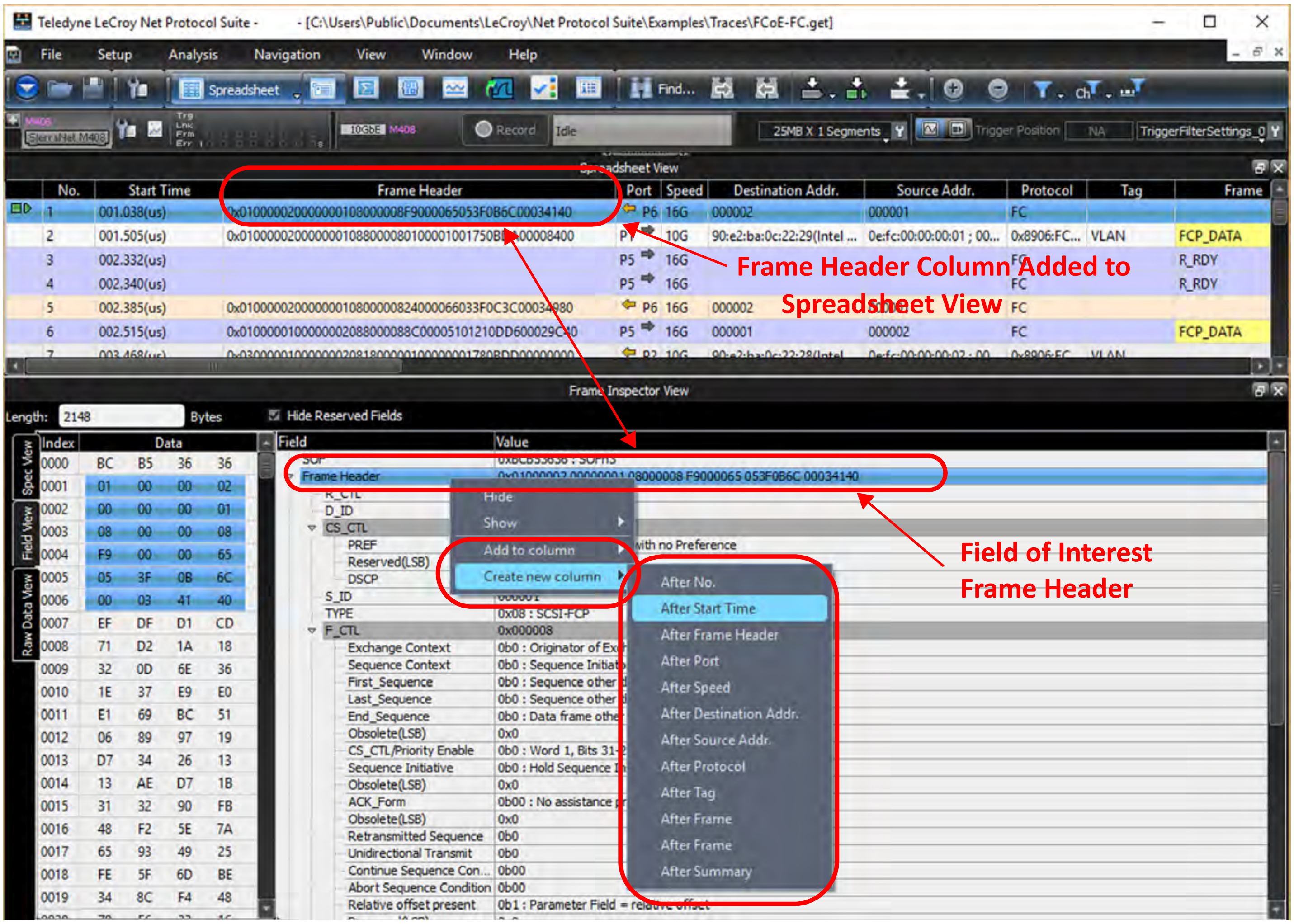


Figure 5.72: Add New Column to Spreadsheet View from Data in Frame Inspector View

In the above example the Frame Header was added after the Start Time.

5.2.4 Traffic Summary View

The Analysis menu option allows you to see a Traffic Summary of the captured Trace. The Traffic Summary View for each captured pattern can be viewed. This Summary View displays the port number, statistics, and the percentage of the total count. See Figure 5.73.

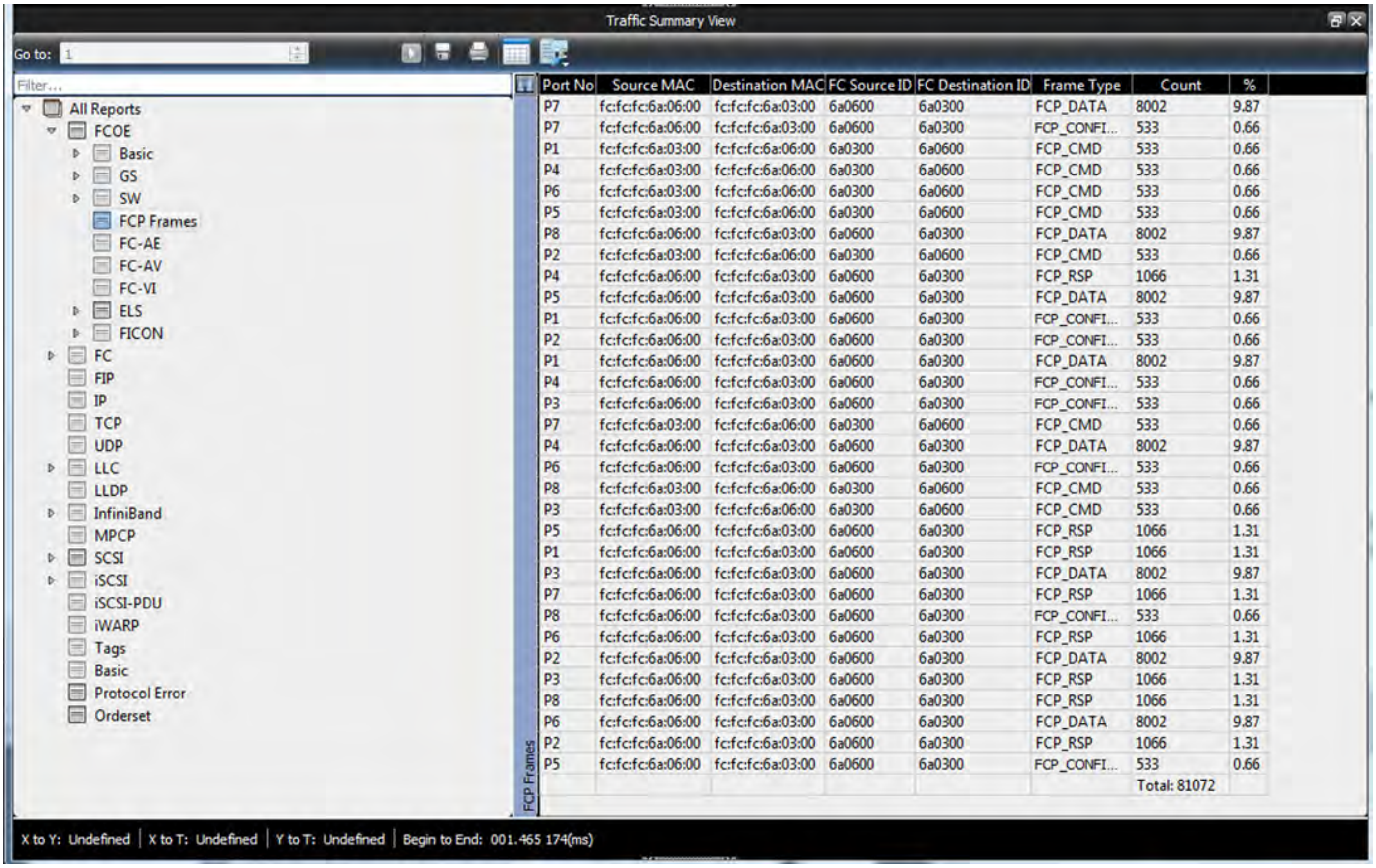


Figure 5.73: Traffic Summary View

5.2.4.1 Traffic Summary Toolbar

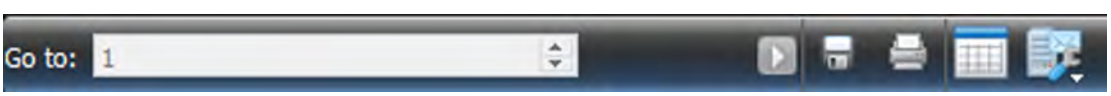


Figure 5.74: Traffic Summary Toolbar

The Traffic Summary Toolbar has the following options:

- Go to: Instance Number
- Save: Save Traffic Summary to specific location
  This saves an HTML file, that can also be opened in Excel.
- Print: Print Traffic Summary Report
- Text: Re-Format Traffic Summary Report into readable text

- Format:
  - Grid Lines ➔ Turn Grid Lines ON or OFF
  - Tight Columns ➔ Turn Tight Columns ON or OFF

5.2.4.2 Viewing Ethernet and Fibre Channel Traces in Traffic Summary View

The application captures and displays both Ethernet and Fibre Channel data.

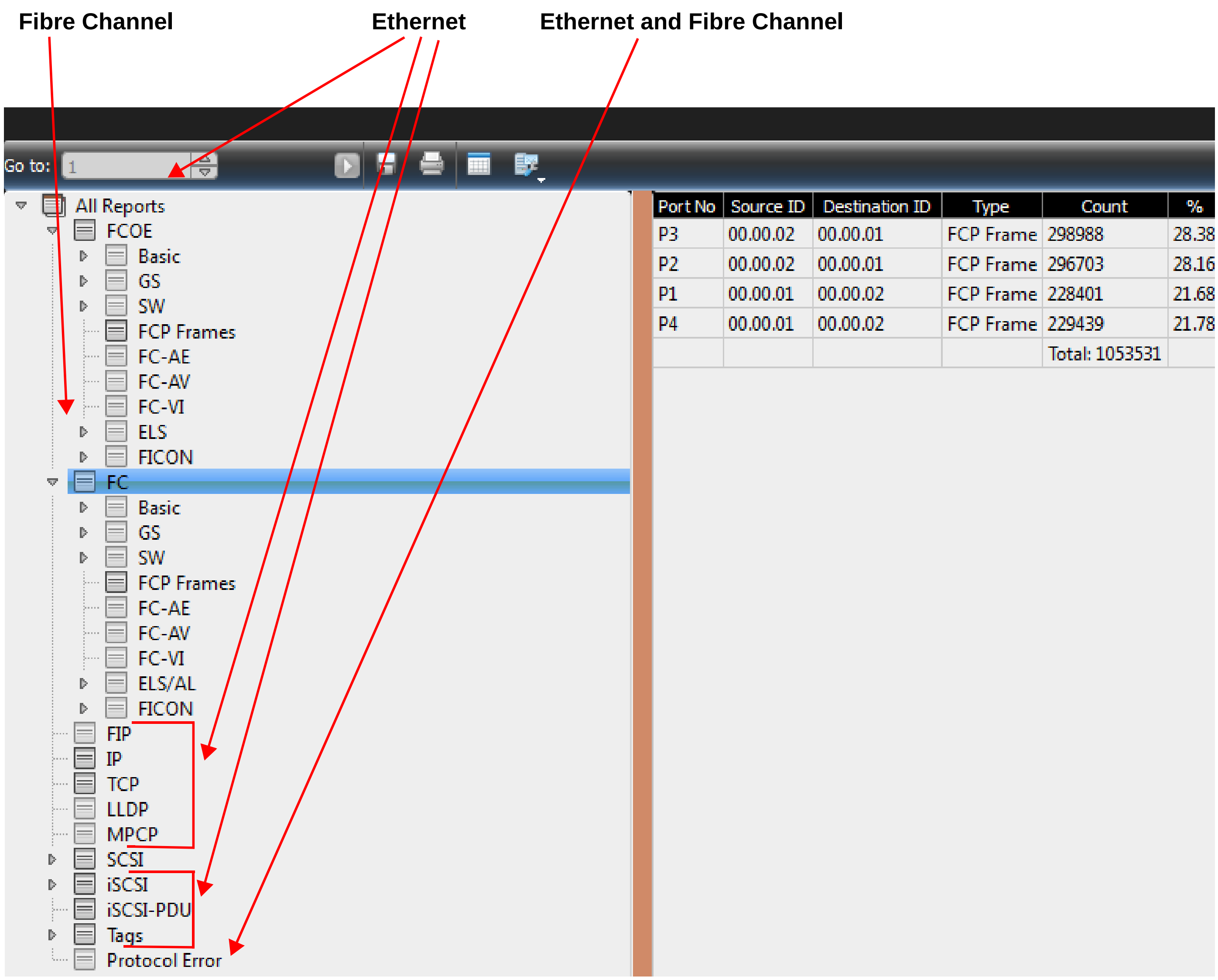


Figure 5.75: Merged FC and Ethernet Traces in Traffic Summary View

5.2.4.3 Performance Metrics (Traffic Summary View)

- Latency = The time between the first frame of the exchange and the last frame of the exchange.
  - This value is valid for first frame of an exchange; it is not applicable for other frames of the exchange.
  - The latency time of an exchange is expressed in nanoseconds.
- Response Time = Time between the command and response in an exchange.
  - This specifies the response time of an exchange in nanoseconds.
  - It is applicable for first frame of each exchange.; it is null (0) for other frames of the exchange.
- Throughput = The total number of transferred bytes of an exchange divided by the duration of the exchange. In MB/s.

5.2.4.4 Traffic Summary Search Capability

The Traffic Summary View highlights the type of transactions present in the currently loaded Trace. It has a Reports Filter Window in the left pane of the dialog and a Find Tool Filter Window in the right pane of the dialog to help searching for specific commands. See Figure 5.76.

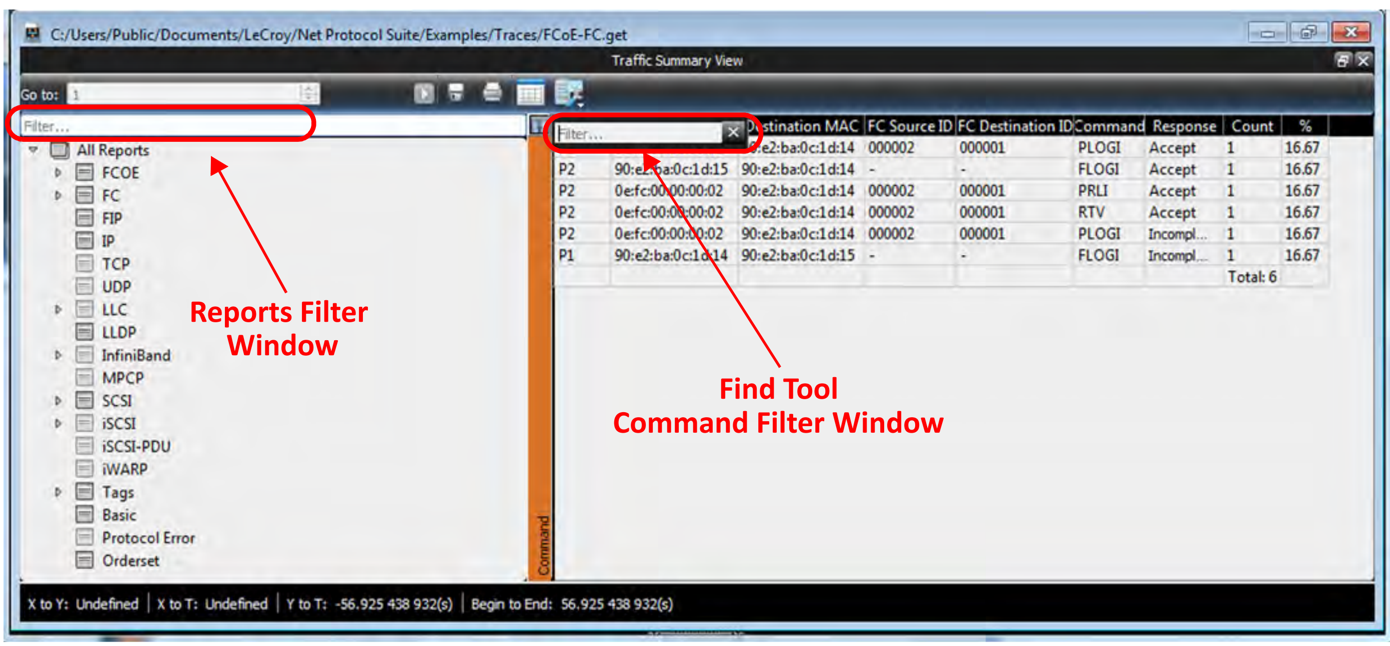


Figure 5.76: Traffic Summary View

In the following examples, we're looking for specific commands within a specific type of transaction, but the methodology can be expanded to search for any type of command within any type of report.

5.2.4.5 FCOE Reports

If you select the **FCOE Reports → ELS → Command** (see Figure 5.77) those types of transactions will show up in the right side window.

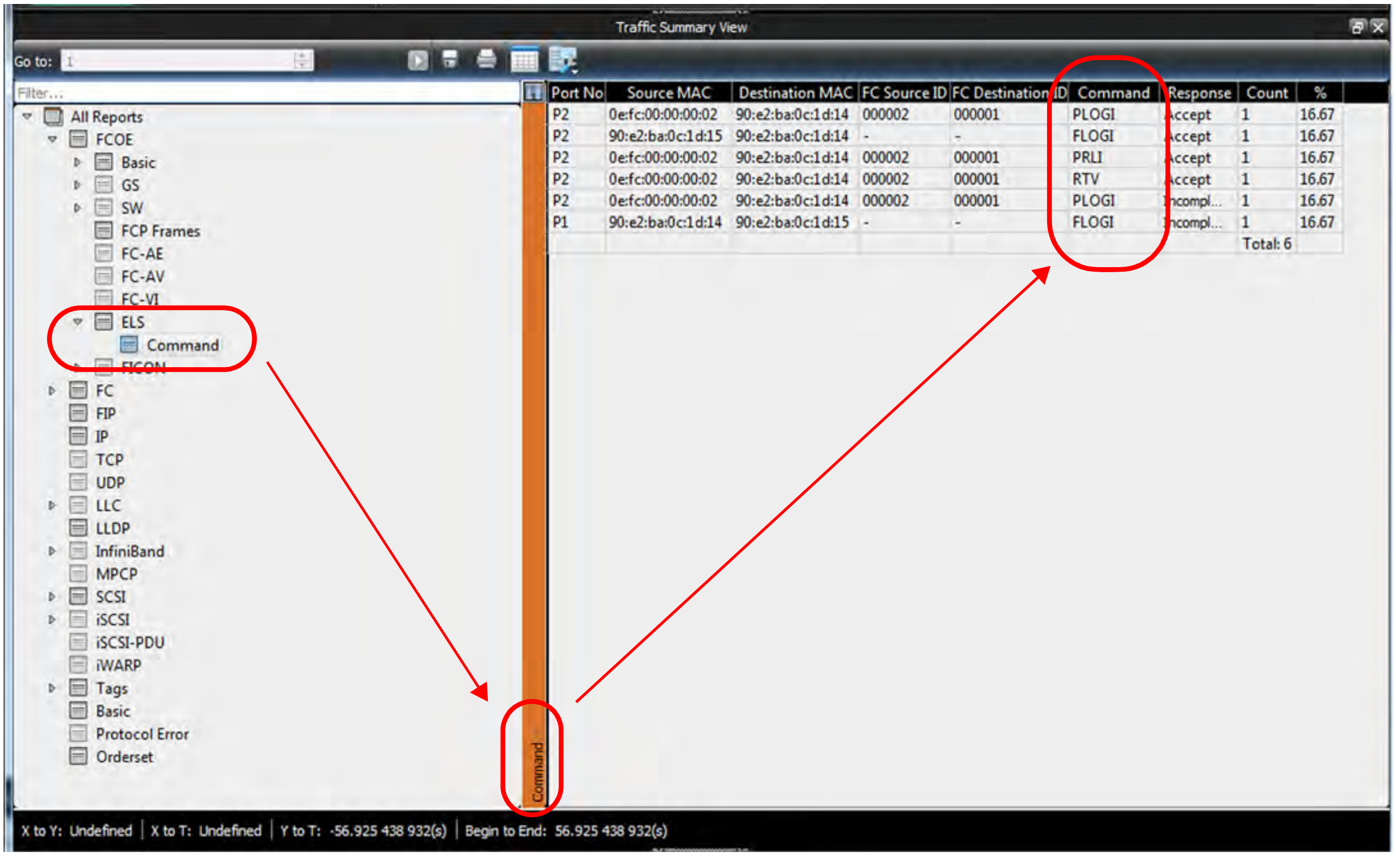


Figure 5.77: FCOE Reports: ELS Commands

You could use the Find Tool to look for a specific command type.

5.2.4.6 FC Reports

If you select **FC → ELS/AL → Commands** (Figure 5.78) those types of transactions will show up in the right side window.

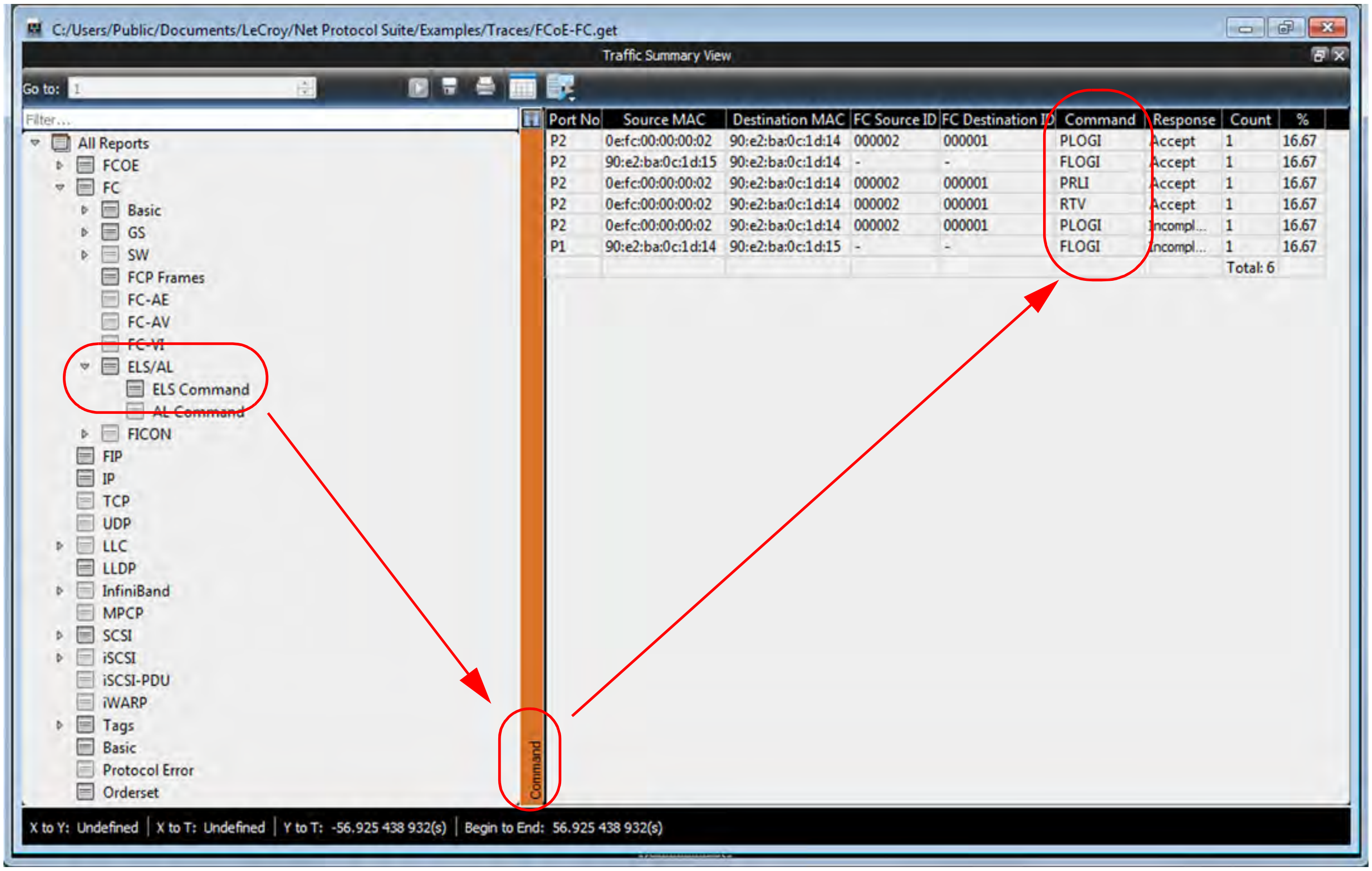


Figure 5.78: FC Reports: ELS Commands

You could use the Find Tool to look for a specific command type.

5.2.4.7 NVMe Traffic Summary Reports

NVMe traffic can be decoded and displayed in the Traffic Report window (Figure 5.79).

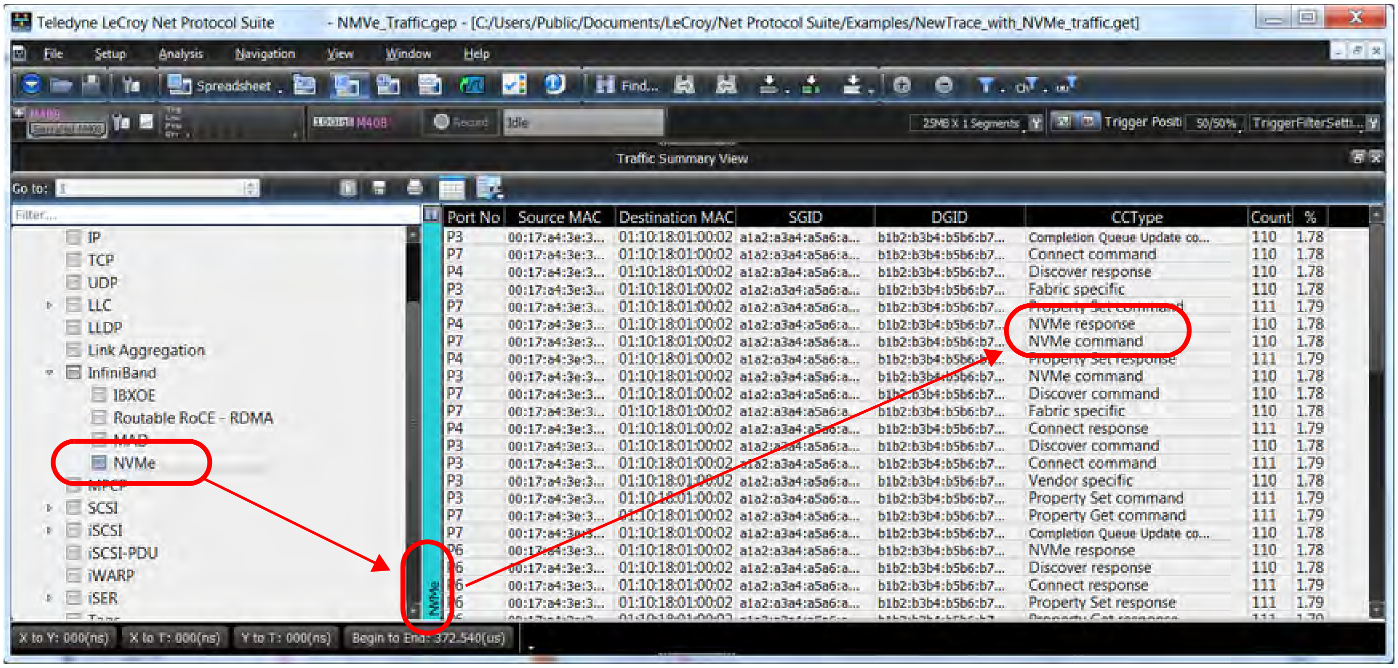


Figure 5.79: NVMe Traffic in Traffic Summary Report

5.2.4.8 Source and Destination Columns in Traffic Summary View

Traffic Summary displays the Source and Destination addresses for the first 10,000 pairs; the rest are grouped in the **Others** row.

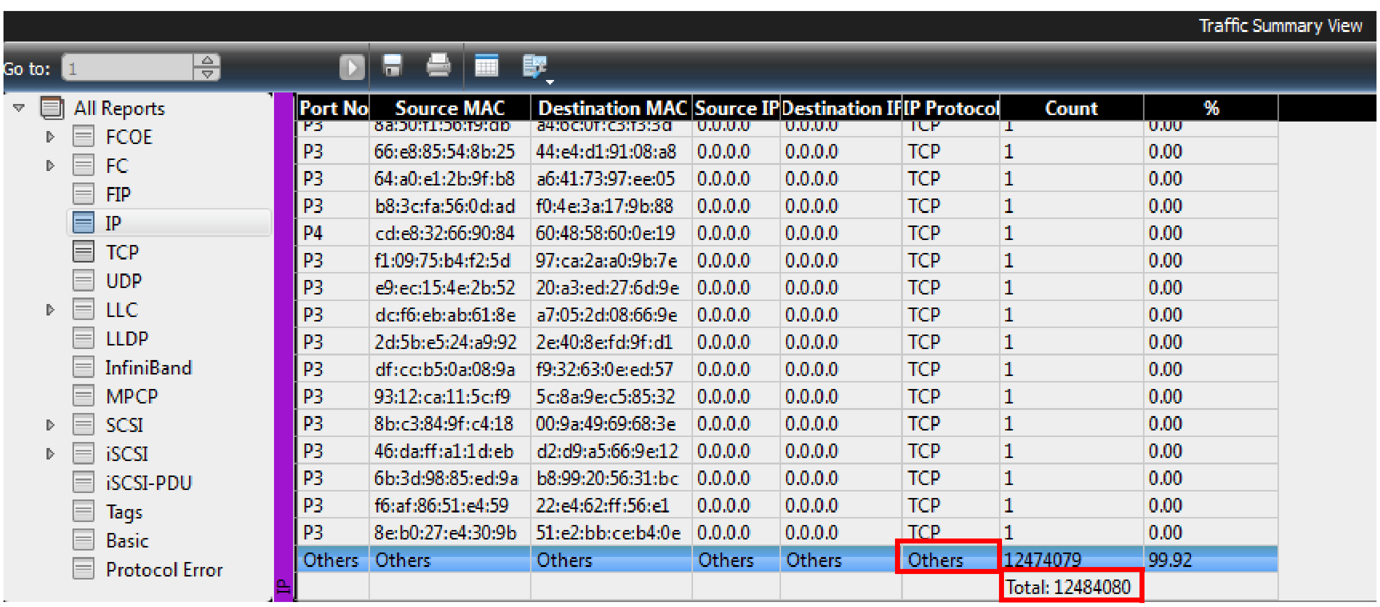


Figure 5.80: Source and Destination Columns in Traffic Summary View

5.2.4.9 Reassembly of Frames

Frames transmitted over the Ethernet break up into PDUs (Protocol Data Units). These PDUs may be received in a different order than they were originally transmitted. The application reassembles and displays them in the original order.

The screen captures below show the details of the reassembled frame in both the Spreadsheet View and the Frame Inspector View. The details of PDU1 in the Spreadsheet View are shown in the Frame Inspector View

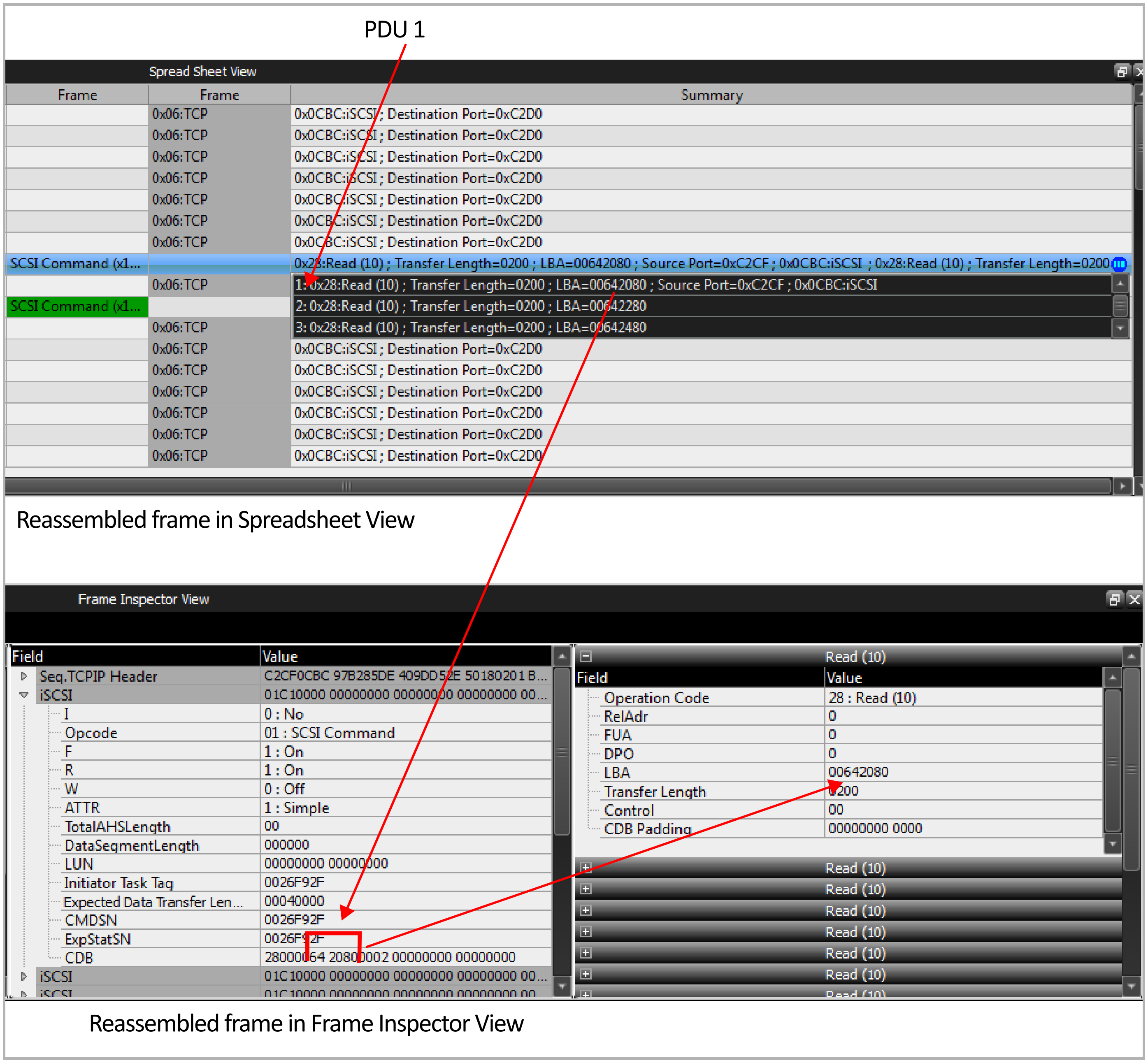


Figure 5.81: Reassembled Frame.

5.2.4.10 MAD Header Decoded: Traffic Summary View

Another example of the Traffic Summary View is shown below with an MAD header decoded, see Figure 5.82.

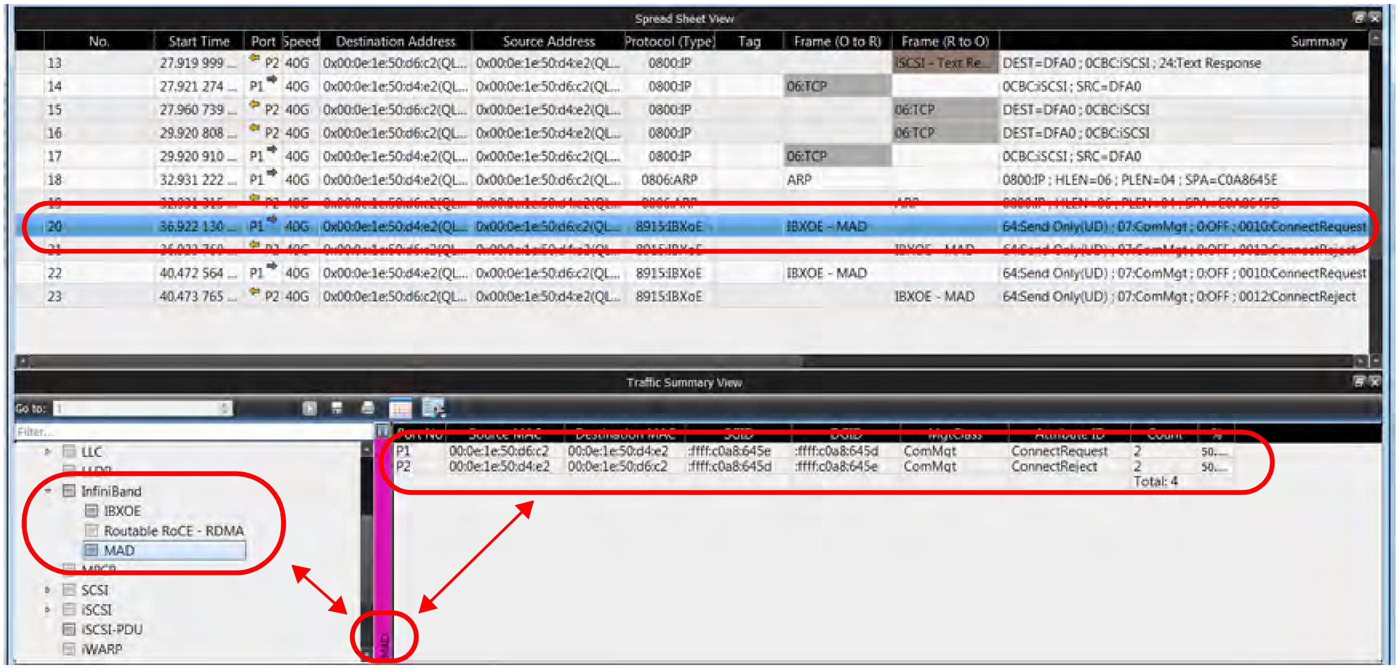


Figure 5.82: MAD Header Decoded in Spreadsheet and Traffic Summary View

5.2.4.11 MAD Header Decoded: Traffic Summary View – Text Report

A slightly different way to view the Traffic Summary is to view the reports as text. See Figure 5.83.

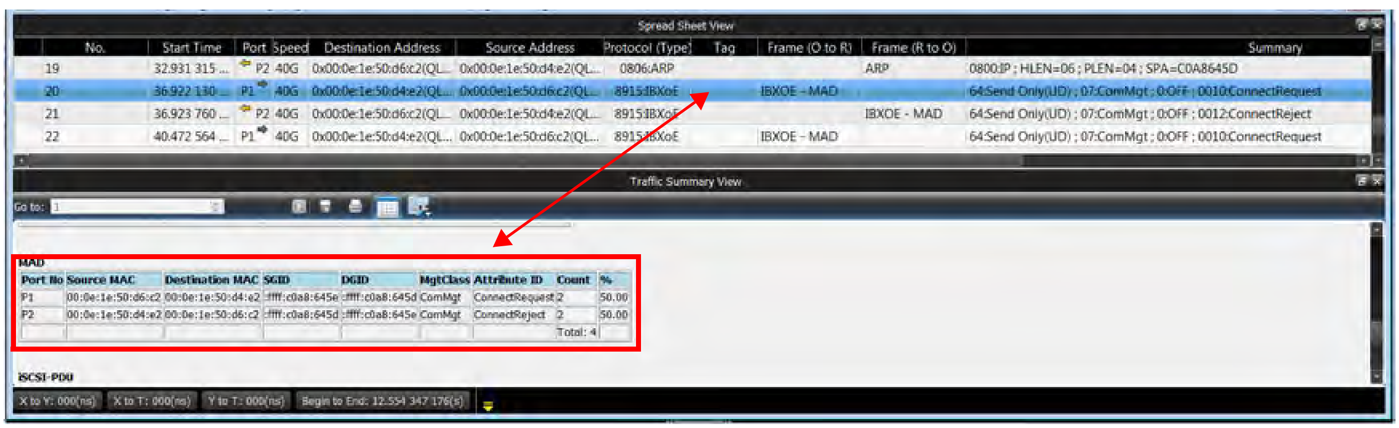


Figure 5.83: Traffic Summary View (Text Format) – MAD Header Decoded

5.2.4.12 iSER Header Decoded: Traffic Summary View

Another example of the Traffic Summary View is shown below with an iSER header decoded (Figure 5.84).

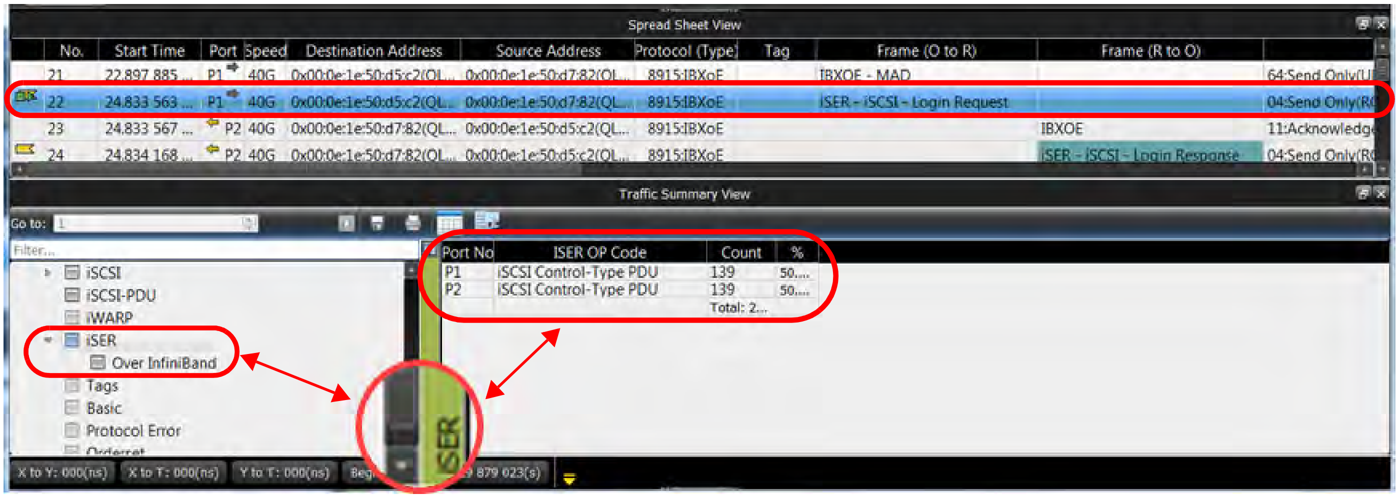


Figure 5.84: iSER Header Decoded in Spreadsheet and Traffic Summary View

5.2.4.13 iSER Header Decoded: Traffic Summary View – Text Report

A slightly different way to view the Traffic Summary is to view the reports as text (Figure 5.85).

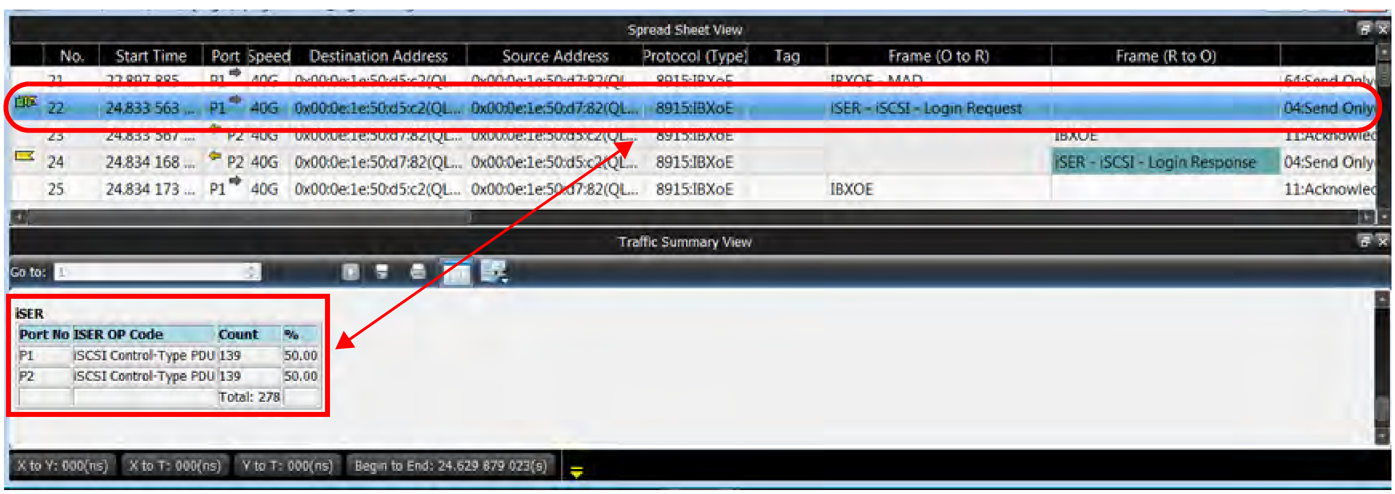


Figure 5.85: Traffic Summary View (Text Format) – iSER Header Decoded

5.2.5 Data View

The Data View displays data in Hexadecimal and ASCII format (Figure 5.86). You can search for data by entering criteria in the Search field. Select an option from Columns and Bytes drop-down list to display the data. The formats available are:

- ❑ Columns: 1,2, 4, 8 and 16
- ❑ Bytes: 1,2, 4, 8 and 16

Click the **Export** button to display the Save Data Payload dialog to save the data.

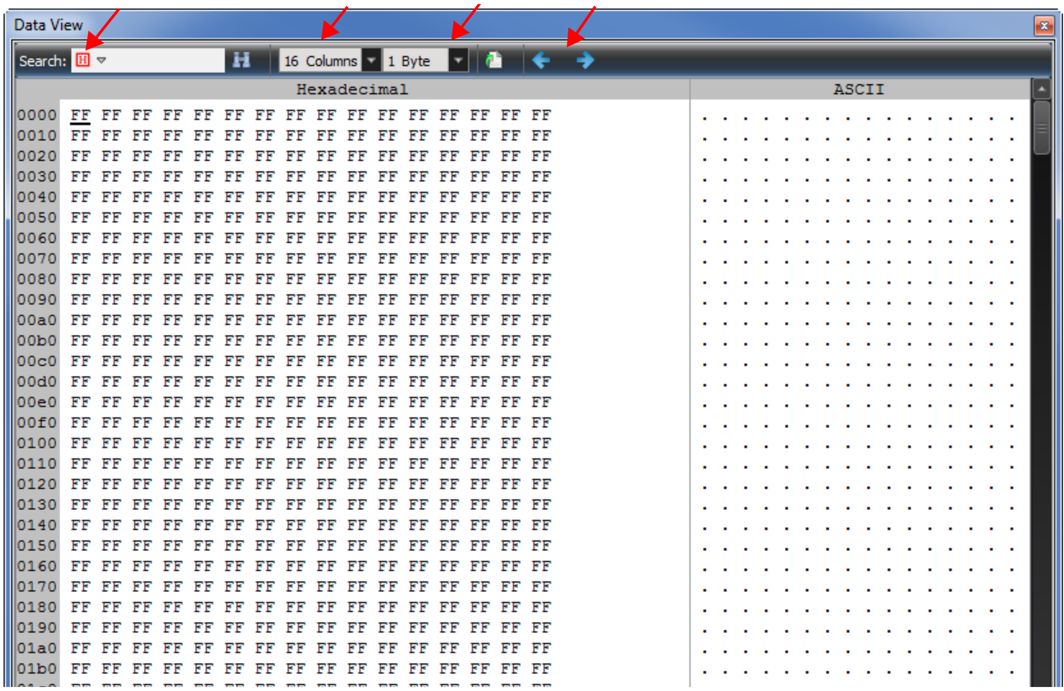


Figure 5.86: Data View

Data View Toolbar

- Search Window (Hex or ASCII)
- Search Icon
- Column Width (1 to 16)
- Bytes per Column (1 to 16)
- Export to File
- Move to Previous Payload
- Move to Next Payload

5.2.6 Bus Utilization View

The Bus Utilization View displays both a Link Utilization and an Error Count over a specific time frame. See Figure 5.87.

Display Controls (More detail is shown in Figures 5.88 and 5.89.)

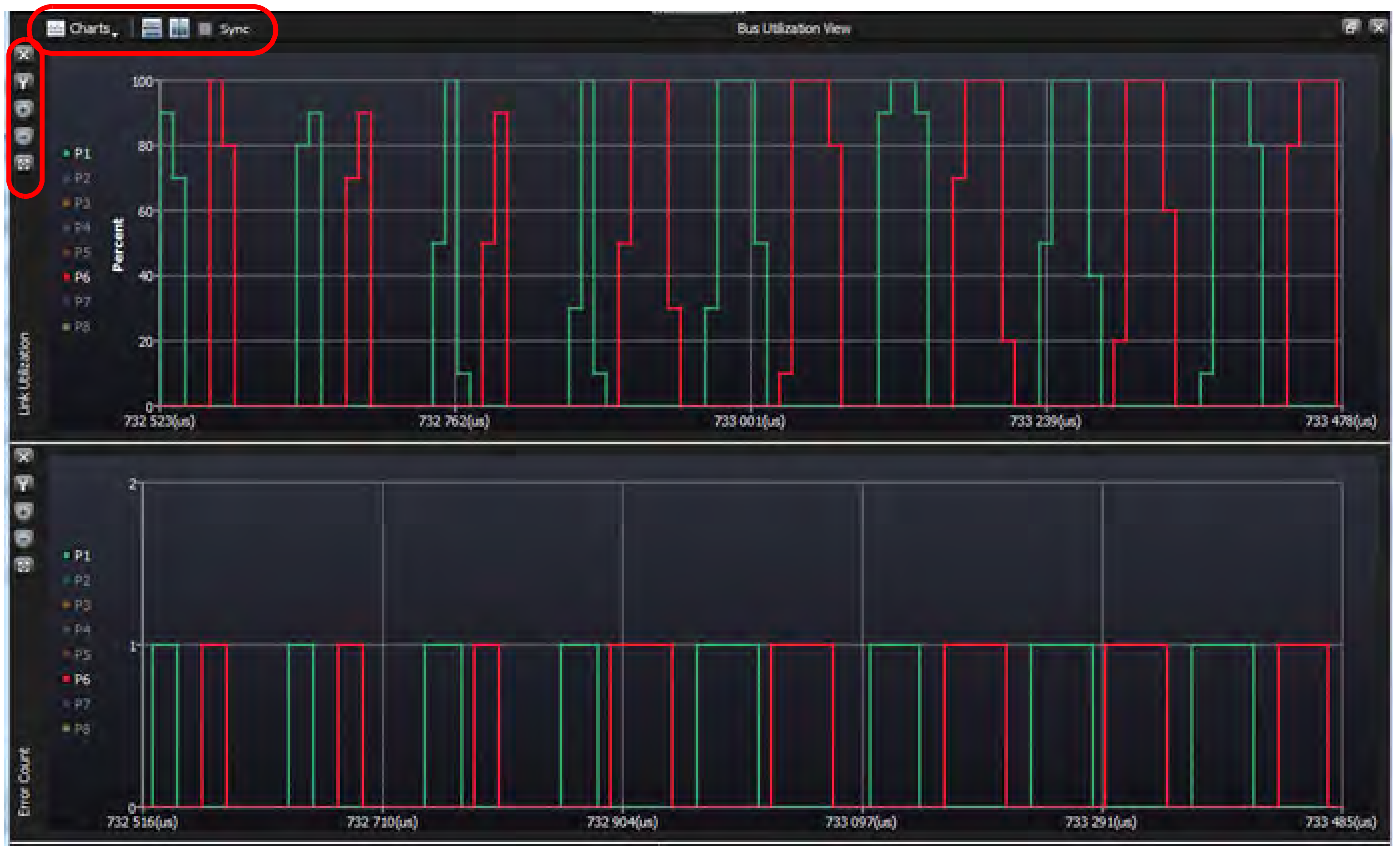


Figure 5.87: Typical Bus Utilization View (Ports P1 and P6 Showing)

5.2.6.1 Controls for Bus Utilization

- Add Charts (Display Error Count or Link Utilization or both; see Figure 5.88.)
- Tile Vertical (Display windows vertically, as shown in Figures 5.87 & 5.95).
- Tile Horizontal (Display window side by side; see Figure 5.94.)
- Synchronize Charts (Time frame is same for both views as in Figure 5.88).
- Delete Chart Setting (Delete display Error Count or Link Utilization or both; see Figure 5.89.)
- Zoom In (Ctrl + Mouse wheel, see Figure 5.89).
- Zoom Out (Ctrl + Mouse wheel, see Figure 5.89).
- Fit to Screen (Full view of Trace, see Figure 5.89).
- Show or Hide Ports (Show/Hide Port1 – Port8, see Figure 5.89).

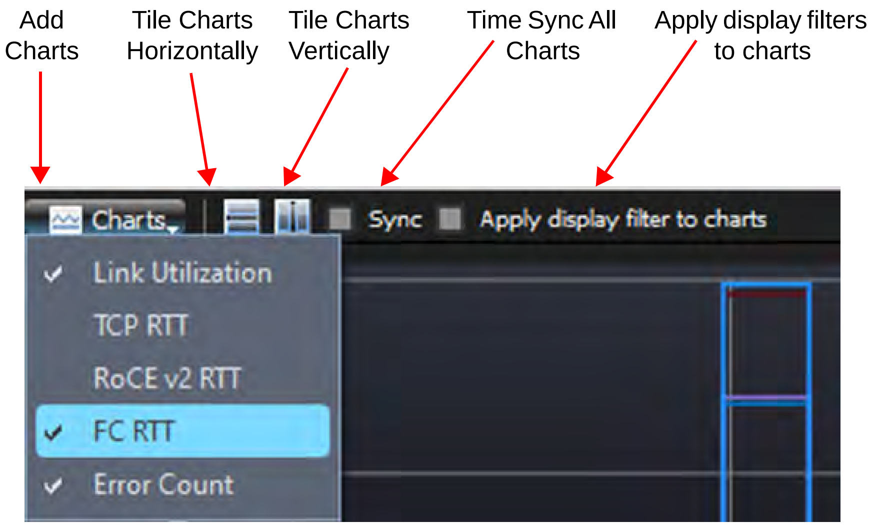


Figure 5.88: Controls for Bus Utilization View (1)

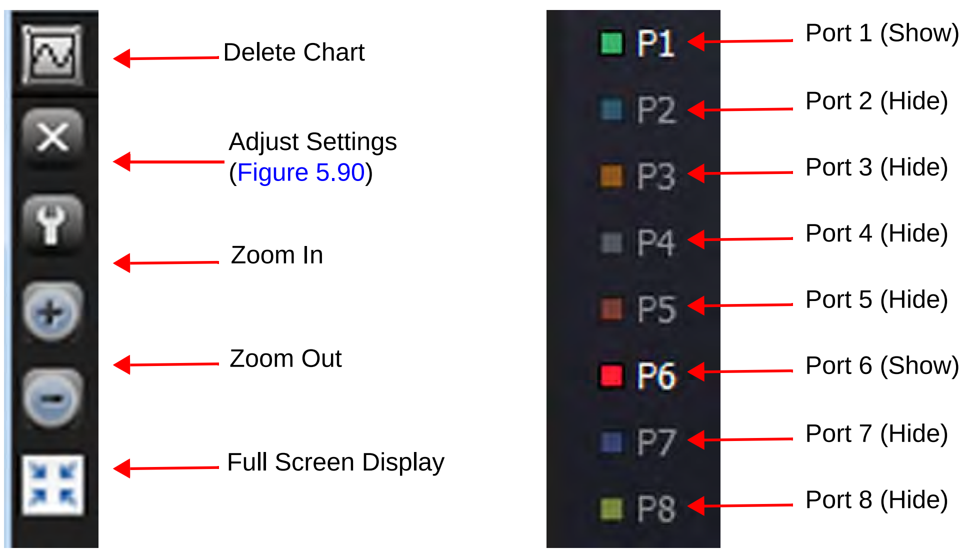


Figure 5.89: Controls for Bus Utilization View (2)

NOTE: **Measurement Interval**: The Measurement Interval parameter defines a sampling period for calculating graph data points. During each time interval, the graph will average all values within that interval and generate one data point for the graph.

- Larger intervals will result in fewer data points, and thus less-precise graphs (Figure 5.91).
- Smaller intervals will result in more data points, and thus more-precise graphs (Figure 5.93).
- Graphs, such as Link Utilization, are usually best-served by larger intervals of >100ms.
- The RTT graph requires high-precision and is best served by a minimum interval of 1ns.

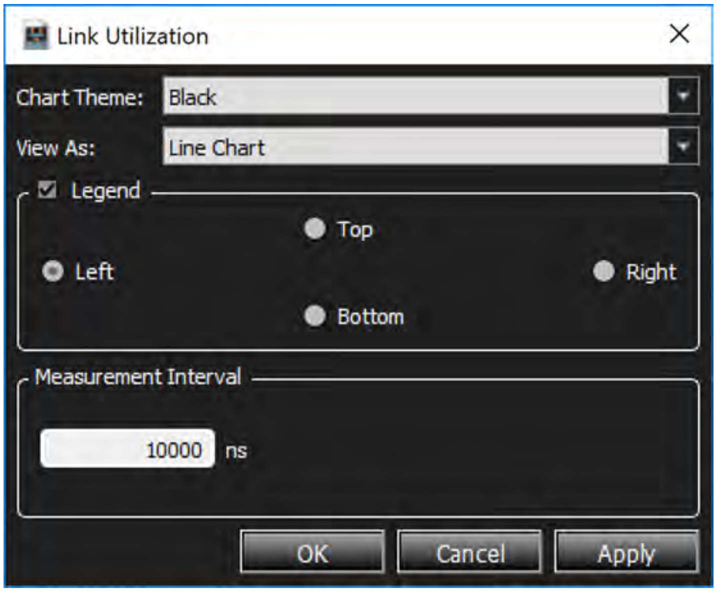


Figure 5.90: Settings Example: Measurement Internal = 10,000 nsec

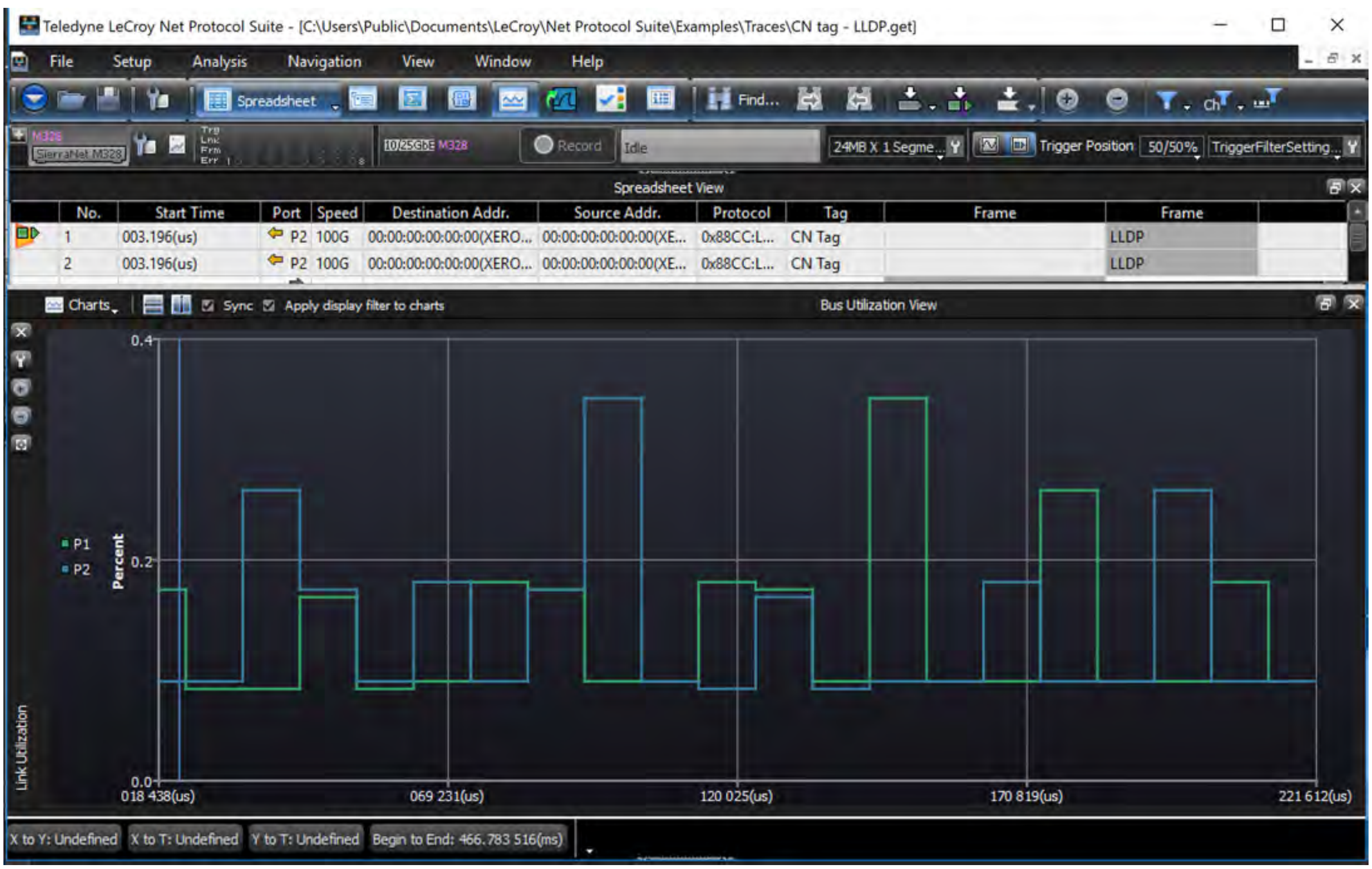


Figure 5.91: Measurement Interval: 10,000 nsec (Fewer number of Samples)

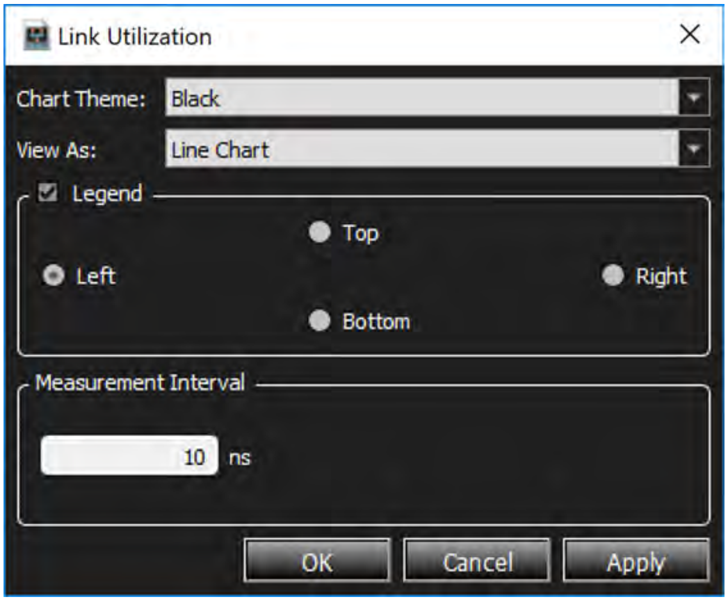


Figure 5.92: Settings Example – Measurement Internal = 10 nsec

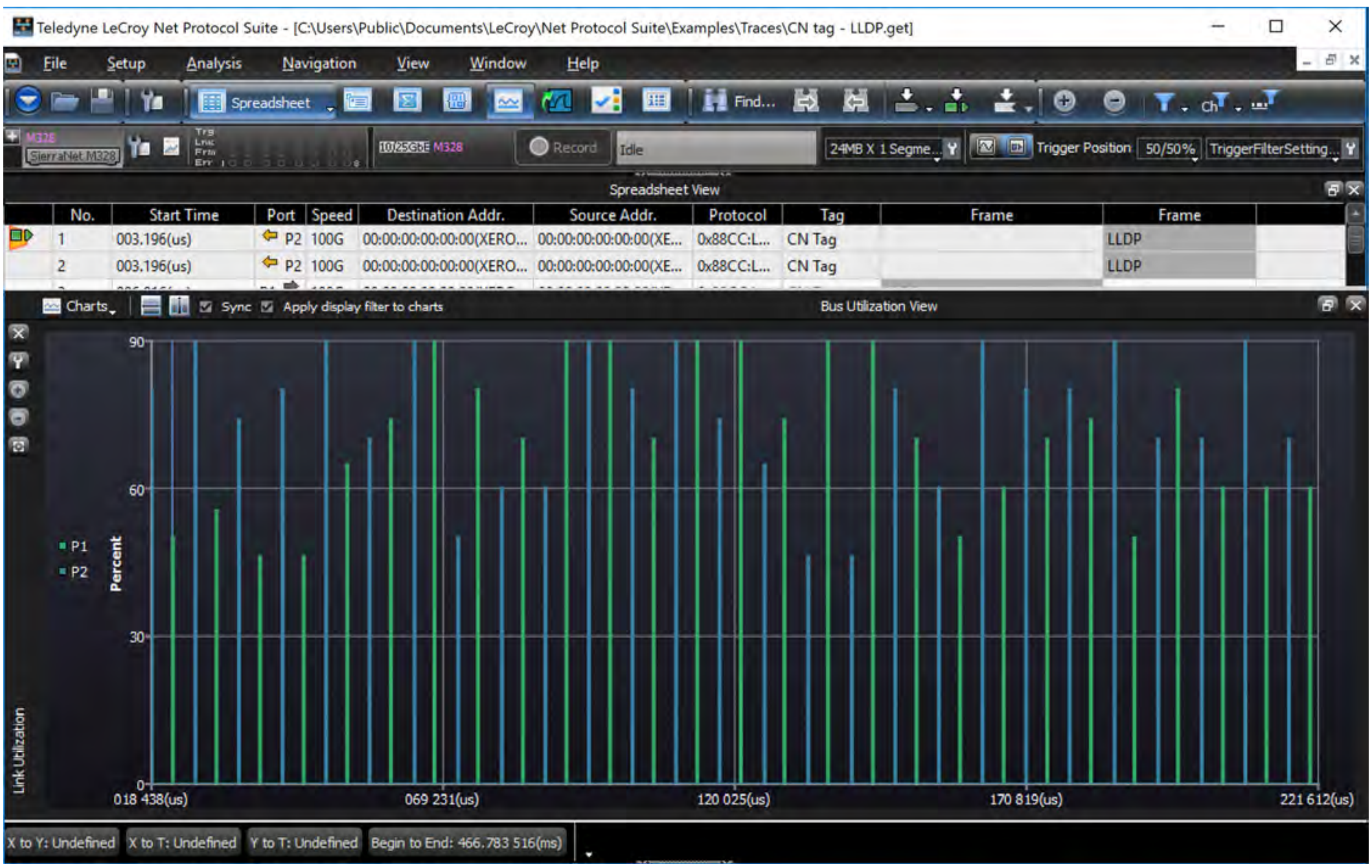


Figure 5.93: Measurement Interval – 10 nsec (Lots of Samples)

5.2.6.2 Tile Horizontally

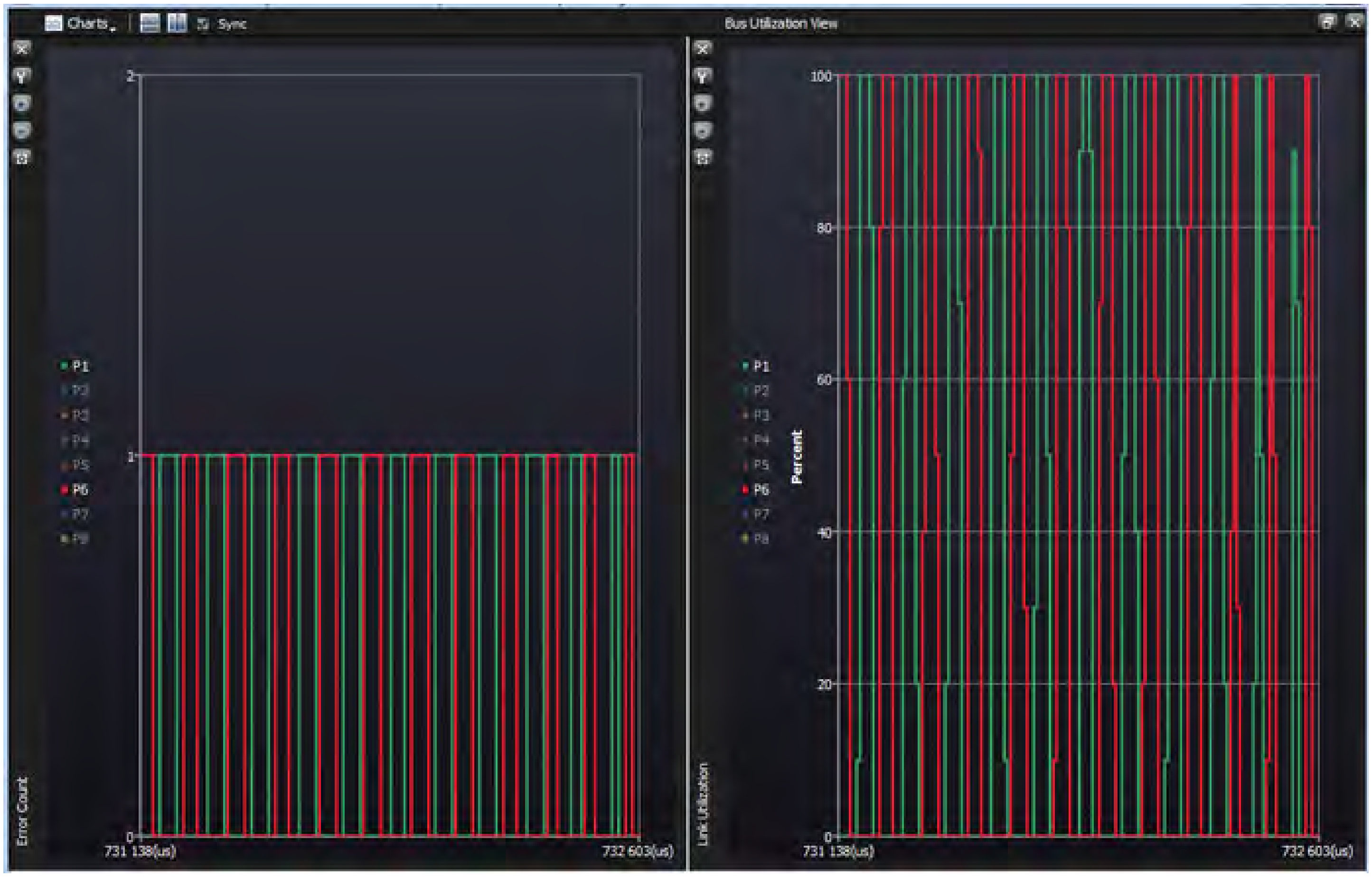


Figure 5.94: Bus Utilization Windows – Tiled Horizontally

5.2.6.3 Adjust Settings

You can Adjust Settings of the Display window. In this case the background color is Blue and the Port Numbers are listed below the Display. See Figure 5.95.

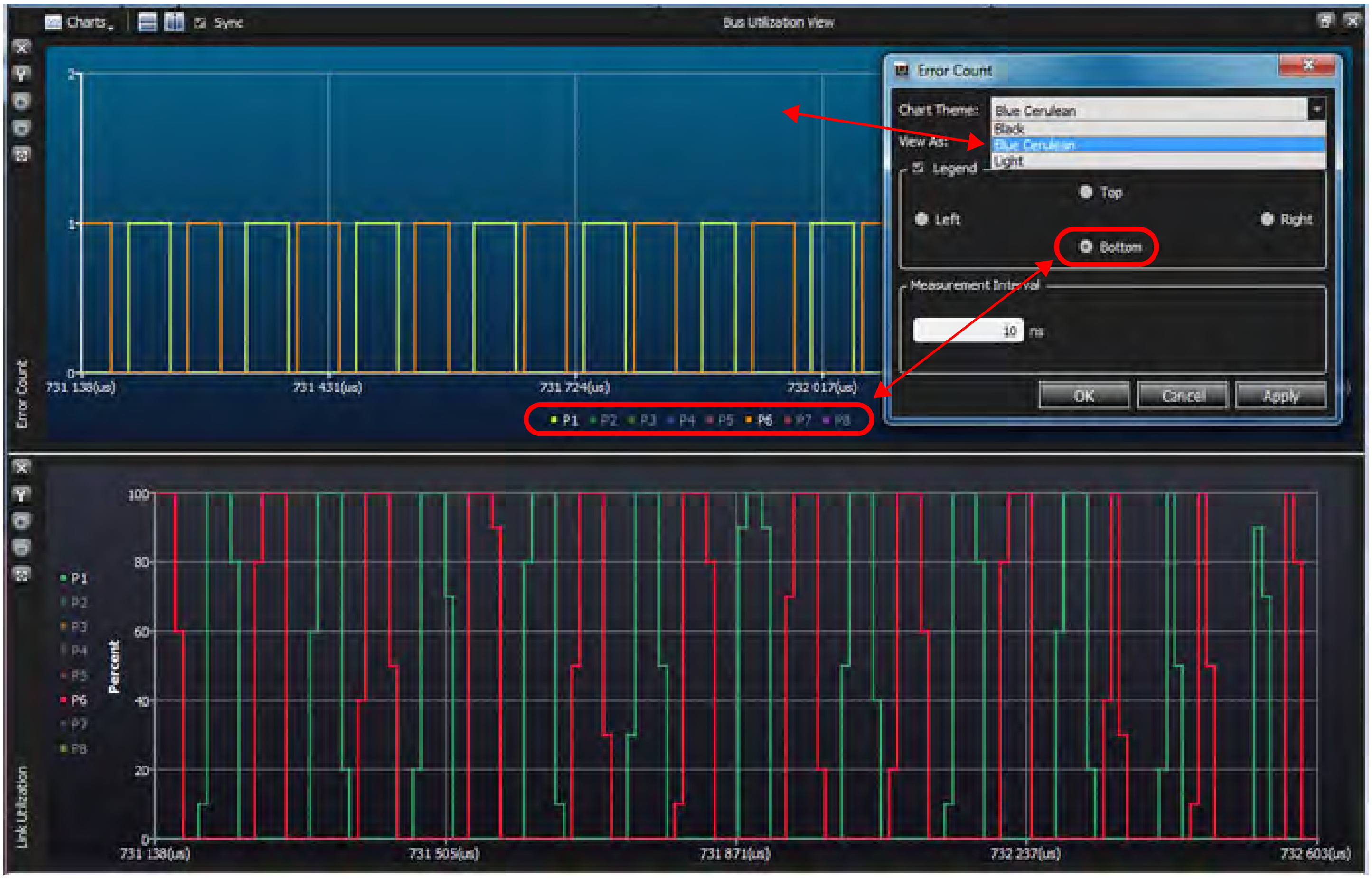


Figure 5.95: Adjust Settings – Error Count Display → Updated, Link Utilization → Defaults

You can also change from a line chart to an Area chart and change the Measurement Interval (Figure 5.96).

Figure 5.96: Adjust Settings – Link Utilization → Area Chart, Measurement Interval = 20 nsec

5.2.6.4 Rolling Cursor Over Point in Display

To find out information about a specific point in the display, roll your cursor over the point of interest and its value will be displayed (Figure 5.97).

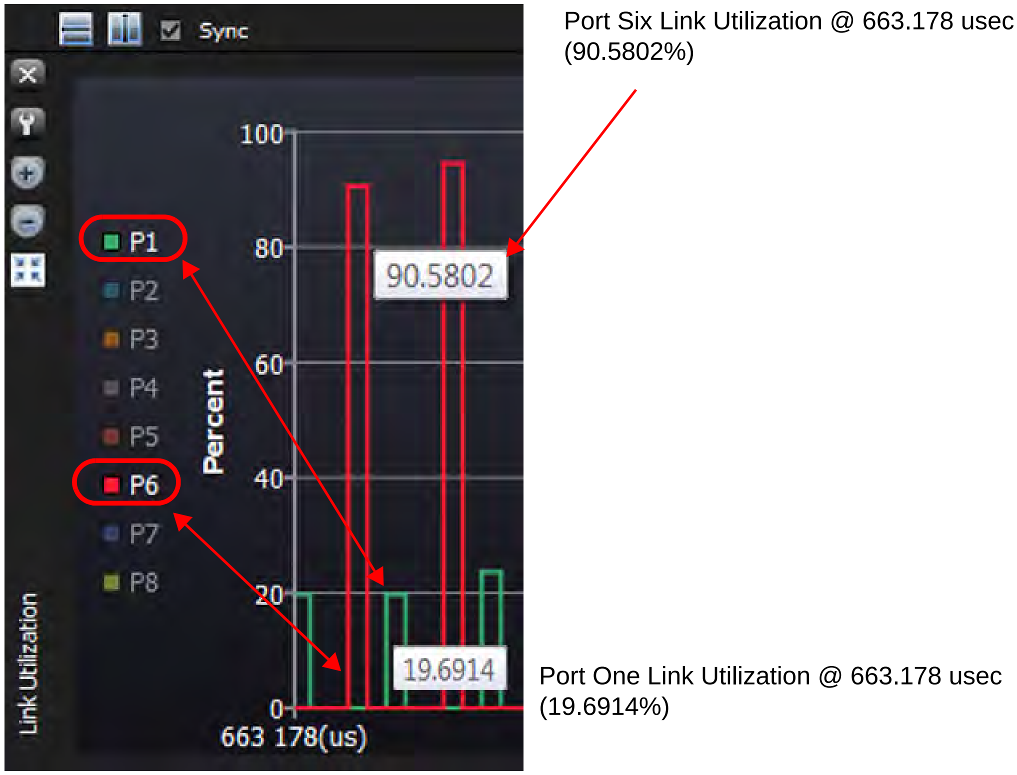


Figure 5.97: Rolling Cursor Over Specific Point on Waveform – Value Displayed

5.2.6.5 Zoom In Using Cursor

Another way to use the Zoom function is to move your cursor into the display panel, hold down the left mouse button and drag it over a section of the display. When you release the mouse the highlighted section will be displayed over the entire width of the display. See Figures 5.98, 5.99 and 5.100.

Figure 5.98: Data of Interest – Compressed, No Details

Figure 5.99: Cursor – Click and Drag over Area of Interest (710 usec to 713 usec)

Highlighted area only displayed in Figure 5.100.

Figure 5.100: Details from 710 usec to 713 usec Displayed

5.2.6.6 Display Bus Utilization and Spreadsheet Views

If you open the Spreadsheet View and the Bus Utilization View, clicking on an item in the Spreadsheet View will highlight that item in the Bus Utilization Charts. Initially, you'll see the entire Trace in the Bus Utilization View. See Figure 5.101.

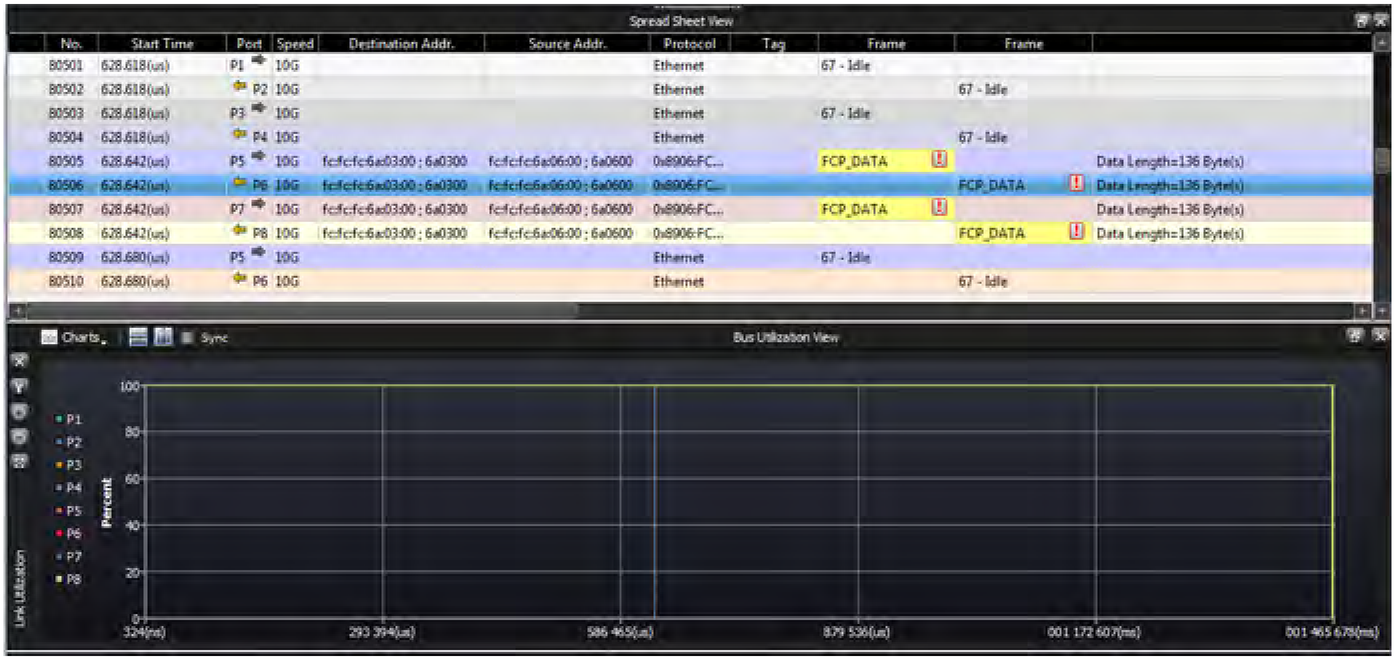


Figure 5.101: Bus Utilization and Spreadsheet Views – Near 628 usec

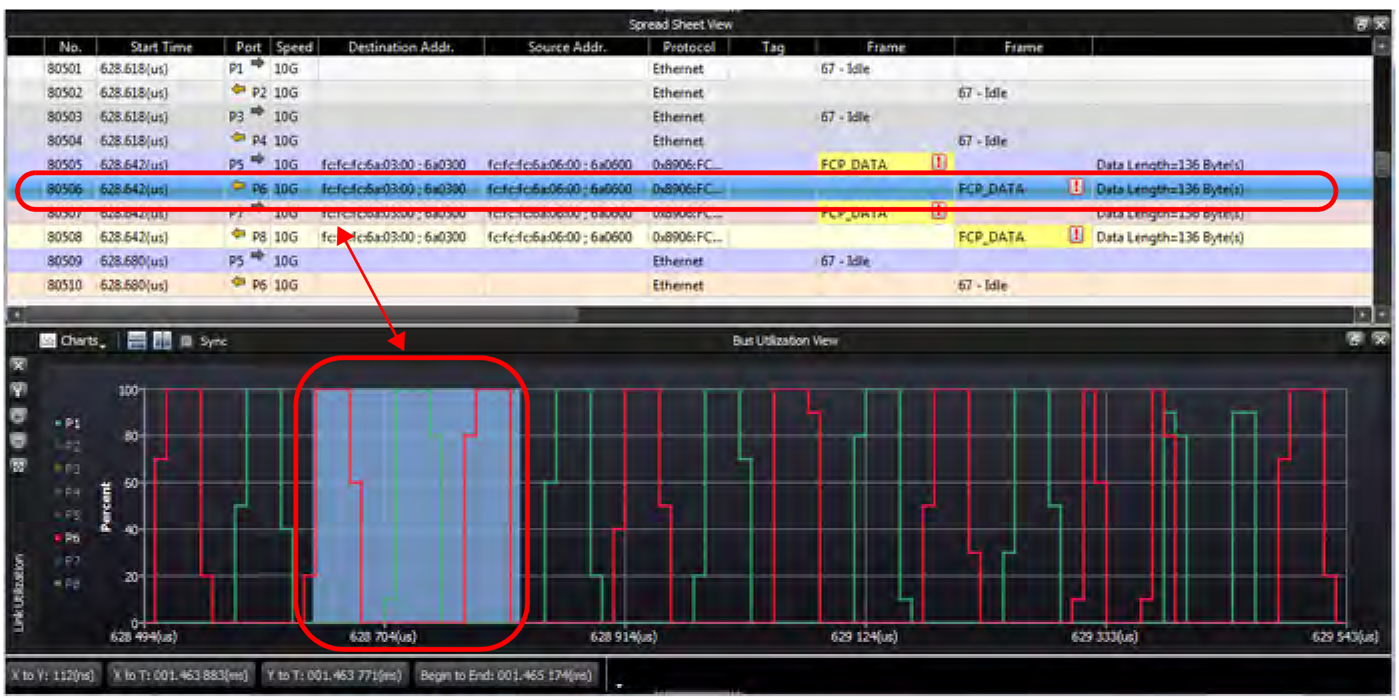


Figure 5.102: Bus Utilization (Zoomed In) and Spreadsheet Views – Near 628 usec

5.2.6.7 Quick Navigation

One other way that the Spreadsheet View and Bus Utilization View work together, is that if you have zoomed in enough to see individual events, you can click the left mouse button on an edge to view the Item Number(s) that contribute to the Utilization number in the graph. See Figure 5.103.

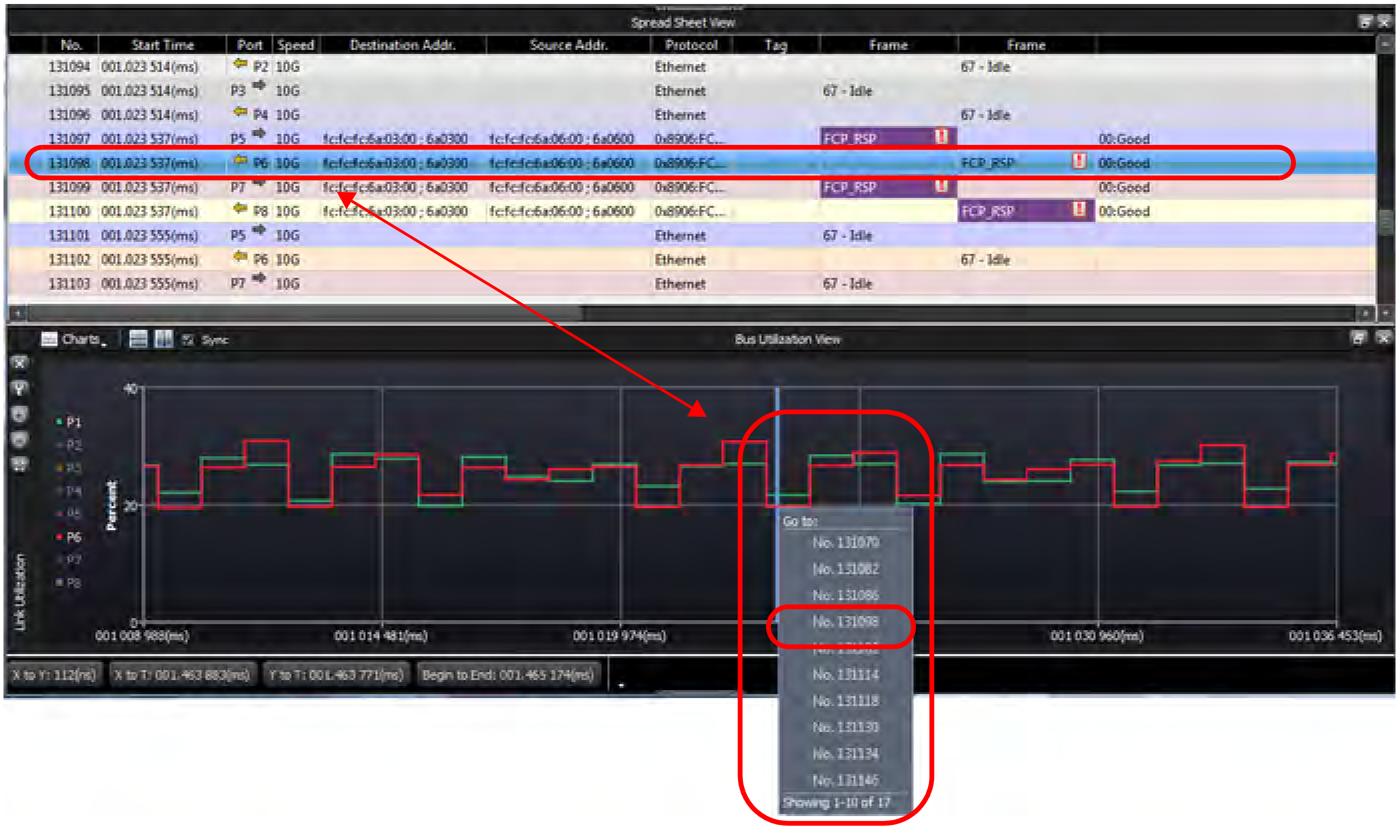


Figure 5.103: Spreadsheet and Link Utilization (Items Averaged)

5.2.7 Export to Wireshark

Clicking the  icon displays the Export to Wireshark dialog.

The Export to Wireshark dialog (Figure 5.104) has an option to choose between Ethernet and FC export. The option is only available if the trace contains both protocols. Only the chosen protocol frames will be exported. To get both types exported the user will have to do the export twice, choosing a different protocol each time.

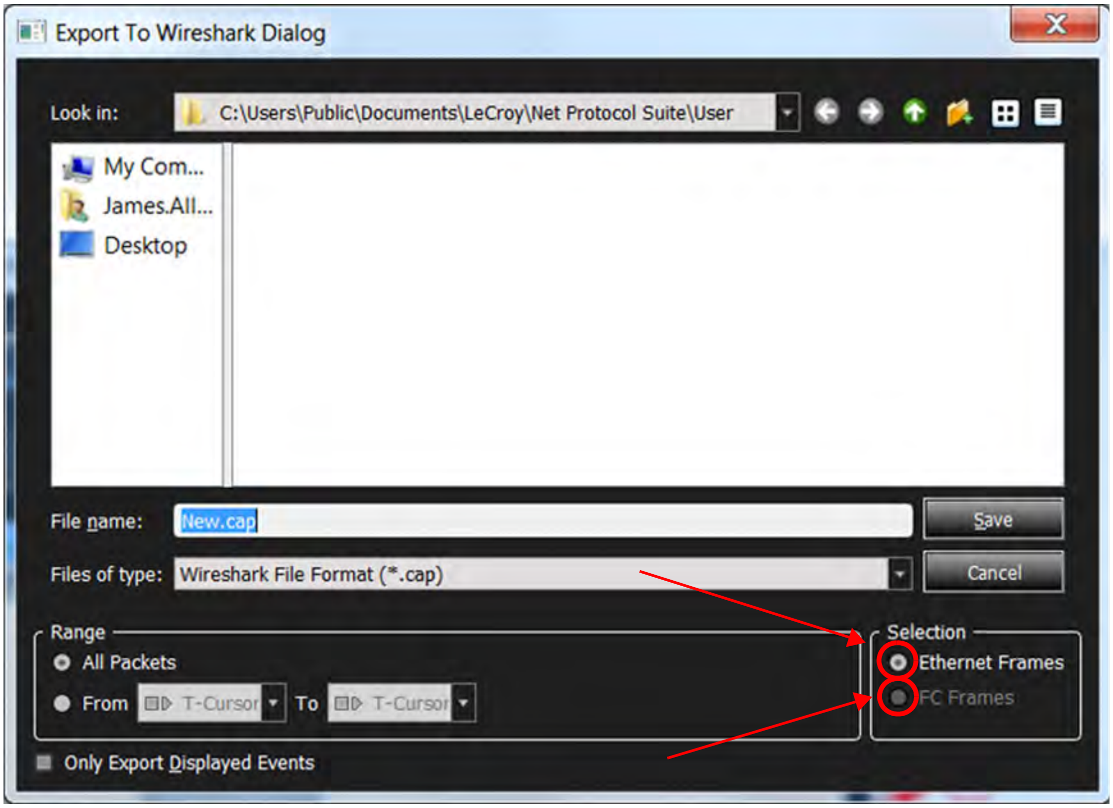


Figure 5.104: Export to Wireshark

5.2.8 Trace Expert

Trace Expert generates the following reports and analysis for the currently loaded trace:

- Performance Analysis
- Error Reports
- Trace Analysis Statistics
- Trace Information

1. To use Trace Expert, load a saved Trace you want to examine.

   In this example, “iSCSI-FC.get” has been loaded. This trace is used as an example and may not be suitable for all analyzers, but the basic steps are the same for any analyzer.

2. Click the Trace Expert icon from the Main Toolbar (Figure 5.105).

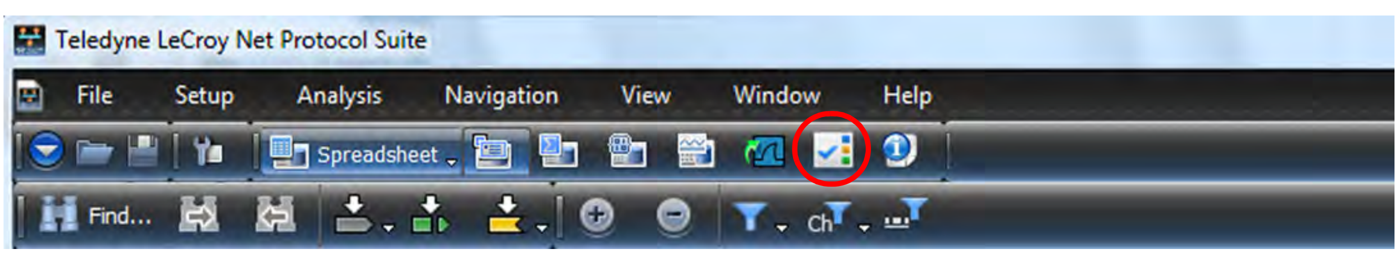


Figure 5.105: Main Toolbar – Trace Expert Icon

The Trace Expert main window appears in your default web browser (Figure 5.106). It contains buttons for **Expand All**, **Collapse All**, and **Print All**. The main window also contains four topics (bottom of screen).

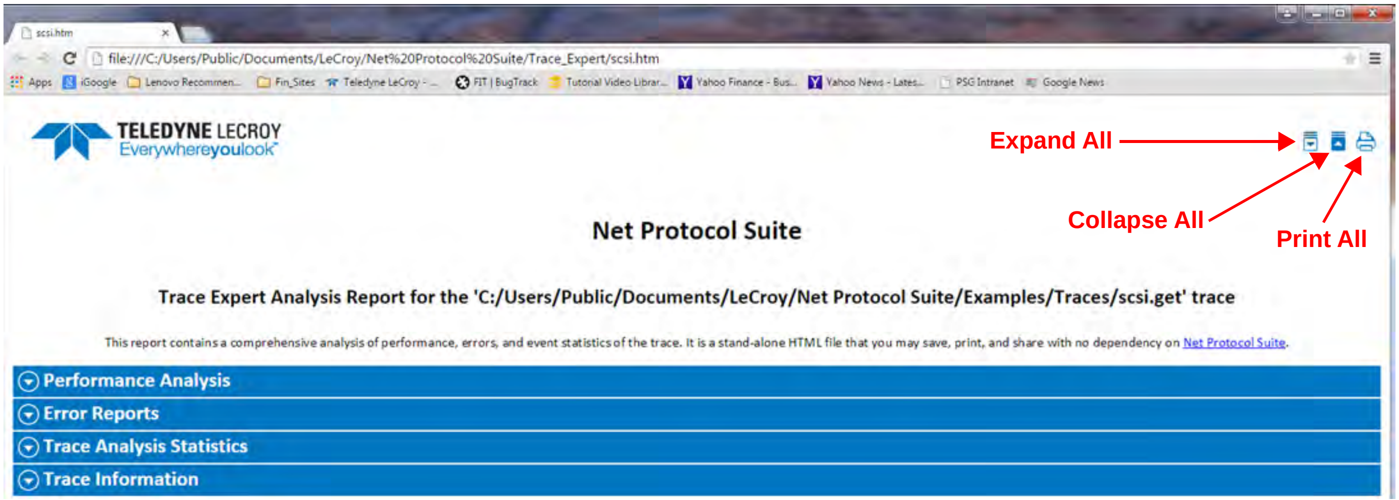
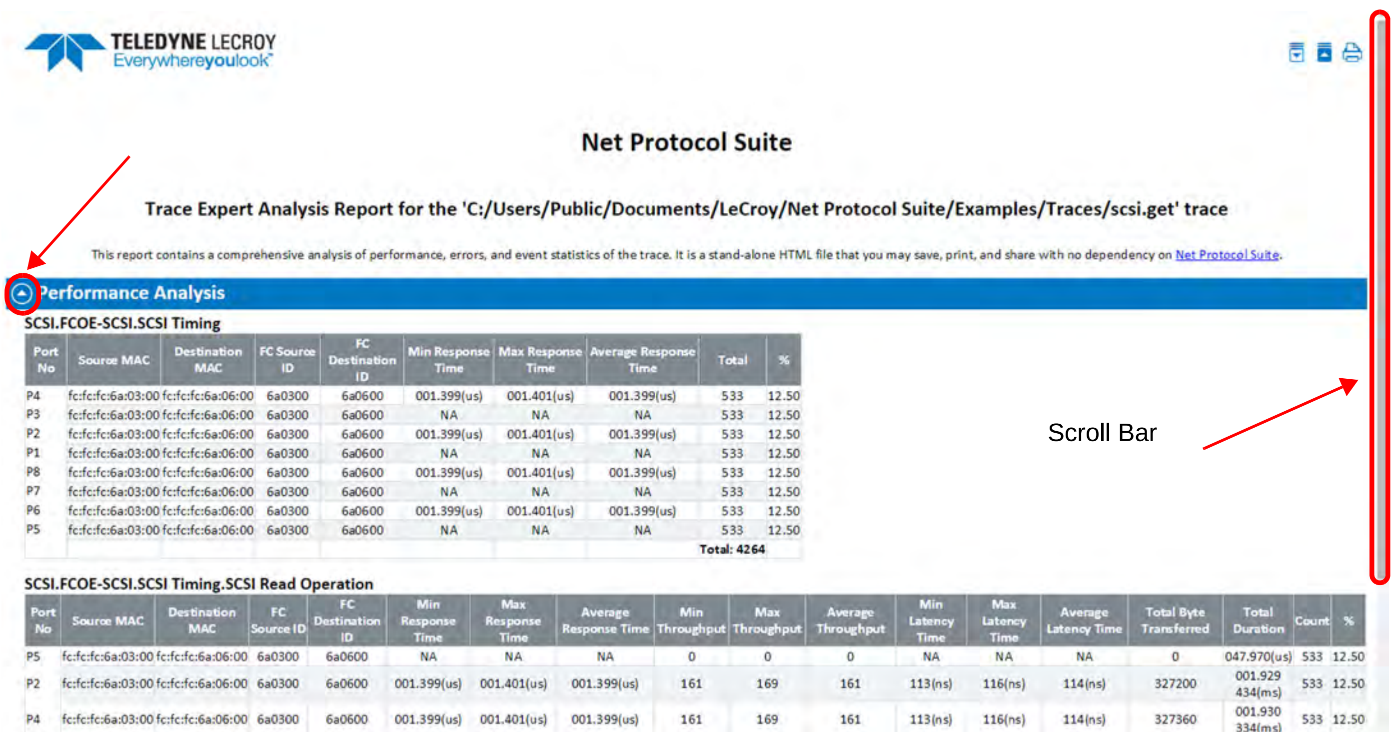


Figure 5.106: Trace Expert Main Report Window

3. Select any of the four topics to display its information.

5.2.8.1 Performance Analysis

1. To view Performance Analysis, click its expansion icon (Figure 5.107).



SCSI.FCOE-SCSI.SCSI Timing

Port No	Source MAC	Destination MAC	FC Source ID	FC Destination ID	Min Response Time	Max Response Time	Average Response Time	Total	%
P4	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	533	12.50
P3	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	NA	NA	NA	533	12.50
P2	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	533	12.50
P1	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	NA	NA	NA	533	12.50
P8	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	533	12.50
P7	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	NA	NA	NA	533	12.50
P6	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	533	12.50
P5	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	NA	NA	NA	533	12.50
								Total: 4264	

SCSI.FCOE-SCSI.SCSI Timing.SCSI Read Operation

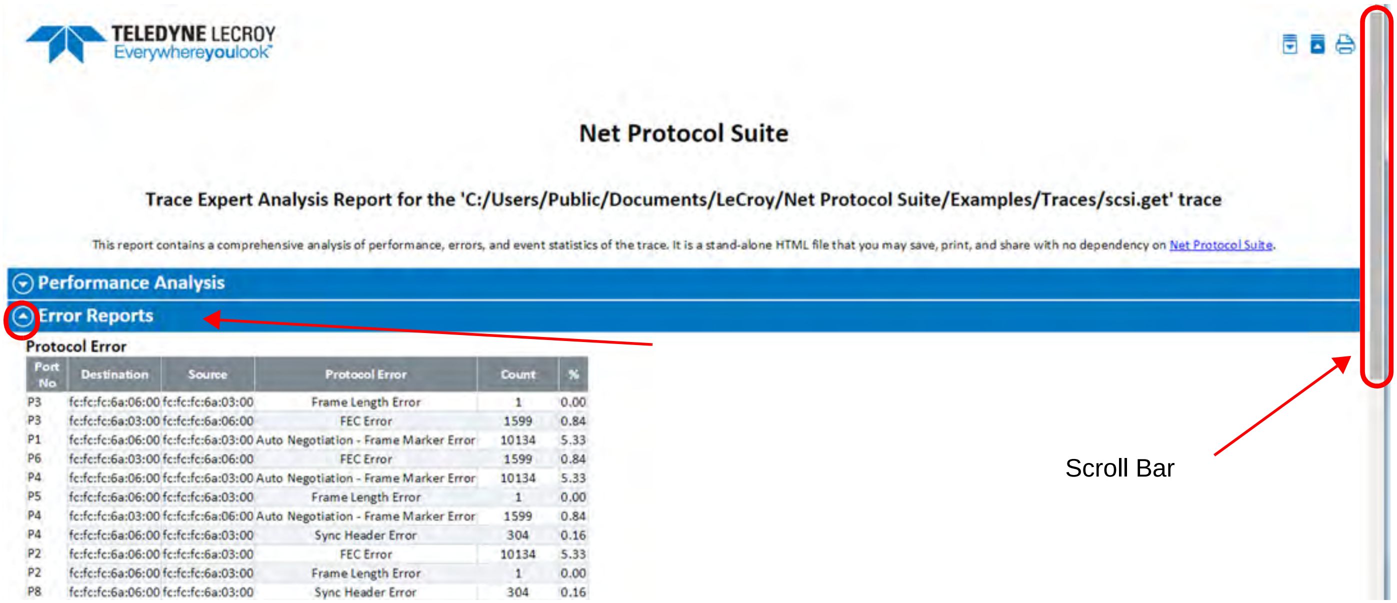
Port No	Source MAC	Destination MAC	FC Source ID	FC Destination ID	Min Response Time	Max Response Time	Average Response Time	Min Throughput	Max Throughput	Average Throughput	Min Latency Time	Max Latency Time	Average Latency Time	Total Byte Transferred	Total Duration	Count	%
P5	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	NA	NA	NA	0	0	0	NA	NA	NA	0	047.970(us)	533	12.50
P2	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	161	169	161	113(ns)	116(ns)	114(ns)	327200	001.929 434(ms)	533	12.50
P4	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	6a0300	6a0600	001.399(us)	001.401(us)	001.399(us)	161	169	161	113(ns)	116(ns)	114(ns)	327360	001.930 334(ms)	533	12.50

Figure 5.107: Trace Expert – Performance Analysis

2. Use the scroll bar to see more data.

5.2.8.2 Error Reports

1. To view the Error Report, click its expansion icon (Figure 5.108).



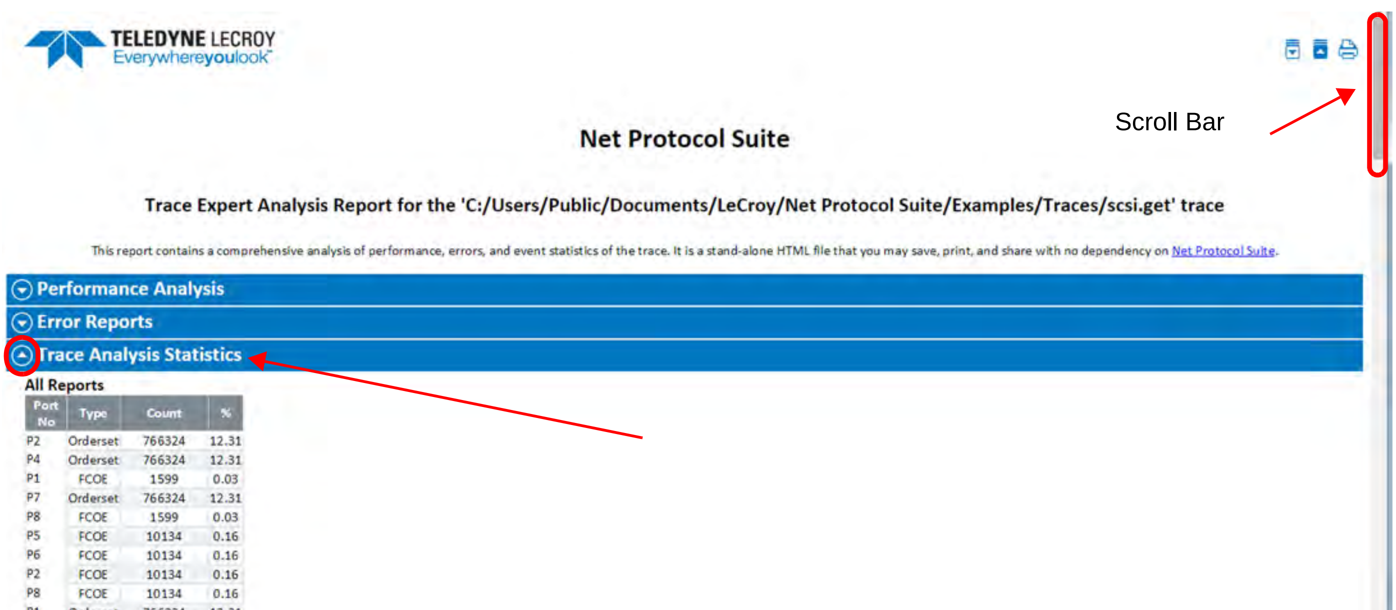
Port No	Destination	Source	Protocol Error	Count	%
P3	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Frame Length Error	1	0.00
P3	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FEC Error	1599	0.84
P1	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Auto Negotiation - Frame Marker Error	10134	5.33
P6	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FEC Error	1599	0.84
P4	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Auto Negotiation - Frame Marker Error	10134	5.33
P5	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Frame Length Error	1	0.00
P4	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	Auto Negotiation - Frame Marker Error	1599	0.84
P4	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Sync Header Error	304	0.16
P2	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FEC Error	10134	5.33
P2	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Frame Length Error	1	0.00
P8	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	Sync Header Error	304	0.16

Figure 5.108: Example Error Reports

2. Use the scroll bar to see more data.

5.2.8.3 Trace Analysis Statistics

1. To view the Trace Analysis Statistics, click its expansion icon (Figure 5.109).



Port No	Type	Count	%
P2	Orderset	766324	12.31
P4	Orderset	766324	12.31
P1	FCOE	1599	0.03
P7	Orderset	766324	12.31
P8	FCOE	1599	0.03
P5	FCOE	10134	0.16
P6	FCOE	10134	0.16
P2	FCOE	10134	0.16
P8	FCOE	10134	0.16
P1	Orderset	766324	12.31

Figure 5.109: Example Trace Analysis Statistics

2. Use the scroll bar to see more data.

5.2.8.4 Trace File Information

To view the Trace File Information, click its expansion icon (Figure 5.110).

The Trace Expert html file is located at:
C:/Users/Public/Documents/LeCroy/Net%20Protocol%20Suite/User/scsi_tmp.htm

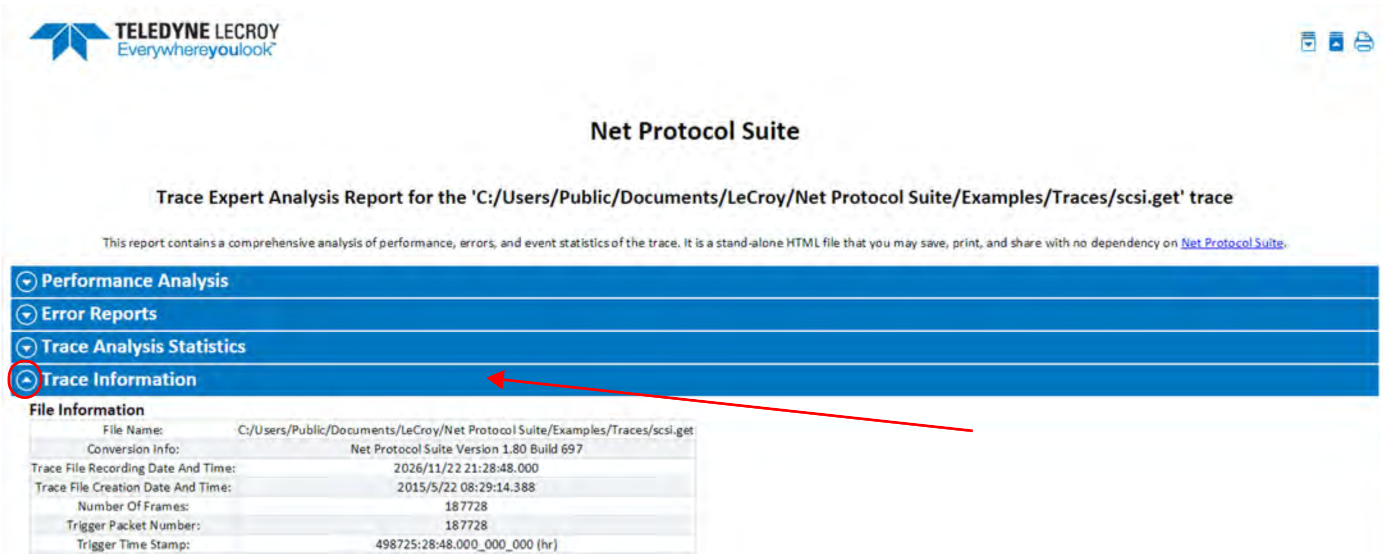


Figure 5.110: Trace Expert – Trace File Information

5.2.9 Trace Information

Click on **Analysis** and select **Trace Information** or click the icon to display the trace Information dialog (see Figures 5.111 and 5.112). You can click on the hyperlinks: **File info**, **Hardware info**, **Project info** or **License info** to navigate to that section. Click **Open Trace Project** to open the project in which the trace was captured.

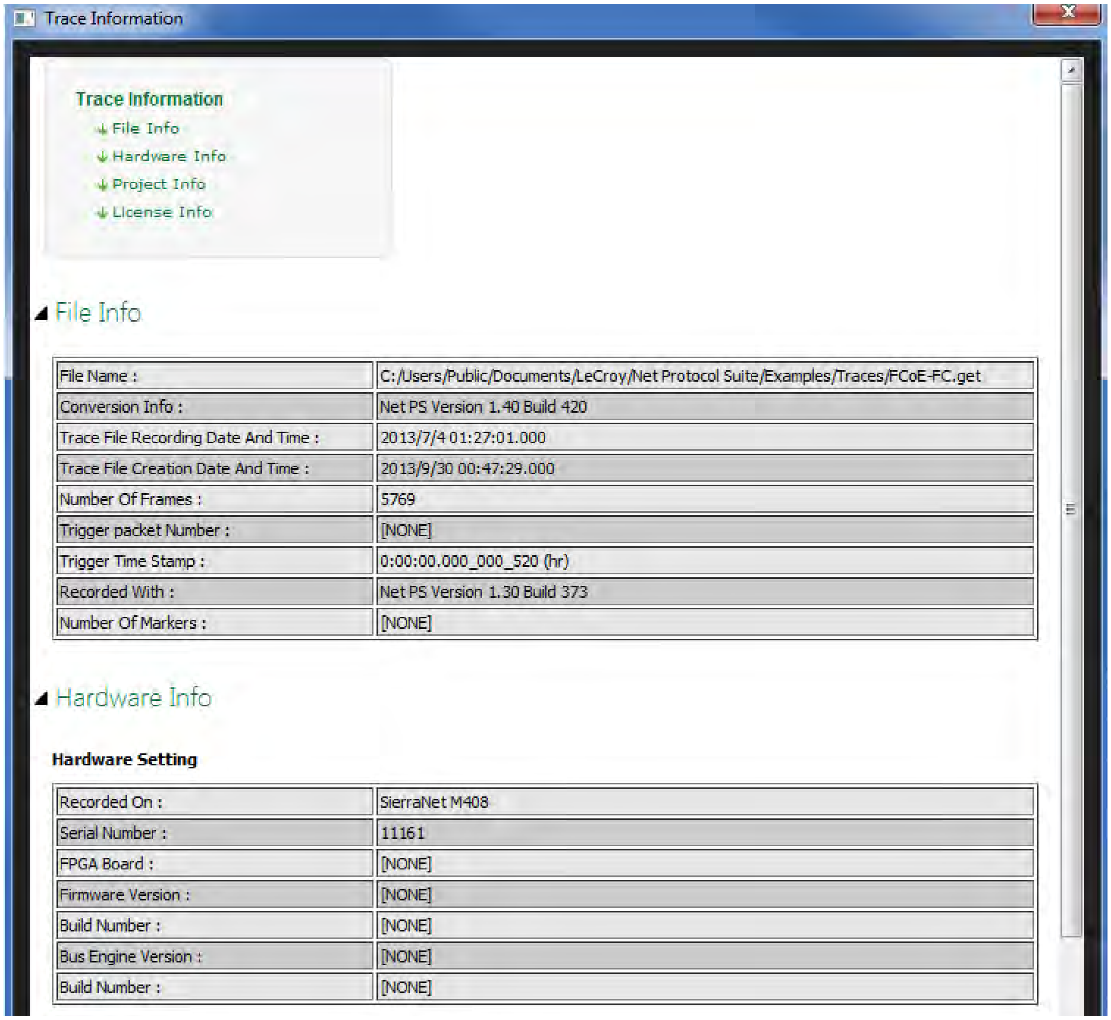


Figure 5.111: Trace Information Window 1

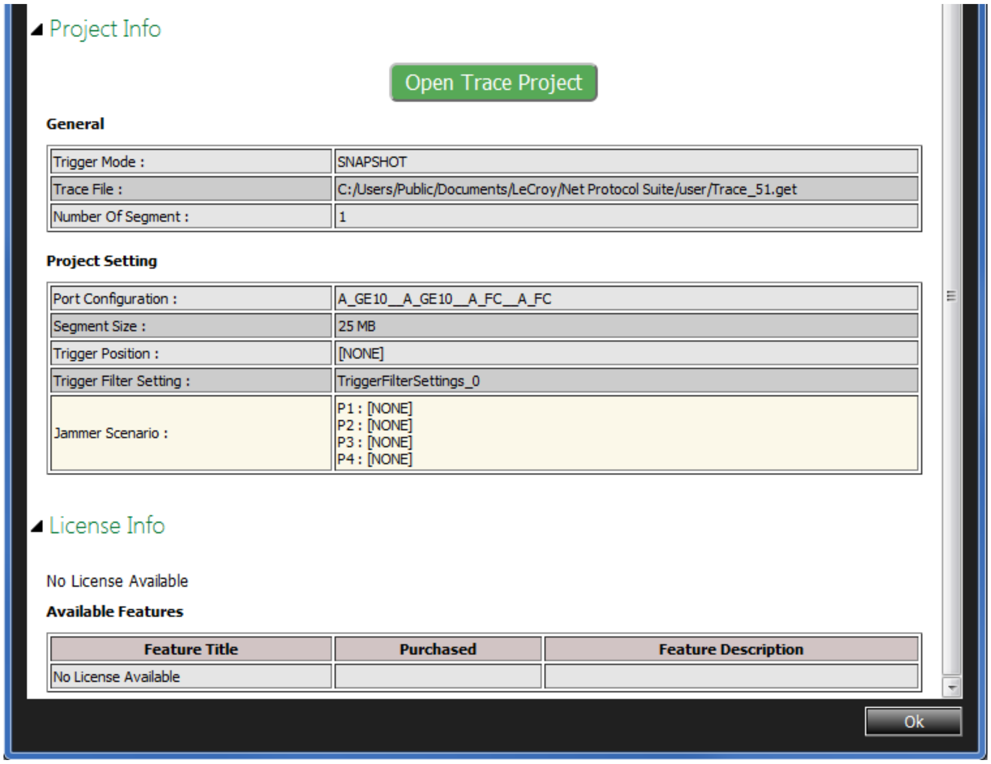


Figure 5.112: Trace Information Window 2

5.3 Verification Script Engine (VSE)

The Verification Script Engine allows you to select from available Traces and execute verification Scripts on them. See the Net Protocol Suite Verification Scripting Engine (VSE) API Reference Manual for additional information. (Click **Help** → **Help** Topics in the application main toolbar.)

1. To access the Verification Script Engine, select **Analysis** from the Main Menu. The Analysis drop-down menu appears (Figure 5.113).

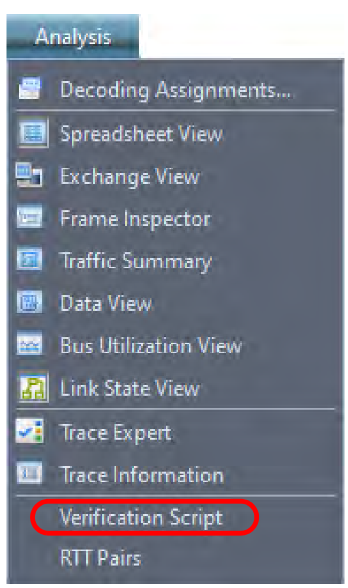


Figure 5.113: Analysis Drop-Down Menu

2. Select **Verification Script**. The Verification Scripts main window displays (Figure 5.114).

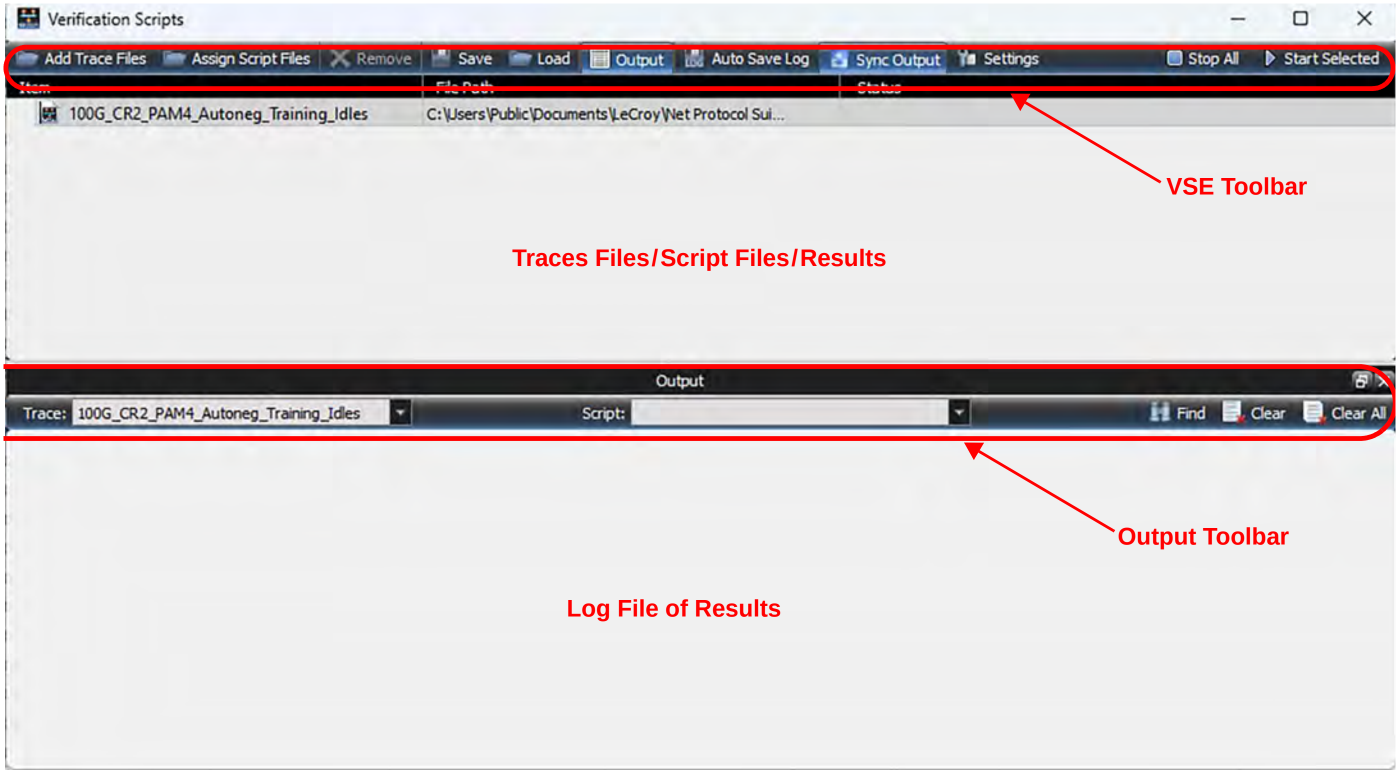


Figure 5.114: Verification Script Engine – Main Menu

5.3.1 Verification Scripts Main Window

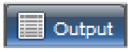
5.3.1.1 Verification Scripts Toolbar

You can use the traces and scripts that ship with the software or take your own traces and write your own scripts:

TABLE 5.3: Verification Scripts Toolbar

Button/Icon	Description
	**Add Trace Files**: Select Examples from C:\Users\Public\Documents\LeCroy\Net Protocol Suite\Examples\Traces
	**Assign Script Files**: Select from example scripts in C:\Users\Public\Documents\LeCroy\Net Protocol Suite\Examples\VSE
	**Remove**: Allows you to selectively remove traces or scripts
	**Save**: Allows you to Save a set of Scripts and Traces
	**Load**: Allows you to Load a set of Scripts and Traces

TABLE 5.3: Verification Scripts Toolbar

Button/Icon	Description
	**Output**: Show or Hide Output Log file
	**Auto Save Log**: Enable/Disable Auto Save Log
	**Settings**: Change VSE Settings. Use this to change the Display, designate Save settings, and enter the path to a preferred editor.
	**Stop All**: Stop all Scripts in progress
	**Start Selected**: Start all Selected Scripts

5.3.1.2 Output Pane Toolbar

The Output Pane shows the results of running each script, with any messages and descriptions that are included in the script. See Figure 5.115 and Table 5.4.

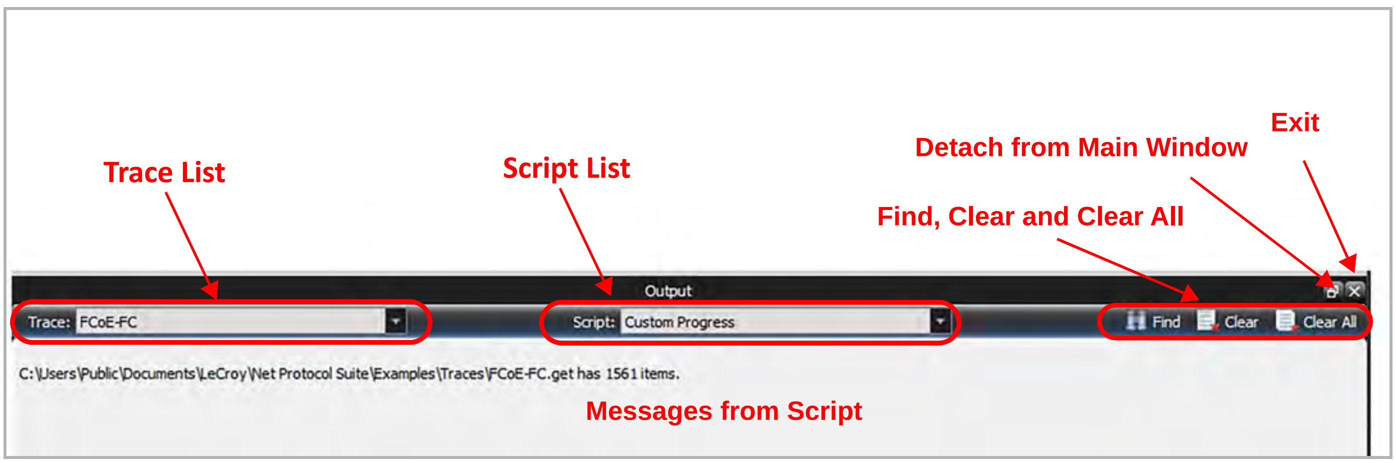


Figure 5.115: Output Pane

TABLE 5.4: Output Pane Toolbar

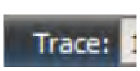
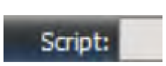
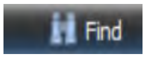
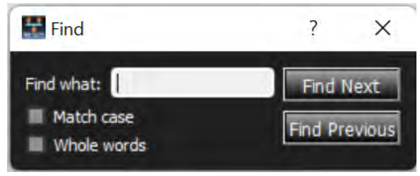
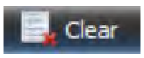
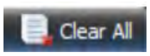
Button/Icon	Description
	**Trace**: Displays a list of the output of the traces attached to the selected scripts. You can scroll thought the list. See Figure 5.126 in section 5.3.10 *Verification Engine Completed*.
	**Script**: Displays a list of the selected scripts and their output. You can scroll thought the list. See Figure 5.126 in section 5.3.10 *Verification Engine Completed*.

TABLE 5.4: Output Pane Toolbar

Button/Icon	Description
	**Find**: Allows you to search through Trace and Script Output. 
	**Clear**: Clears the selected output.
	**Clear All**: Clears all output.

5.3.2 Setting up the Trace Analysis

The Verification Script Settings dialog window allows you to specify Display Settings, where and how to save the Log, and specify a preferred Script editor.

Click  to access the Verification Script Settings window (Figure 5.116).

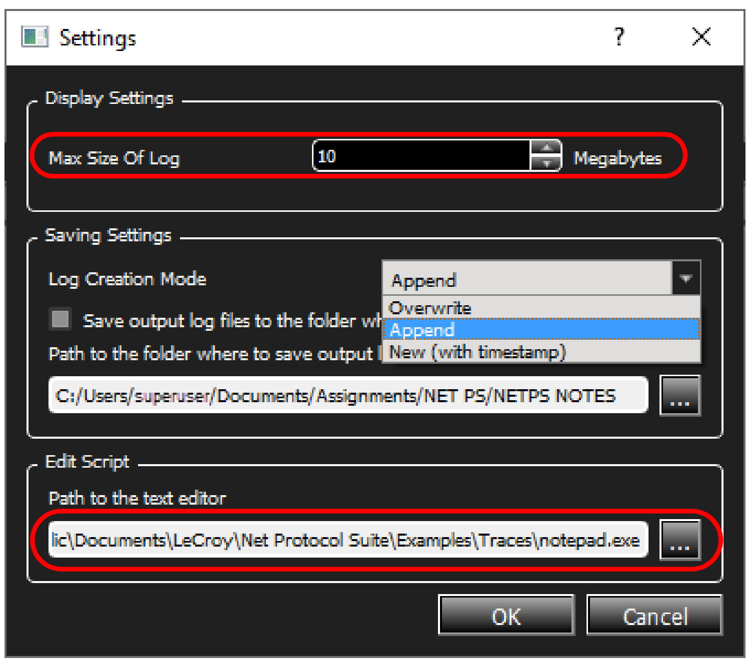


Figure 5.116: Verification Script Settings Dialog Window

- **Display Settings**. Use the up/down arrows to set the maximum size of the log file in megabytes.
- **Saving Settings**. You can set the following for the output file:
  - Log Creation Mode—You can choose whether to Append, Overwrite, or create a New (with timestamp) the output file.

- Select the Path to the folder where you wish to save the output files.

NOTE: You must enter a path to a valid directory.

- **Edit Script**. Use this to specify a preferred text editor. You can enter the path, or you can click ... and choose an editor from the drop-down list.

5.3.3 Loading Traces

To get started, you can choose any (or all) or the Example Traces that ship with the software (C:\Users\Public\Documents\LeCroy\Net Protocol Suite\Examples\Traces).

1. Click on **Add Trace Files** in the toolbar. A window containing Trace files appears (Figure 5.117). If you have already opened a Trace file(s), it will appear in the right pane.

NOTE: You can also drag Trace files directly from Windows Explorer to the VSE pane.

2. Select from one to all files.

   If you select all of the example traces, they will populate the middle column of the Verification Scripts window with the path to their location (Figure 5.118).

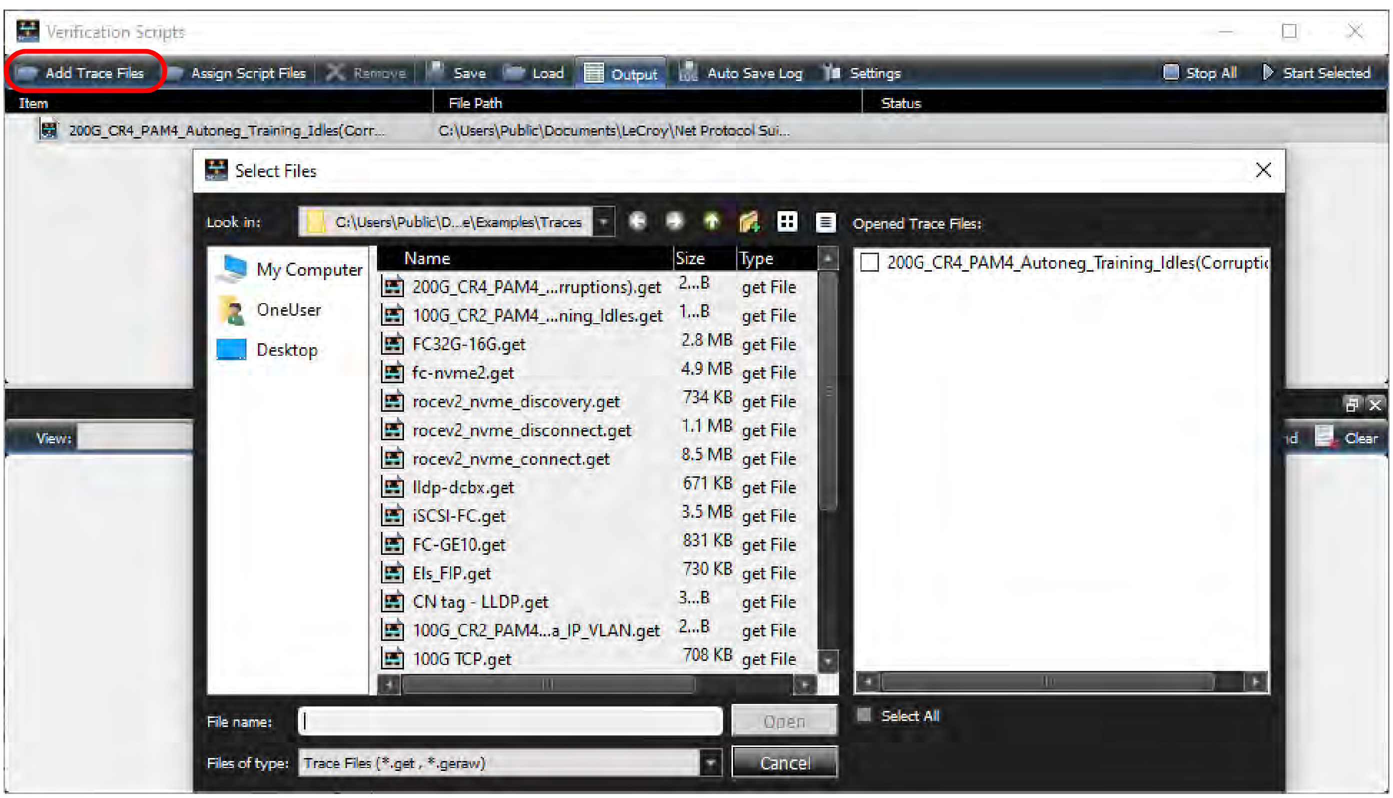


Figure 5.117: Example Traces

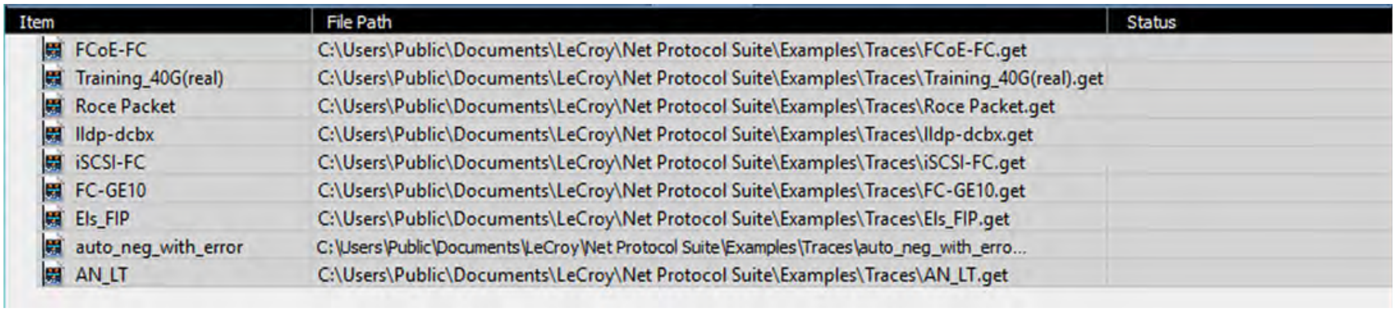


Figure 5.118: Example Traces Loaded into the Verification Engine

5.3.4 Loading Scripts

The next step is to load Test Scripts to run with the loaded Traces. A set of example Scripts, which ship with the software, is located in the C:\Users\Public\Documents\LeCroy\Net Protocol Suite\Examples\VSE folder. See Figure 5.119.

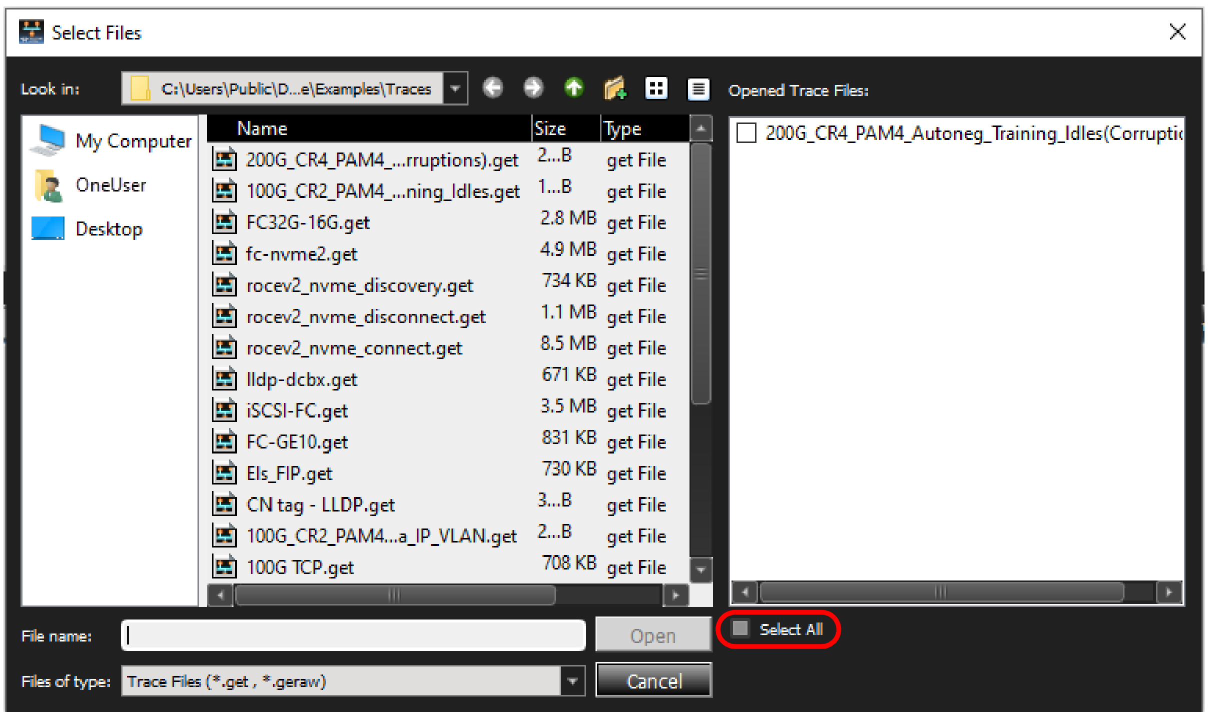


Figure 5.119: Example Scripts

1. Select a specific Script to be run on a specific Trace or check the box for **Select All**. If you choose Select All, the selected scripts will be run on all of the assigned traces. See Figure 5.120.

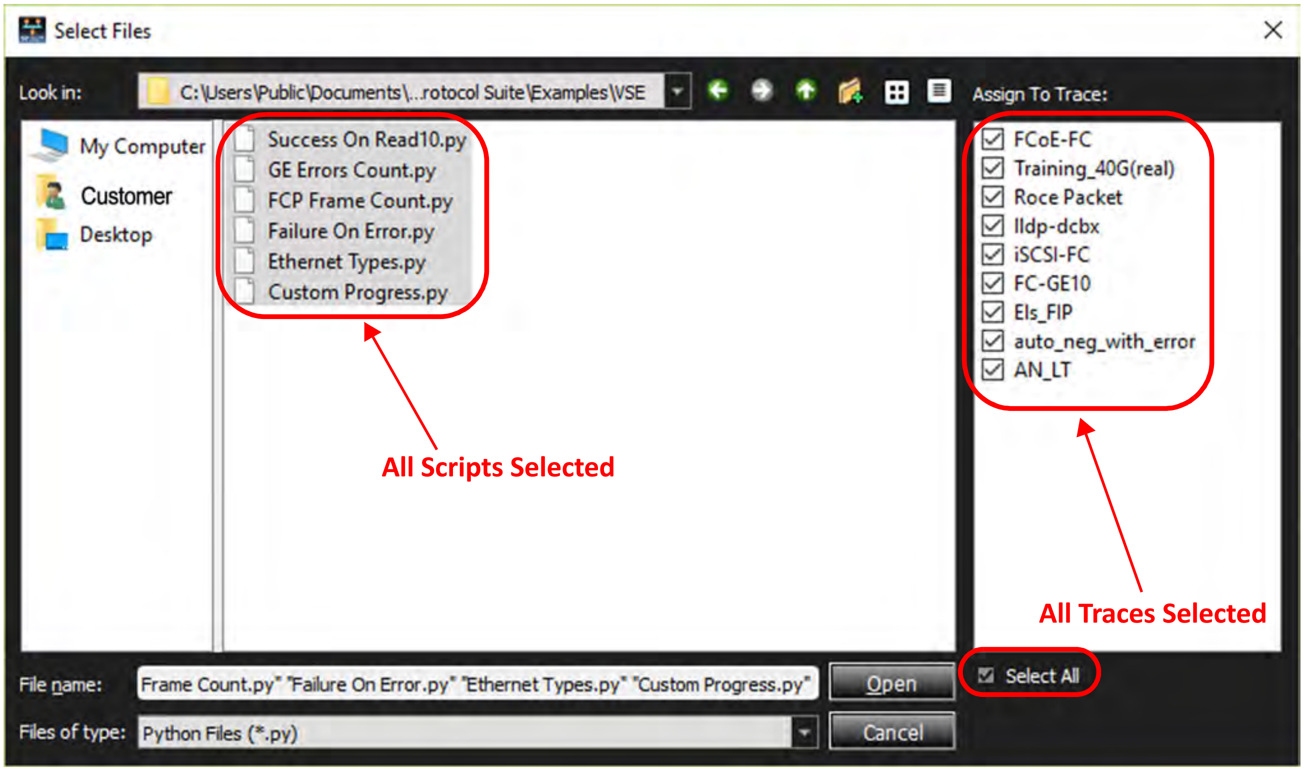


Figure 5.120: All Scripts Selected and All Traces Selected

2. Click on the **Open** button. The Main Verification Script Window is populated with the selected Traces and Scripts. The middle column (File Path) shows the path to either the Trace or the Script. Figure 5.121.

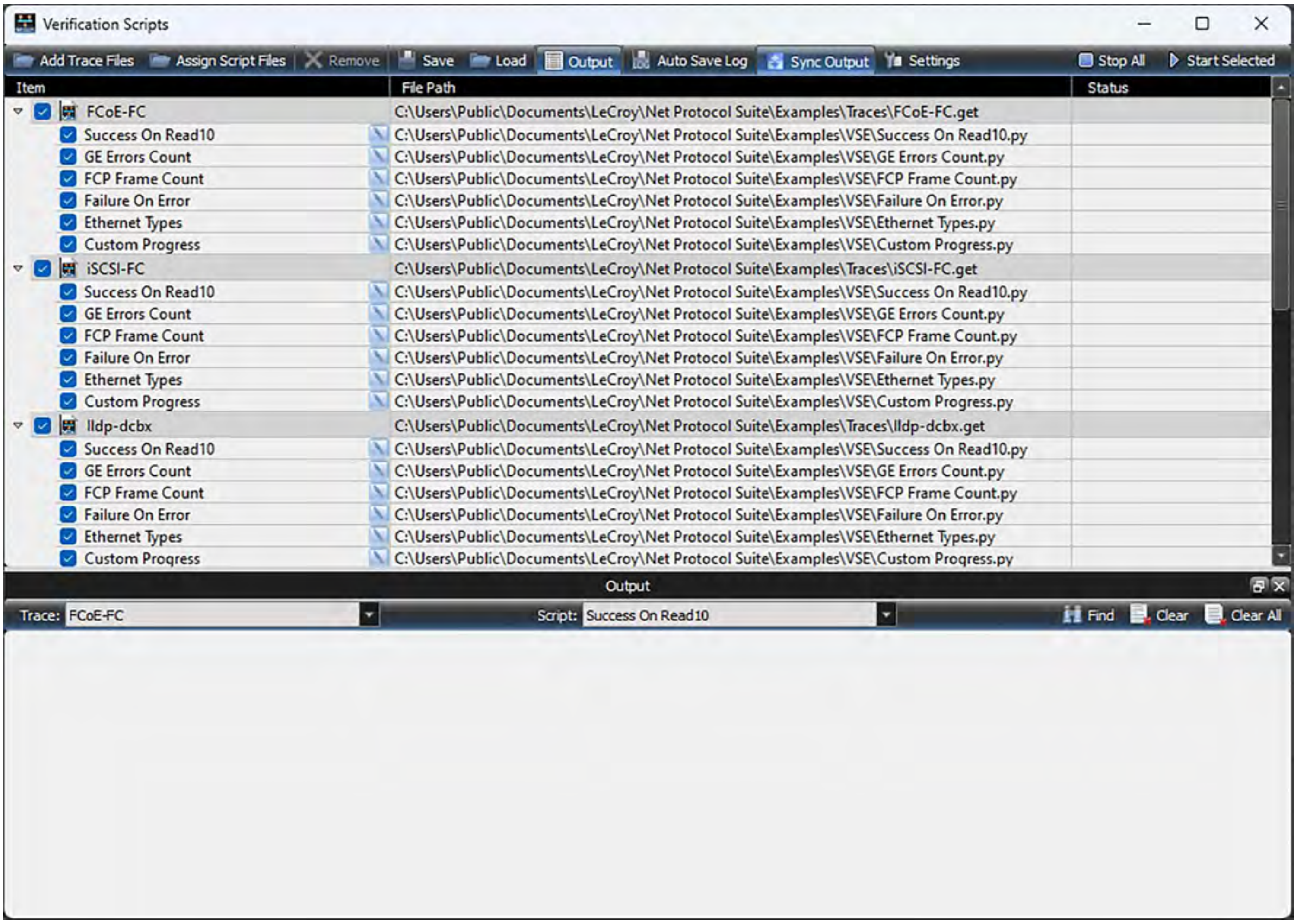


Figure 5.121: All Scripts Assigned to All Traces

5.3.5 Trace Context Menu

Hover the cursor over a Trace and perform a right-click. This brings up the Trace Context Menu. From the Context Menu you can:

- Remove Trace
- Assign Script
- Start the Script running on the Trace
- Stop the Script
- Open the Containing Folder
- Copy Full Path

See Figure 5.122.

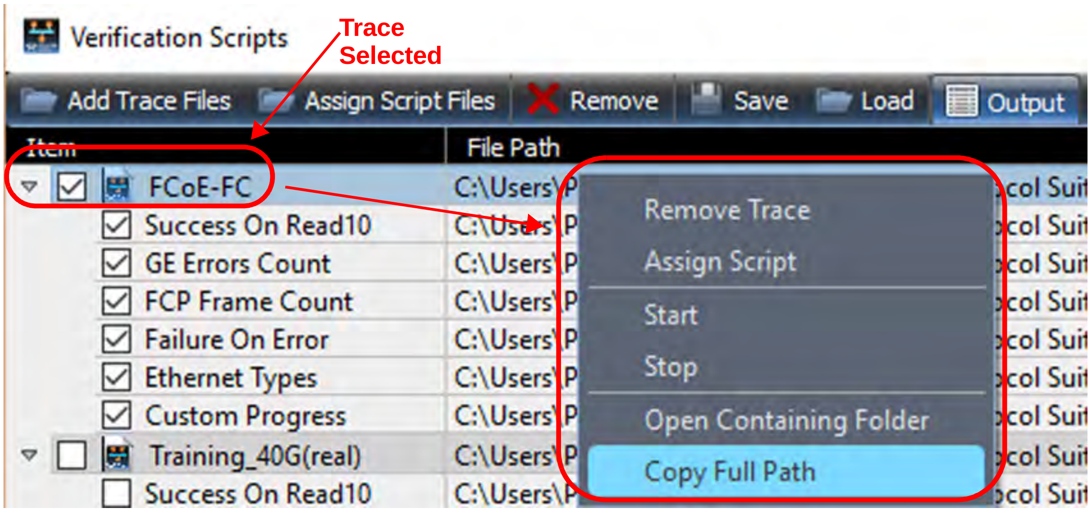


Figure 5.122: Trace Context Menu

5.3.6 Script Context Menu

Hover the cursor over a Script and perform a right-click. This brings up the Script Context Menu (Figure 5.123). From the Script Context Menu you can:

- Remove Script
- Show Log
- Start the Script running on the Trace
- Stop the Script
- Open the Containing Folder
- Copy the Full Path

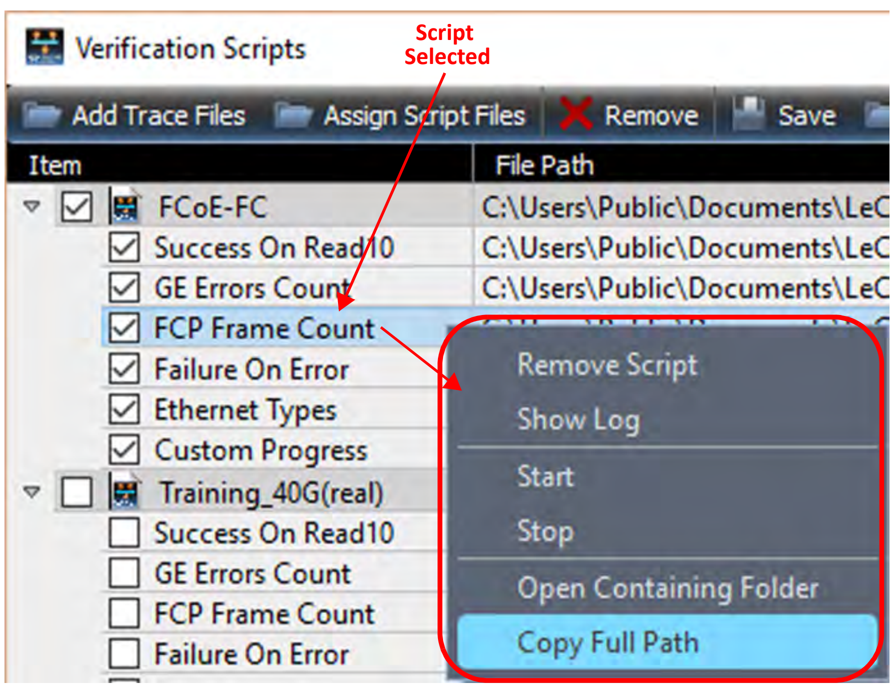


Figure 5.123: Script Context Menu

5.3.7 Status Pane

The Status pane shows the current status when the script has been started (Figure 5.124. The Status states are:

- Idle
- Enqueued
- Running
- Passed
- Failed

5.3.8 Start Selected

When the “Start Selected” button is clicked, all of the selected scripts will start running in parallel. For each Trace, the scripts attached to it will be run sequentially.

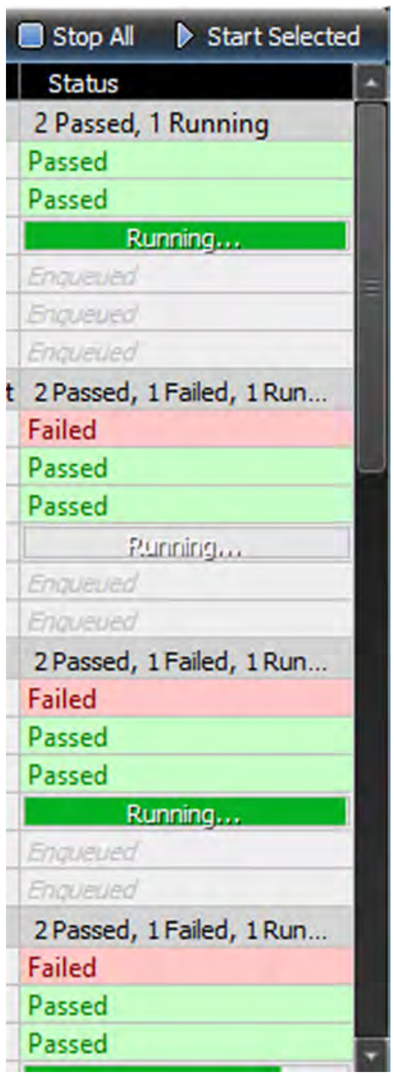


Figure 5.124: Status Pane – Several Scripts Running on Several Traces

5.3.9 Verification Engine In Process

In this case, all the scripts have been assigned to all the traces, so when you click on the "Start Selected" button you'll see the Output Window and the Status pane start to populate with results and Pass or Fail indications. See Figure 5.125.

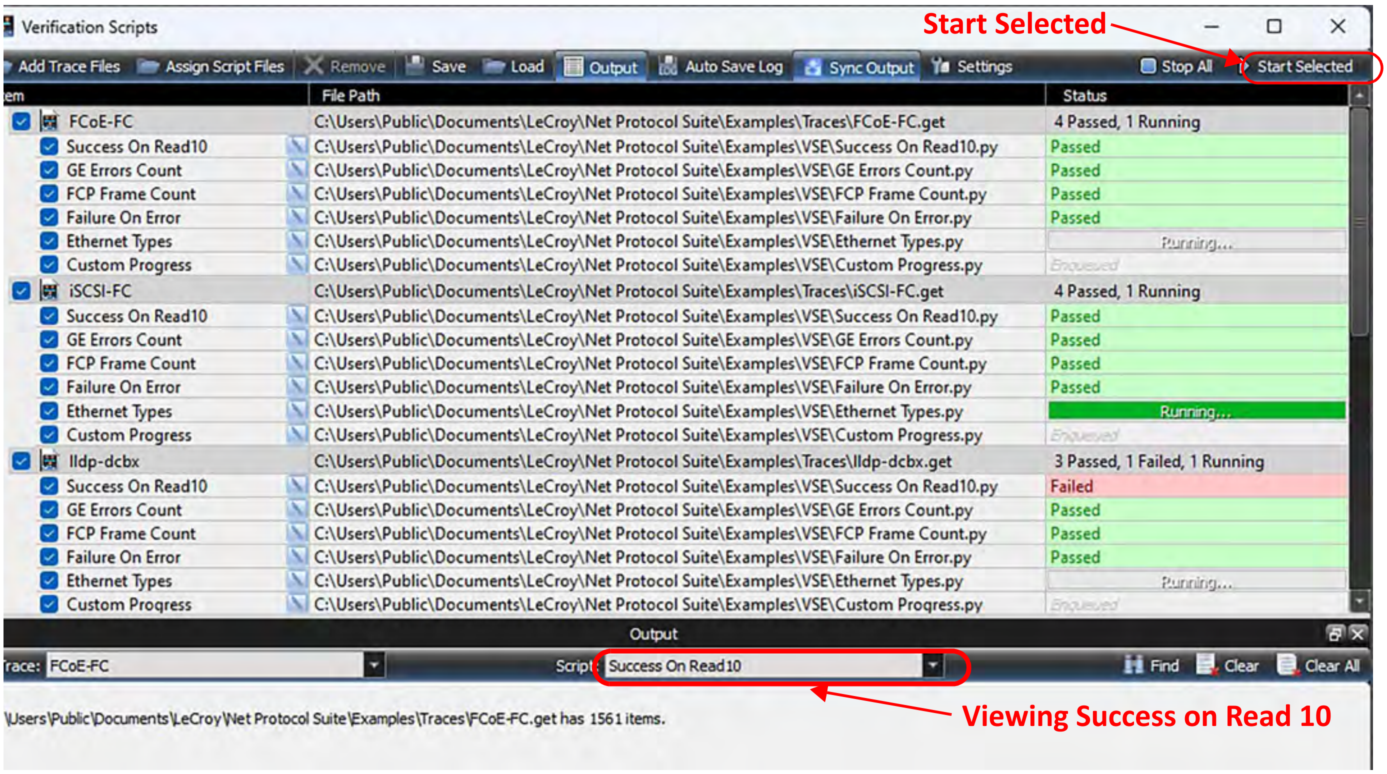


Figure 5.125: All Scripts Attached to All Traces in Process

5.3.10 Verification Engine Completed

If you wait for all the scripts to finish on all the traces, you can scroll through the Output from each Script attached to each Trace. See Figure 5.126.

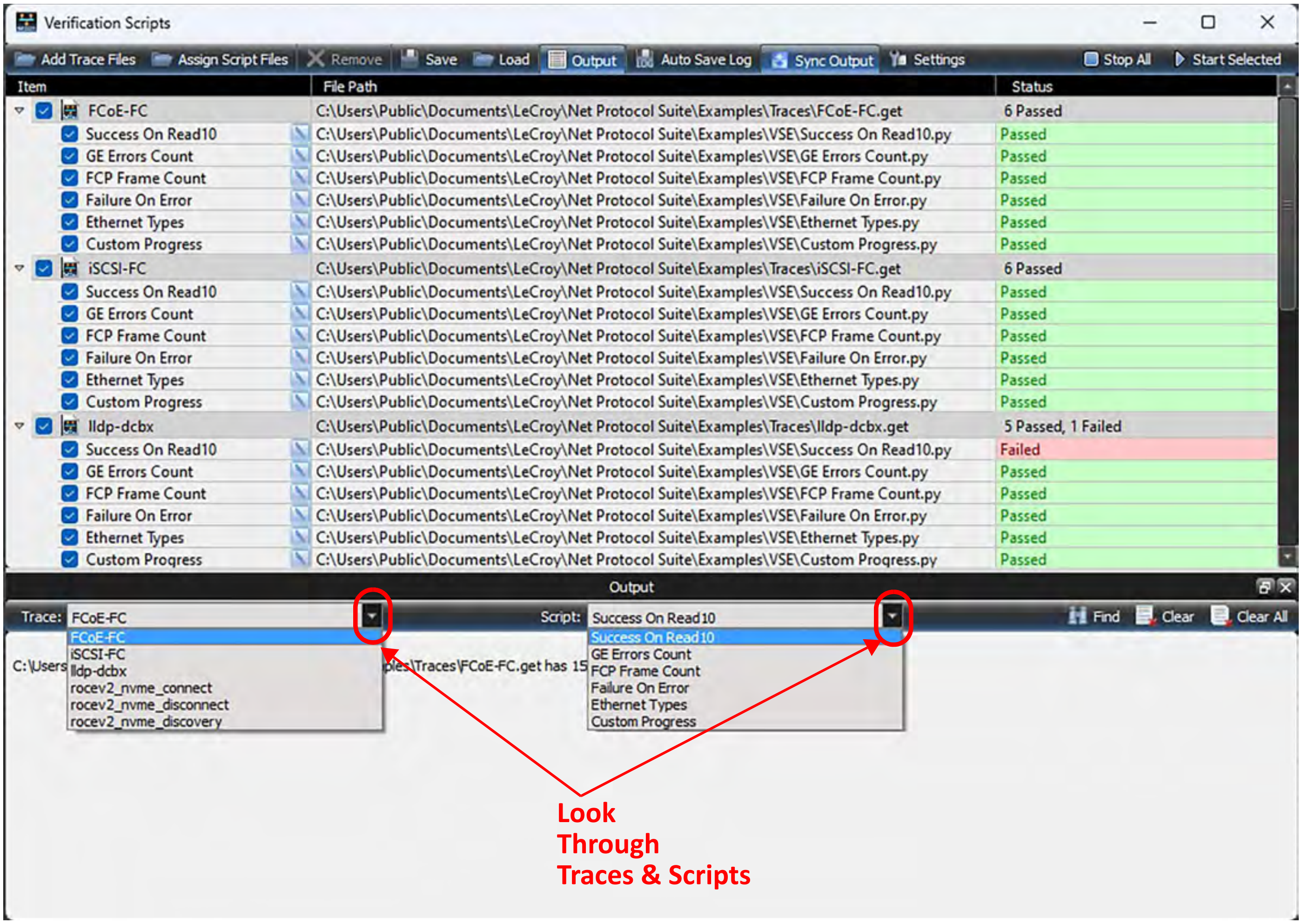


Figure 5.126: Results From Each Script After Running on Each Trace

5.4 Round Trip Time (RTT) Pairs

Round-trip time, also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

5.4.1 RTT for TCP

Net Protocol Suite tracks the RTT of each TCP segment, based on SeqNo and ACK, on a per-connection basis.

If you select RTT Pairs from the Analysis tab in the Main Toolbar, the following dialog will pop up showing a lot of activity on Ports 1 and 2. Select those port and click on **OK**. See Figure 5.127.

Figure 5.127: RTT Pairs: Dialog

If you open Traffic Summary View, you'll see Min RTT, Max RTT and Average RTT. See Figure 5.128.

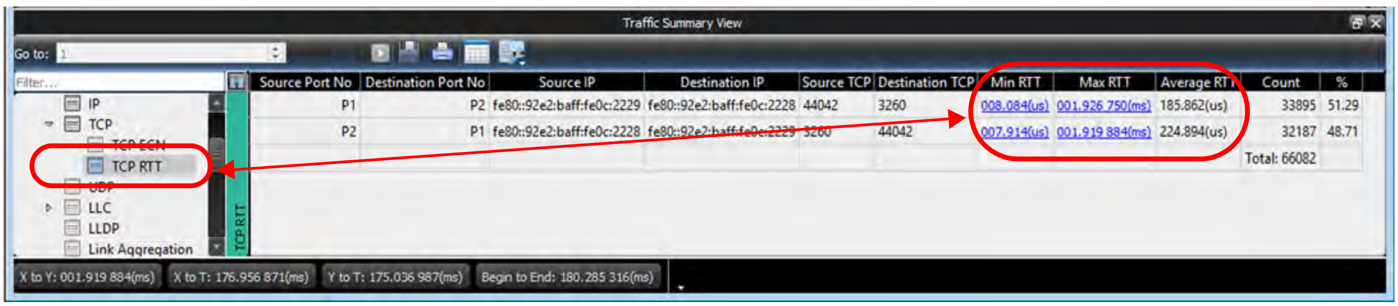


Figure 5.128: RRT Pairs – Traffic Summary View

You can also see more details of the RTT in the Bus Utilization View. See Figure 5.129.

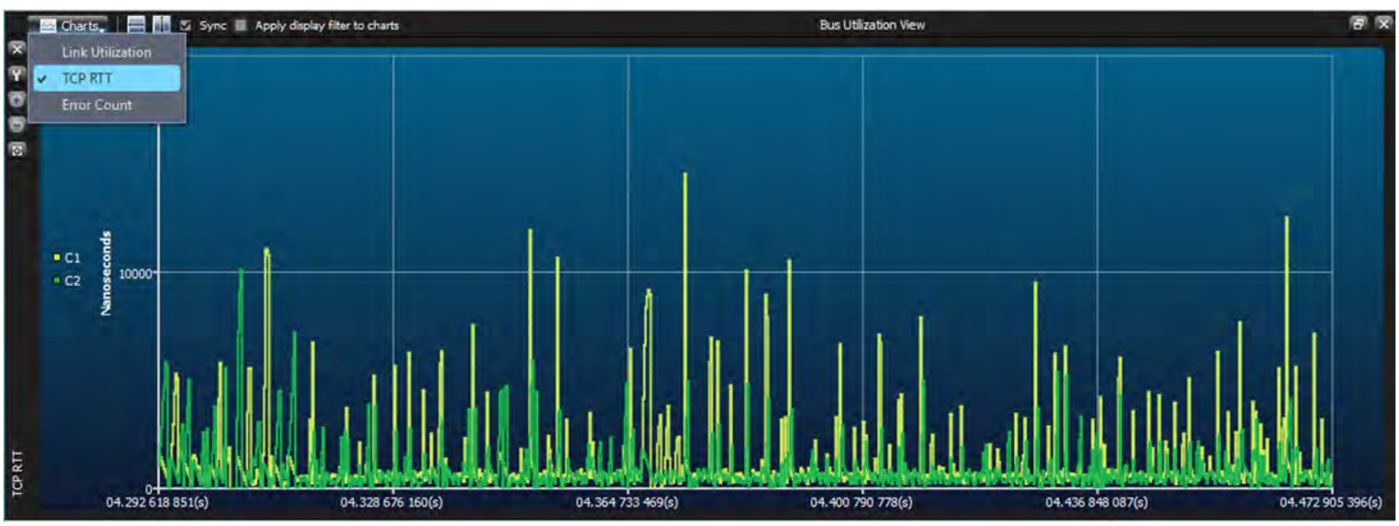


Figure 5.129: RTT Pairs – Bus Utilization View

You can zoom in to a transaction of interest to get more details. You can also scroll over the C1 and C2 labels to see timing from Port 1 and Port 2 and from Port 2 to Port 1.

Figure 5.130: RTT Pairs – Zoom in

5.4.2 RTT for RoCE v2

RTT analysis is fully supported for RoCE v2 RC connections. Support for RoCE v2 RD and XRC connections is experimental.

5.5 Navigation Toolbar Icons

The Navigation menu option enables the user to navigate the application (see Figure 5.131). You can go to the trigger, marker or where any cursor is located. Markers can also be added and removed. Find menu options are available as shown in the screen capture below.

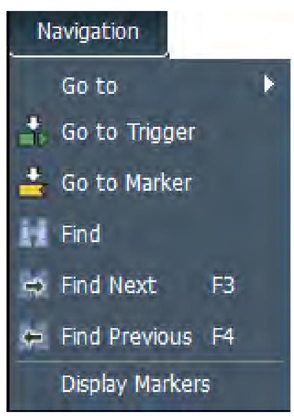


Figure 5.131: Navigation Menu Option.

The Navigation Toolbar has the same options:

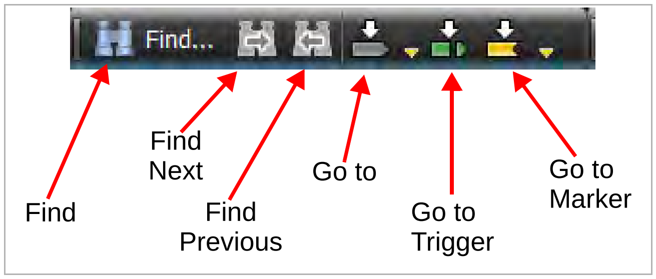


Figure 5.132: Navigation Toolbar

- **Go To** menu options allows location of cursors or specific events: Timestamp, X Position, Y Position, Event, Begin, and End. Refer to Figure 5.133.

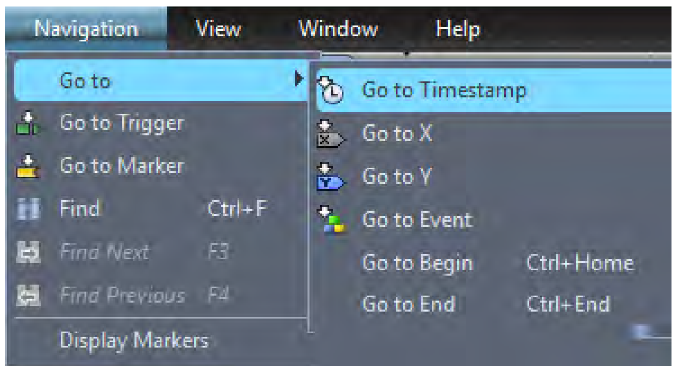


Figure 5.133: Navigation Go to Menu Option

- Go to Trigger- Allows you to go to the trigger point in the trace.
- Go to Marker- Allows you to go to a specific Marker (see 5.2.1.7, *Markers*).
- Find – Allows you to examine any data capture file to quickly locate an event or data pattern (see 5.5.1, *Find*).
- Find Next – Gives you the option to search for the next instance (see 5.5.1, *Find*).
- Find Previous – Gives you the option to search for the previous instance (see 5.5.1, *Find*).
- Display Markers – Displays the list of markers (see 5.2.1.7, *Markers*).

5.5.1 Find

The Find menu and toolbar options enable you to examine any data capture file to quickly locate the event or data pattern.

Select **Navigation → Find** or click **Find**  to open the **Quick Find** dialog (Figure 5.134). You can also right-click in the Trace and select **Quick Search**.

NOTE: Only items captured in the trace file are enabled for search.

5.5.1.1 Quick Find

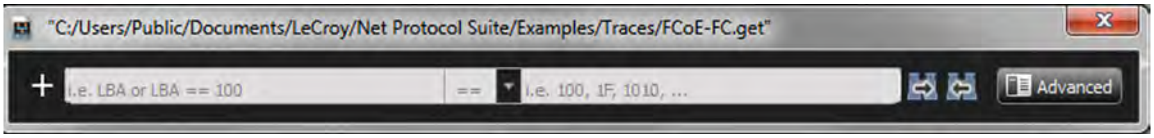


Figure 5.134: Quick Find Dialog

Click inside the first gray box and a dialog will pop up with Item-Types, Addresses, events and Fields of interest that occurred in the Trace. See Figure 5.135.

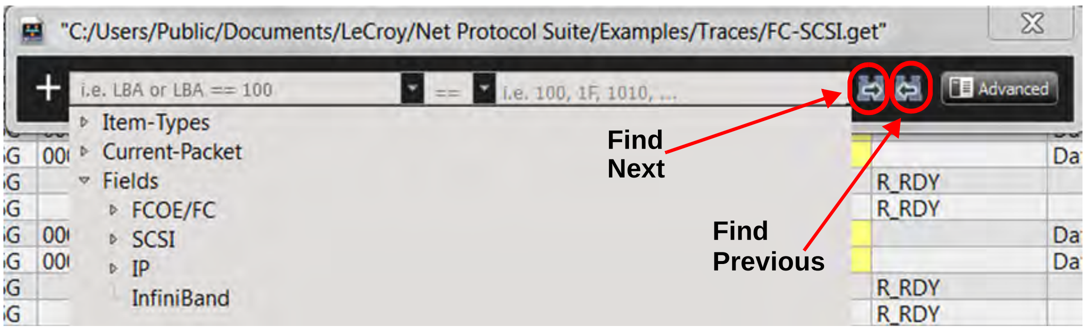


Figure 5.135: Quick Find: Item-Types, events, Fields, Find Next, Find Previous

The Find function will populate Item-Types with Addresses and Commands that occurred in the Trace. See Figures 5.136 and 5.137.

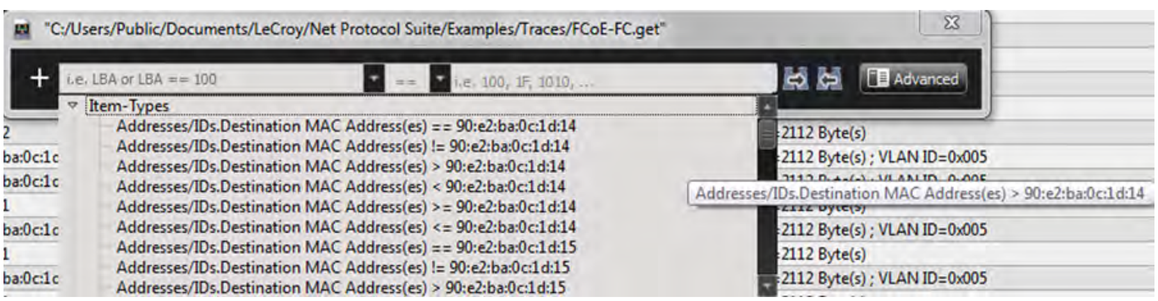


Figure 5.136: Addresses of Interest

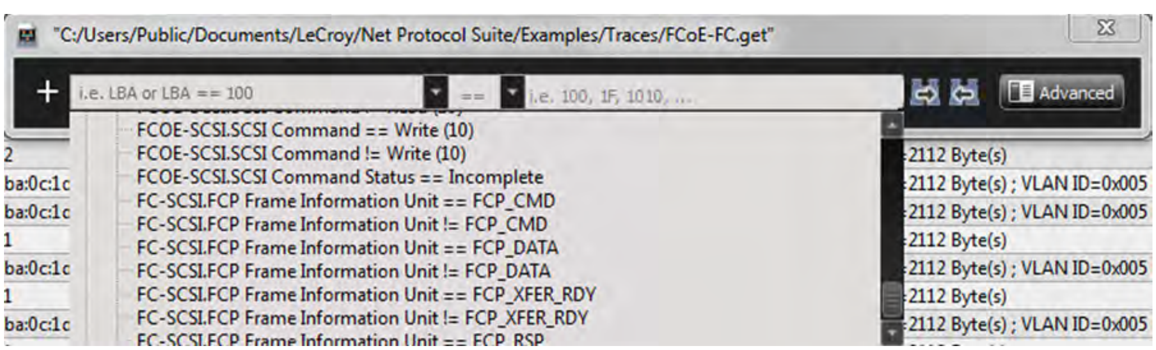


Figure 5.137: Commands of Interest

Click the **==** symbol in the middle of the screen to define a function (equal to, not equal to, greater than, less than, greater than or equal to, less than or equal to). See Figure 5.138.

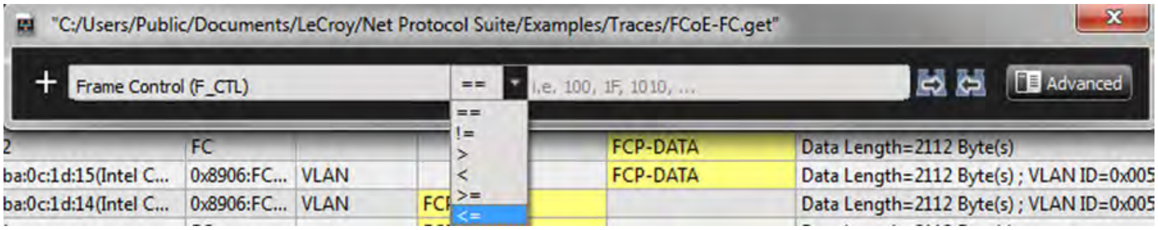


Figure 5.138: Function Definition

Click on the third gray window to set the data value to compare against.

Click the red format button to toggle between Decimal, Hexadecimal, Binary, and ASCII input formats; or right-click in the third window to select the input format from the popup menu. See Figure 5.139.

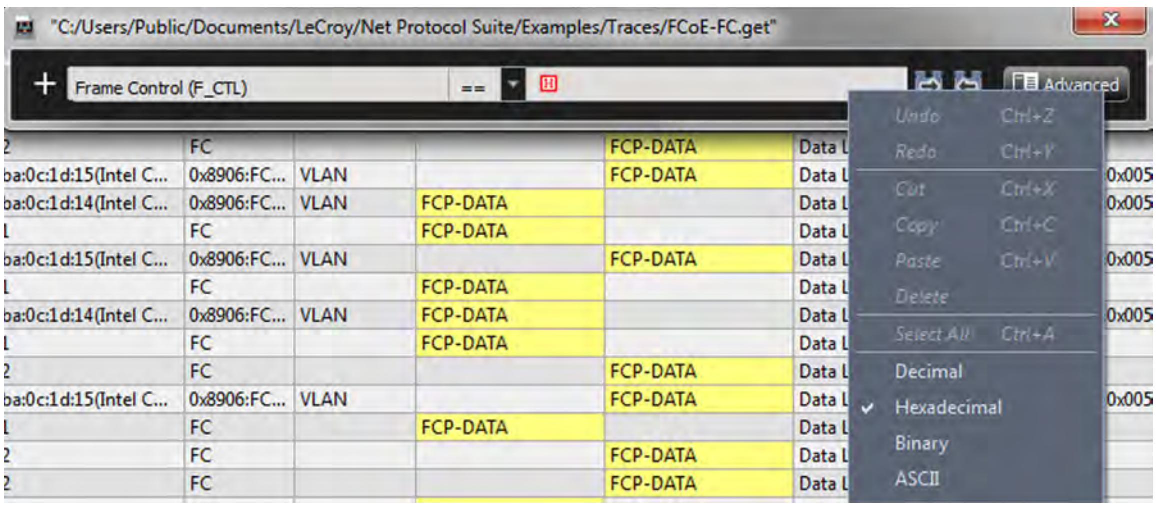


Figure 5.139: Data Format

5.5.1.2 Advanced Find

1. You can access Advanced Find in one of two ways:

   a. Click **Find**  in the main toolbar, then click **Advanced** in the Quick Search dialog (Figure 5.140).

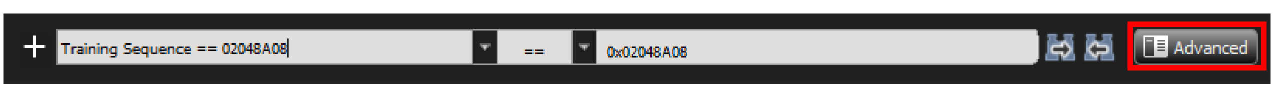


Figure 5.140: Quick Search → Advanced

   b. In the Spreadsheet View window, right click in a column/line of a Trace and select **Quick Search** from the drop-down menu (Figure 5.141), then click **Advanced**.

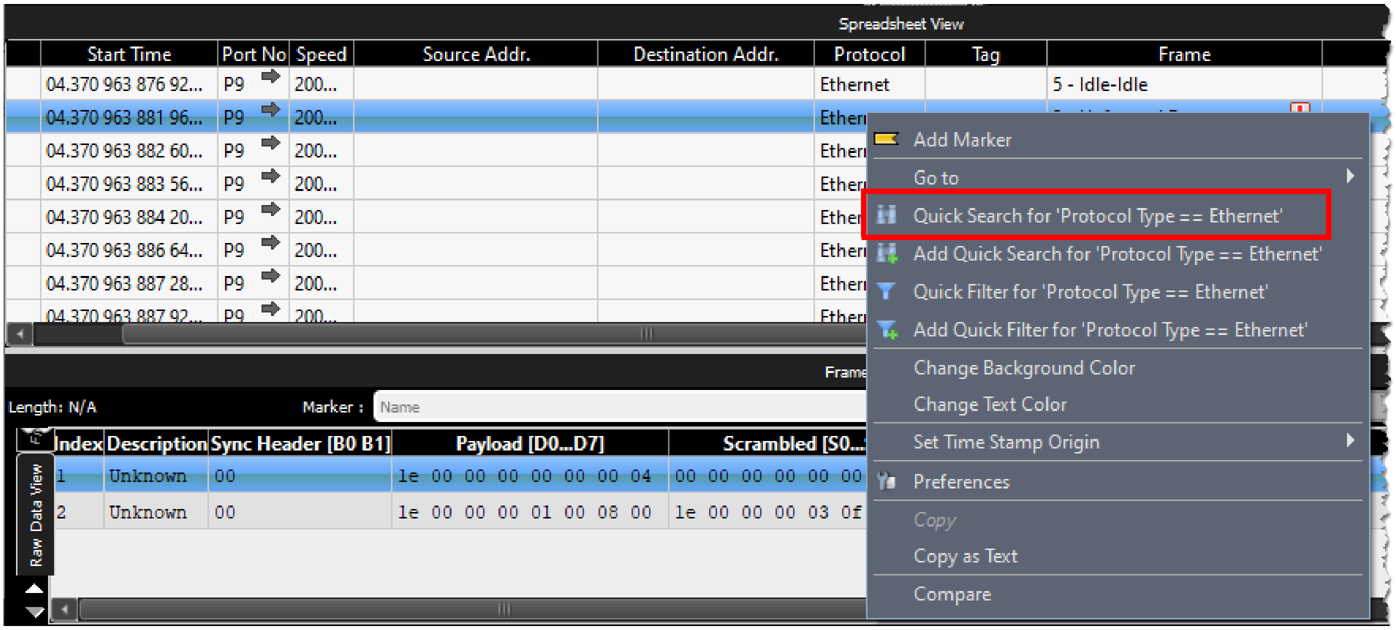


Figure 5.141: Quick Search Drop-Down Menu

NOTE: If you click in an area containing data, the Quick Search menu will show that data for filters and searches.

2. Highlight an item in the left pane, then click the left arrow to move it to the search pane (Figure 5.142).

TIP You can double-click an item in the left pane to move it to the Search pane.

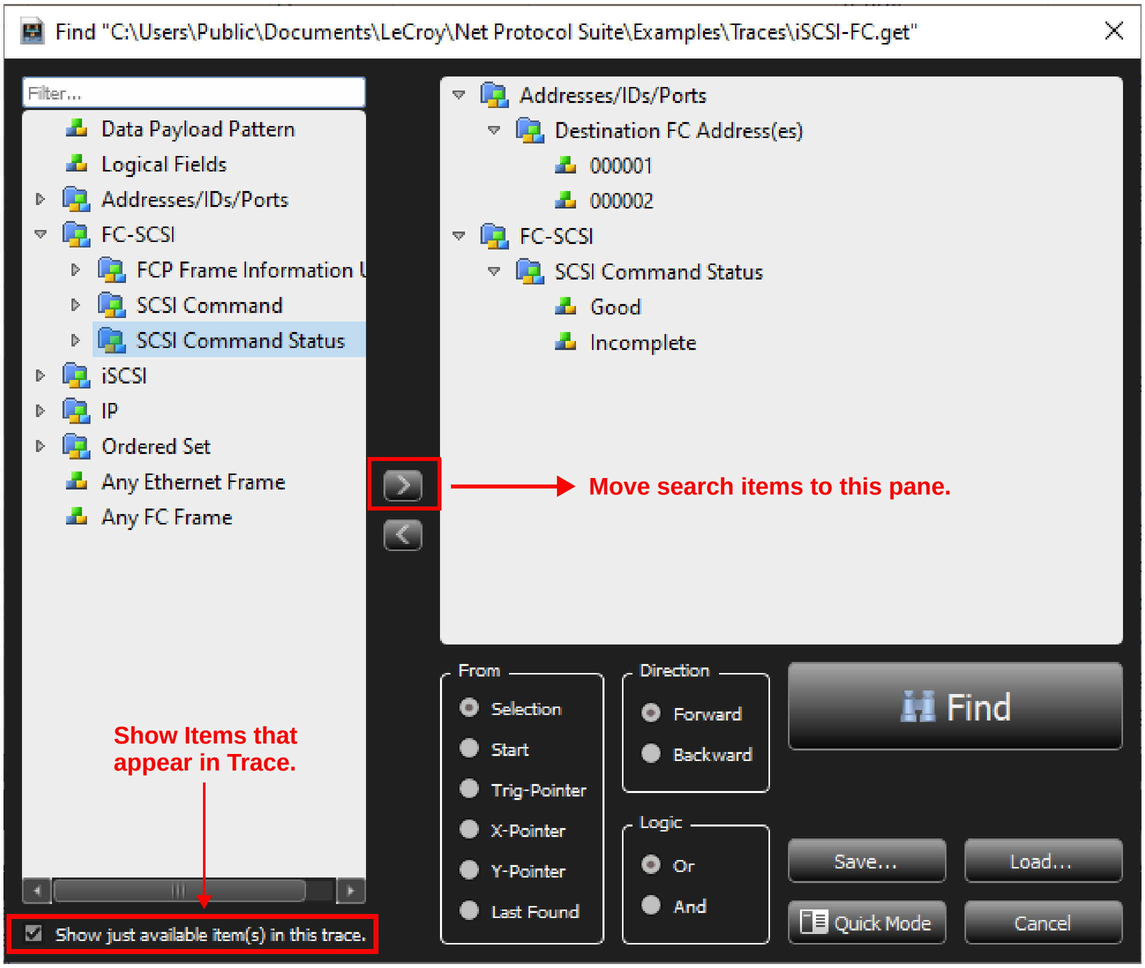


Figure 5.142: Advanced Find Window

3. Click **Find**. Results (if any) are displayed in Spreadsheet and Frame Inspector views.

5.5.1.3 Find Large or Repeating Data Payload Patterns

The Advanced Find feature allows you to define a large or repeating data payload to search for. See Figure 5.143.

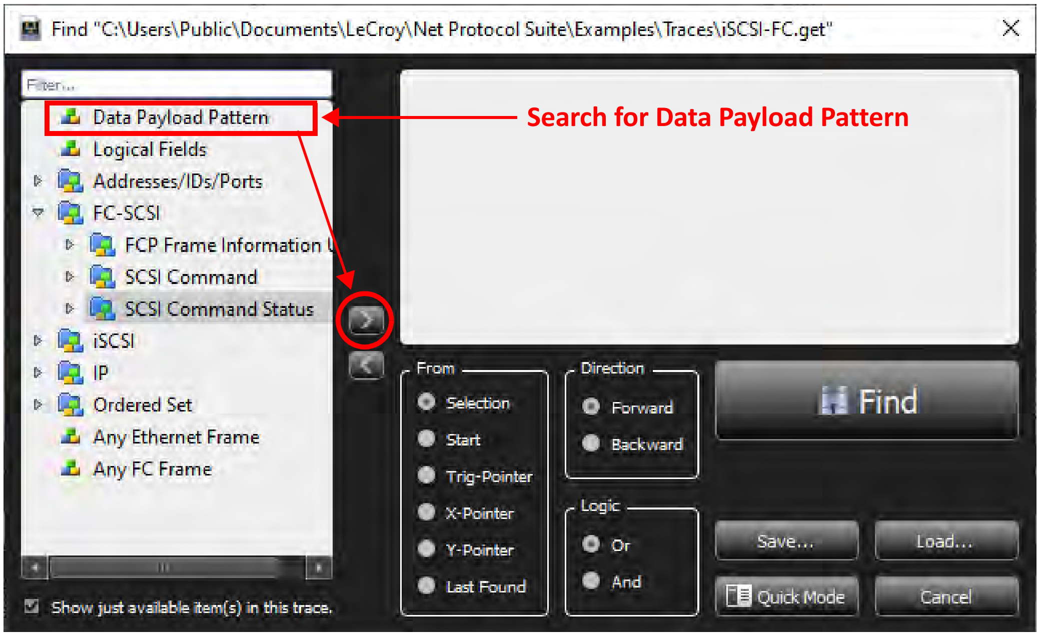


Figure 5.143: Search for Data Pattern

1. Select the **Data Payload Pattern** and click the **>** to move it to the search window. The Data Pattern window appears in which you can define a repeating pattern and/ or a very large pattern.
2. Use the Up/Down arrows to set the number of Repeats.
3. Click the radio button for either **And** or **Or**.
4. To set the Payload Length, check the box and enter the length.
5. Once you are satisfied with your settings, click **OK**.

   The example shown in Figure 5.144 shows the Data Pattern set to Repeat 4 times. That is 876543210 is repeated 4 times or a payload length of ≤99,999. The maximum payload length is 99,999. The maximum number of data patterns you can repeat is 256.

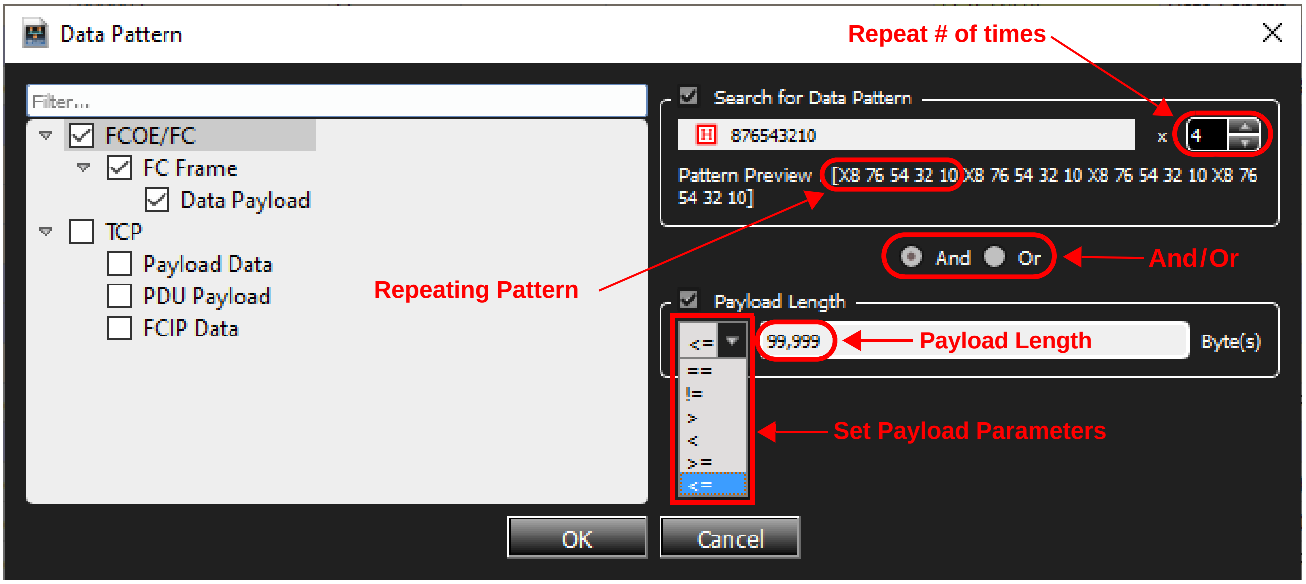


Figure 5.144: Data Pattern Definition

5.5.1.4 Find Specific Event

You can build up a specific type of event you want to Find and then Save it for later analysis of a Trace by unchecking the “Show just available item(s) in this trace” button. See Figure 5.145.

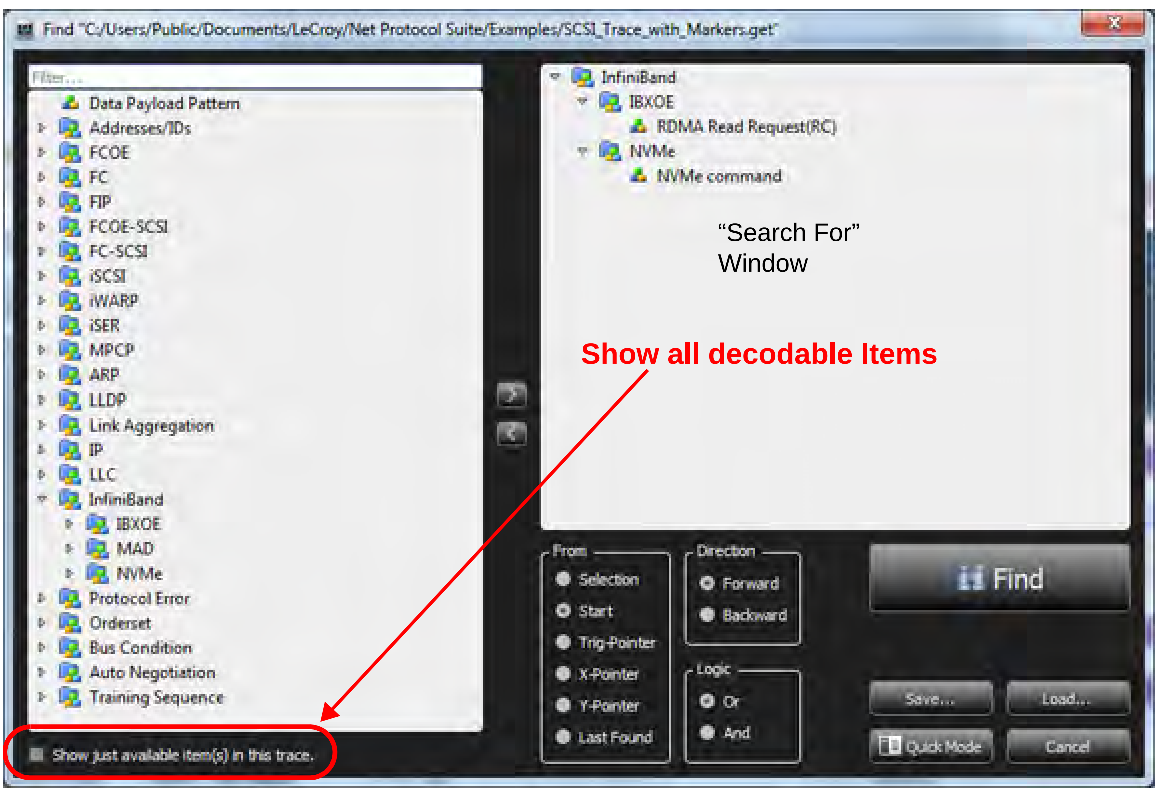
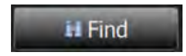


Figure 5.145: Advanced Find with “Show just available item(s) in this trace” – Unchecked

Filter

Select a type of event you want to search for from the list on the left. Use the >> arrows to move it into the "Search For" window on the right. To choose a different type of event simply select the current event type in the "Search For" window and use the << arrows to remove it. Then select a new event type.

Find

You can find specific events by selecting one and clicking the Find button 

in the Advanced Find dialog.

You can continue to search the output file using **Find Next (F3)** or **Find Previous (F4)** for the same pattern, until you redefine the data capture search parameters. You can also click the **Find Next**  icon or the **Find Previous**  icon. Alternatively, select **Navigation → Find Next** or **Navigation → Find Previous**.

Save

After you have set up a Filter configuration, you can save it as a Filter file by clicking **Save**.

Load

You can use a previously saved filter by clicking **Load** in the Filter dialog.

Save Find Setup

After you have set up a Find configuration, you can save it as a Search configuration file by clicking **Save**. You can then use it on a different capture by clicking **Load** in the Find dialog.

Search From

Choose a starting point to begin or continue a search:

- Selection (you select a event to be the starting point for the search)
- Start of the trace file
- Trigger Pointer
- X Pointer
- Y Pointer
- Last Found

Find Direction

Choose either **Forward** or **Backward** direction in which to perform the find.

Find Logic

The default setting is **Or**. With this setting, clicking **Find Next** locates all selected items in turn. If you choose **And,** you can set a logical AND combination of items to find. Both options allow setting Advanced find features.

Finding LUNs and LBAs

Perform the following steps to find LUNs and LBAs:

1. Click the **Find** icon to display the Quick Find dialog.
2. Click **Advanced** to display the Find dialog.
3. Select FCP_CMD in the left pane and drag it in to the right pane or click the right arrow.

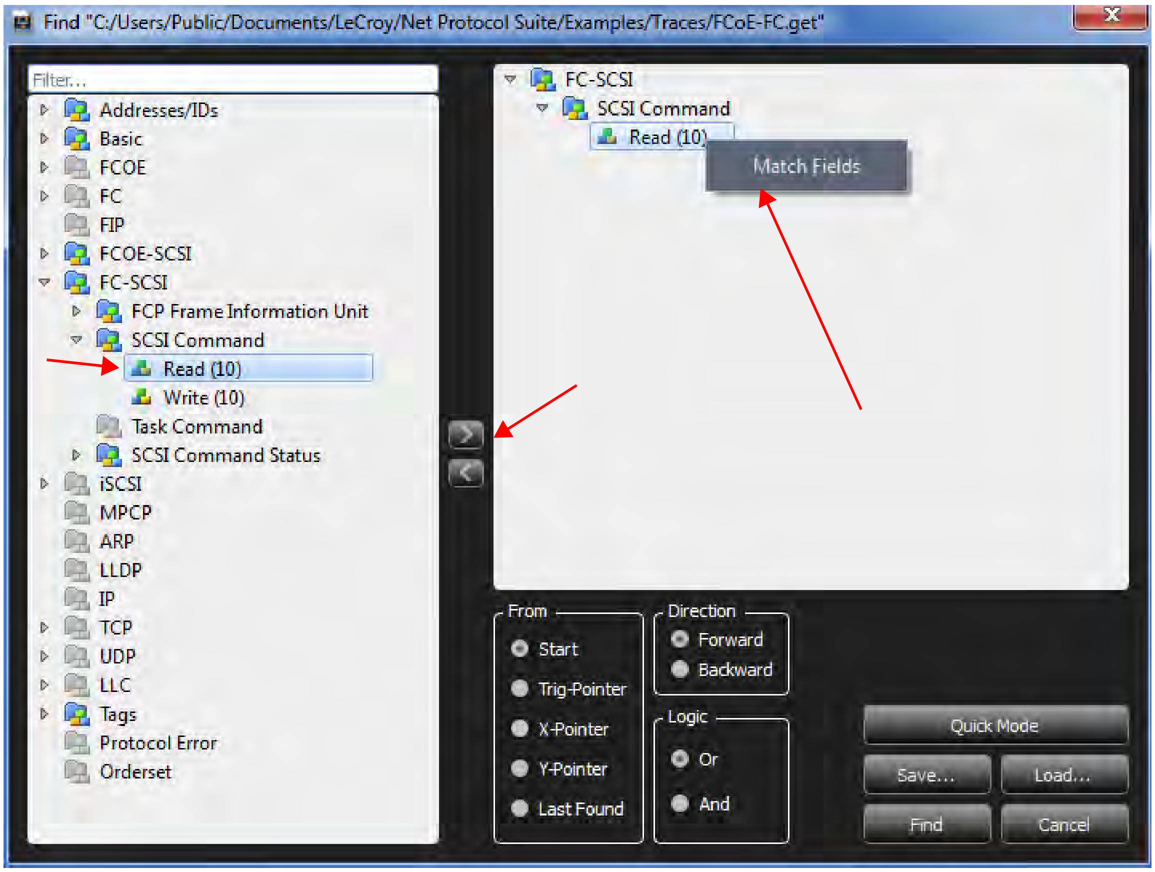


Figure 5.146: Find LUNs and LBAs 1

4. Select the command, double-click or right-click, and select **Match Fields**. The following dialog displays (see Figure 5.147).
5. Enter the values in the fields.
6. Click **OK** twice.

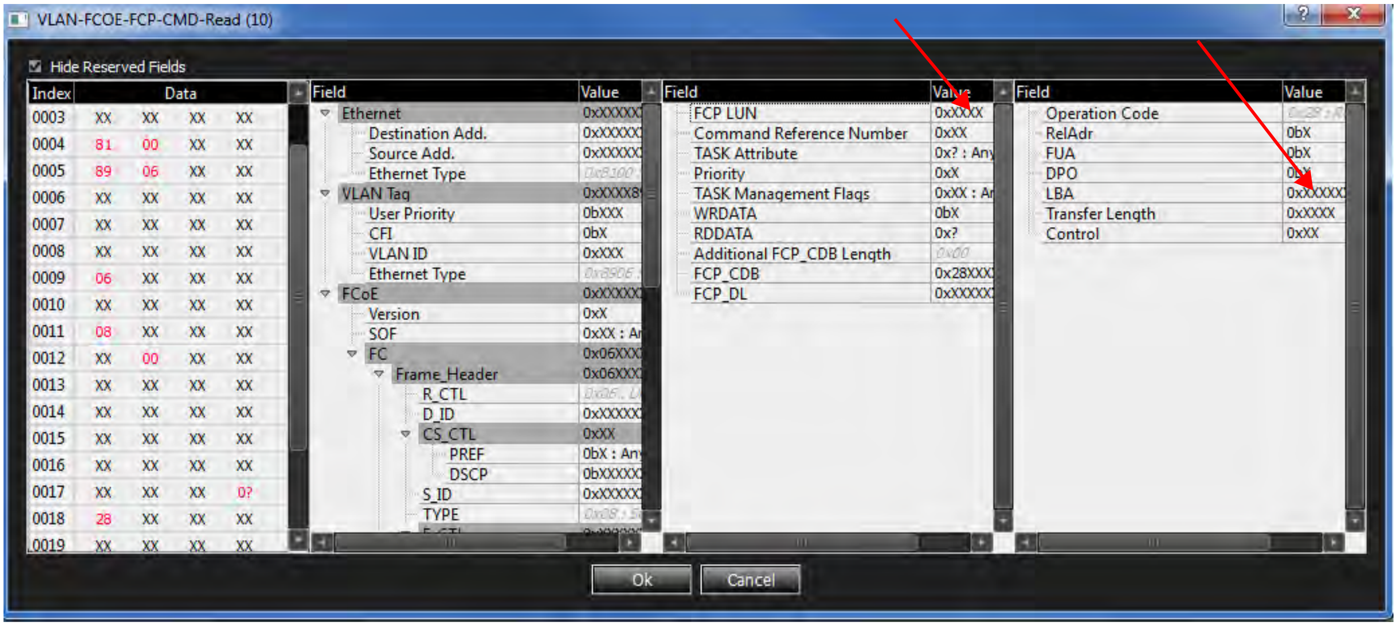


Figure 5.147: Find LUNs and LBAs 2

NVMe Command Search

You can search for a specific kind of NVMe command. This example demonstrates a search for an NVMe Discover Command. See Figure 5.148.

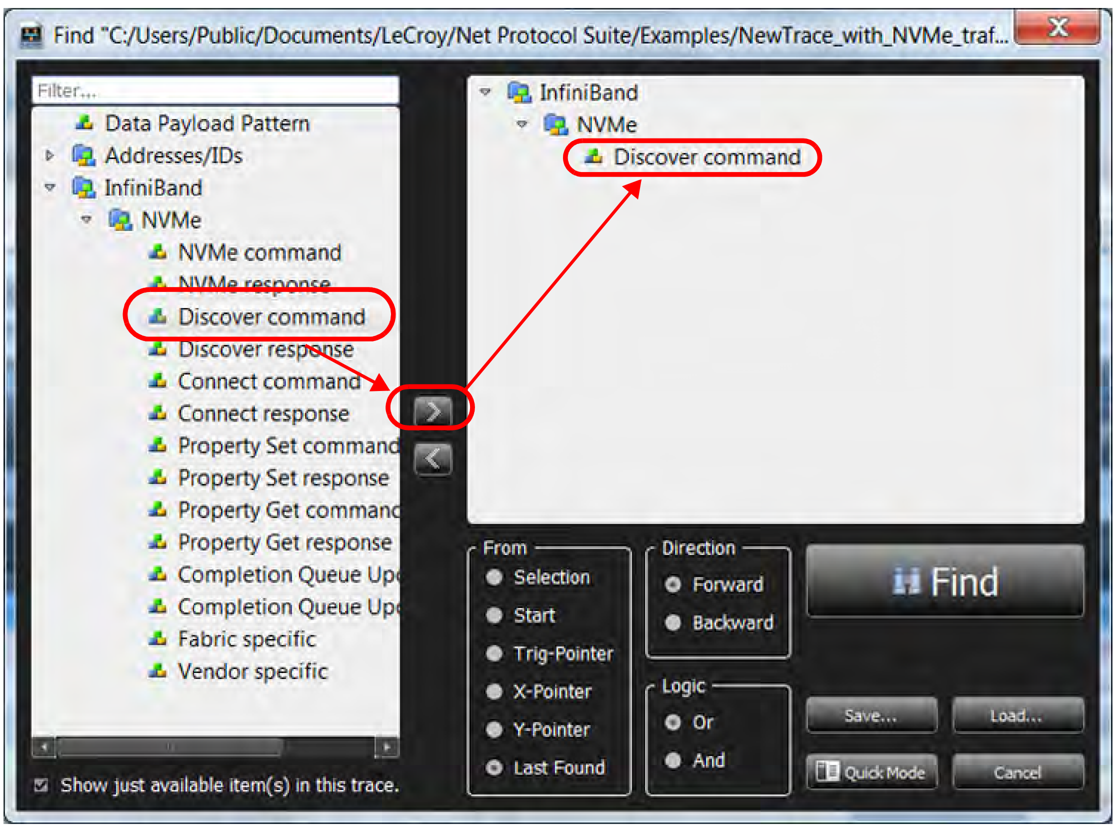


Figure 5.148: Search for NVMe

Click on the Find button and the event with the NVMe Discover Command will pop up to the top of the Spreadsheet View.

Data Pattern Search

From the Advanced Find/Filter dialog, there is a Data Pattern item available (Figure 5.149).

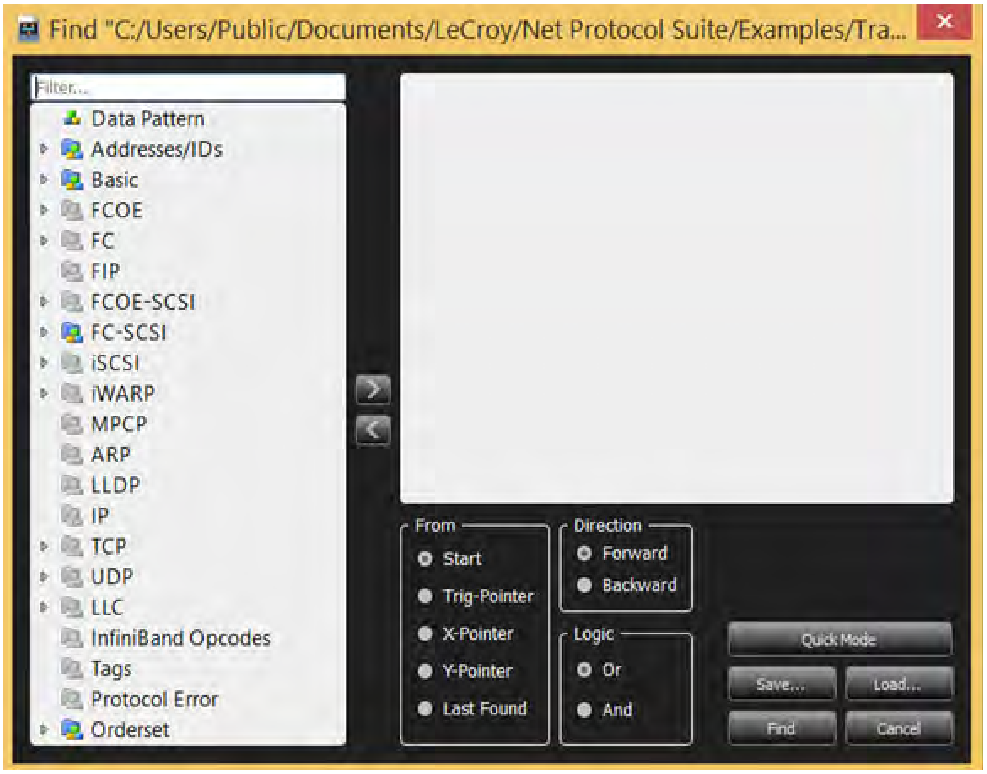


Figure 5.149: Data Pattern Search Menu

You may use this feature to set criteria based on Data Patterns in the frame payloads.

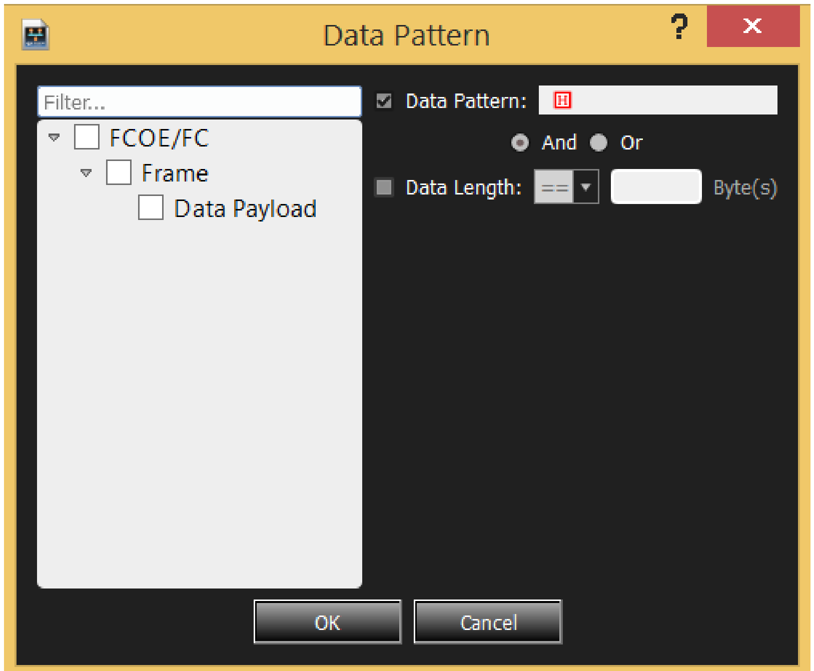


Figure 5.150: Data Pattern Search Filter

1. From the tree list on the left, select the types of payloads you want to search/filter against.
2. Check the boxes next to **Data Pattern** and **Data Length** to set whether you check based on those criteria or not.
3. If you check both the **Data Pattern** and **Data Length** boxes, also select the **And/Or** radio button to set whether you want to combine the criteria with AND or OR logic.
4. If **Data Pattern** is checked, enter the pattern you wish to match against. You may specify any size of pattern in this field. Click the red format button to toggle between different input format modes:
   - Hex
   - Binary
   - ASCII
   - Decimal
5. If **Data Length** is checked, enter the length in bytes you wish to match against, and set the desired comparison operator:
   - == (equal)
   - != (not equal)
   - > (greater than)
   - < (less than)
   - >= (greater than or equal)
   - <= (less than or equal)

5.5.1.5 Decode MAD Headers

Another example of using the Find function would be to locate a specific type of decoded header. In this example we're looking for an MAD header.

Open the File function from the Main toolbar, click on Advanced and type in MAD in the filter window. If the trace has any MAD headers they will be shown in the Spreadsheet View. See Figure 5.151

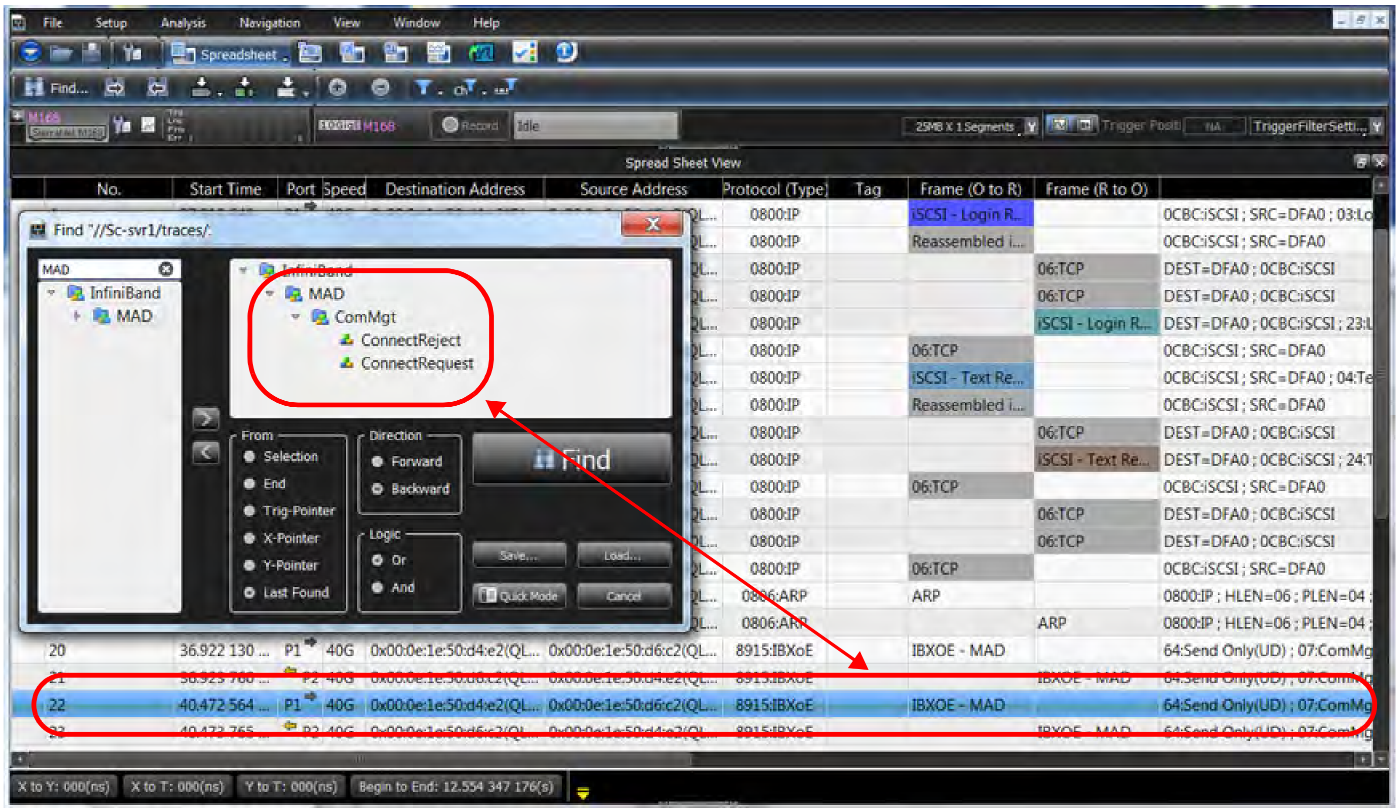


Figure 5.151: MAD Header Decoded

5.5.1.6 Decode iSER Headers

In this example, a search for an ISER header is performed:

1. Click the **Find** button on the Main Toolbar.
2. Select **Advanced** and enter **iSER** in the filter field at the top of the left pane (Figure 5.152).

   If the trace has any iSER headers they will be shown in the Spreadsheet View (Figure 5.153).

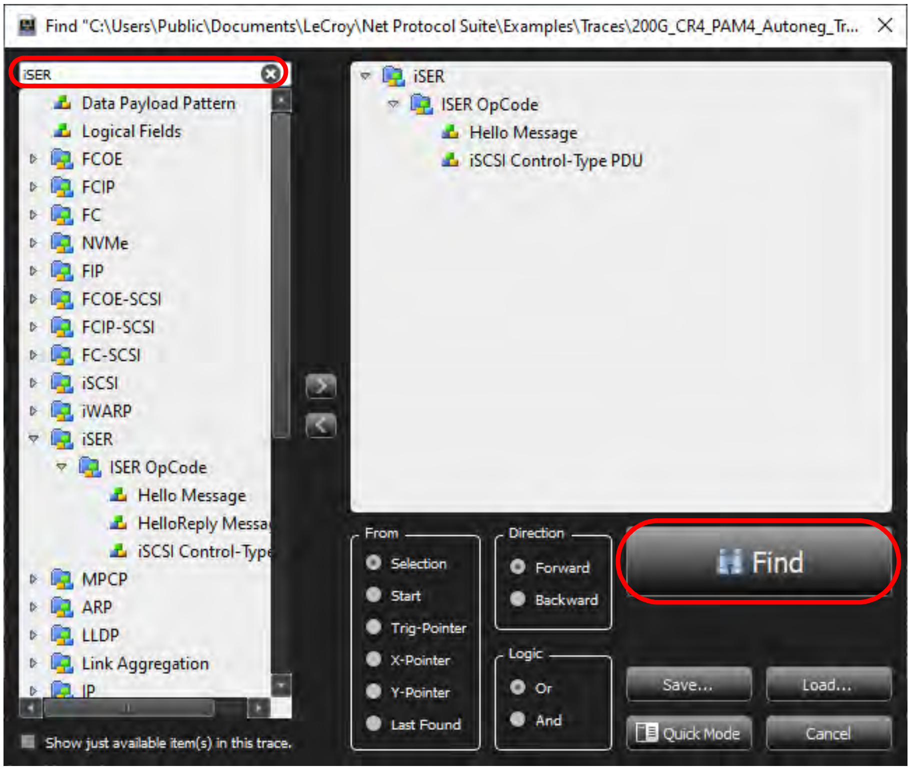


Figure 5.152: Advanced Find – iSER

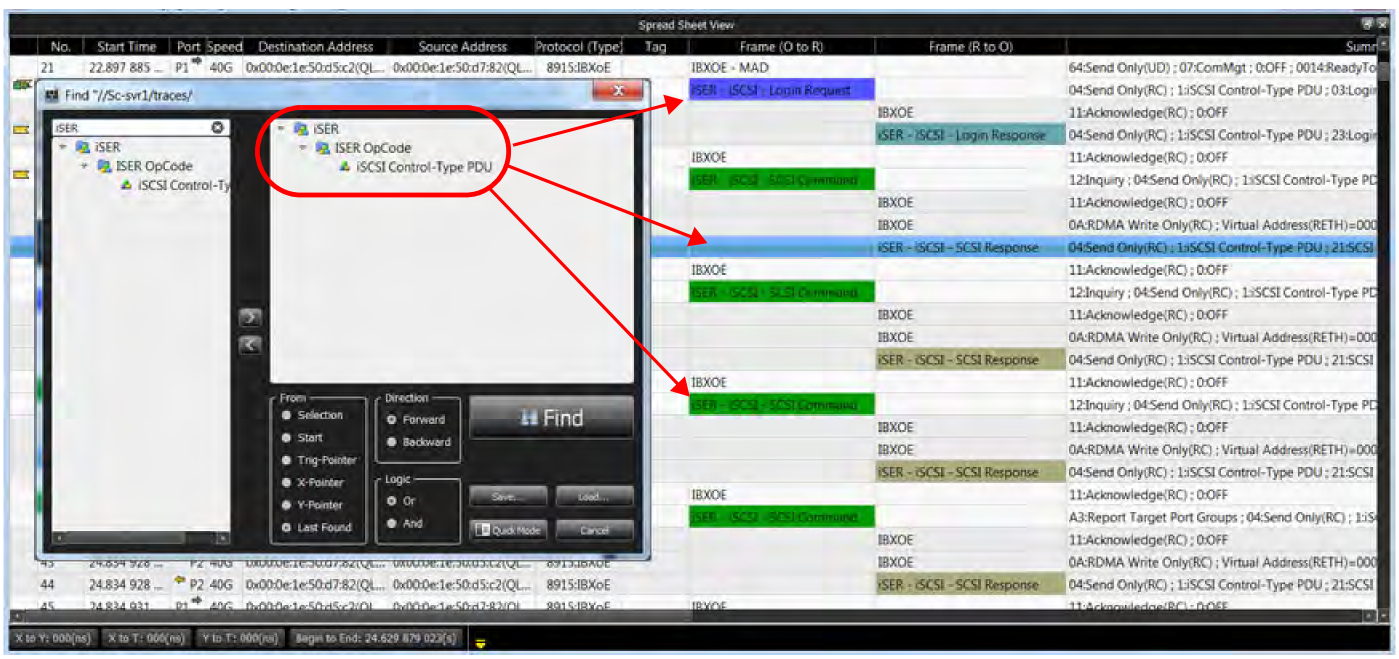


Figure 5.153: iSER Header Decoded

5.5.2 Go To Event

Selecting the large white down arrow/Go to icon  will pop up the Go to Event dialog (see Figure 5.154).

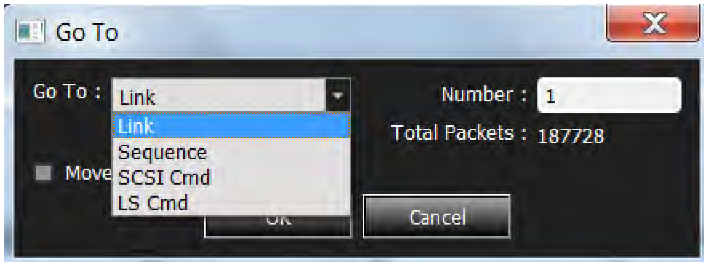


Figure 5.154: Go To Event – Link, Sequence, SCSI Cmd, LS Cmd

Select a particular Event you are interested in and click OK. The Spreadsheet View will move to that event.

Selecting the small arrow next to the Go To Icon pops up the menu below:

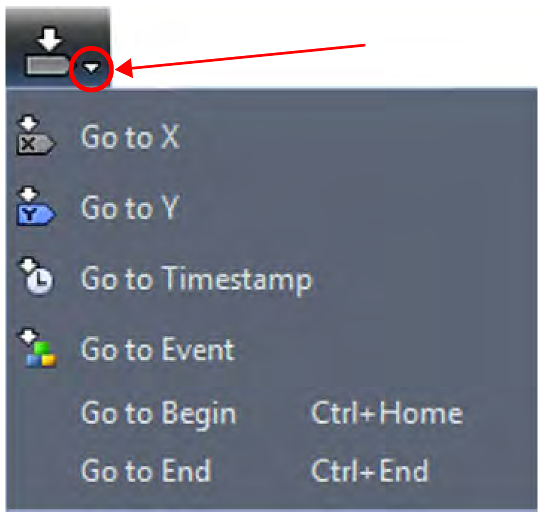


Figure 5.155: Navigation – Go To Tab in Navigation Toolbar

- Go to X: Takes you to the X-Cursor
- Go to Y: Takes you to the Y-Cursor
- Go to Timestamp: Takes you to the specified time (see Figure 5.156)
- Go to Event: Choose which type of Event and Number to go to (see Figure 5.154).
- Go to Begin: Takes you to first Event in the Trace
- Go to End: Takes you to the last Event in the Trace

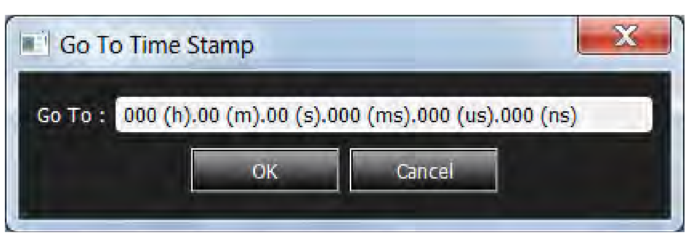


Figure 5.156: Navigation – Go to Time Stamp

Enter a specific time you are interested in and click OK. The Spreadsheet View will move to that time.

5.5.3 Go to Trigger

Selecting the Go to Trigger icon  and the Spreadsheet View will move the trigger to the top of the Spreadsheet View display. See Figure 5.157.

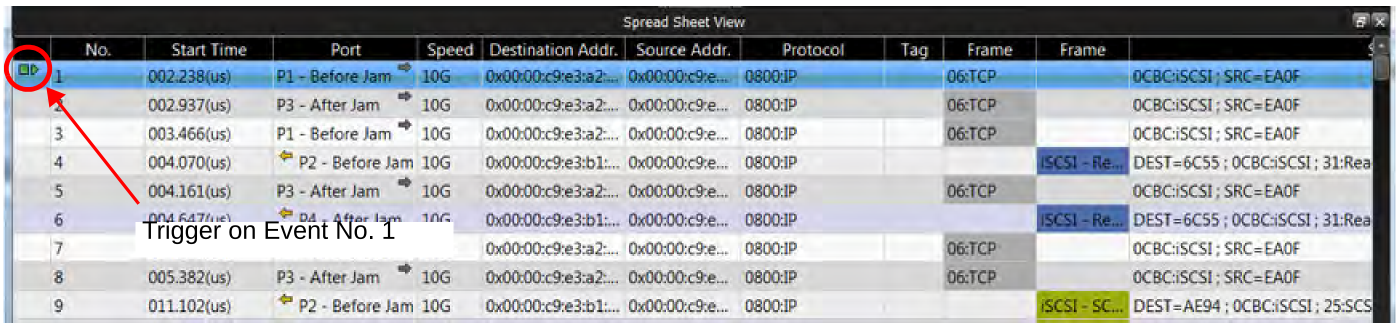


Figure 5.157: Navigation: Go to Trigger

5.5.4 Go to Marker

Selecting the large white down arrow/Go to Marker icon  will pop up the Go to Marker dialog box (Figure 5.158).

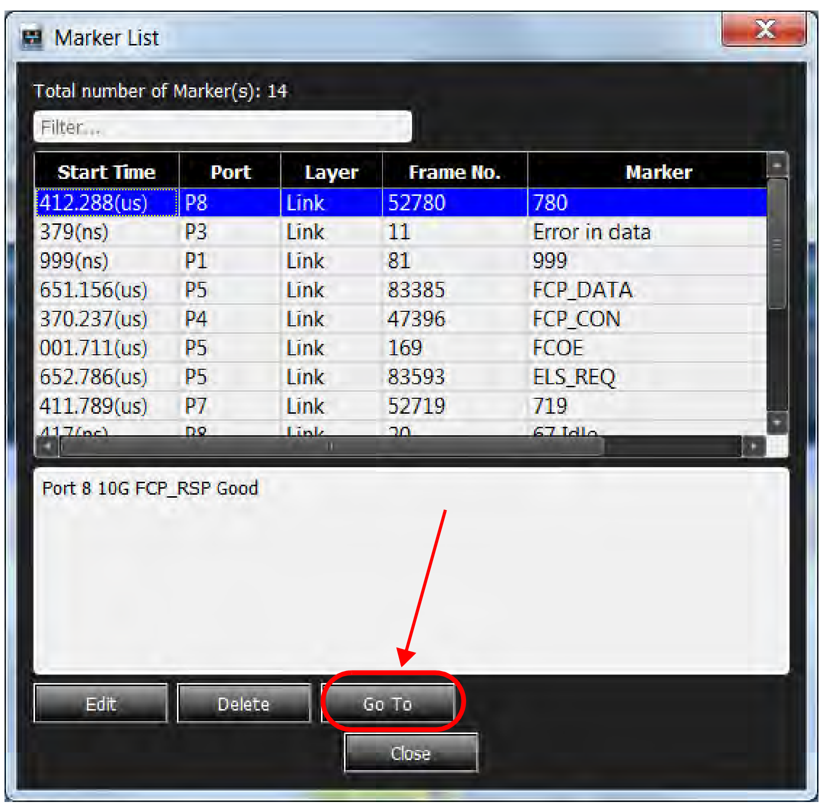


Figure 5.158: Marker List Dialog Box

Selecting a Marker and clicking on the Go To button will move the Spreadsheet View to that point. The generation of Markers has already been discussed in 5.2.1.7, *Markers*.

If you select the small white triangle to the right of the icon, the following list of Markers appears (Figure 5.159).

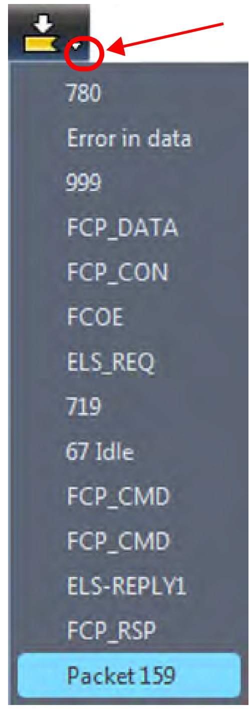


Figure 5.159: List of Markers

Selecting one of the Markers in the list will move that event to the top of the Spreadsheet View.

5.6 View: Pull Down Menu

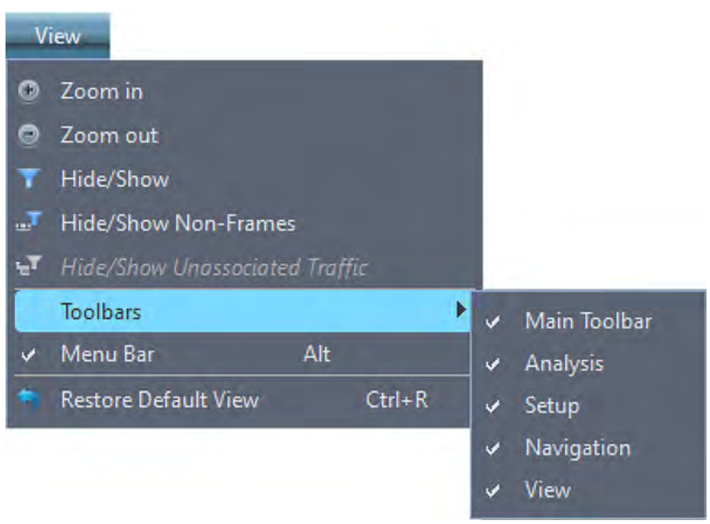


Figure 5.160: View Toolbar ➔ Pull Down Menu

5.6.1 Zoom In

Clicking on the  expands the Spreadsheet or Exchange View.

5.6.2 Zoom Out

Clicking on the  compresses the Spreadsheet or Exchange View.

5.6.3 Enable Hide/Show (Filter Events)

The Enable Hide/Show icon  allows you to either Hide or Display the filtered events shown in the Spreadsheet or Exchange Views.

To set up filtering, you must have a viewer display open.

5.6.3.1 Filter Setup

To display the Quick Filter dialog (Figure 5.161), click the drop-down arrow  to the right of the **Enable Hide/Show** button on the toolbar or select **View → Hide/Show**. When Filter criteria are set, click the funnel icon on the Filter button to toggle the filters on and off.

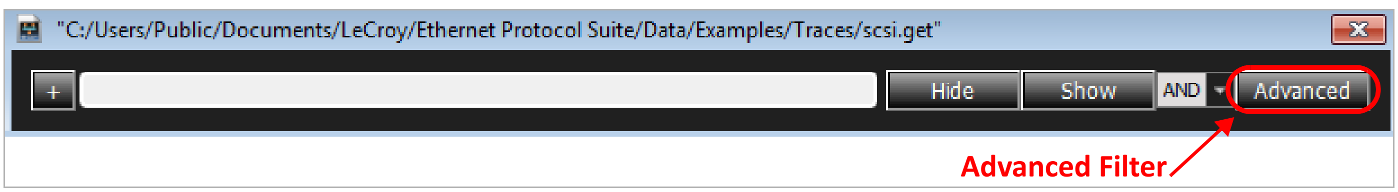


Figure 5.161: Quick Filter Dialog

You can use the Quick Search and Filter dialog on a Frame by right-clicking on it in the trace and selecting **Quick Search**. Select a field to filter/search for. Click in between the two lines in the center to display logical operators to select from the drop-down list.

Figure 5.162: Search/Quick Filter for Frame Dialog Window

Click the **Advanced** button (see Figure 5.161 or Figure 5.162) in the Quick Filter dialog to display the Advanced Filter dialog (Figure 5.163).

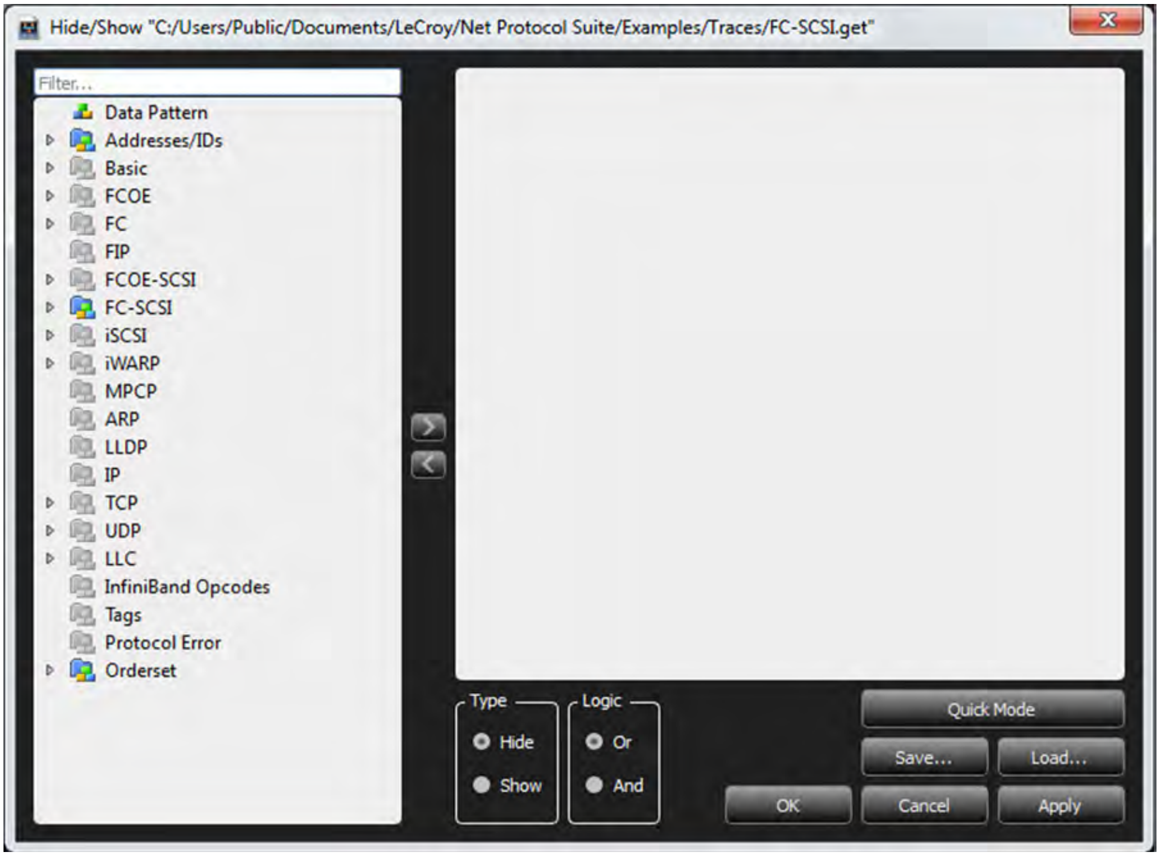


Figure 5.163: Advanced Filter Dialog

You can select or deselect each of the items shown in the left pane for filtering. Items not in the current trace are grayed out.

NOTE:
- If you select a group, that also selects all child items.
- Only events captured at run time are available for selection for filtering.

Filter Type

You can choose to show or hide the Filter Type items by checking the Show or Hide option button.

Filter Logic

After you have set up Filter options, you can set filter logic to **And** to apply “AND” logic on related selected options or **OR** to apply “OR” logic on all selected options.

Save Filter

After you have set up a Filter configuration, you can save it as a Filter file by clicking **Save**.

Load

You can use a previously saved filter by clicking **Load** in the Filter dialog.

Apply

You can apply the current filter by clicking **Apply** in the Filter dialog.

5.6.3.2 Filtering LUNs and LBAs

Perform the following steps to filter for LUNs and LBAs:

1. Click the drop-down arrow of the **Enable Hide/Show** button  to display the Quick Filter dialog.
2. Click **Advanced** to display the Hide/Show dialog.
3. Select FCP_CMD in the left pane and drag it in to the right pane or click the right arrow.

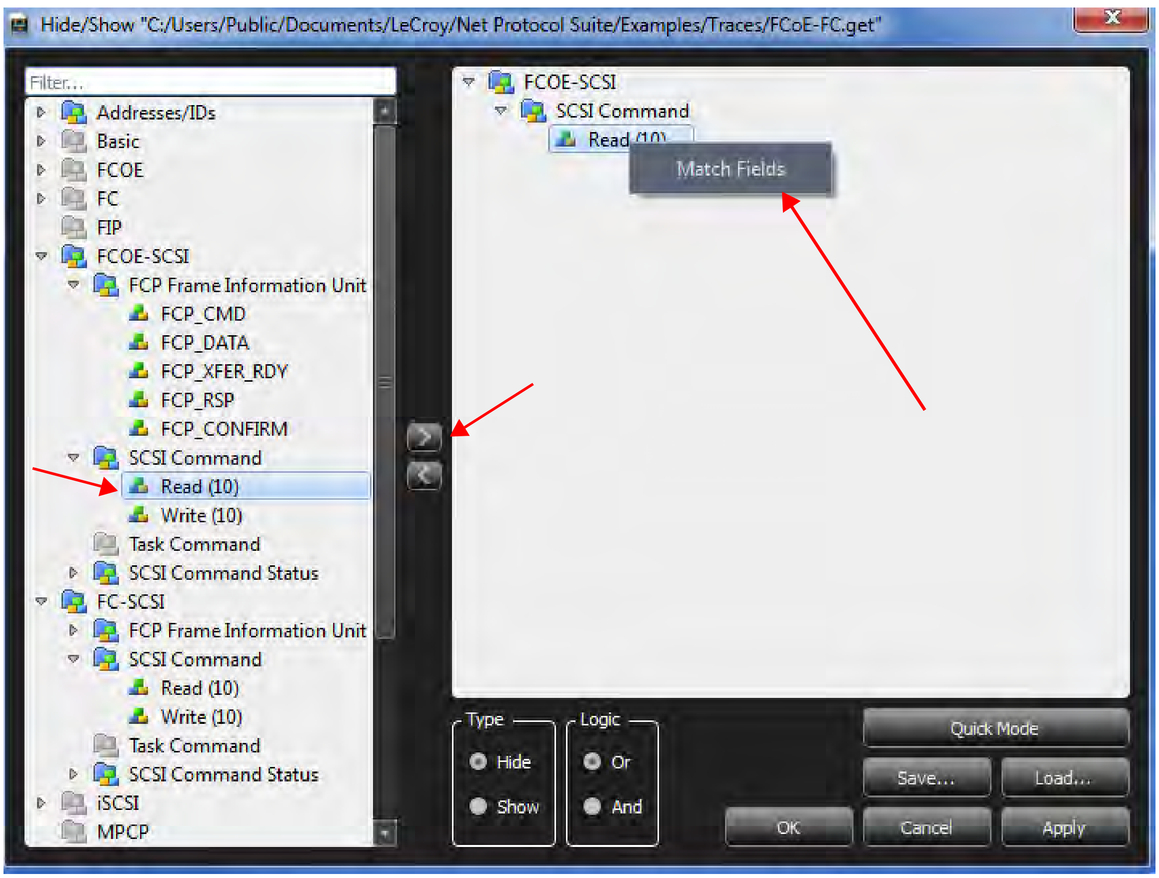


Figure 5.164: Filtering for LUNs and LBAs

4. Select the command, double-click or right-click, and select **Match Fields**. The following filter dialog appears (Figure 5.163).
5. Enter the values in the field.
6. Click **OK** twice.

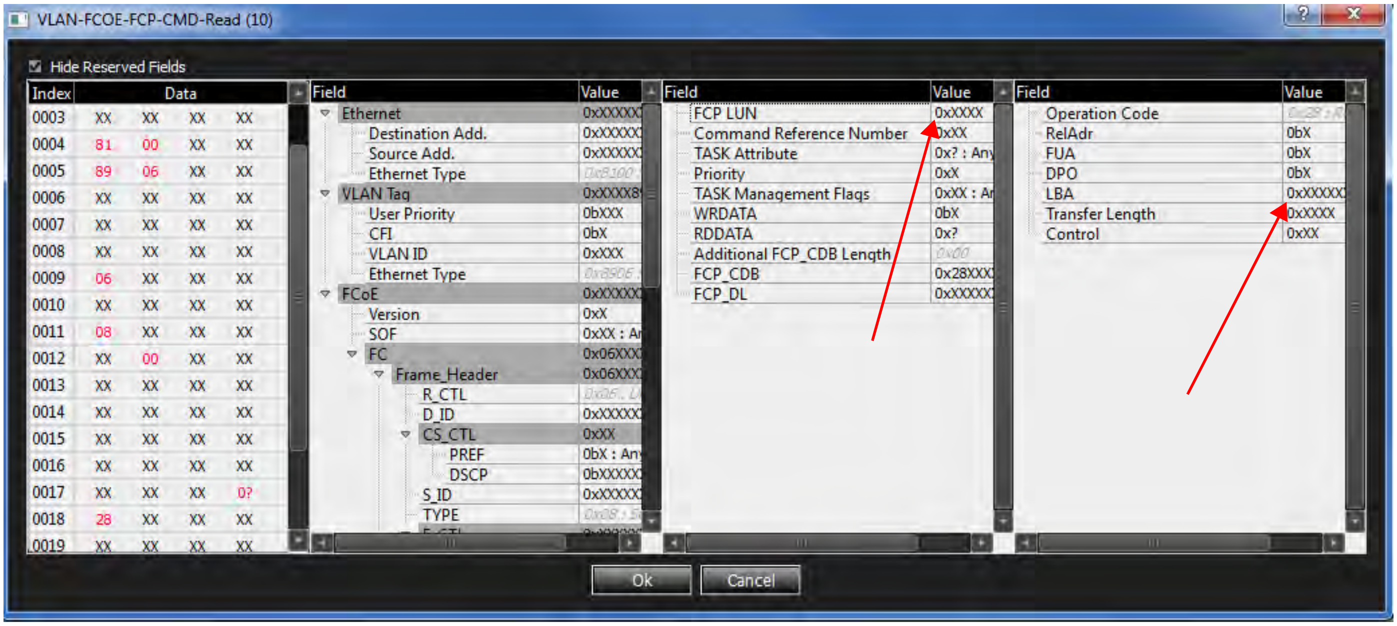


Figure 5.165: LUN and LBA Filter

5.6.3.3 Filter MAD Header

Another use of Filter would be to find Decoded MAD Headers. See Figure 5.166.

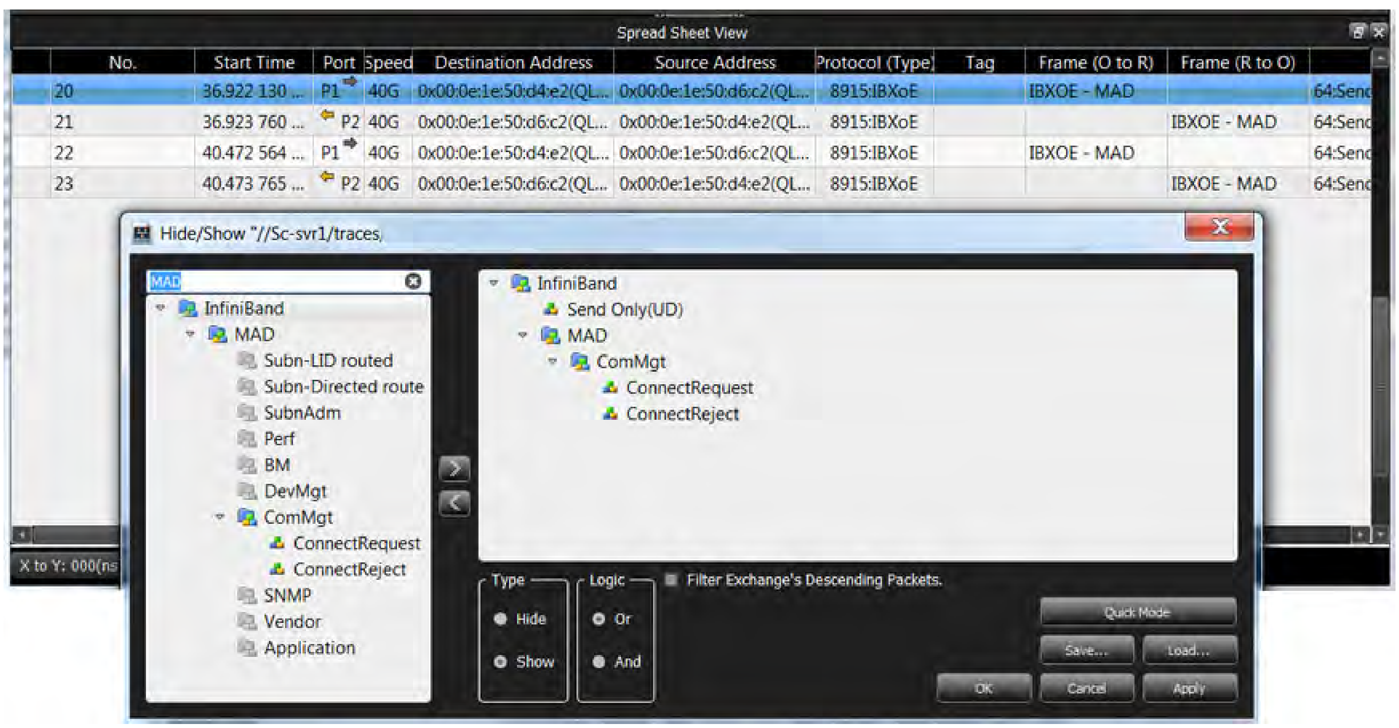


Figure 5.166: MAD Header Filter

5.6.3.4 Filter iSER Header

The Filter function could also be used to find Decoded iSER Headers. See Figure 5.167.

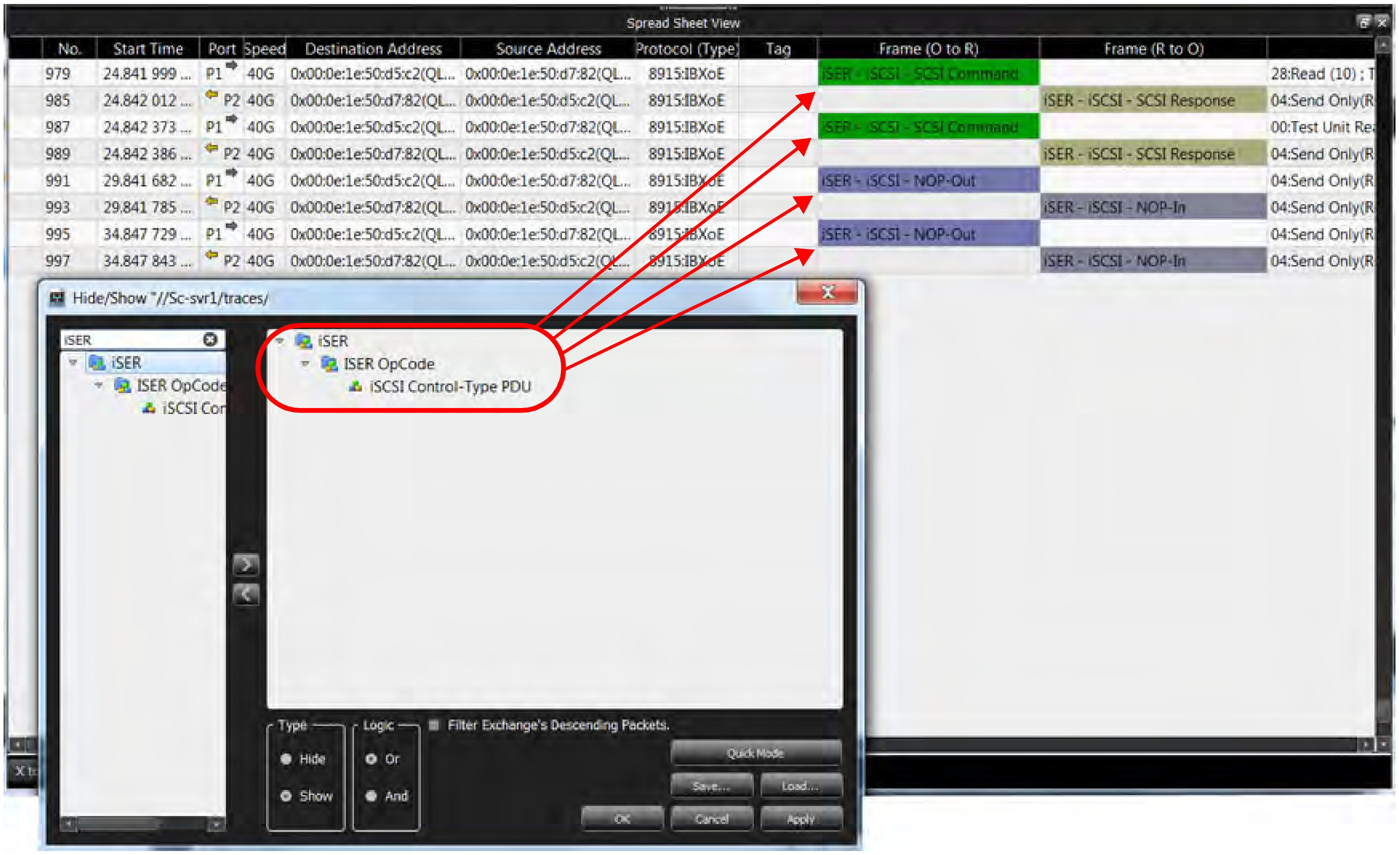


Figure 5.167: iSER Header Filter

5.6.3.5 Ports

All active ports are highlighted on the Show/Hide Ports toolbar. Click the Ports  button on the top toolbar to display the ports. Click a port button to hide the captured frames for that port. Frames can be displayed or hidden based on which port they were captured.

Figure 5.168: Show/Hide Ports Toolbar

5.6.4 Show/Hide Non-Frames

You can show or hide Non-Frames by clicking on the  Hide/Show Non-Frames icon.

5.6.5 Toolbars

5.6.5.1 Enabling Tool Bars

To customize the Viewer Display workspace, you can enable and reposition the available toolbars. To display or hide toolbars, select **View > Toolbars**, then check or uncheck toolbars.

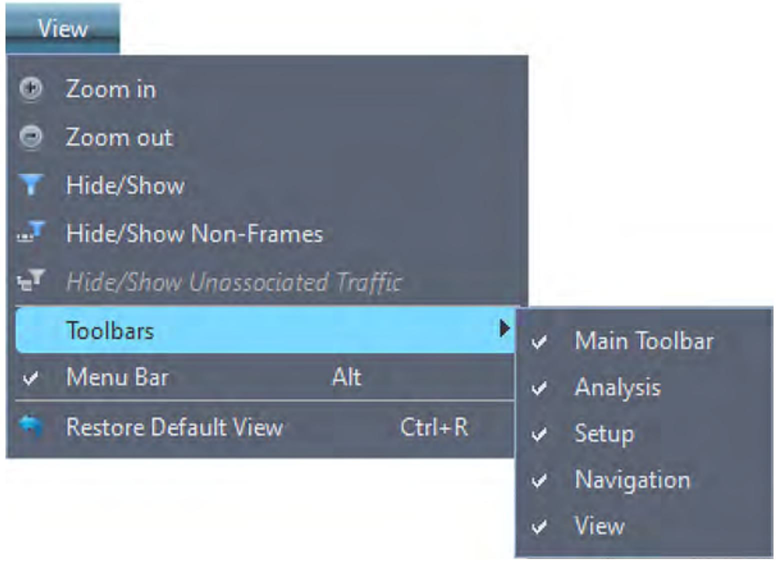


Figure 5.169: Customizing the Toolbar

Toolbars are:

- Main Toolbar
- Analysis
- Setup
- Navigation
- View

Once enabled, the toolbars can dock at the Viewer Display window or float on the windows desktop.

5.6.5.2 Main Toolbar

The Main or standard toolbar has the Hide Menubar, File Open and File Save. See *3.3, Toolbar Options* for more information.


Figure 5.170: Main Toolbar

5.6.5.3 Analysis Toolbar

The Analysis toolbar displays various views. See *5.2, Switching Analysis Views* for more information.

Figure 5.171: Analysis Toolbar

5.6.5.4 Navigation Toolbar

The Navigation toolbar allows searching, filtering, collapsing/expanding, and data reporting. See *5.5, Navigation Toolbar Icons* for more information.

Figure 5.172: Navigation Toolbar

5.6.5.5 View Toolbar

The View toolbar allows wrapping, zooming, and configuration. See 5.6, *View: Pull Down Menu* for more information.

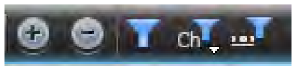


Figure 5.173: View Toolbar

5.6.5.6 Setup Toolbar

The Setup toolbar is used to set preferences.

	The **Preferences** button displays the Preferences dialog (see 3.2.2.2, *Preferences*.)

5.6.6 Restore Default View

If you added a number of different views and the screen has become somewhat cluttered (Figure 5.174), you can select **View → Restore Default View** to declutter the display (Figure 5.175).

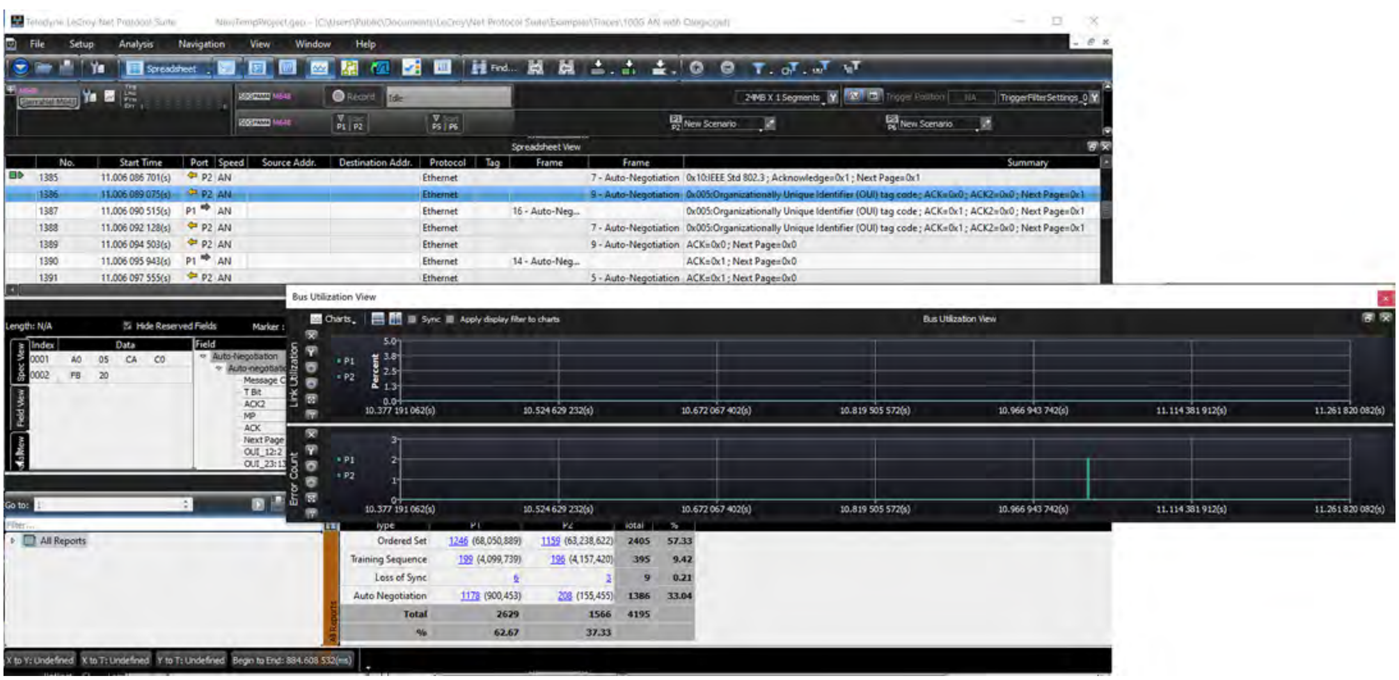


Figure 5.174: Many Views of Trace

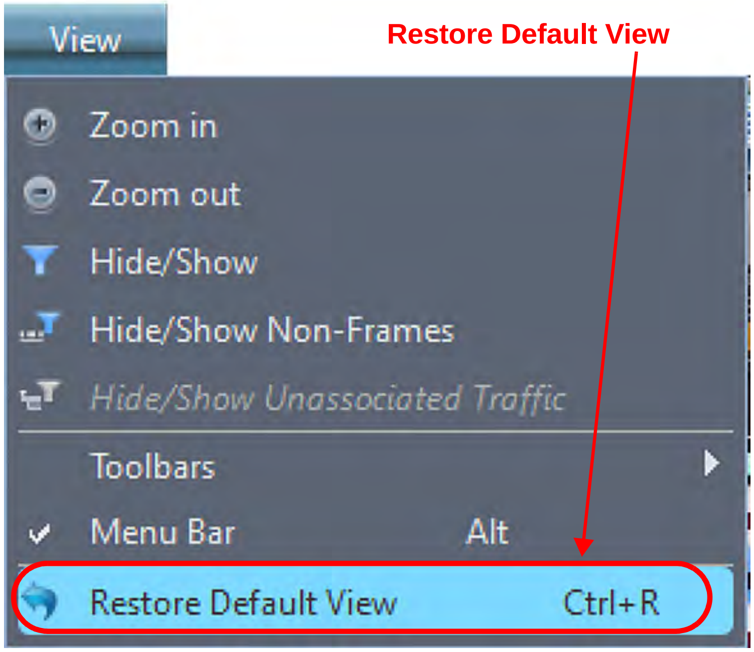


Figure 5.175: Select View → Restore Default View

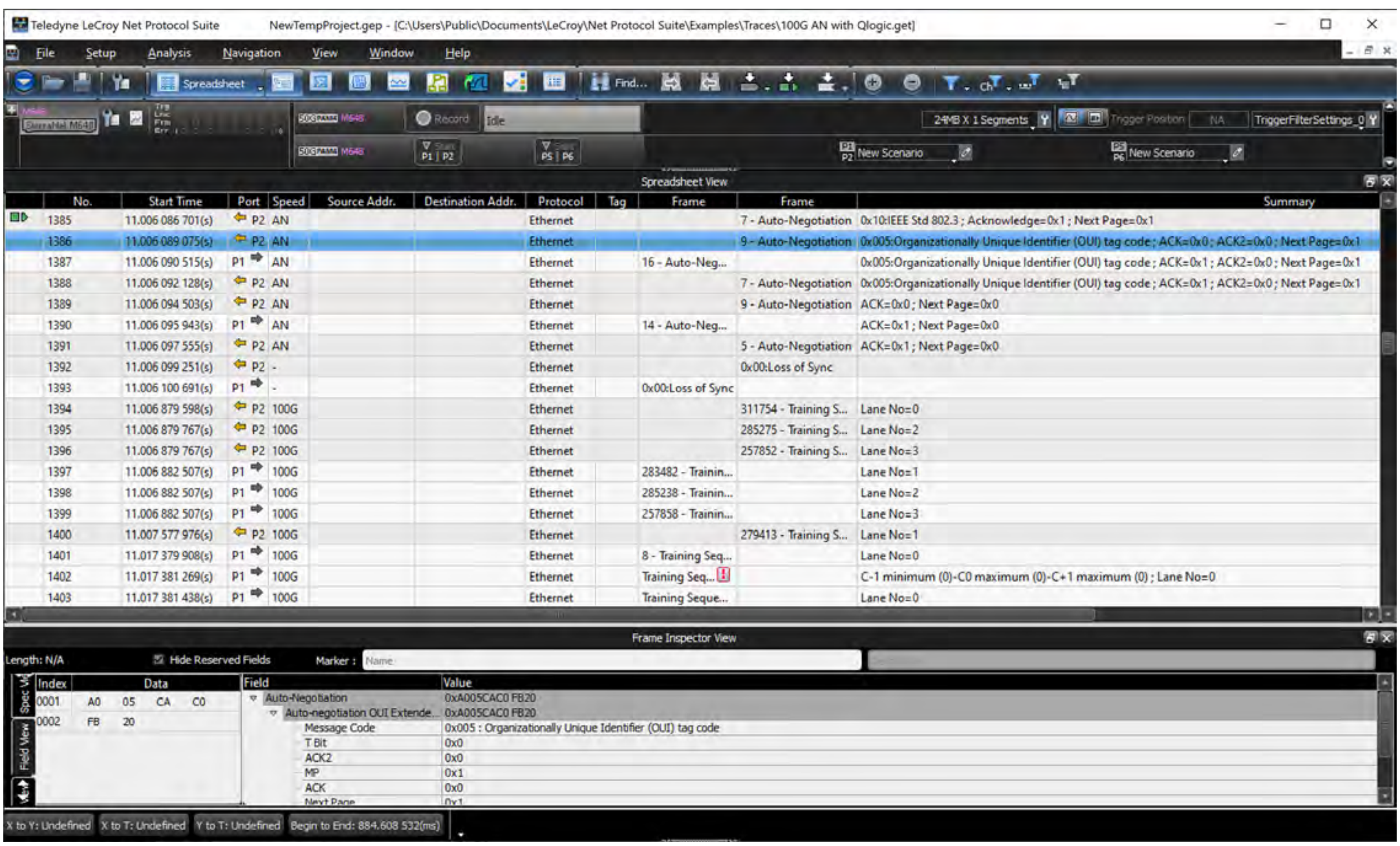


Figure 5.176: Restore Default View – Spreadsheet and Frame Inspector Only

5.6.7 Status Bar

The Status bar is located at the bottom-left of the main display window. Depending on the current activity, the bar can be divided into as many as four segments.

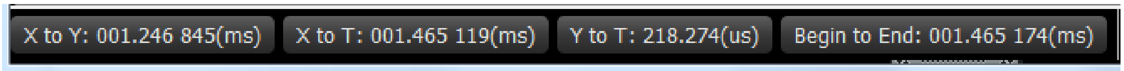


Figure 5.177: Status Bar

Chapter 6

InFusion

6.1 InFusion Overview

The Teledyne LeCroy InFusion™ Error Injector and Traffic Modifier is an error injector and traffic modification tool that allows you to verify real-world fault handling for Fibre Channel or EtherNet systems. InFusion can sit unobtrusively in the data path on a live system to programmatically alter or corrupt traffic. InFusion is the ideal tool for stress-testing systems using actual workloads.

InFusion supports Ethernet and Fibre Channel links. InFusion monitors traffic from both directions in real-time and relies on predefined rules to replace any bit, ordered-set, or parameter with one you specify. InFusion can change traffic when it detects a specific sequence or reaches a designated time interval, yet it requires no complicated scripts, programming, or simulation tools. It supports “Jumbo” events up to 16K.

InFusion can monitor traffic in both directions and act on Events occurring in either direction of the communications link. InFusion can modify traffic in only one direction within a given test Scenario, but that direction can be either from the Originator or from the Responder. InFusion checks the direction of traffic as the Scenario is generated to make sure the direction of Events and Actions are the same as the Scenario. If the direction of data traffic of an Event doesn’t agree with the direction of data traffic set up in the Scenario, a warning message is generated and the Event won’t be generated.

InFusion is specifically designed to verify recovery characteristics within a subsystem. An easy, user friendly menu interface with icons and hyperlinks allows you to create specific test Scenarios in just minutes.

Once an InFusion session starts, the system automatically handles protocol handshaking between devices. InFusion transmits a faithful copy of the original data stream down to the CRC value which, if needed, it recalculates. InFusion allows test engineers to systematically verify error recovery in ways not possible with other test platforms.

6.2 Key Features

The key features of InFusion are:

- **Error Injection**: Injects CRC, disparity, 8b/10b encoding, framing, and coding errors.
- **Break Link Recovery**: Programmatically breaks the connection to test link recovery.

- **Value Replacement**: Monitors the link for specific values, patterns, or ordered-sets (as low as bit level) and replace with user-defined values. You can replace values on every occurrence, after a specified number of occurrences, or after a specified time interval.
- **Event Drop**: Removes individual ordered-sets or frames from the stream to verify retry behavior.
- **Ordered-set Manipulation**: Replaces handshaking and flow control ordered-sets to help validate robustness of a design.
- **Traffic Monitoring:** Operates as a traffic monitor, collecting statistical data on user-specified parameters. In this mode, data passes unchanged in both directions.
- **Menu-Driven Interface:** Allows easy set-up of test Scenarios.

With respect to traffic modification, in the Link Layer you can modify ordered-sets, CRC, scrambled data, and connection Events. You cannot modify clock skew management and signal integrity.

InFusion consists of a hardware device that connects to the line under test and a Windows-based software application used to create and download test scripts to the device. You also can use the software application to configure and control the device across an Ethernet or USB link.

InFusion test scripts are called Scenarios. Scenarios determine how the hardware device monitors and modifies line traffic. In order to create and download Scenarios the Teledyne LeCroy Net Protocol Suite application must be used.

For the InFusion connections, the device is connected between the PHYs of the originator and responder.

6.3 Starting InFusion

To start the InFusion program for the first time, do the following:

1. Select **File** → **New Project** from the Main Net Protocol Suite Menu (see Figure 6.1). This brings up the Add Device to Project window. See Figure 6.2.

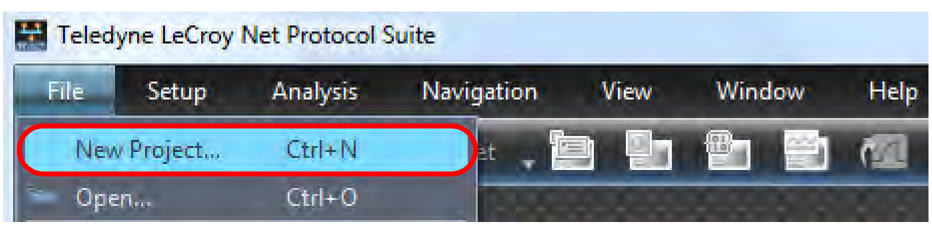


Figure 6.1: Starting InFusion

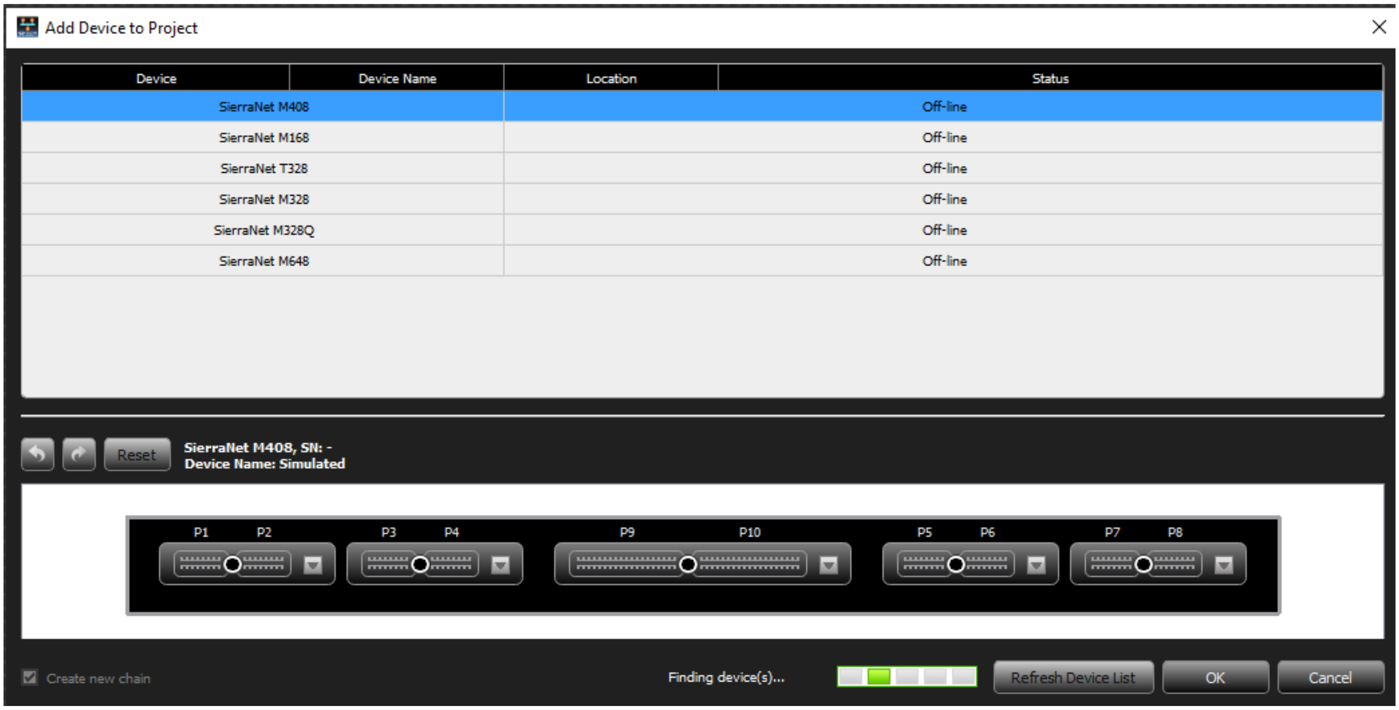


Figure 6.2: Add Device to Project

2. Select the Analyzer you plan on using (or the one you are connected to). In this example, the SierraNet M168 has been chosen.

NOTE: Although the figures show the SierraNetM408, the InFusion Scenario Manager works with all SierraNet Products including the M168/M328/M328Q and M648.

6.3.1 Selecting the Configuration

1. Click the expansion icon  to the right of the port pair to view available configurations.

2. Select **Analyzer**, then click the radio button for the **Speed** you want (Figure 6.3).

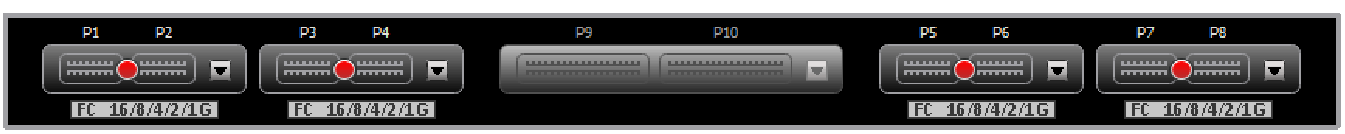


Figure 6.3: Analyzer Port Configurations

3. Continue to configure the available port pairs, then click **OK**.

4. Scroll through the list and select the AJA (FC) on Ports 1/2 and AJA (FC) on Ports 5/6.

   This configuration allows you to analyze and jam data traffic coming into and out of the analyzer on both Ports 1/2 and Ports 5/6. It also assumes you are targeting Fibre Channel devices.

5. Click **OK**. The Add Device to Project dialog returns with the selected configuration. See Figure 6.4.

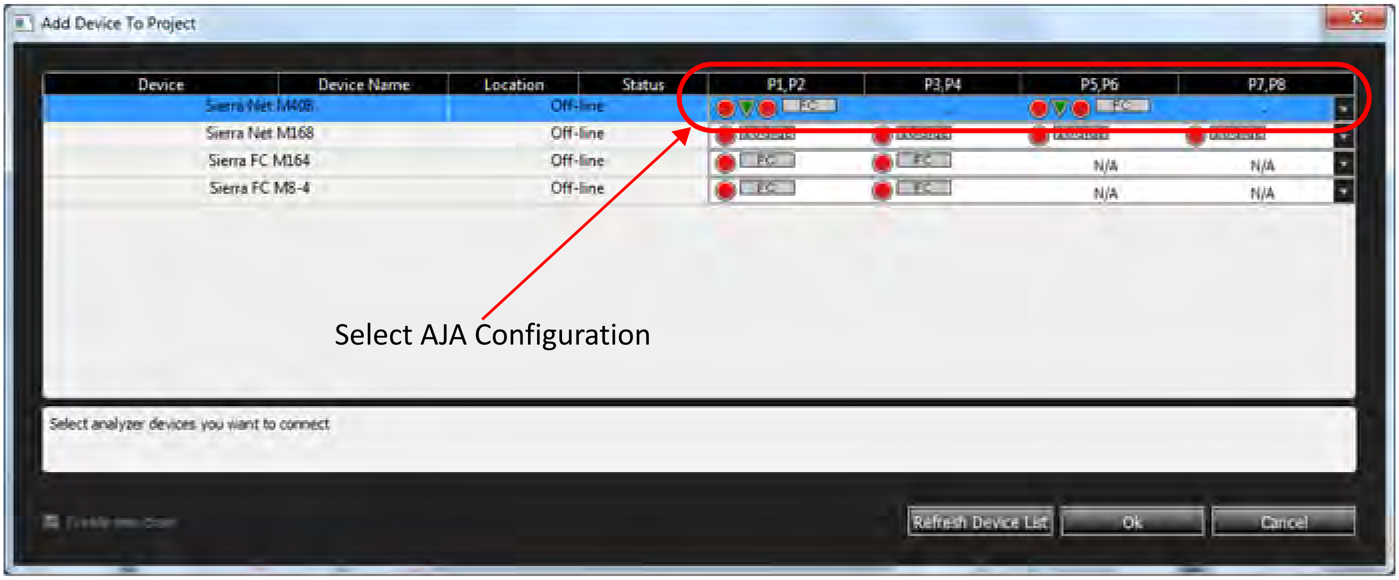


Figure 6.4: Add Device to Project Dialog with Configuration Selected

---

NOTE: You can select only one Jammer port at a time when using the AJA configuration

---

6. To record traffic from other ports after the InFusion modifies (jams) them, select a combination of ports that have **Jammer/Analyzer** specified. The different configurations accommodate different possible user setups and requirements.

6.3.2 Bidirectional Jammer and Analyzer Operations

A Jammer intercepts and delays traffic on both directions simultaneously, so Originator sends to Jammer, Jammer delays and sends to Responder, Responder sends to Jammer, Jammer delays and sends to Originator.

For the SierraNet M408 40GbE Jammer and the SierraNet M328 Jammer, a single scenario can be configured to modify traffic on both directions of the link simultaneously.

However, on the SierraNet M408 10GbE/16GFC Jammer and the SierraNet M168 Jammer, a single scenario can modify traffic only in one direction at a time. For information on bidirectional jamming operation on these platforms, see *, AJAJ – Bidirectional Jamming Operation* .

6.3.3 Selection/Creation of an InFusion Scenario

Click **OK** in the “Add Device to Project” window. The Main Net Suite Protocol Menu appears with the Configuration you selected on the display. See Figure 6.5.

Figure 6.5: Main Net Suite Protocol Dialog with Chosen Configuration

A closer look at the configuration dialog is shown in Figure 6.6.

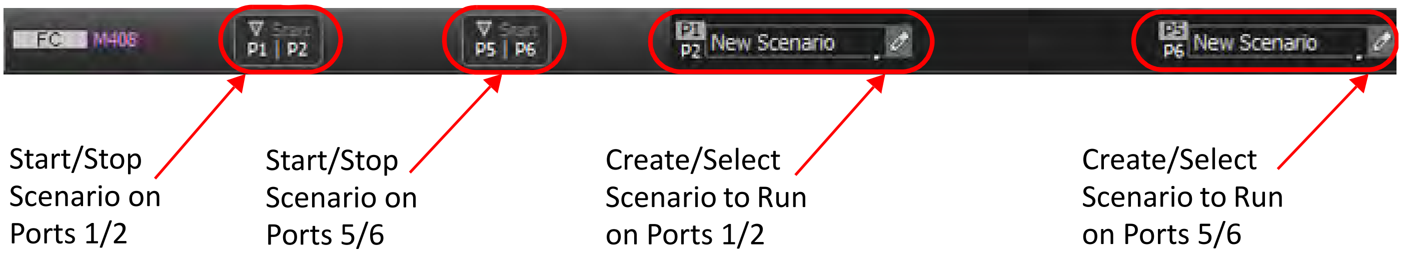
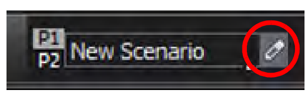


Figure 6.6: InFusion Control Interface Menu

Now we can start building an InFusion Scenario, which once completed, can then be used to generate traffic to drive and see the responses of the devices under test (DUTs).

6.4 Generating an InFusion Scenario

Click the New Scenario 

icon to display the Infusion Scenario Manager dialog.

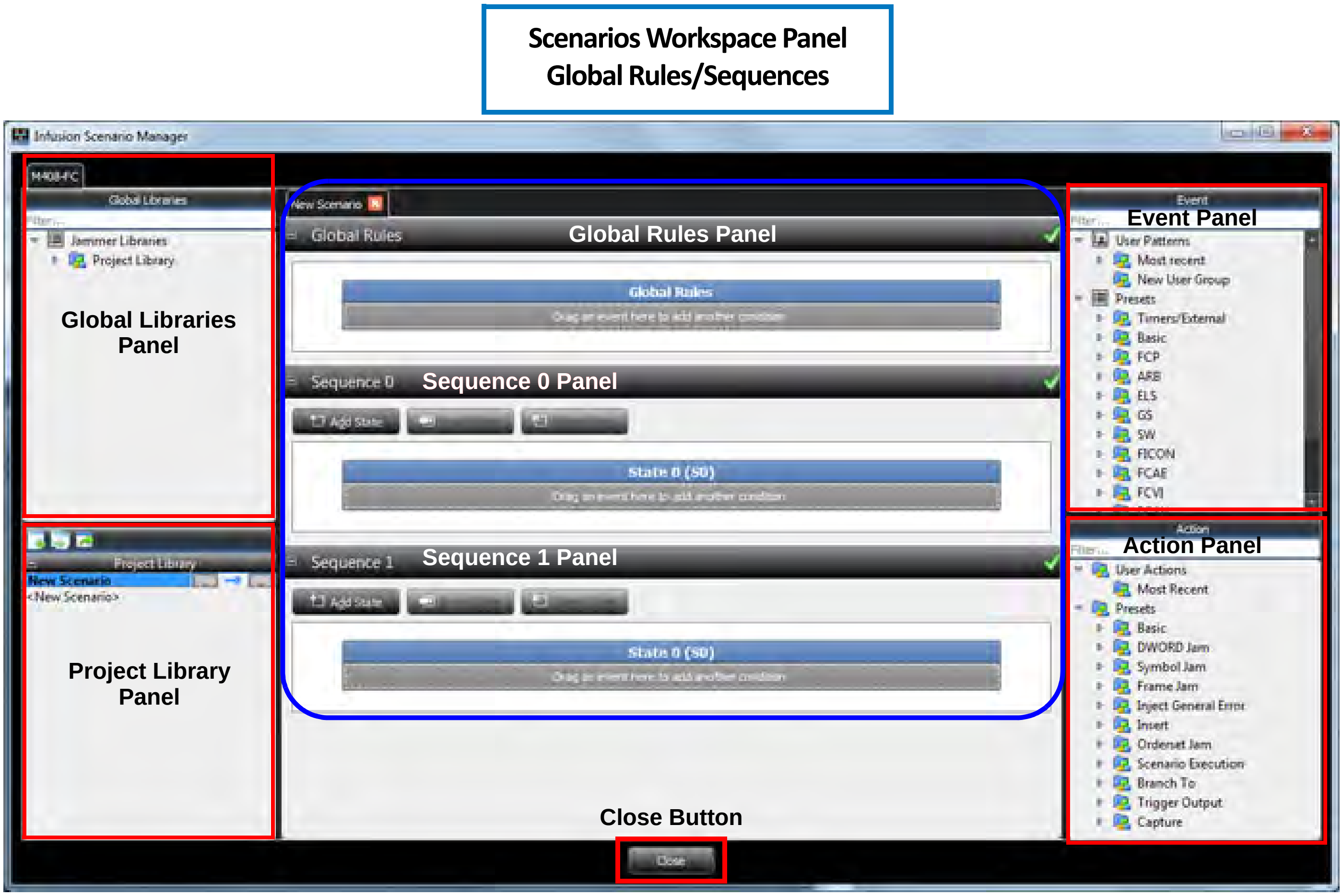


Figure 6.7: InFusion Windows

The InFusion Scenario Manager includes the following sections:

- Global Libraries Panel; see *6.4.1, Global Libraries Panel*.
- Project Library Panel; see *6.4.2, Project Library Panel*.
- Event Panel; see *6.4.3, Event Panel*.
- Action Panel; see “Action Panel” on page 441.
- Scenario Elements (Global Rules/Sequence 0/Sequence 1); see *6.4.5, Scenarios Workspace Panel*.
- Close Button (click on Close Button to Exit the InFusion Scenario Manager)

6.4.1 Global Libraries Panel

The Main Library window (on the left), which displays the available Scenarios. You can create a New Scenario, Open Containing Folder, Copy Container Folder Path, Add New Library, Rename Library or Remove Library. The scenarios saved on a specific platform in the Global Library are available in all projects for the same platform.

Right-click inside the Global Libraries Panel at the Scenario Level to do the following:

- Cut a Scenario
- Copy a Scenario
- Paste a Scenario
- Delete a Scenario
- Rename a Scenario
- Sort Scenarios
- Sort All Scenarios
- Export Scenarios to a File
- Import Scenarios from a File

See Figure 6.8.

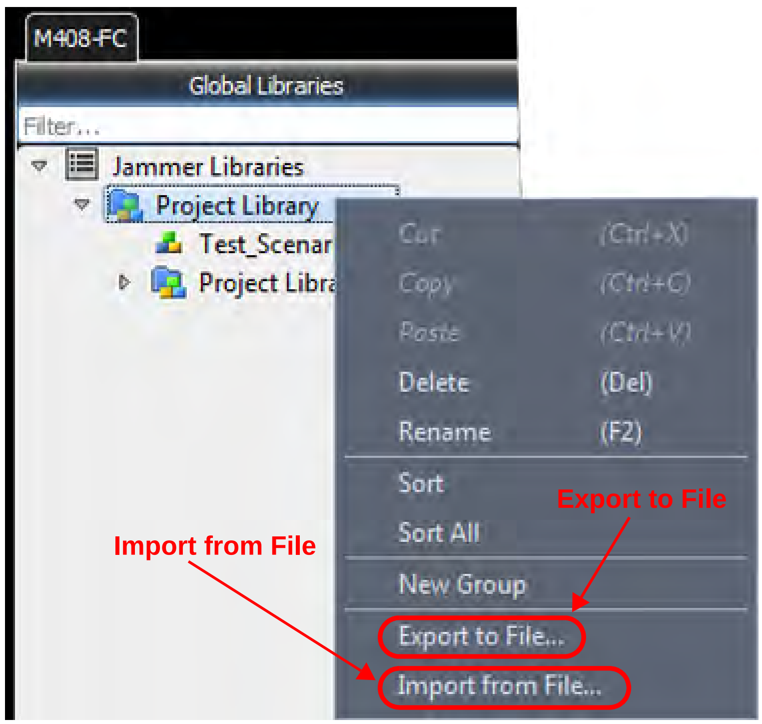


Figure 6.8: Operations Available from Global Libraries Panel

If you select “Export to File”, the window shown in (Figure 6.9) will appear. This allows you to navigate to the Project folder where you can export your Project Library to a File.

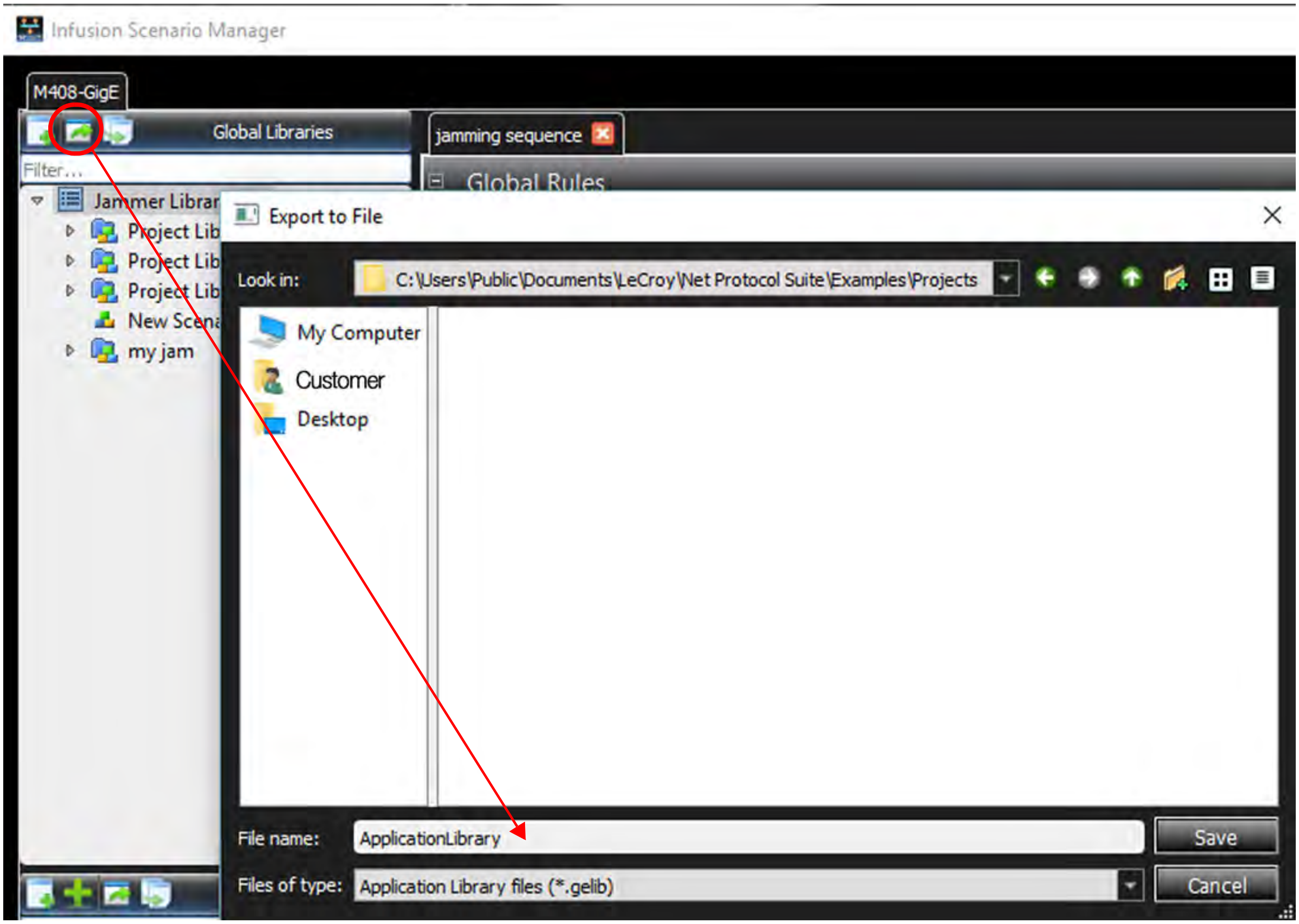


Figure 6.9: Export Jammer Library to a File

You can also Export a Scenario to a File. See Figure 6.10.

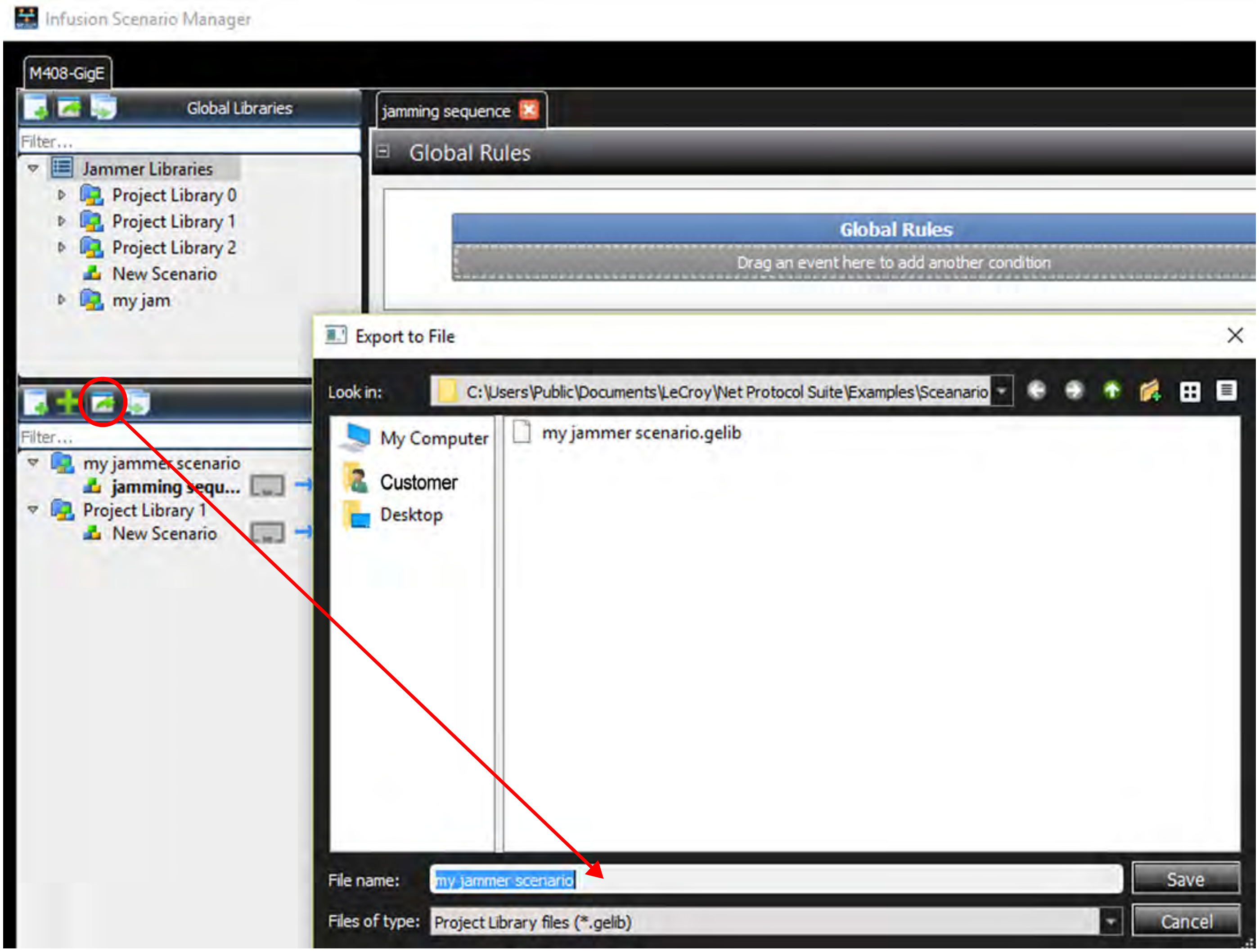


Figure 6.10: Export Jammer Sequence to File

You can also Import Libraries and Scenarios from a File. See Figure 6.11 and Figure 6.12.

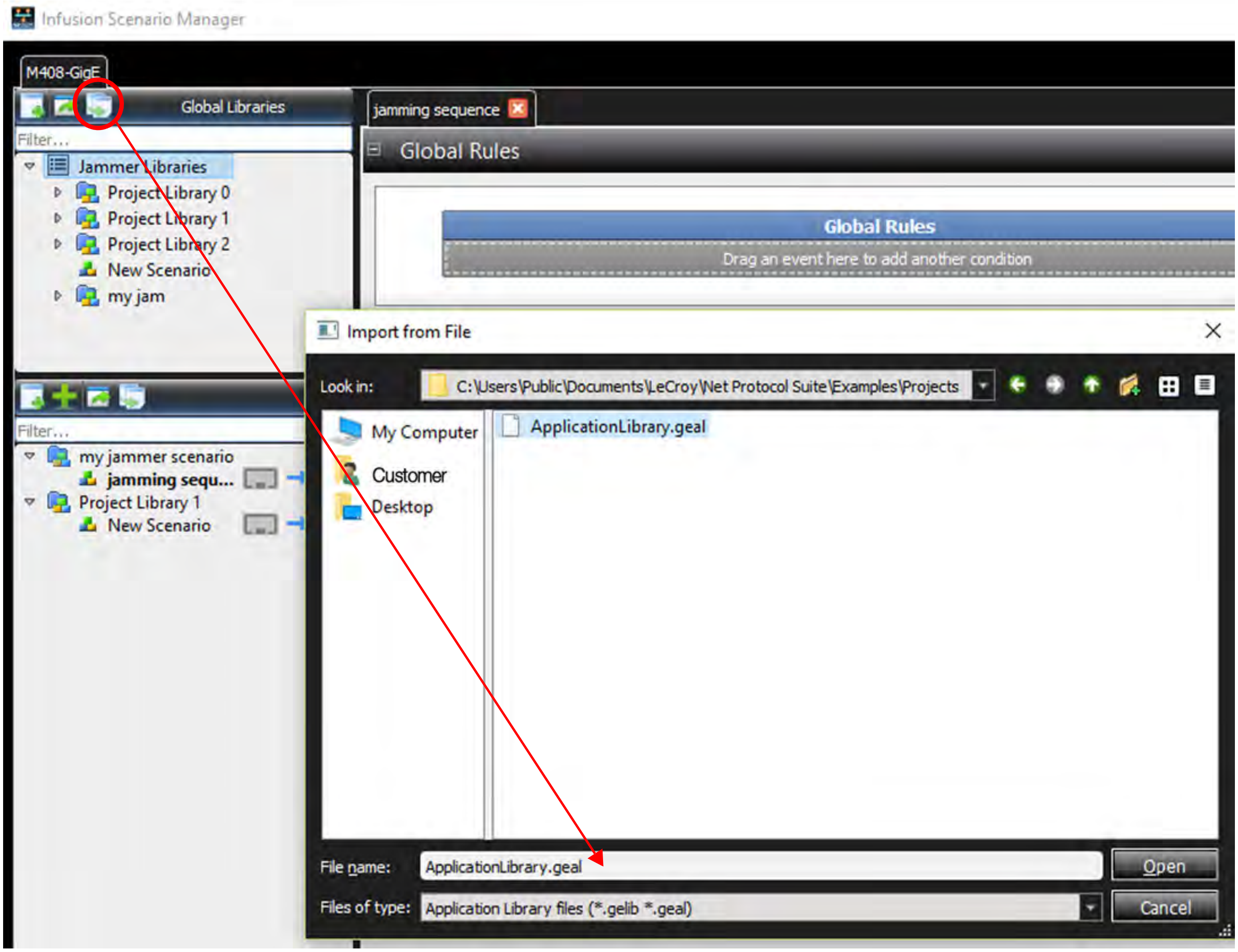


Figure 6.11: Import Jammer Library from File

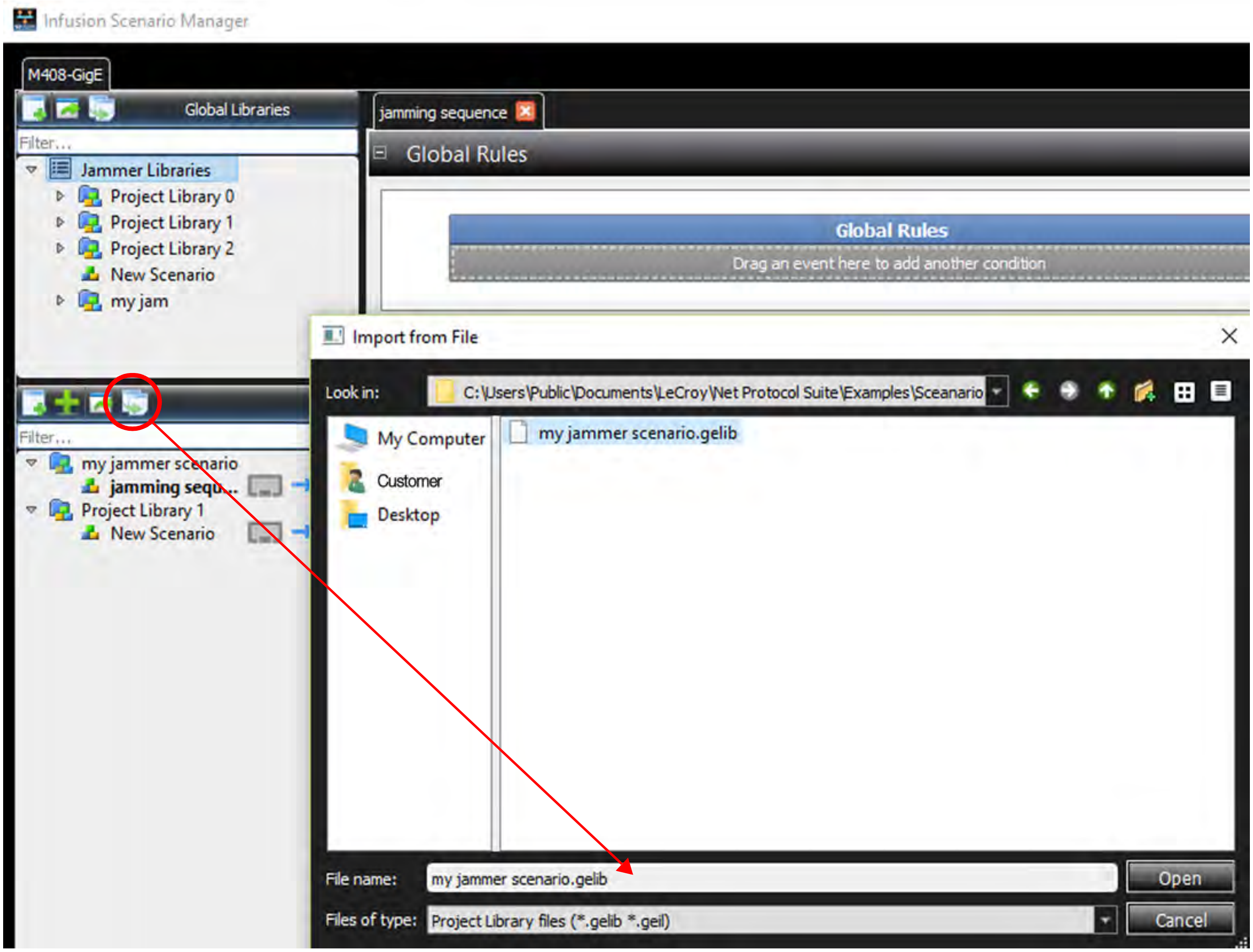


Figure 6.12: Import Sequence from File

6.4.2 Project Library Panel

The Project Library window (on the left) displays the project libraries. The scenarios saved in the Project Library are only available for the current project.

In the Project Libraries Panel at the Scenario Level (with a Right Click) you can:

- Cut a Library
- Copy a Library
- Delete a Library
- Rename a Library
- Add a New Library
- Export a Library

See Figure 6.13.

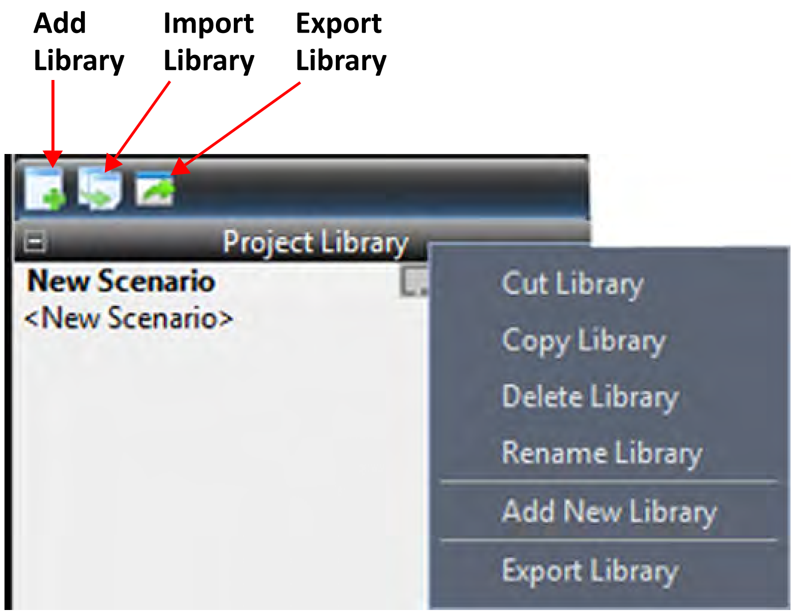


Figure 6.13: Operations Available from Project Library

6.4.2.1 Add New Library

Selecting the Add New Library Icon will produce a new Project Library (see Figure 6.14).

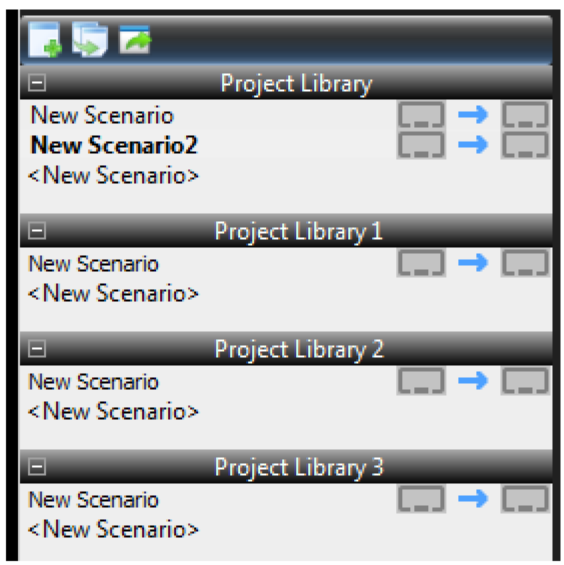


Figure 6.14: Add New Library Icon

6.4.2.2 Import Library

Click the **Import Library** icon. The window shown in Figure 6.15 appears.

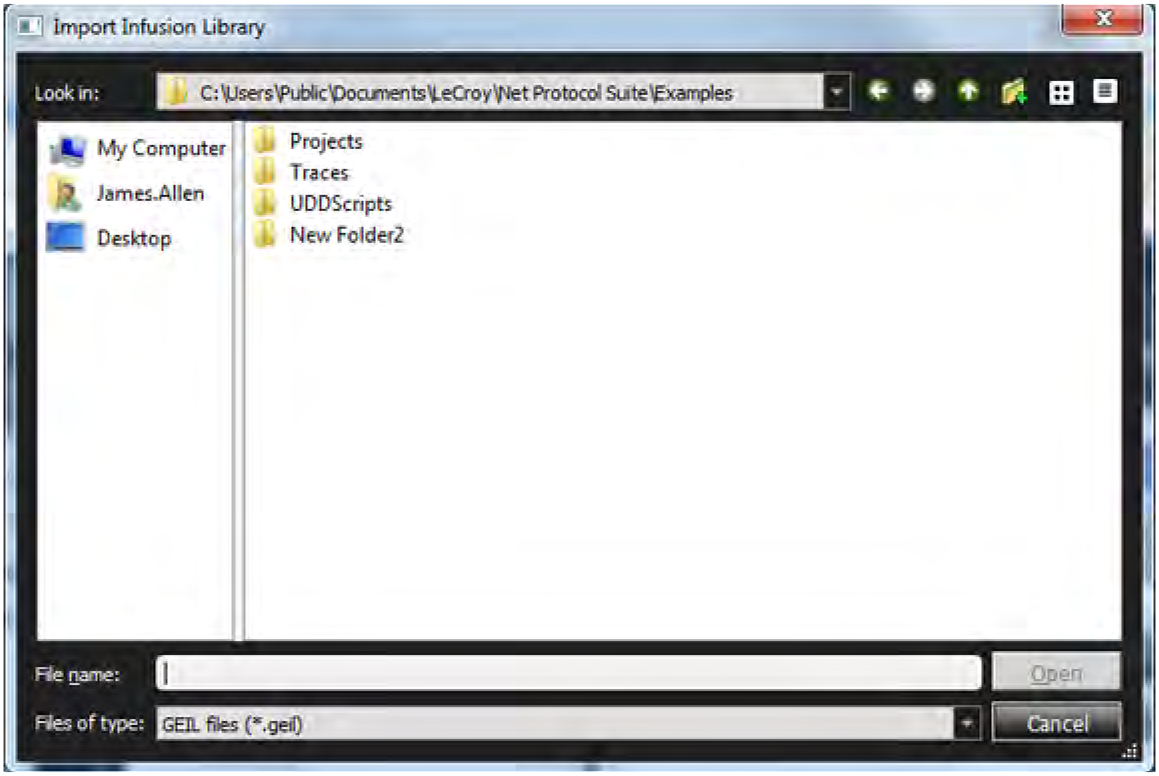


Figure 6.15: Import InFusion Library Dialog

6.4.2.3 Export InFusion Library

1. Click the **Export Library** icon to view the Project Library menu. Use this to choose a library to Export. See Figure 6.16.

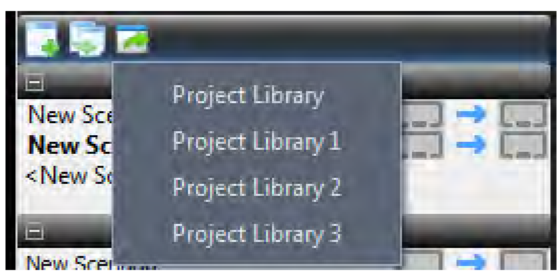


Figure 6.16: Export InFusion Library Icon

2. Select the **Project Library** you need. A window containing the contents of the selected library appears (Figure 6.17).

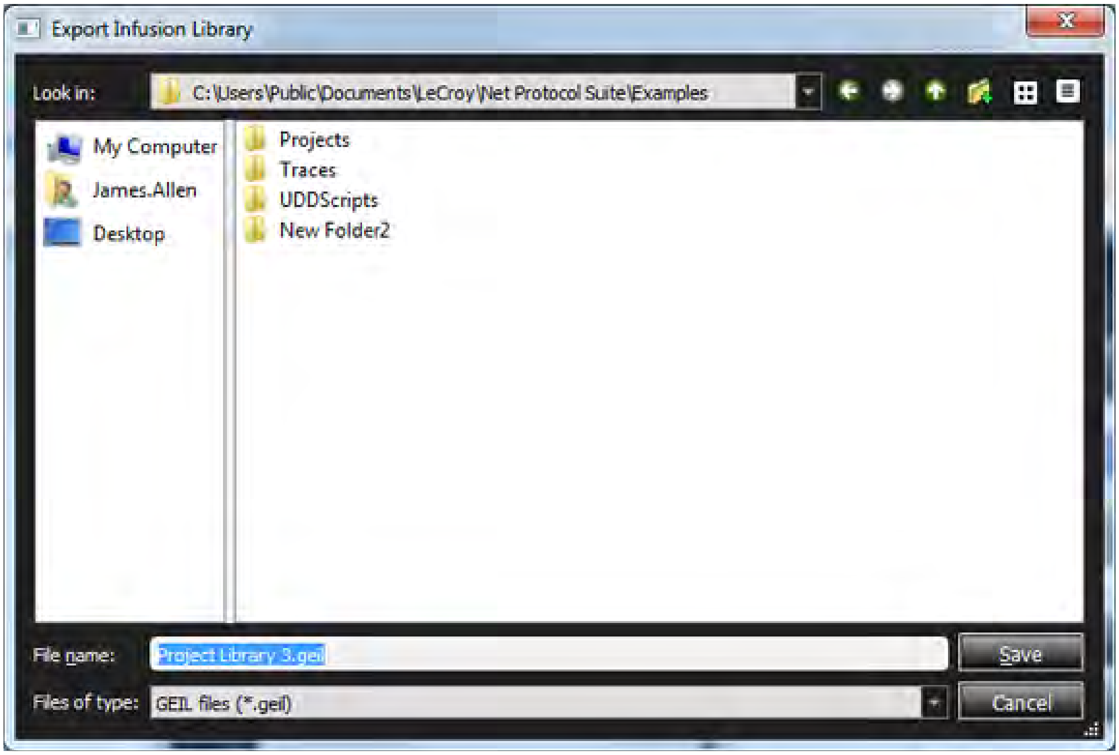


Figure 6.17: Select a Project Library to Export

3. Choose the **Projects Folder**, then click **Save**. The selected Project Library is stored under the Projects Folder (Figure 6.18).

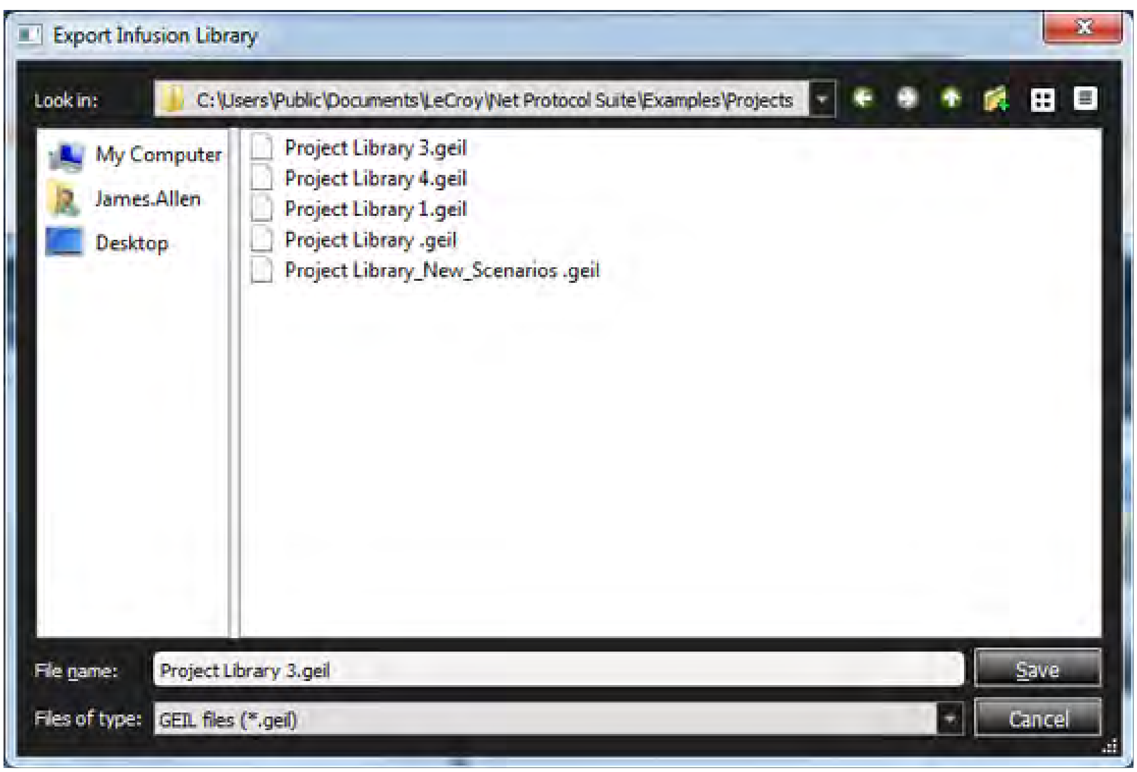
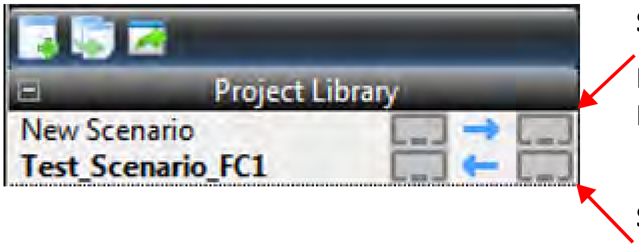


Figure 6.18: Exported Project InFusion Library in Project Folder

6.4.2.4 Scenario Traffic Modification Direction

You can select the Scenario Traffic Direction in the Project Library Panel. See Figure 6.19



Scenario Traffic Modification Direction

From Lower Port Numbers to Higher Port Numbers

Scenario Traffic Modification Direction

From Higher Port Numbers to Lower Port Numbers

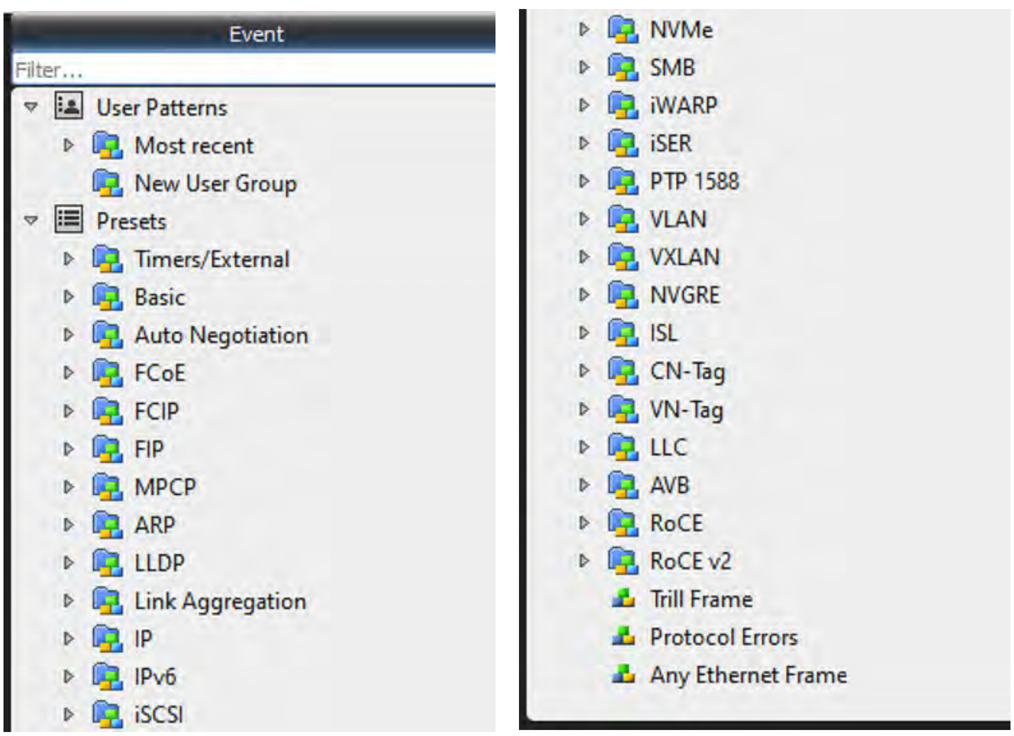
Figure 6.19: Scenario Traffic Direction

NOTE: The Scenario Traffic Modification Direction sets the direction in which traffic may be modified for the Scenario. If you define an Event with a direction property that doesn't match the Scenario Traffic Modification Direction the system will pop up a Warning message to change the direction of traffic of the event.

6.4.3 Event Panel

Lists all the available events to be used in the Scenarios Workspace.

6.4.3.1 Ethernet Events



Top of Events List **Bottom of Events List**

Figure 6.20: Ethernet Events

Table 6.1 describes the Presets that can be used as FCoE (Ethernet) Events. See 6.5.4, *Available Resources* for details.

NOTE: You can have multiple Events and Actions in Global Rules and in each State.

TABLE 6.1: Events & Their Descriptions (Ethernet) (Sheet 1 of 5)

Event	Description
User Patterns	
Most Recent	Lists the most recent Events.
New User Group	Lists the new user groups.
Presets	
Timers/External	
Timer	The Event occurs when the timer expires.
Other Trigs	Analyzer: the Event occurs when the Analyzer triggers. External: the Event occurs when the external Trigger In is asserted.
Basic	
Basic Link Service	Refer to Section 4.2.5.2, *Basic Link Service*.
Link Control Frame	Refer to *Link Control Frame* in Chapter 4.
Link Speed	The Event occurs when the link is at the specified speed.
Both Linkup	The Event occurs when both ports are out of electric idle.
DWORD Reuse	Refer to Section 6.5.7, *Using Captured Data DWORDs*.
DWORD Matcher	Refer to Section 6.5.8, *DWORD Matcher*.
Training Sequence	**Inject Error on Control**: Generates Manchester Coding violation on Control field bits corresponding to the defined mask: One means violation, and zero means no error. **Inject Error on Status**: Generates Manchester Coding violation on Status field bits corresponding to the defined mask: One means violation, and zero means no error. **Frame Marker Error**: Generates training sequence with an invalid frame marker. **Recode Manchester Coding**: Forces jammer to recalculate Manchester Coding for each bit of training frame.
Auto Negotiation	
Auto Negotiation (Any)	Refer to , *Auto Negotiation*
Auto Negotiation IEEE.std 802.3	Refer to , *Auto Negotiation*.
Auto Negotiation OUI Tagged Formatted Next Page	Refer to , *Auto Negotiation*.
Auto Negotiation OUI Tagged Unformatted Next Page	Refer to , *Auto Negotiation*.

TABLE 6.1: Events & Their Descriptions (Ethernet) (Sheet 2 of 5)

Event	Description
Auto Negotiation Null Message Page	Refer to , *Auto Negotiation*.
Auto Negotiation OUI Tag Code Message Page	Refer to , *Auto Negotiation*.
Auto Negotiation PHY ID Tag Message Page	Refer to , *Auto Negotiation*.
Auto Negotiation EEE Technology Message Page	Refer to , *Auto Negotiation*.
Auto Negotiation Any Message Page	Refer to , *Auto Negotiation*.
FCP	
FCP SCSI Command	Refer to *FCP Patterns* in Chapter 4.
FCP Frame Information Unit	Refer to *FCP Patterns* in Chapter 4.
SCSI Command Status	Refer to *SCSI* under *FCP Patterns* in Chapter 4.
FCP Task Management	Refer to *FCP Task Management* in Chapter 4.
ELS	
Extended Link Service – Request	Refer to *ELS Patterns* in Chapter 4.
Extended Link Service – Request, Reply	Refer to *ELS Patterns* in Chapter 4.
Extended Link Service – Reply	Refer to *ELS Patterns* in Chapter 4.
GS	
Generic Link Service – Request	Refer to *Generic Link Service-Request* in Chapter 4.
Generic Link Service – Request, Reply	Refer to *GS Reply* in Chapter 4.
Generic Link Service – Reply	Refer to *GS Reply* in Chapter 4.
SW	
Switch Internal Link – Request	Refer to *SW Request* in Chapter 4.
Switch Internal Link – Request, Reply	Refer to *SW Request* in Chapter 4.
Switch Internal Link – Reply	Refer to *SW Request* in Chapter 4.
FICON	
FICON (Any Data Information Block Type)	Refer to *FICON Patterns* in Chapter 4.
FICON (Data)	Refer to *FICON Patterns* in Chapter 4.
FICON (Command)	Refer to *FICON Patterns* in Chapter 4.
FICON (Status)	Refer to *FICON Patterns* in Chapter 4.
FICON (Control)	Refer to *FICON Patterns* in Chapter 4.
FICON (Command-Data)	Refer to *FICON Patterns* in Chapter 4.
FICON (Link-Control)	Refer to *FICON Patterns* in Chapter 4.
FCAE 1553	

TABLE 6.1: Events & Their Descriptions (Ethernet) (Sheet 3 of 5)

Event	Description
FCAE – ASM	Refer to *FCAE_ASM* in Chapter 4.
FCAE 1553 (Any)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Data)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Command)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Status)	Refer to *FCAE-1553* in Chapter 4.
FCVI	
FCVI(Any)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(SEND_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(WRITE_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(READ_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(SEND_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(WRITE_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(READ_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(DISCONNECT_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP1)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP2)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP3)	Refer to *FCVI Patterns* in Chapter 4.
FCVI (DISCONNECT_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCAV	
FCAV(Simple)	Refer to *FCVI Patterns* in Chapter 4.
FCAV(Extended)	Refer to *FCVI Patterns* in Chapter 4.
VSAN	
Basic	
VSAN-Basic Link Service	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Link Control Frame	Refer to *VSAN Patterns* in Chapter 4.
FCP	
VSAN-FCP SCSI Command	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCP Frame Information Unit	Refer to *VSAN Patterns* in Chapter 4.
VSAN-SCSI Command Status	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCP Task Management	Refer to *VSAN Patterns* in Chapter 4.
ARB	
VSAN-ARB Loop Initialization	Refer to *VSAN Patterns* in Chapter 4.
ELS	
VSAN-Extended Link Service-Request	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Extended Link Service-Reply	Refer to *VSAN Patterns* in Chapter 4.

TABLE 6.1: Events & Their Descriptions (Ethernet) (Sheet 4 of 5)

Event	Description
GS	
VSAN-Generic Link Service-Request	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Generic Link Service-Reply	Refer to *VSAN Patterns* in Chapter 4.
SW	
VSAN-Switch Internal Link-Request	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Switch Internal Link-Reply	Refer to *VSAN Patterns* in Chapter 4.
FICON	
VSAN-FICON (Any Data Information Block Type)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Command)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Status)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Control)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Command-Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Link-Control)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE-ASM	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553	
VSAN-FCAE 1553 (Any)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Command)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Status)	Refer to *VSAN Patterns* in Chapter 4.
FCVI	
VSAN-FCVI(Any)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(SEND_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(WRITE_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(READ_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(SEND_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(WRITE_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(READ_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(DISCONNECT_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP1)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP2)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP3)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(DISCONNECT_RESP)	Refer to *VSAN Patterns* in Chapter 4.
FCAV	
VSAN-FCAV(Simple)	Refer to *VSAN Patterns* in Chapter 4.

TABLE 6.1: Events & Their Descriptions (Ethernet) (Sheet 5 of 5)

Event	Description
VSAN-FCAV(Extended)	Refer to *VSAN Patterns* in Chapter 4.
FIP	Refer to 4.2.4.4, *FIP Patterns*.
MPCP	Refer to 4.2.4.5, *MPCP Pattern*.
Address Resolution Protocol	Refer to Section 4.2.4.6, *Address Resolution Protocol Pattern*.
Link Layer Discovery Protocol	Refer to Section 4.2.4.7, *Link Layer Discovery Protocol Pattern*.
Internet Protocol	Refer to Section 4.2.4.8, *Internet Protocol Pattern.*
iSCSI	Refer to Section 4.2.4.9, *iSCSI Pattern.*
iWARP	Refer to Section 4.2.4.10, *iWARP Patterns*
VLAN	Refer to Section 4.2.4.11, *VLAN Patterns.*
VXLAN	Refer to Section 4.2.4.12, *VXLAN Patterns*
ISL	Refer to Section 4.2.4.14, *ISL Patterns.*
CN-Tag	Refer to Section 4.2.4.15, *CN Tag Patterns.*
VN-Tag	Refer to Section 4.2.4.16, *VN Tag Patterns.*
LLC	Refer to Section 4.2.4.17, *LLC*.
InfiniBand	
RDMA	Refer to *InfiniBand Over Ethernet: RDMA and NVMe Triggers* in Chapter 4.
NVMe	Refer to *InfiniBand Over Ethernet: RDMA and NVMe Triggers* in Chapter 4.
Trill Frame	Refer to Section 4.2.4.19, *Trill Frame.*
Protocol Errors	Refer to Section 4.2.4.20, *Protocol Errors.*
Jammer Internal Triggers	Refer to Section 6.5.18, *Synch Jammer Scenarios with Jammer Internal Triggers*.

6.4.3.2 Fibre Channel Events

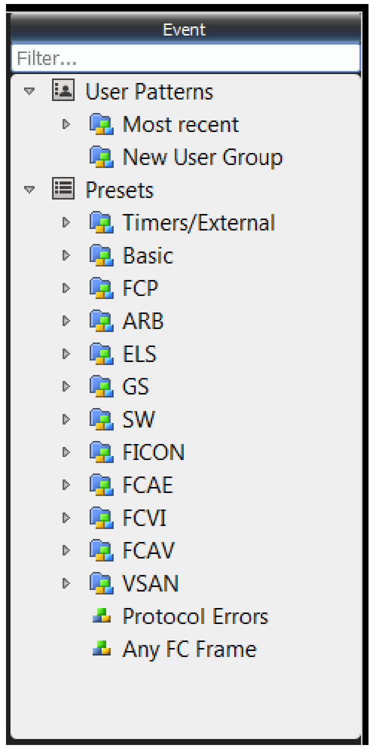


Figure 6.21: Fibre Channel (FC) Events

The following table (Table 6.2) describes the Presets that can be used as Fibre Channel (FC) Events.

TABLE 6.2: Events & Their Descriptions (FC) (Sheet 1 of 5)

Event	Description
User Patterns	
Most Recent	Lists the most recent Events.
New User Group	Lists the new user groups.
Presets	
Timers/External	
Timer	The Event occurs when the timer expires.
Other Trigs	Analyzer: the Event occurs when the Analyzer triggers. External: the Event occurs when the external Trigger In is asserted.
Basic	
Ordered Set	Refer to *Ordered Set* in Chapter 4.
Basic Link Service	Refer to 4.2.5.2, *Basic Link Service*.
Link Control Frame	Refer to *Link Control Frame* in Chapter 4.
Link Speed	The Event occurs when the link is at the specified speed.
Both Linkup	The Event occurs when both ports are out of electric idle.

TABLE 6.2: Events & Their Descriptions (FC) (Sheet 2 of 5)

Event	Description
Training Sequence	**Inject Error on Control**: Generates Manchester Coding violation on Control field bits corresponding to the defined mask: One means violation, and zero means no error. **Inject Error on Status**: Generates Manchester Coding violation on Status field bits corresponding to the defined mask: One means violation, and zero means no error. **Frame Marker Error**: Generates training sequence with an invalid frame marker. **Recode Manchester Coding**: Forces jammer to recalculate Manchester Coding for each bit of training frame. Refer to *Training Sequence* in Chapter 4.
FCP	
FCP SCSI Command	Refer to *SCSI* in Chapter 4.
FCP Frame Information Unit	Refer to *FCP Task Management* in Chapter 4.
SCSI Command Status	Refer to *SCSI* in Chapter 4.
FCP Task Management	Refer to *FCP Task Management* in Chapter 4.
ELS	
Extended Link Service – Request	Refer to *ELS Patterns* in Chapter 4.
Extended Link Service – Request, Reply	Refer to *ELS Patterns* in Chapter 4.
Extended Link Service – Reply	Refer to *ELS Patterns* in Chapter 4.
GS	
Generic Link Service – Request	Refer to *Generic Link Service-Request* in Chapter 4.
Generic Link Service – Request, Reply	Refer to *GS Reply* in Chapter 4.
Generic Link Service – Reply	Refer to *GS Reply* in Chapter 4.
SW	
Switch Internal Link – Request	Refer to *SW Request* in Chapter 4.
Switch Internal Link – Request, Reply	Refer to *SW Reply* in Chapter 4.
Switch Internal Link – Reply	Refer to *SW Reply* in Chapter 4.
FICON	
FICON (Any Data Information Block Type)	Refer to *FICON Patterns* in Chapter 4.
FICON (Data)	Refer to *FICON Patterns* in Chapter 4.
FICON (Command)	Refer to *FICON Patterns* in Chapter 4.
FICON (Status)	Refer to *FICON Patterns* in Chapter 4.
FICON (Control)	Refer to *FICON Patterns* in Chapter 4.
FICON (Command-Data)	Refer to *FICON Patterns* in Chapter 4.
FICON (Link-Control)	Refer to *FICON Patterns* in Chapter 4.

TABLE 6.2: Events & Their Descriptions (FC) (Sheet 3 of 5)

Event	Description
FCAE 1553	
FCAE – ASM	Refer to *FCAE_ASM* in Chapter 4.
FCAE 1553 (Any)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Data)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Command)	Refer to *FCAE-1553* in Chapter 4.
FCAE 1553 (Status)	Refer to *FCAE-1553* in Chapter 4.
FCVI	
FCVI(Any)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(SEND_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(WRITE_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(READ_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(SEND_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(WRITE_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(READ_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(DISCONNECT_RQST)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP1)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP2)	Refer to *FCVI Patterns* in Chapter 4.
FCVI(CONNECT_RESP3)	Refer to *FCVI Patterns* in Chapter 4.
FCVI (DISCONNECT_RESP)	Refer to *FCVI Patterns* in Chapter 4.
FCAV	
FCAV(Simple)	Refer to *FCAV Patterns* in Chapter 4.
FCAV(Extended)	Refer to *FCAV Patterns* in Chapter 4.
VSAN	
FCP	
VSAN-FCP SCSI Command	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCP Frame Information Unit	Refer to *VSAN Patterns* in Chapter 4.
VSAN-SCSI Command Status	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCP Task Management	Refer to *VSAN Patterns* in Chapter 4.
ARB	
VSAN-ARB Loop Initialization	Refer to *VSAN Patterns* in Chapter 4.
ELS	
VSAN-Extended Link Service-Request	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Extended Link Service-Reply	Refer to *VSAN Patterns* in Chapter 4.
GS	
VSAN-Generic Link Service-Request	Refer to *VSAN Patterns* in Chapter 4.

TABLE 6.2: Events & Their Descriptions (FC) (Sheet 4 of 5)

Event	Description
VSAN-Generic Link Service-Reply	Refer to *VSAN Patterns* in Chapter 4.
SW	
VSAN-Switch Internal Link-Request	Refer to *VSAN Patterns* in Chapter 4.
VSAN-Switch Internal Link-Reply	Refer to *VSAN Patterns* in Chapter 4.
FICON	
VSAN-FICON (Any Data Information Block Type)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Command)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Status)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Control)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Command-Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FICON (Link-Control)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE-ASM	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553	
VSAN-FCAE 1553 (Any)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Data)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Command)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAE 1553 (Status)	Refer to *VSAN Patterns* in Chapter 4.
FCVI	
VSAN-FCVI(Any)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(SEND_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(WRITE_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(READ_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(SEND_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(WRITE_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(READ_RESP)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(DISCONNECT_RQST)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP1)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP2)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(CONNECT_RESP3)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCVI(DISCONNECT_RESP)	Refer to *VSAN Patterns* in Chapter 4.
FCAV	
VSAN-FCAV(Simple)	Refer to *VSAN Patterns* in Chapter 4.
VSAN-FCAV(Extended)	Refer to *VSAN Patterns* in Chapter 4.
FIP	Refer to 4.2.4.4, *FIP Patterns*.

TABLE 6.2: Events & Their Descriptions (FC) (Sheet 5 of 5)

Event	Description
MPCP	Refer to Section 4.2.4.5, *MPCP Pattern*.
Address Resolution Protocol	Refer to Section 4.2.4.6, *Address Resolution Protocol Pattern*.
Link Layer Discovery Protocol	Refer to Section 4.2.4.7, *Link Layer Discovery Protocol Pattern*.
Internet Protocol	Refer to Section 4.2.4.8, *Internet Protocol Pattern*.
iSCSI	Refer to sections 4.2.4.9, *iSCSI Pattern* and *ISCSI Cmd* in Chapter 4.
VLAN	Refer to Section 4.2.4.11, *VLAN Patterns*.
ISL	Refer to Section 4.2.4.14, *ISL Patterns*.
CN-Tag	Refer to Section 4.2.4.15, *CN Tag Patterns*.
VN-Tag	Refer to Section 4.2.4.16, *VN Tag Patterns*.
Trill Frame	Refer to Section 4.2.4.19, *Trill Frame*.
Protocol Errors	Refer to Section 4.2.4.20, *Protocol Errors*.
Jammer Internal Triggers	Refer to Section 6.5.18, *Synch Jammer Scenarios with Jammer Internal Triggers*.

NOTE: You can specify additional Sequences and States. The application automatically checks for the maximum number of terms (sequences/states). When you exceed the limit, an error is flagged, prompting you to jump to the place that caused the error.

6.4.4 Action Panel

After you enter the set of Events for a test state, the menu-driven interface prompts you for the corresponding Action or set of Actions. If you define multiple Actions, the Actions occur simultaneously.

Lists all the available actions to be used in the Scenarios Workspace.

NOTE: The Actions displayed are dependent on the Events selected.

6.4.4.1 Actions in Simple Mode (Ethernet)

The following figure displays the options for a set of Actions in the Simple Mode (Ethernet). See Figure 6.22.

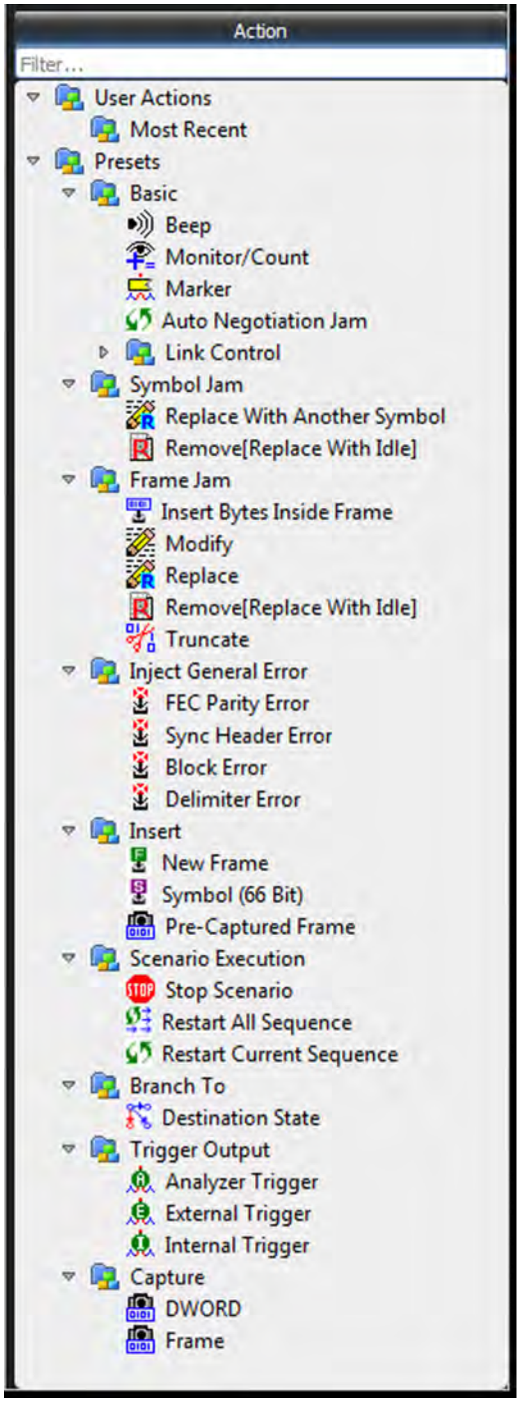


Figure 6.22: Ethernet Action Properties Dialog

6.4.4.2 Test State Actions in Simple Mode

The following table lists the supported Actions. Note that some of these Actions only apply to creating sequences.

TABLE 6.3: Test State Actions in Simple Mode (Sheet 1 of 3)

Action		Description
Basic	Beep	Emits audible sound of duration selectable via a drop-down list.
	Monitor Count	Opens a window to count the number of Events that occur during a session. A session is a time interval during which a Scenario runs.
	Auto Negotiation Jam	Opens a window to set Code Values, Code Settings and General parameters (Ethernet only).
	Link Control	Reconnect – Starts traffic pass-through immediately. This Action restarts traffic after a previous disconnect command. Once traffic is passing through, the originator and responder resume link bring up. Disconnect – Puts InFusion ports at electrical idle immediately. This action is only in effect while the scenario is running, and the Jammer will reconnect the line when the scenario is stopped.
		Reconnect/Disconnect can be applied in either direction separately: ◆ From P1/P3/P5/P7 direction: Reconnect/ Disconnect only the originator link. ◆ From P2/P4/P6/P8 direction: Reconnect/ Disconnect only the responder link. (See Figure 6.35.)
Symbol Jam	Replace with Another Symbol	Replaces the Symbol with the selected Symbol.
	Remove [Replace with Idle]	Removes the Symbol.
DWORD Jam	Replace DWORD	Replace DWORD (FC 16 only).

TABLE 6.3: Test State Actions in Simple Mode (Sheet 2 of 3)

Action		Description
Frame Jam	Insert Bytes Inside Frame	Allows to insert up to 60 Bytes inside the frame, at the specified offset or at the “current” DWORD, meaning the DWORD that caused the Event.
	Modify [Keep Length]	Allows to manipulate each DWORD in the header, with the selected Action (click on Pass though to get a drop-down list).
	Replace	Replaces the whole frame with the selected frame.
	Remove [Replace with IDLE]	Removes the whole frame.
	Truncate	Removes some of the payload, as specified in the Frame Length.
Inject General Error	Invalid 10-bit-Error Code	Injects invalid 10b code into the line (FC8 only).
	Running Disparity Error	Injects a Running Disparity (RD) error into traffic(FC8 only).
	FEC Parity Error	Injects a FEC error into traffic.
	Sync Header Error	Injects a Sync Header error into traffic.
	Block Error	Injects a Block error into traffic.
	Order Set Error	Injects a Order Set error into traffic, (Not available with 40GigE).
Insert	Insert New Frame	Allows to insert a whole frame as specified from the list of available frames.
	Symbol (66 Bit)	Allows to insert a Symbol 66 bits.
	Pre-captured Frame	Allows to insert a Pre-captured Frame (Ethernet only).
	Insert Bytes/ Ordersets	Allows to insert Bytes or Ordersets (FC 16 only). See 6.5.3, *Insert Byte/Orderset*.
Ordered Set Jam	Delete	Delete an Ordered Set Jam.
	Remove [Replace with IDLE]	Remove an Ordered Set Jam or Replace with another Ordered Set.
	Replace with Another Ordered Set	Only replace with another Ordered Set.
Scenario Execution	Stop Scenario	Stops the current Scenario. This Action should be the only Action in a State as it has higher priority over other Actions.
	Restart All Sequence	Restart all sequences in the Scenario.[1]
	Restart Current Sequence	Restart the sequence that contains this Action definition.[1]
Branch To	Destination State	Go to a state in this Sequence.[1]

TABLE 6.3: Test State Actions in Simple Mode (Sheet 3 of 3)

Action		Description
Trigger Output		Sends a signal out the trigger port to the device downstream.
	Analyzer Trigger	1. The Action is to send a trigger to the Analyzer. 2. The trigger point in the Analyzer that caused the analyzer trigger action will not be the selected event, it will be the selected event with some offset.
	External Trigger Output	The Action is to cause an external trigger output.
	Marker Trigger	Add a marker to captured data.
Capture	DWORD	Capture DWORD.
		Reuse of Captured DWORDs. (See 6.5.9, *Reusing Captured DWORDS in Events*.)
	Frame	Capture Frame (applies to both Ethernet and FC frames).

1. Only shown in Action Properties dialog box when creating a sequence.

Changes made in the gray area in the screen below when modifying events do not take effect and will not be jammed.

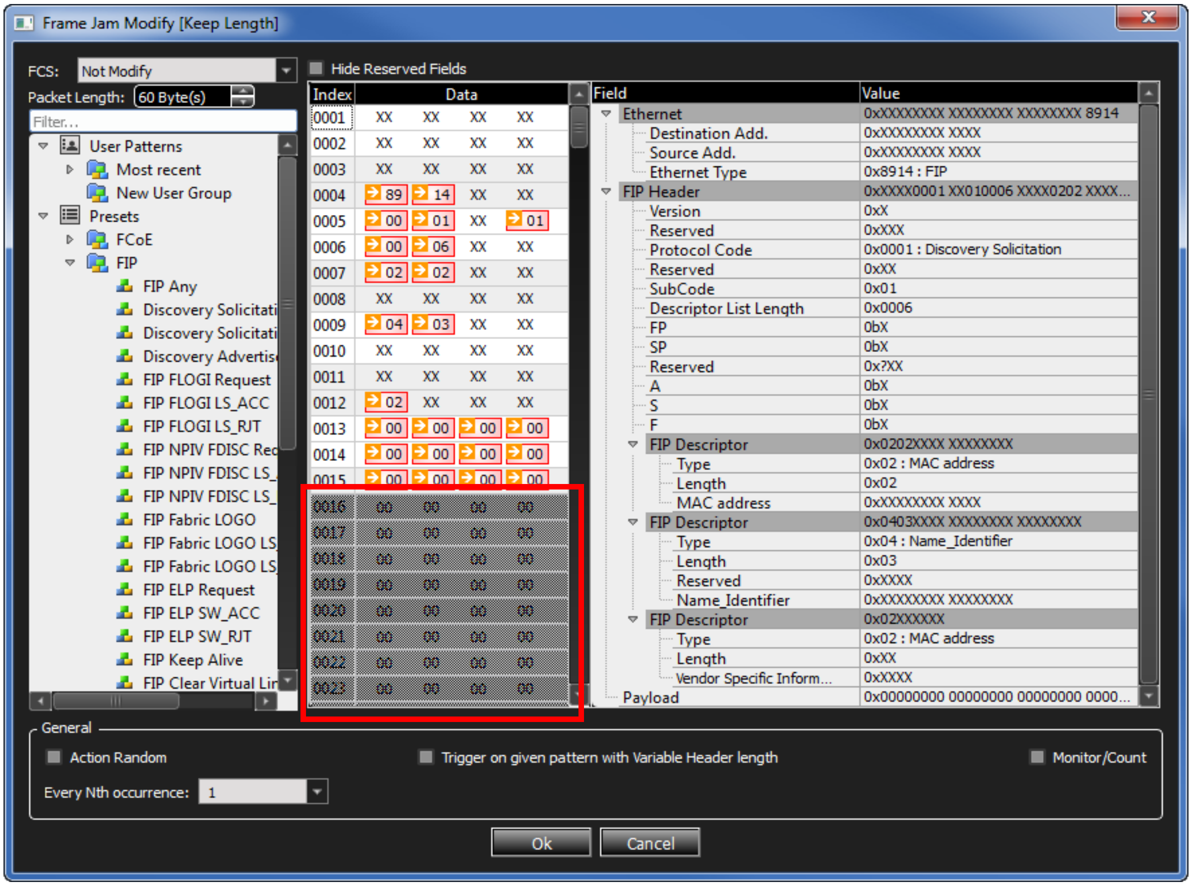


Figure 6.23: Frame Jam Action – Modify Dialog

6.4.4.3 Actions in Simple Mode – Fibre Channel (FC)

The following figure displays the options for a set of Actions in the Simple Mode (FC). See Figure 6.24.

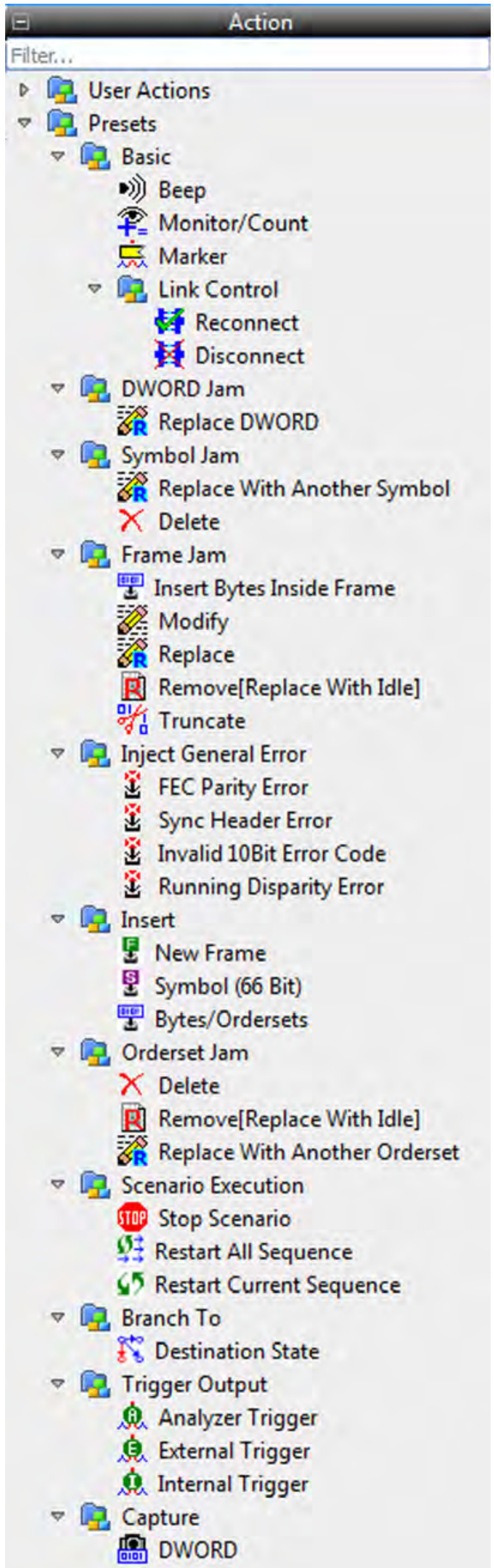


Figure 6.24: FC Action Properties Dialog

6.4.5 Scenarios Workspace Panel

This is the middle section of the Infusion Scenario Manager (Figure 6.7), where you will construct and manipulate the logic of the scenario by defining Events and Actions.

- You can drag and drop events in the Global Rules panel and assign actions to them.
- You can also drag and drop events into Sequence 0 or Sequence 1 states and assign actions to them.

6.4.5.1 Global Rules

Global Rules are a portion of the Scenario that can define only one test state. To create the Global Rules, you use the menu-driven interface to enter an Event or Combined Event and the corresponding Action or set of Actions (the response of InFusion hardware to the Event).

In the case of a Combined Event, the Action is taken upon occurrence of any of the Events stated for the Event combination. It is a logical OR association, meaning any of the Events can trigger the Action.

After you enter the Event or Combined Event, the interface prompts you for Actions. An Action might be, for example, injecting a particular ordered-set or error into the traffic stream. You can enter multiple Actions, which take place simultaneously. If one of the Actions is Stop Scenario, the other Actions will NOT be carried out. To stop the Scenario after the requested Actions have been carried out, you should branch to a new state which stops the Scenario.

After defining the Event and Actions within the Global Rules panel, you can save the Scenario and run it.

As an example, an NVMe Command is dragged over as the Event and a Modify Frame is dragged over as the Action. See Figure 6.25.

6.4.5.2 NVMe Command in Global Rules

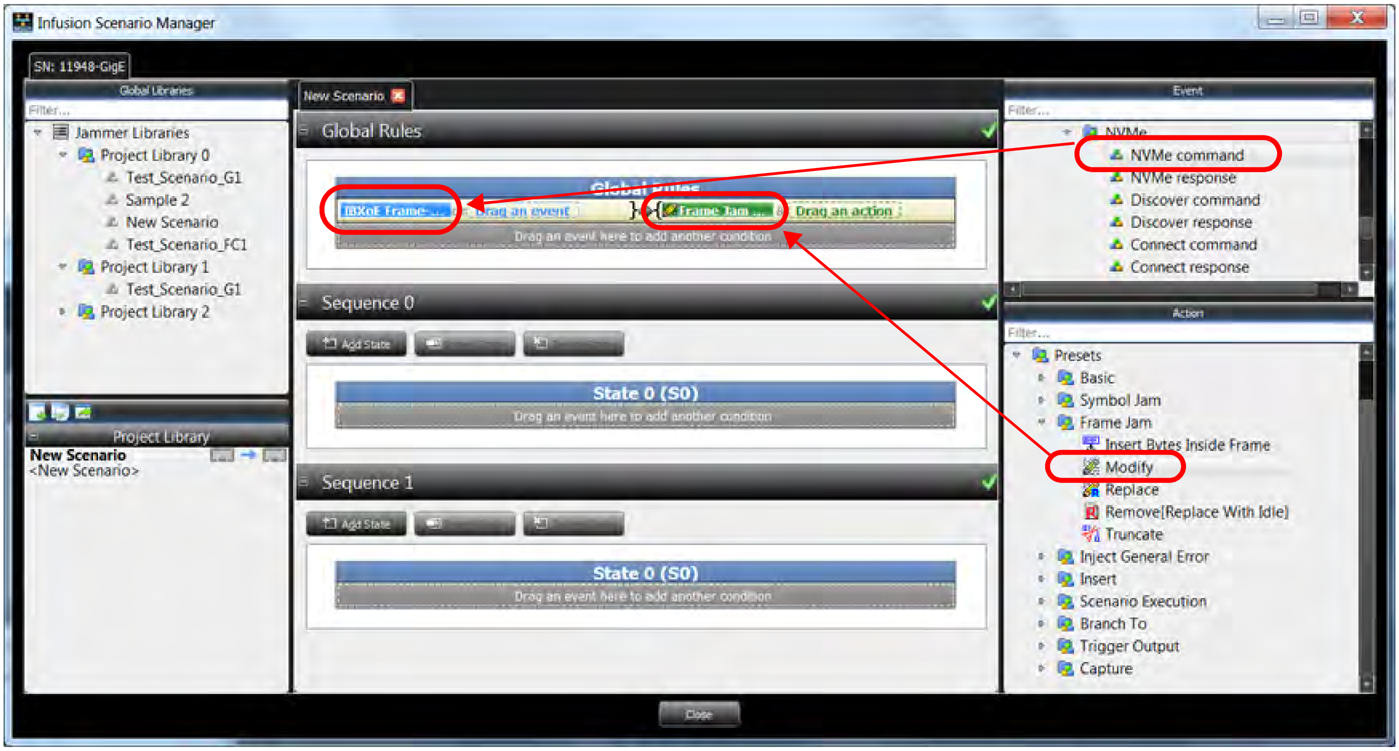


Figure 6.25: Global Rules Example – NVMe Command (Event) Frame Modify (Action)

A close up view of the Global Rules Event and Action shows more detail and the context windows that pop up. See Figure 6.26.

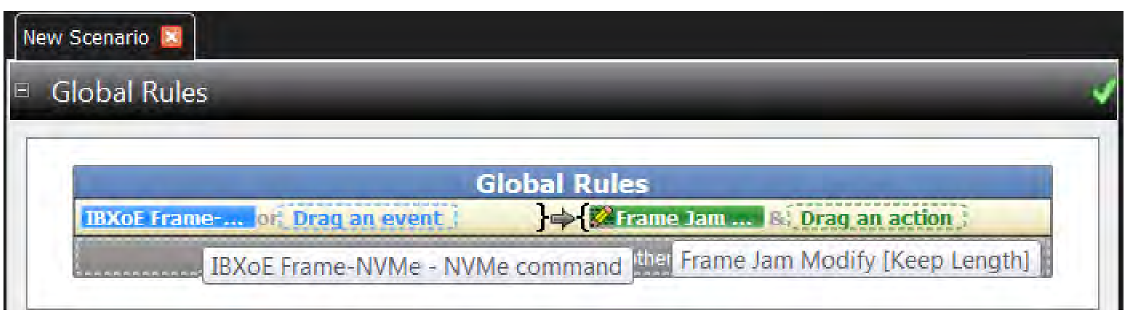


Figure 6.26: Global Rules – NVMe Command (Event) Frame Jam Modify (Action)

6.4.5.3 Sequences

The Global Rules are all you need for simple test Scenarios. However, a Scenario also can contain one or two sequences, which can define multiple states and allow branching between states. With a sequence, you also can do looping, which allows you to repeat a test state or to execute a test for a specified period of time.

As with Global Rules, the menu-driven interface guides you in building a sequence. Some of the prompts are different, however, because you now are encapsulating groups of Events and Actions as distinct states. Recall that a state is a combination of Events and Actions at a specific point in time. If the Event or Combined Event defined by a state occurs, the corresponding Action or set of Actions follows. You can enter multiple Actions, which take place simultaneously. If one of the

Actions is Stop Scenario, the other Actions are carried out. To stop the Scenario after the requested Actions have been carried out, you should branch to a new state that stops the Scenario.

InFusion hardware provides the capacity to have up to two sequences co-existing in a Scenario in addition to the Global Rules. Recall that both the Global Rules and any sequences are active at all times. Each is a separate “state machine,” having the behavior of a particular test state at any point in time. Because the Global Rules has the capacity for only one state, you can view it as a “degenerative state machine.”

6.4.5.4 Scenario Libraries

Libraries are repositories that hold Scenarios. This section describes the ways that you can manipulate Scenarios within Libraries.

Scenario Library Item Multi-Selection

The Scenario Library lists support conventional multi-selection via mouse-clicks and keyboard modifiers. The Copy Scenario item from the right-click context menu will operate on all selected items:

- Hold down the **Ctrl** key on the keyboard and click on items to toggle their selection state.
- Select a first item, then hold down the **Shift** key and select a second item; all items from the first item to the second item will be selected.

Global and Project Libraries

The scenarios saved in the Global Library are available to reuse for all projects. The scenarios saved in the Project Library are only available for the current project. You may transfer Scenarios between these libraries by drag-n-drop or copy/paste.

Adding Scenarios from Global to Project can only work if the protocol is similar, else it will be grayed out and unselectable.

Import/Export of Scenarios

Users can export a scenario (or multiple scenarios) to a file. Export is available via right click pop up menu. Scenarios can then be archived on your host machine’s hard drive.

There are two ways to import a library, if the user wants to import file into a existing library, they have to right click on the existing library and select import library. If the user wants to make a new library, there is an icon to import a library in library pane toolbar.

Creating InFusion Scenarios is easy, but it requires an understanding of the following terms defined in Table 6.4.

TABLE 6.4: Key Scenario Terms (Sheet 1 of 2)

Term	Definition
Action	InFusion response to an Event. See 6.4.4, *Action Panel*.
Event	Condition that is detectable by InFusion. See 6.4.4.1, *Actions in Simple Mode (Ethernet)*.
Combined Event	Logical OR association of Events (for example, Event A OR Event B).

TABLE 6.4: Key Scenario Terms (Sheet 2 of 2)

Term	Definition
Global Rules	Portion of a Scenario that can define a single InFusion test state. You can think of the Global Rules and each Sequence as a separate test routine or program operating within the Scenario. Each operates independently and in parallel with the others. The purpose of each is to detect Events and then respond with the appropriate Action or set of Actions. In essence, you can operate up to three test states simultaneously within InFusion – one is the Global Rules, and the other two are the 2 active states, one in each Sequence. See 6.5.10, *Traffic Modification Direction*.
Sequence	Portion of a Scenario that can define multiple InFusion test states. More flexible than the Global Rules, a Sequence allows more powerful Scenarios that include branching and looping between test states (Global Rules can define only a single test state, so there is no branching). See 6.4.5.3, *Sequences*.
State	“Behavior” of the Global Rules or a Sequence at any point in time. In terms of InFusion testing, behavior is “waiting” for a set of Events and responding with a set of Actions.

6.4.5.5 Add a State to a Sequence

Click **Add State** to drag and drop events in the Sequence 0 and Sequence 1 panels and assign actions to them.

If Actions are not assigned a yellow Caution message displays. If invalid actions are assigned then a red Warning icon displays. See Figure 6.27.

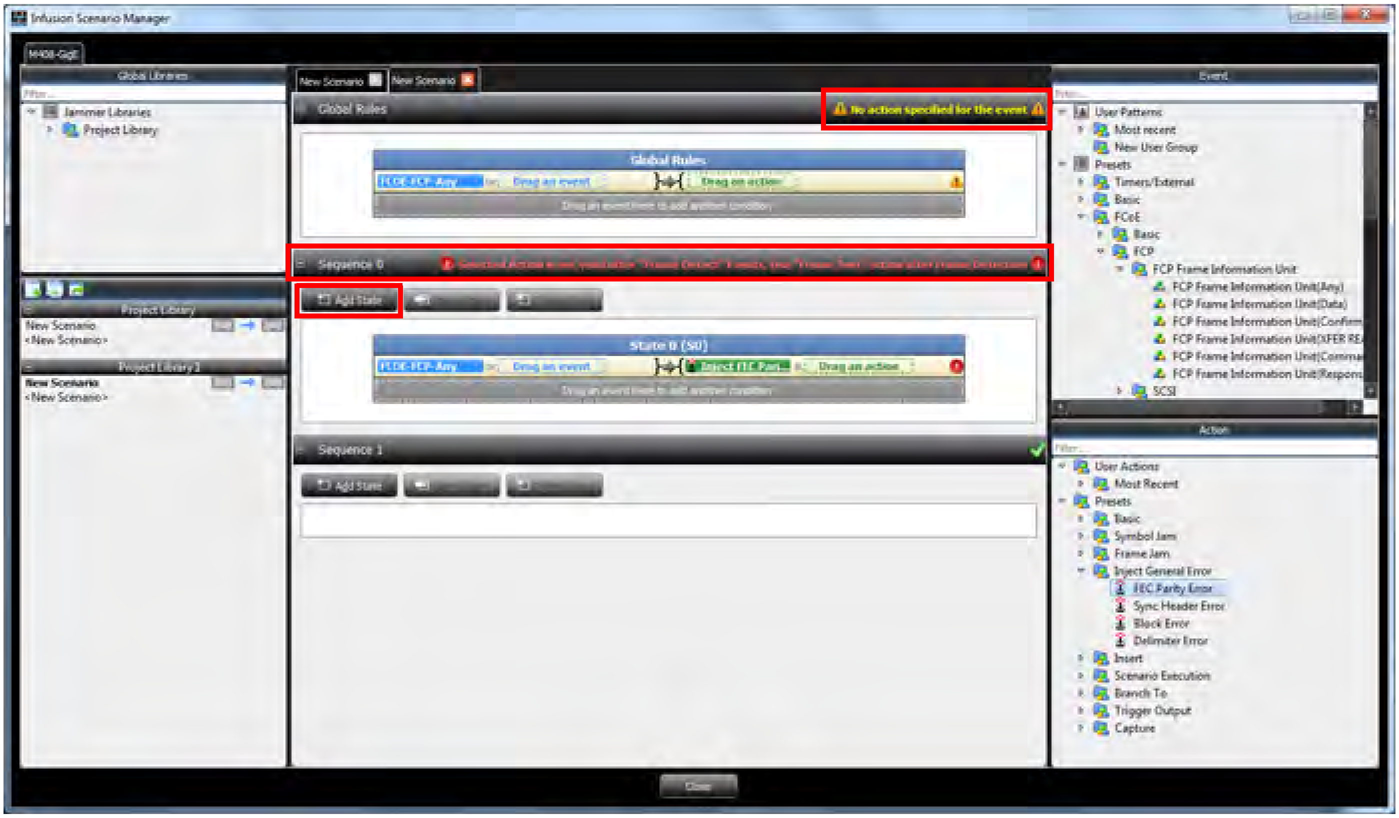


Figure 6.27: Add State InFusion Scenario Manager

NOTE: The Insert State command inserts a new state after the current state. Plan carefully while creating scenarios or you might have to insert a state after state 0, copy and paste from state 0 to the new state, and clear out state 0, in order to accomplish what “Insert State” does.

6.4.5.6 Global Rules and States

The Global Rules and States are part of the new Scenario.

1. Once the scenario is created, right-click the **New Scenario** tab and select **Rename** to name it in the Project Library panel.
2. Click the **Close** icon to save it in the Library for later use.

   All the Scenarios that are created are displayed in the Library panel. See Figure 6.28.

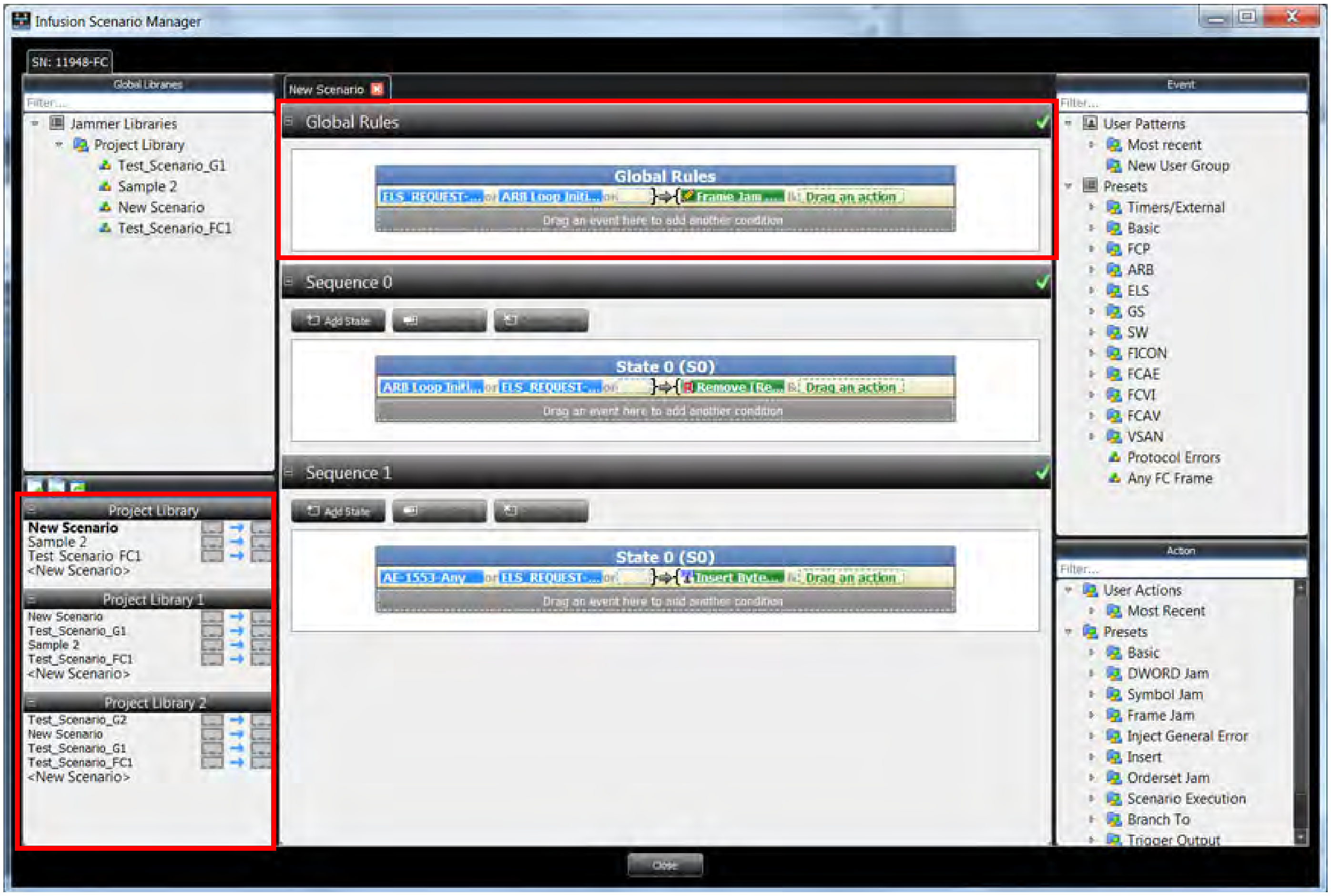


Figure 6.28: Global Rules and States InFusion Scenario Manager

6.4.5.7 Scenario and Event Data Traffic Directions Conflict

If the Scenario and Event Data Traffic directions conflict you will see the messages shown in Figure 6.29.

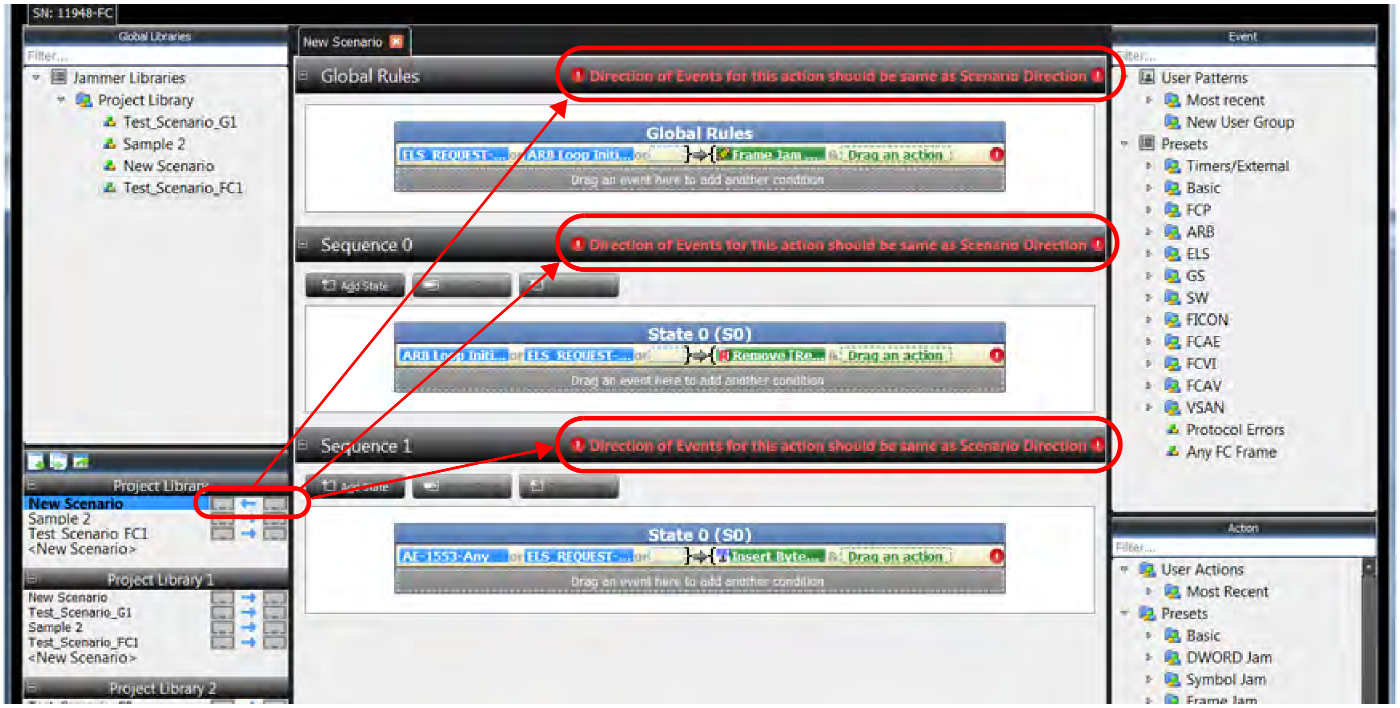


Figure 6.29: Scenario & Event Data Traffic Directions Conflict

6.4.6 Edit State Name

You can change a state name by doing the following:

1. Right-click inside the blue **State** box. The dialog box shown in Figure 6.30 appears.

Figure 6.30: Edit a State Label: Step 1

2. Select the **Edit State Label**. The State Label slides over to the left of the blue box where you can edit it (Figure 6.31).

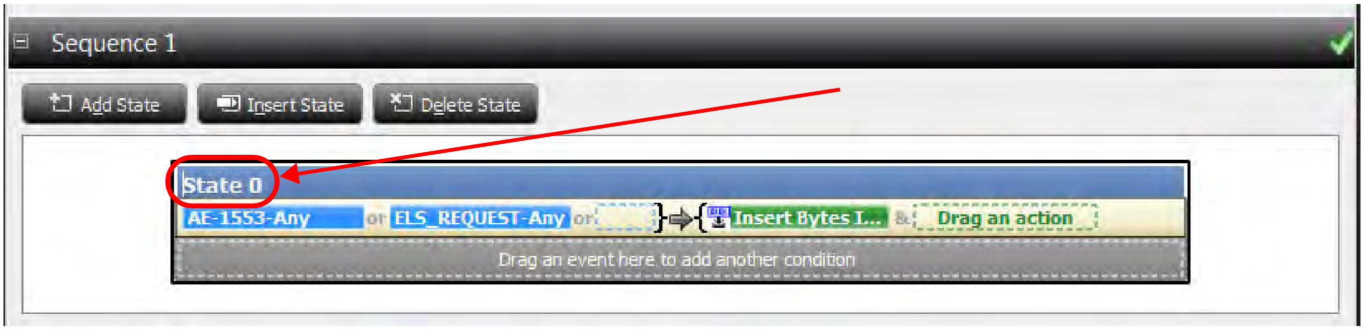


Figure 6.31: Edit a State Label: Step 2

Edit the State Label and then hit Return, the State will display the new name. (Figure 6.32).

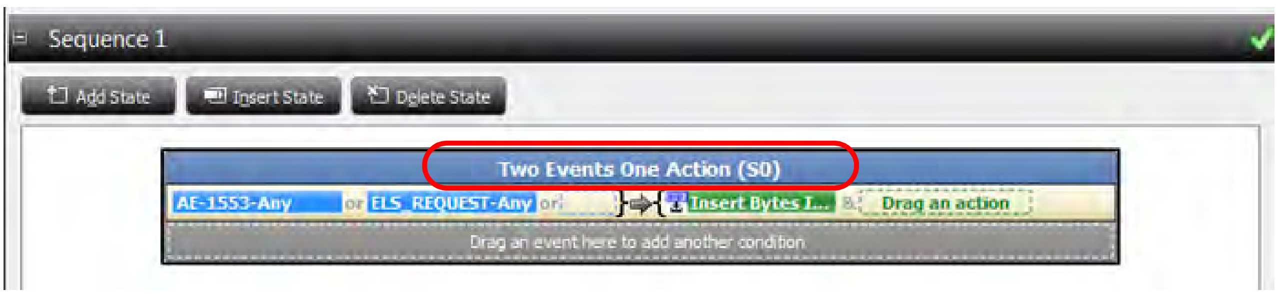


Figure 6.32: Edit a State Label – New Label Displayed

6.4.7 Copy State

To copy a State:

1. Right-click inside the blue **State** label box (Figure 6.33).

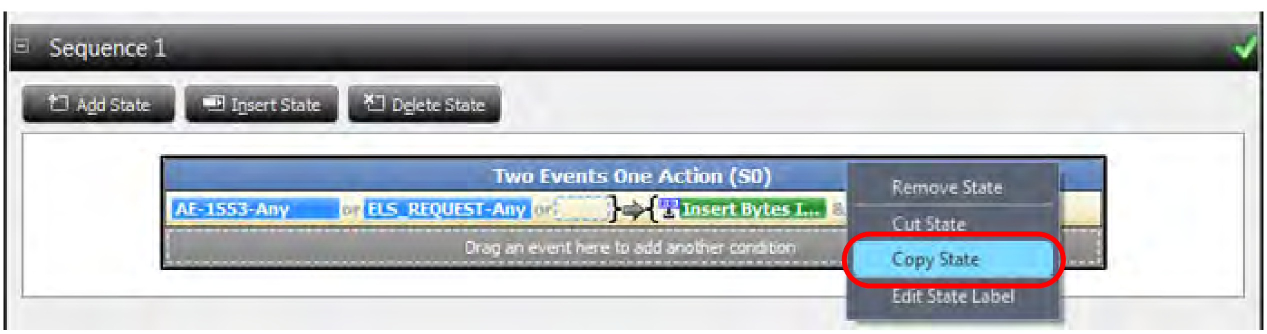


Figure 6.33: Copy State – Step 1

2. Select **Copy State**.
3. Right-click inside the white area below the current state. The Paste State option appears.
4. Release the mouse button. The new state appears below the current state (Figure 6.34).

Figure 6.34: New State

6.5 Event and Action Examples

6.5.1 Jam Details

- **Jam Event**: To set a Jam Event, drag an Event to the Global Rules or Sequence panel. The Events and their descriptions are listed in Table 6.1 (Ethernet) and Table 6.2 (FC).
- **Jam Action**: To set a Jam Action, drag an Action to the Global Rules or Sequence panel. See Table on page 461.

After the first Jam Action has been specified, you can set a consequent Jam Action by dragging more Actions to the **Drag an Event here to add another condition** area. The Jam Actions and their descriptions are listed in Table 6.5.

6.5.2 Reconnect Menu for Selecting Direction

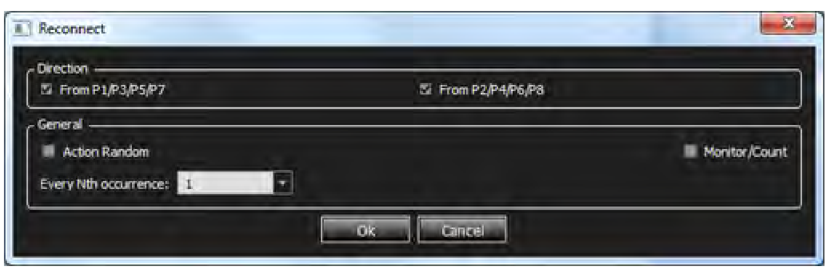


Figure 6.35: Reconnect Menu for Selecting Direction

6.5.3 Insert Byte/Orderset

If you select Insert Byte/Orderset, you can select and drag the icon to the Scenario window and substitute an Ordered Set for a Byte. See Figure 6.36.

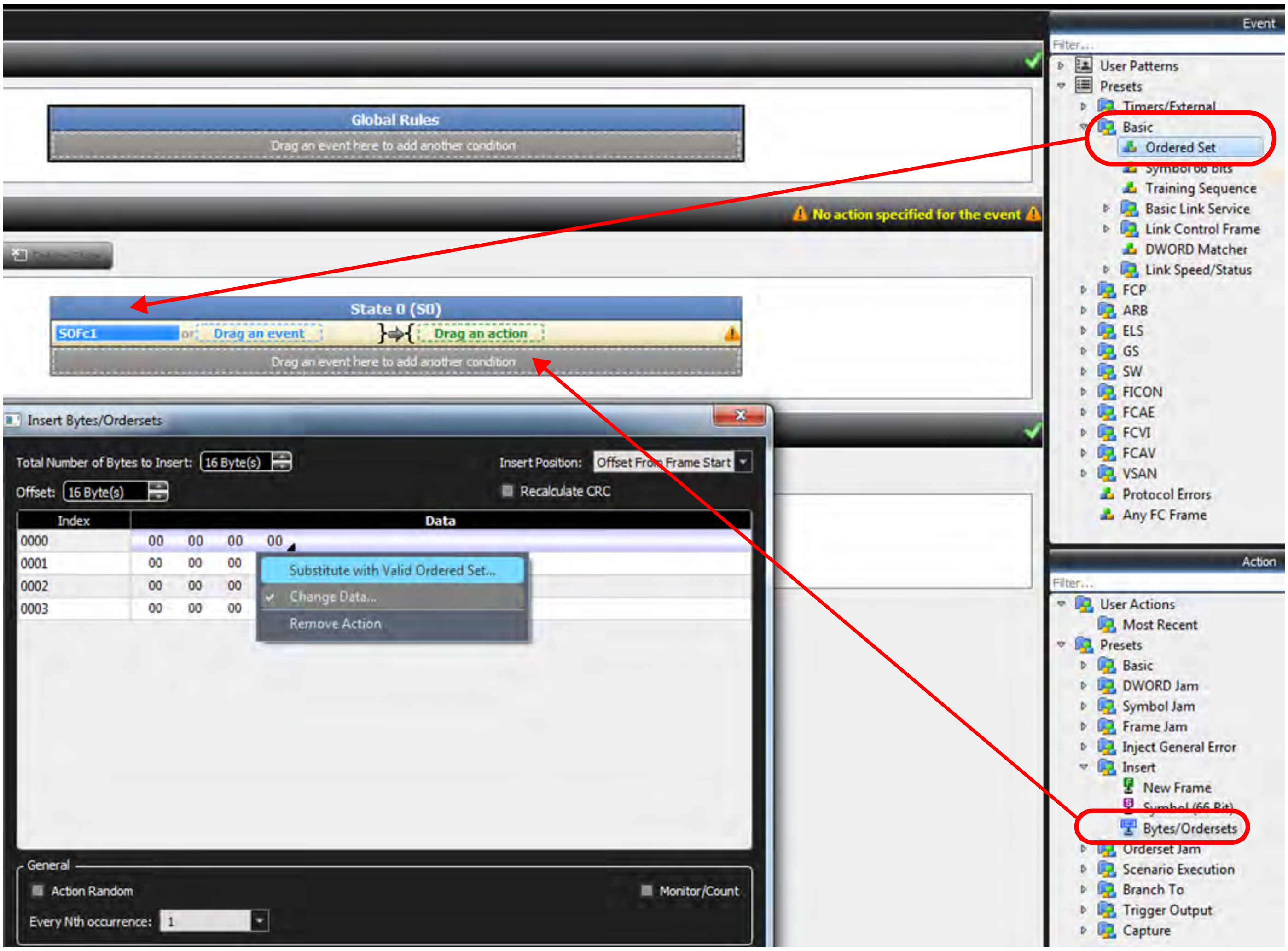


Figure 6.36: Jammer Scenario – Insert Ordered Set

You can now define the Ordered Set (Figure 6.37).

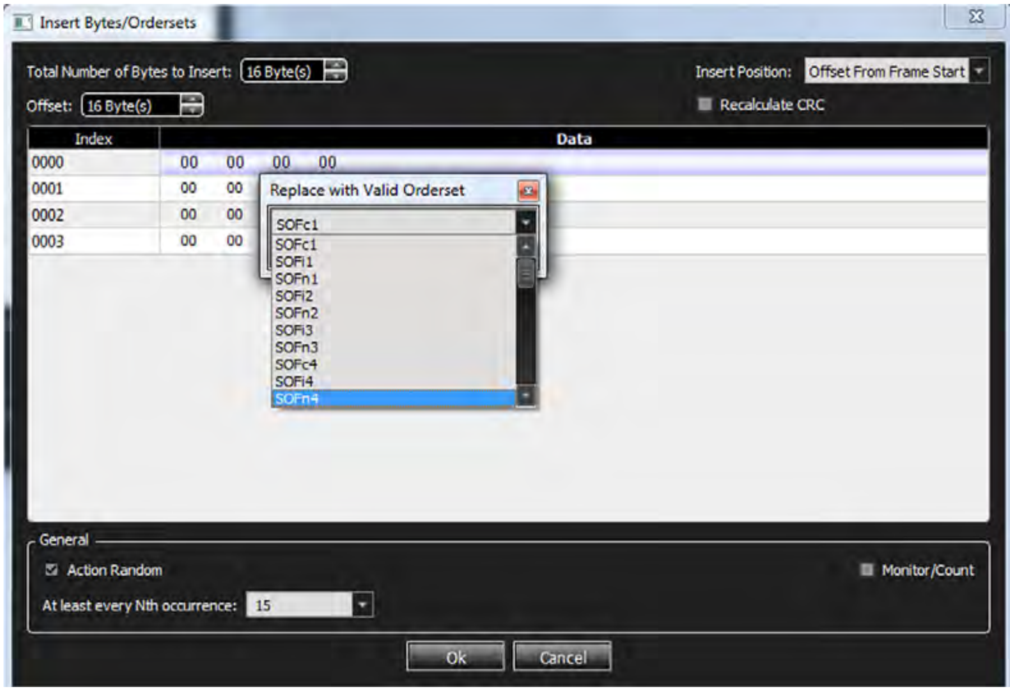


Figure 6.37: Defining the Ordered Set

You can insert as many Ordered Sets as you have bytes defined. See Figure 6.38.

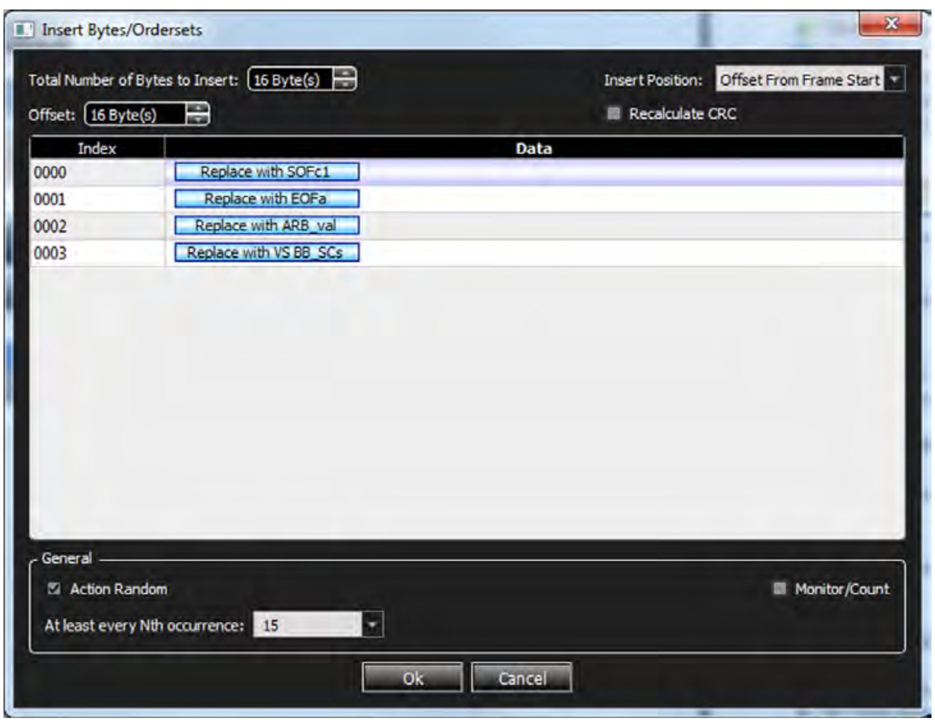


Figure 6.38: Ordered Sets Defined (Replacing Bytes)

Now you can insert the defined Ordered Sets into the Jammer Scenario.

Figure 6.39: Insert Bytes/Orderset Added to State 0 Actions

The following table lists the supported Actions. Note that some of these Actions only apply to creating sequences.

TABLE 6.5: Test State Actions in Simple Mode (Sheet 1 of 3)

Action		Description
Basic	Beep	Emits audible sound of duration selectable via a drop-down list.
	Monitor Count	Opens a window to count the number of Events that occur during a session. A session is a time interval during which a Scenario runs.
	Link Control	Reconnect – starts traffic pass-through immediately. This Action restarts traffic after a previous disconnect command. Once traffic is passing through, the originator and responder resume link bring up. Disconnect – puts InFusion ports at electrical idle immediately. This action is only in effect while the scenario is running, and the Jammer will reconnect the line when the scenario is stopped.
		Reconnect/Disconnect can be applied in either direction separately: From P1/P3/P5/P7 direction: Reconnect/ Disconnect only the originator link. From P2/P4/P6/P8 direction: Reconnect/ Disconnect only the responder link. (See Figure 6.35.)
DWORD Jam	Replace DWORD	Replace DWORD.
Symbol Jam	Replace with Another Symbol	Replaces the Symbol with the selected Symbol.
	Delete	Deletes the Symbol Jam.

TABLE 6.5: Test State Actions in Simple Mode (Sheet 2 of 3)

Action		Description
Frame Jam	Insert Bytes Inside Frame	Allows to insert up to 60 Bytes inside the frame, at the specified offset or at the “current” DWORD, meaning the DWORD that caused the Event.
	Modify [Keep Length]	Allows to manipulate each DWORD in the header, with the selected Action (click on Pass though to get a drop-down list).
	Replace	Replaces the whole frame with the selected frame.
	Remove [Replace with IDLE]	Removes the whole frame.
	Truncate	Removes some of the payload, as specified in the Frame Length.
Inject General Error	FEC Parity Error	Injects a FEC error into traffic.
	Sync Header Error	Injects a Sync Header error into traffic.
	Invalid 10-bit-Error Code	Injects invalid 10b code into the line (FC8 only).
	Running Disparity Error	Injects a Running Disparity (RD) error into traffic (FC8 only).
Insert	Insert New Frame	Allows to insert a whole frame as specified from the list of available frames.
	Symbol (66 Bit)	Allows to insert a Symbol 66 bits.
	Insert Bytes/ Ordersets	Allows to insert Bytes or Ordersets (FC 16 only).
Ordered Set Jam	Delete	Delete an Ordered Set Jam.
	Remove [Replace with IDLE]	Remove an Ordered Set Jam or Replace with another Ordered Set.
	Replace with Another Ordered Set	Only replace with another Ordered Set.
Scenario Execution	Stop Scenario	Stops the current Scenario. This Action should be the only Action in a State as it has higher priority over other Actions.
	Restart All Sequence	Restart all sequences in the Scenario.[1]
	Restart Current Sequence	Restart the sequence that contains this Action definition. [1]
Training Sequence Jam	Modify	Modify the Training Sequence Action Jam.
Branch To	Destination State	Go to a state in this Sequence.[1]

TABLE 6.5: Test State Actions in Simple Mode (Sheet 3 of 3)

Action		Description
Trigger Output		Sends a signal out the trigger port to the device downstream.
	Analyzer Trigger	1. The Action is to send a trigger to the Analyzer. 2. The trigger point in the Analyzer that caused the analyzer trigger action will not be the selected event, it will be the selected event with some offset.
	External Trigger Output	The Action is to cause an external trigger output.
	Internal Trigger Output	The Action is to cause an internal trigger output.
	Marker Trigger	Add a marker to captured data.
Capture	DWORD	Capture DWORD.
		Reuse of Captured DWORDs. (See 6.5.9, *Reusing Captured DWORDS in Events*.)
Jammer Internal Triggers		Refer to Section 6.5.18, *Synch Jammer Scenarios with Jammer Internal Triggers*.

[1]Only shown in Action Properties dialog box when creating a sequence.

6.5.4 Available Resources

You can specify Events, Combined Events and Actions and additional Events. The application automatically checks for the maximum number of terms (Events/Actions). When you exceed the limit, an error is flagged, prompting you to jump to the place that caused the error.

The list of available resources for Ethernet on SierraNet M168 is shown below:

- Symbol Detector (each has its own Embedded counter) X 4
- Auto-Neg Detector X 4
- Counter X 12
- Frame Detector X 8
- Timer X 8

- Frame Jammer X 8
- Symbol Substitute X 16
- Aut-Neg Jammer X 4
- Capture DWORD slot X 8
- Insert/Save frame slot (up to 16K bytes) X 7
- Insert BYTEs/Symbols inside frame (up to 128 bytes) X 8

- Global Action Register X 8
- State per sequencer X 256
- Action Register per state X 8

Usage of Action Register:

- Each Counter in Global Rules = 2
- Each Counter in State = 3
- Each Timer in Global Rules = 2
- Each Timer in State = 3
- Other Actions = 1

The following is a list of available resources for Fibre Channel:

- Symbol Detector (each has its own Embedded counter) X 4
- Ordered-set Detector (each has its own Embedded counter) X 8
- Pattern (32bit) Detector (each has its own Embedded counter) X 12
- Training Sequence Detector X 4
- Counter X 12
- Frame Detector X 8
- Timer X 8
- Frame Jammer X 8
- Symbol Substitute X 4
- Pattern/Ordered-set Substitute X 12 (shared with Pattern detectors)
- Training Sequence Jammer X 4
- Capture DWORD slot X 8
- Insert frame slot (up to 4K bytes) X 1
- Insert DWORD inside frame (up to 64 bytes) X 8
- Global Action Register X 8
- State per sequencer X 256
- Action Register per state X 8

Usage of Action Register:

- Each Counter in Global Rules = 2
- Each Counter in State = 3
- Each Timer in Global Rules = 2
- Each Timer in State = 3
- Other Actions = 1

6.5.5 Using Counters in Events and Actions

Many of the Events and Actions supported by InFusion also support counters that can control functions. See Figure 6.40.

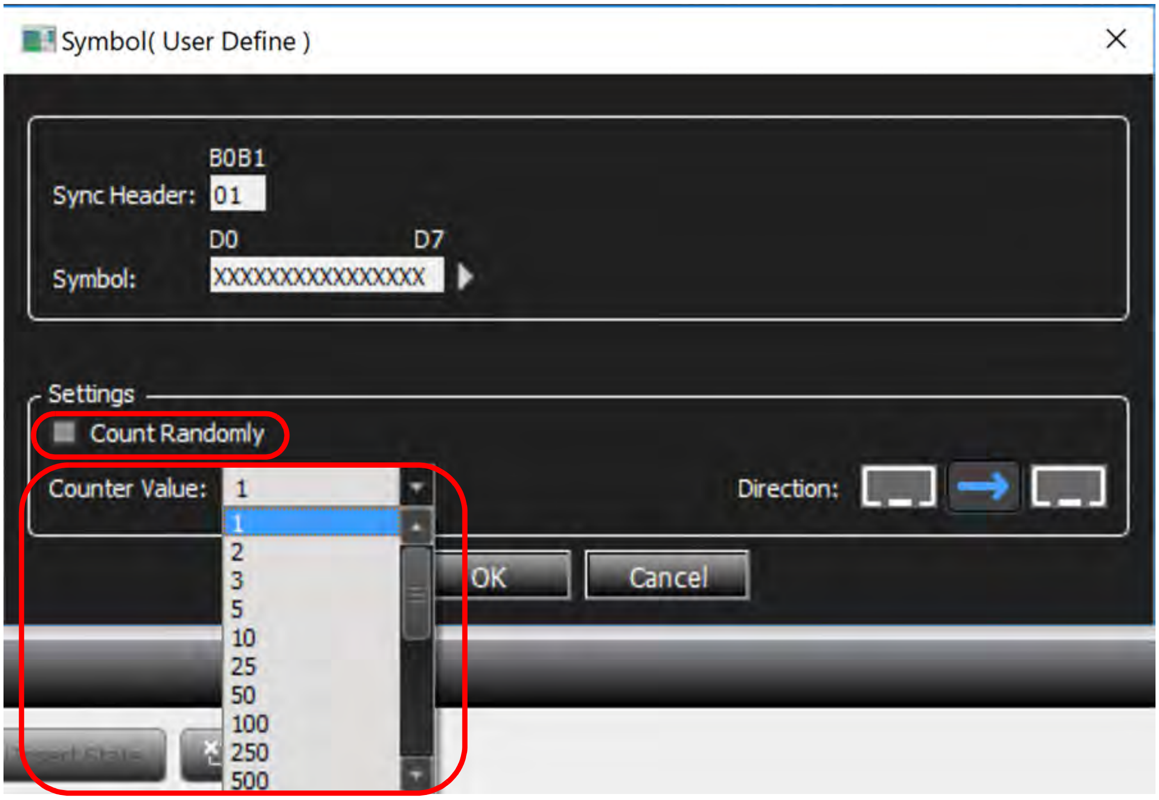


Figure 6.40: Typical Event: User Defined Symbol

Within Events, counters determine how many times the Event must occur before the associated Actions are triggered. Event counters typically have two properties:

- **Count Randomly**: Can be set to **Yes** or **No** (default value is No). If **Count Randomly** is checked, the Event repeats a random number of times (between 1 and the value set in the property **Max Random Count**, which replaces the property **Counter Value** when **Yes** is selected), before the Action is triggered.
- **Counter Value**: Number of repeats required when the **Count Randomly** check box is not selected. The default value is 1 but the range is from 1 to 500,000,000.

Within Actions, counters determine how many times the Event happens before it executes the Action. Note that an Event can be defined for a number of occurrences, so in total, the Event will have to occur for Event counter multiplied by the Action counter times before the Action gets executed. For example, if the Event is defined with a counter of 5, and Action with a counter of 10 such Events, the Event looked at will have to occur 50 times before the Action is taken. See Figure 6.41.

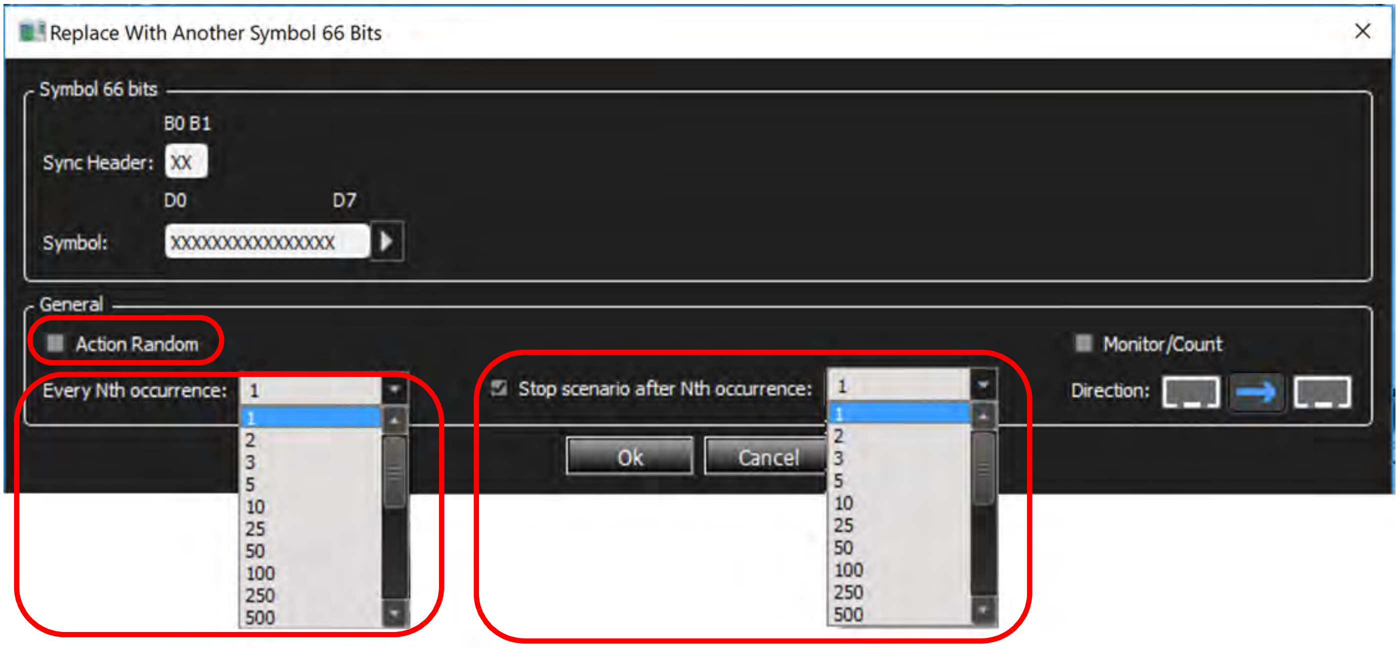


Figure 6.41: Jammer Action: Replace with Another Symbol

NOTE: Some deleteable symbols (e.g., Alignment Markers and others) are stripped by the logic before reaching the jammer, then reinserted as needed. Therefore, these symbols cannot be jammed.

Action counters typically have three properties:

- **Action Random**: Can be set to "Yes" or "No" (default value is "No"). If the **Action Random** check box is selected, the Action triggers a number of occurrences before the Action takes place. That number ranges randomly between 1 and the value set in the property **Every Nth occurrence**, which replaces the property **Every Nth occurrence** when the **Action Random** check box is selected.
- **Every Nth occurrence**: Number of times the system calls the Action before it acts (from 1 to 500,000,000).
- **Stop Scenario after Nth occurrence**: Stops the Jammer action after the number of actions you specify (from 1 to 500,000,000).

Note that there is some overlap in the way these counters can be used. For example, in the simple case of a single Event leading to a single Action, it makes no difference whether you specify the Event to require five repeats before triggering the Action, or the Action to require five occurrences before it acts.

However, in the case of combined Events and/or Actions, the separate counters provide flexibility in designing test cases. For example, consider the case where Event_1 OR Event_2 leads to Action. If Event_1 has a counter of 5, then the Action triggers either when Event_1 has repeated five times or when Event_2 happens the first time, whichever occurs first.

But if the Event counters are set to 1 and the Action counter is set to 5, then the Action happens after five occurrences of EITHER Event_1 or Event_2.

6.5.6 Capturing a Data DWORD

InFusion provides the ability to capture individual data DWORDs and provides different registers to store captured DWORDs. When your detector is DWORD Matcher, you can use DWORD #0, #1, #2, and #3. When your detector is Pattern Detector you can use DWORD #4, #5, #6 and #7. When trying to use the captured DWORD, for example in Replace DWORD Action, you can actually select from 8 captured DWORDs, numbered 0 through 7.

1. To capture a data DWORD, select **Capture DWORD** from the Action Properties screen (Figure 6.42).

2. Select the location you would like the captured DWORD to be stored in, where it can be used in a later replacement or insertion.

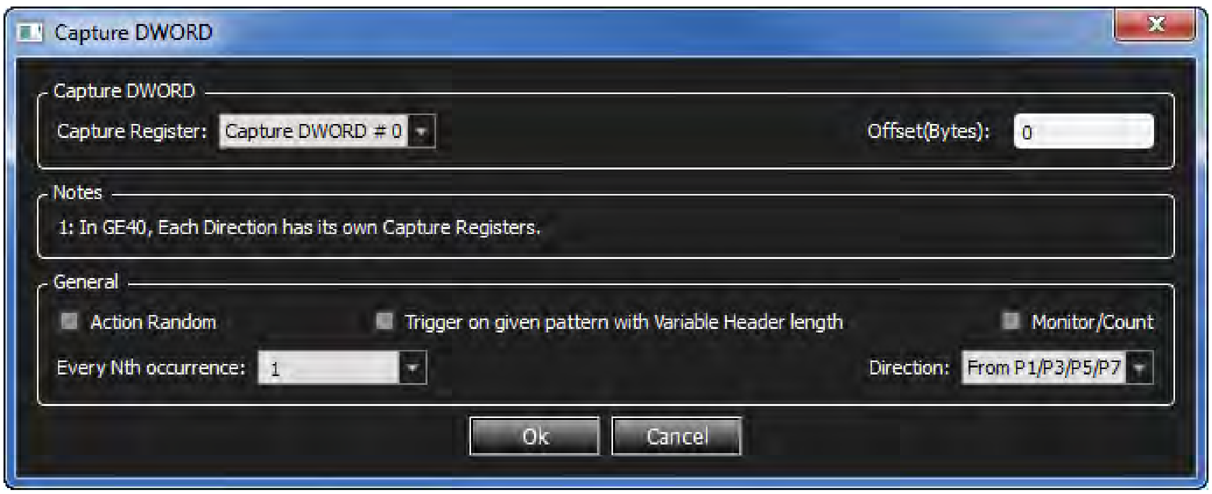


Figure 6.42: Capture Data DWORD Action

6.5.7 Using Captured Data DWORDs

Captured data DWORDS can be used in creating Events for data that match the captured DWORD(s), or in creating Actions to substitute or insert the captured DWORD(s) into the data stream.

1. To create an Event using the captured DWORD, in the Add Event dialog (Figure 6.43), select DWORD Matcher and change the Type to the desired Captured DWORD number.

   Note that choice of a mask and an offset are still available.

2. Select the code mask from the drop-down menu.

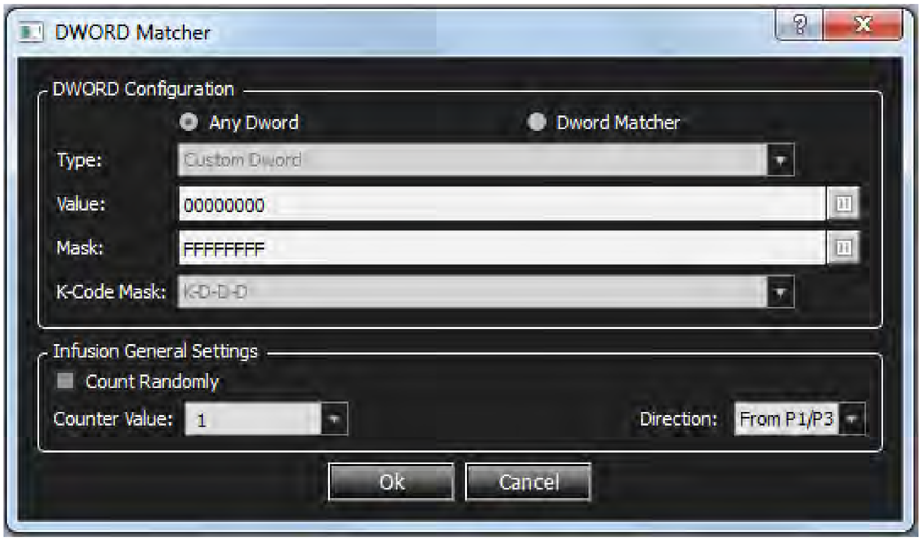


Figure 6.43: Using Captured DWORD as an Event

Captured data DWORDs may also be used in the **Substitute Data DWORD** Action:

1. From the Action Properties screen, click the **DWORD Jam** icon.
2. Click **Replace DWORD**, then choose **Property** from the Substitute For drop-down list.

   The drop-down list is provided (see below) to allow the choice of a custom DWORD or any of the four captured DWORD registers.

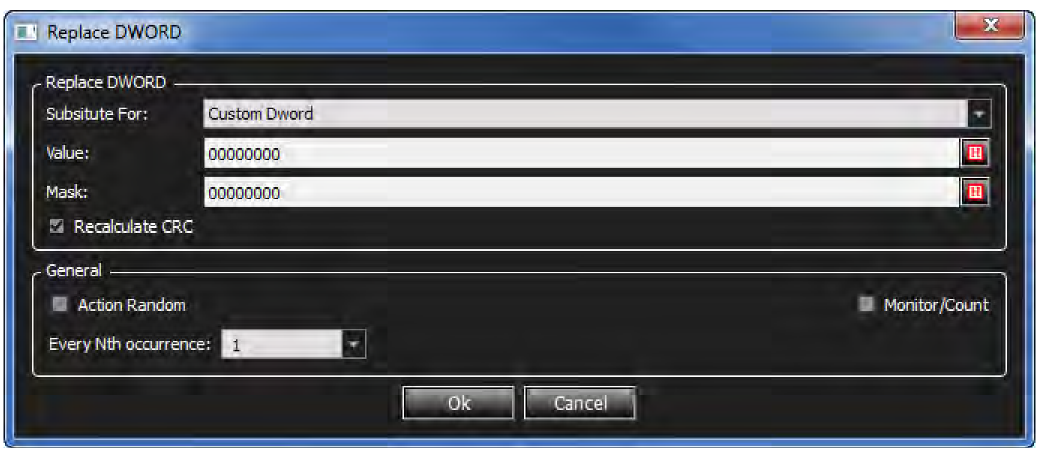


Figure 6.44: Using a Captured Data DWORD in Substitute DWORD Test Action

6.5.8 DWORD Matcher

DWORD Matcher is a DWORD pattern matcher that presents match and mask fields and a K-Code Mask field. K-Codes are control characters that are always used in the first byte of a four-byte ordered-set. Of the K-Code masks listed in the menu, D-D-D-D is used for data bytes, and K-D-D-D is used for all ordered-sets.

When you create a DWORD match, keep the following in mind:

- The pattern can be inside or outside of frames (it does not matter if the pattern is inside a frame or not).
- Because the pattern can be inside or outside of frames, there is no offset.
- You can make user-defined ordered-sets. (This is the reason this feature was created.)
- You can use any K/D pattern.

6.5.9 Reusing Captured DWORDS in Events

This feature enables you to reuse previously captured data inside a Frame event; therefore, some parts of the frame event can be changed during the jammer running period in real time.

To use a captured DWORD in a Frame Event:

1. Right click in the Data pane of the Frame Event Properties dialog and choose **Replace with Captured DWORD**. A new dialog box pops up.
2. Specify which captured DWORD (Capture DWORD#0 to Capture DWORD#3) to use to replace the selected DWORD at run time.

   You can mask any of the bytes of the captured DWORD by using the Mask buttons provided in "Replace With Captured Data".

Figure 6.45: Replace with Captured DWORD Menu

Figure 6.46: Replace with Captured Data Dialog

3. To remove or edit the existing captured DWORD in an event, right-click on the desired DWORD and choose **Remove** or **Edit**.

Figure 6.47: Remove or Edit Captured DWORD

6.5.10 Traffic Modification Direction

The direction for traffic modification is defined on a global basis for the entire Scenario. In other words, any Scenario Action that modifies line traffic only affects the traffic flowing in the direction established at the top of the Scenario, in the Scenario Properties. Scenario Events can be monitored in either direction, and therefore the parameters for Events provide the ability to specify the intended direction for monitoring traffic for that Event. See Figure 6.48.

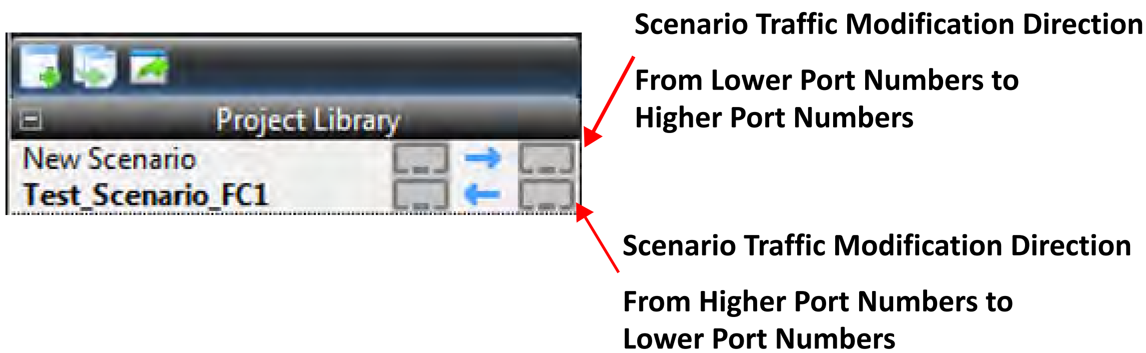


Figure 6.48: Scenario Traffic Modification Direction

6.5.11 Copy and Paste Events and Actions

1. To copy an Event or Action, right-click on the **Event** or **Action** and select **Copy**.
2. Right-click and select **Paste**.

You can also remove, cut or copy a selected Event or Action; and double-click the **State name** and edit it.

6.5.12 Copy and Paste Scenarios

You can copy and paste scenarios from one project to another project. Perform the following steps to do so:

1. To select the scenario you want to copy, do one of the following:
   - In the scenario name tab, select **Copy**.
   - In the Library pane, right-click and select **Copy Scenario** (see Figure 6.49).

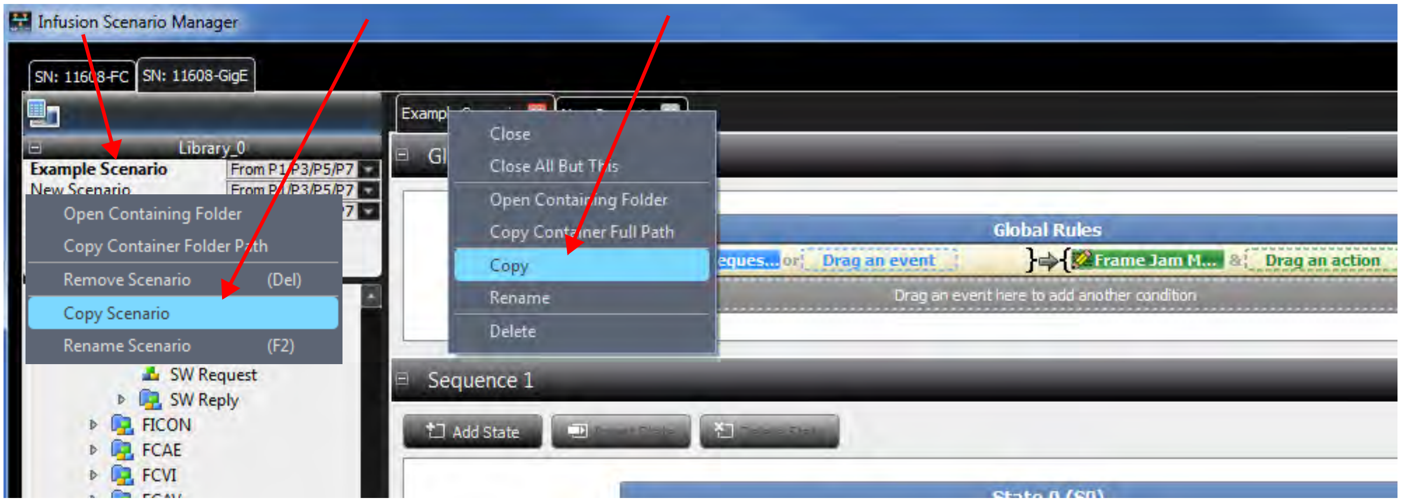


Figure 6.49: Copy Scenario

2. Place the cursor in the area below <New Scenario> in the Library pane of the project you want to paste in, then right-click and select **Paste Scenario**.

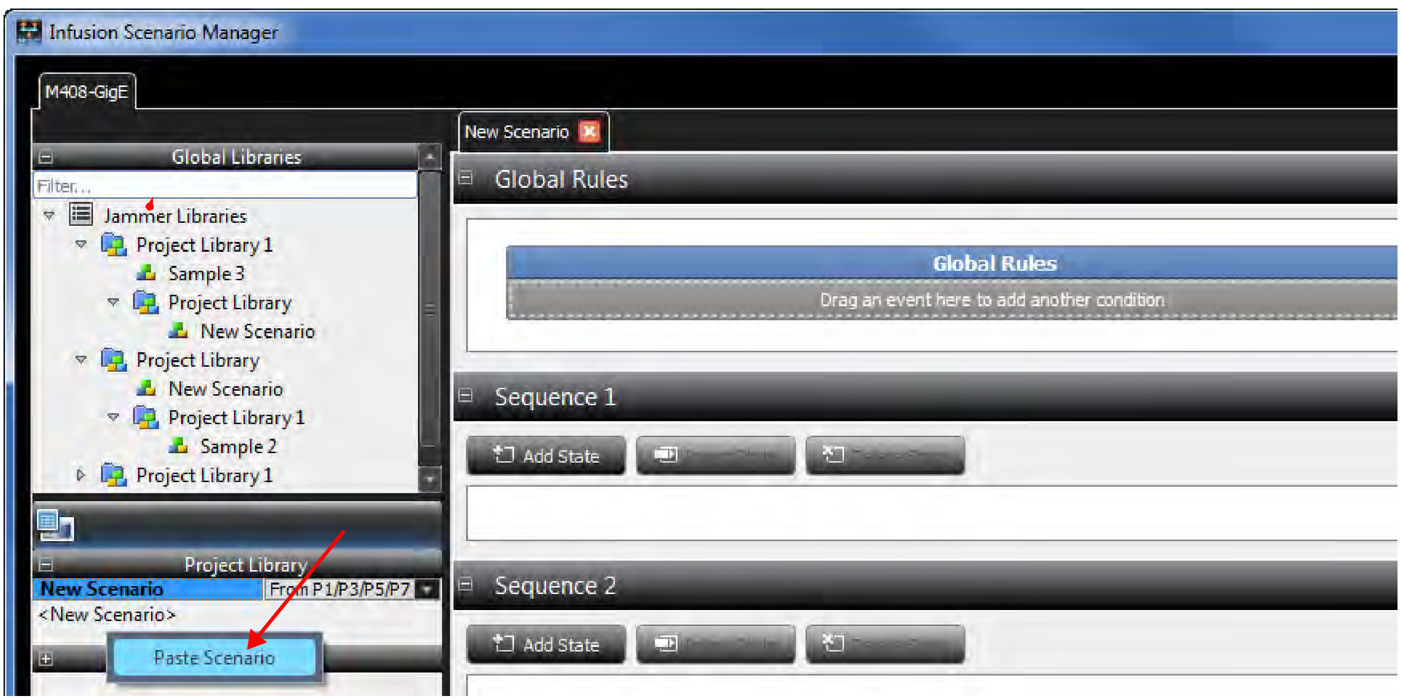


Figure 6.50: Paste Scenario

6.5.13 Copy and Paste Library

You can copy and paste libraries from one project to another project. Perform the following steps to do so:

1. Select the library you want to copy, then right-click and select **Copy Library**.

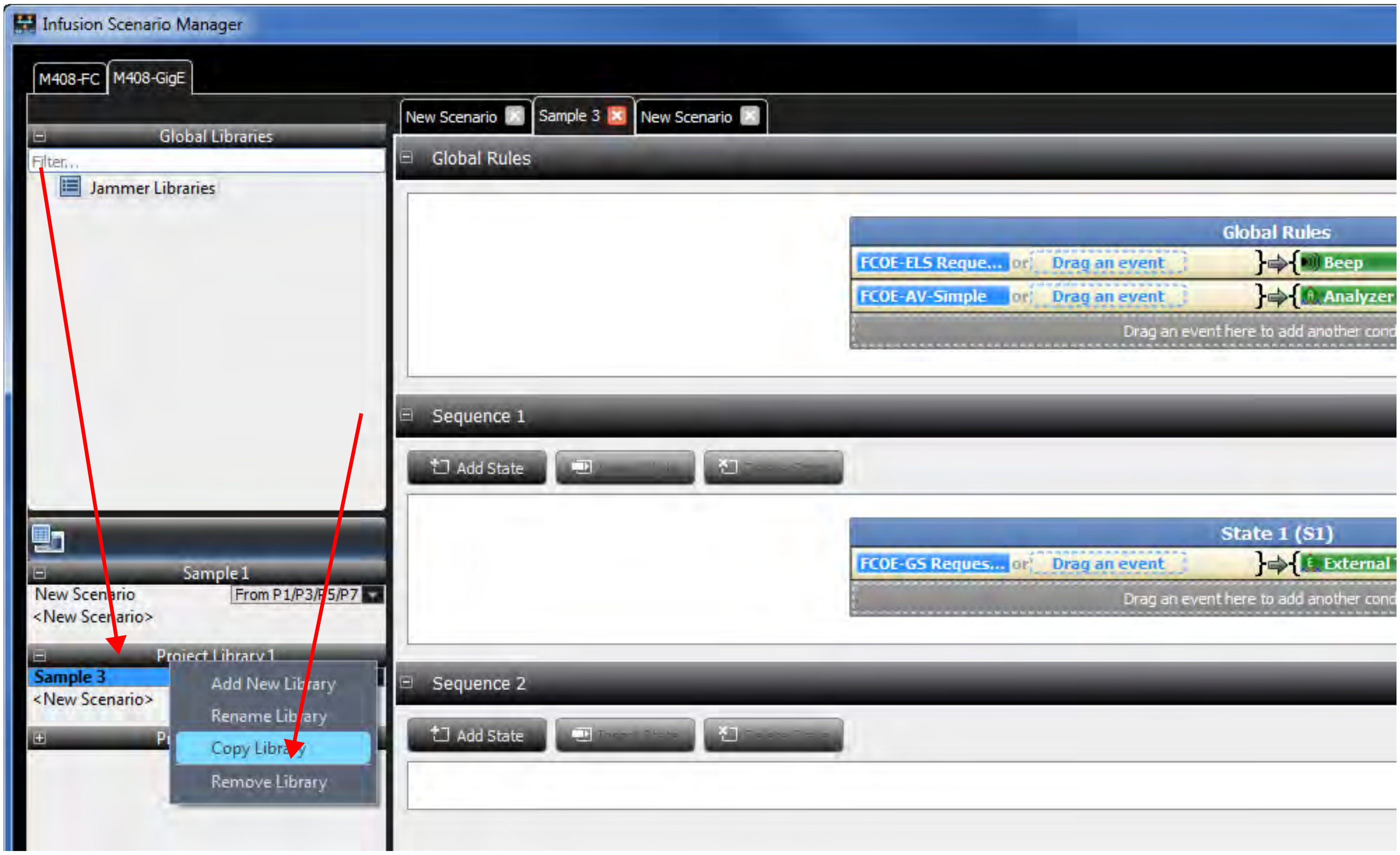


Figure 6.51: Copy Library

2. Place the cursor on the Jammer libraries icon in the Global Libraries panel, right-click and select **Paste**.

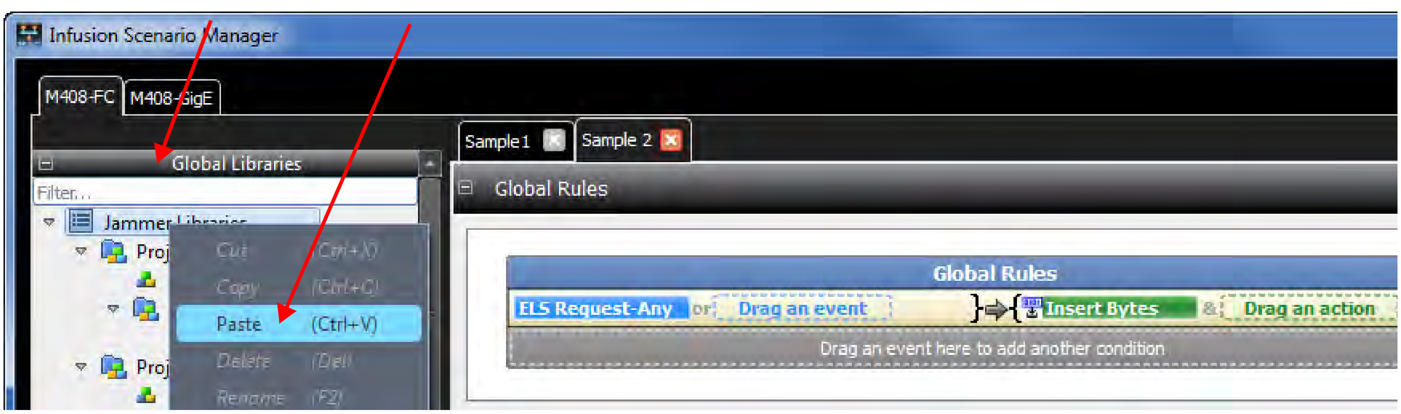


Figure 6.52: Paste Library

6.5.14 Copy/Cut and Paste States

You can copy and paste states from Global Rules to Sequences. You can also copy/cut and paste states between Sequences. You cannot cut a state from nor paste a state into Global Rules.

1. Right-click in the blue title area of the State you want to copy and select **Copy State** (or Cut State if applicable).

2. Right-click in the white workspace of the desired target Sequence and select **Paste State.**

6.5.15 Copy/Cut and Paste Conditions

You can copy and paste Conditions within and between States.

1. Right-click in the empty yellow space of the Condition you want to copy and select **Copy Condition** (or Cut Condition if applicable).
2. Right-click in the gray placeholder area (i.e., in the area that says “Drag an event here...”) of the desired target State and select **Paste**.

6.5.16 Copy/Cut and Paste Events

You can copy and paste Events within and between States.

1. Right-click on the Event you want to copy and select **Copy** (or **Cut** if applicable).
2. Right-click in the empty yellow space of the desired target Condition or in the gray placeholder area (i.e., in the area that says “Drag an event here...”) of the desired target State and select **Paste**.

6.5.17 Marker Trigger

The main purpose of this feature is enabling the user to mark specific parts of the captured traffic for better tracking.

6.5.17.1 Solution

The Marker Trigger action will be added to Jammer under Trigger Output category. Also, for differentiating various markers, the action will has an Index parameter that will be shown in the captured traffic as well. Therefore 8 Marker actions will be as bellow:

- Jammer Marker 1
- Jammer Marker 2
- Jammer Marker 3
- Jammer Marker 4
- Jammer Marker 5
- Jammer Marker 6
- Jammer Marker 7
- Jammer Marker 8

Adding above markers can be used as an action in the Jammer. When the Jammer runs this action, the result is adding a marker (bookmark) in captured trace in analyzer. The added markers will be shown as a normal marker (bookmark) in trace and you can see list of marker in book mark dialog.

NOTE: The limitation for adding markers is 10,000, it means you can add up to 10,000 marker to a trace.

GUI

Figure 6.53 shows the Marker trigger added under the "Trigger output" node in the action tree.

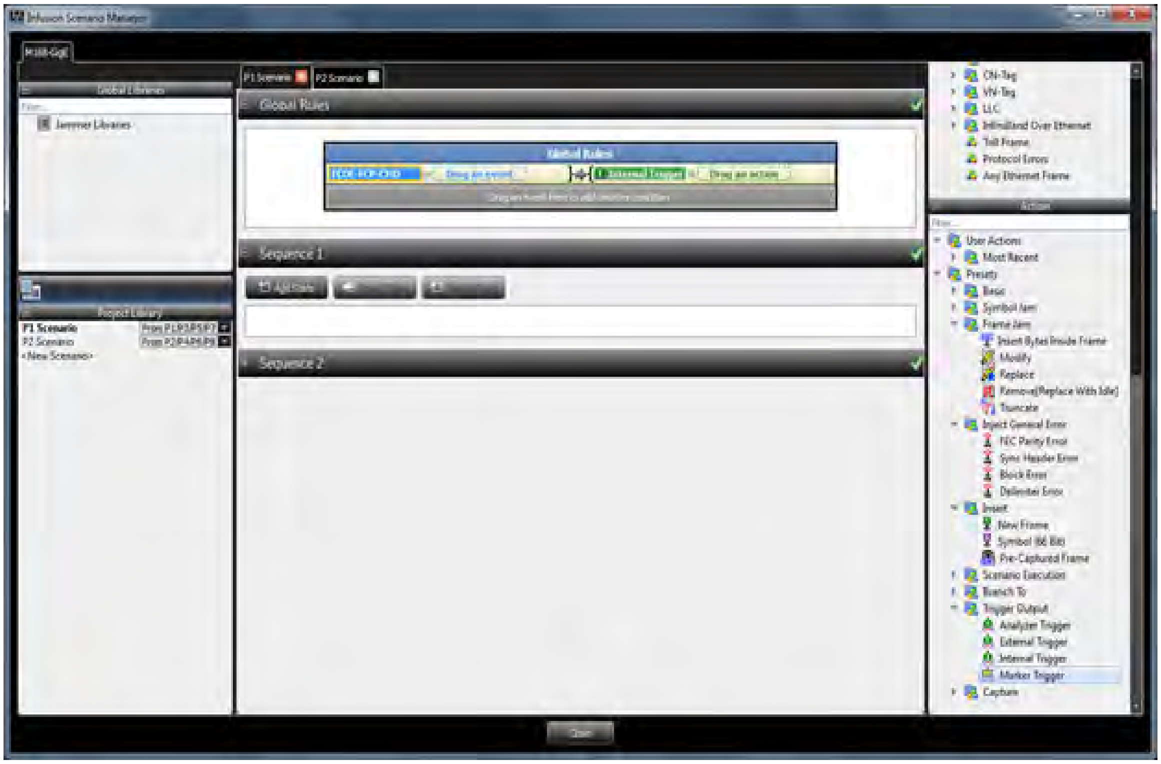


Figure 6.53: Marker Trigger Added to Action Tree

There is a dropdown list in Marker Trigger dialog to choose which marker user wants to insert to analyzer trace. (Marker 1 to Marker 8).

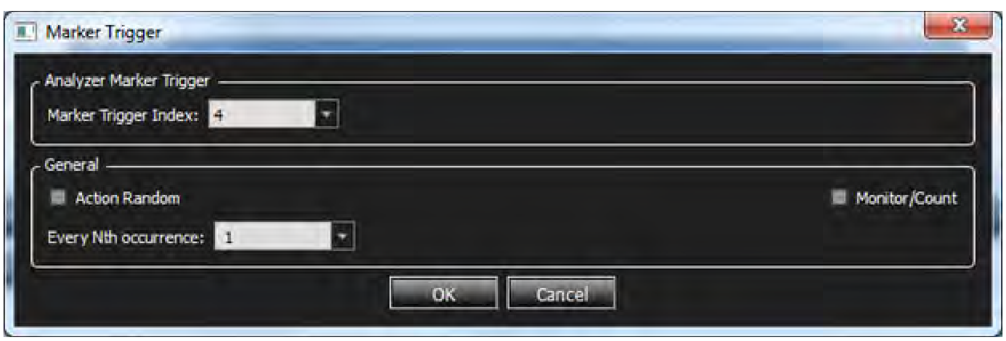


Figure 6.54: Marker Trigger Menu

6.5.18 Synch Jammer Scenarios with Jammer Internal Triggers

By design, each Jammer port pair runs its own independent scenario, and each one can be controlled independently. However, there may be advanced cases where you would need to synchronize the Jammer operation of 2 or more port pairs.

6.5.18.1 M408/M168

With the M408/M168 analyzers, you might want to create a setup in which you jam both directions of a single link; you can achieve this by looping the link through the P1/P2 port pairs and the P5/P6 port pairs or P3/P4 and P7/P8 with external cabling, running separate scenarios on each of P1/P2 and P5/P6 as well as the P3/P4 and P7/P8 and synchronizing those scenarios with the Jammer Internal Triggers.

6.5.18.2 M164/M8-4

With these analyzers (and fewer port pairs), you might want to create a setup in which you jam both directions of a single link; you can achieve this by looping the link through P1/P2 port pairs and P3/P4 port pairs with external cabling, running separate scenarios on each of P1/P2 and P3/P4, and synchronizing those scenarios with the Jammer Internal Triggers. For information on bidirectional jamming operation with the M164 see *Appendix C, AJAJ – Bidirectional Jamming Operation*.

Jammer Internal Triggers are pairs of events and actions that enable cross-port signaling; these events and actions are manipulated like any other event and action. The Internal Trigger Action allows one port pair to signal an Internal Trigger Event on a different port pair. Note that the Internal Trigger Action will NOT signal an Internal Trigger Event on the same port pair. There are four independent Jammer Internal Trigger event/action pairs available.

For supporting this feature, a specific signal between different paths should be added, such that one scenario will be able to notify the scenarios of other paths.

Thus, firstly, it is needed to add a new Action for notifying other paths and secondly, adding a new event for waiting on any notify signal that is raised on other paths. This will be implemented as below:

1. Adding ‘Internal Trigger’ action to notify all other paths:
   a. Internal Trigger Action 0
   b. Internal Trigger Action 1
   c. Internal Trigger Action 2
   d. Internal Trigger Action 3
2. Adding ‘Internal Trigger’ event to wait for others’ notifications:
   a. Internal Trigger Event 0 which is corresponded to Internal Trigger Action 0
   b. Internal Trigger Event 1 which is corresponded to Internal Trigger Action 1
   c. Internal Trigger Event 2 which is corresponded to Internal Trigger Action 2
   d. Internal Trigger Event 3 which is corresponded to Internal Trigger Action 3

Example

For example, the user would like to insert a new frame on P1/P2 path (ACTION1) when there is a specific symbol on P3/P4 path (EVENT1), this scenario will be implemented in 2 different scenarios as below:

1. In the first scenario for P1/P2, in the global state define a condition that waits for EVENT1 and then raise ‘Internal Trigger’ action.
2. In the second scenario for P3/P4, in the global state define a condition that waits for the same ‘Internal Trigger’ event and the does ACTION1.

Scenario 1

Figure 6.55: Scenario 1 using Jammer Internal Trigger

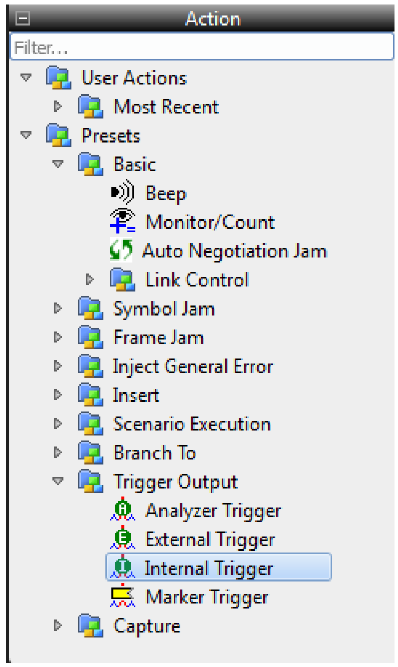


Figure 6.56: Internal Trigger action in the Actions pane

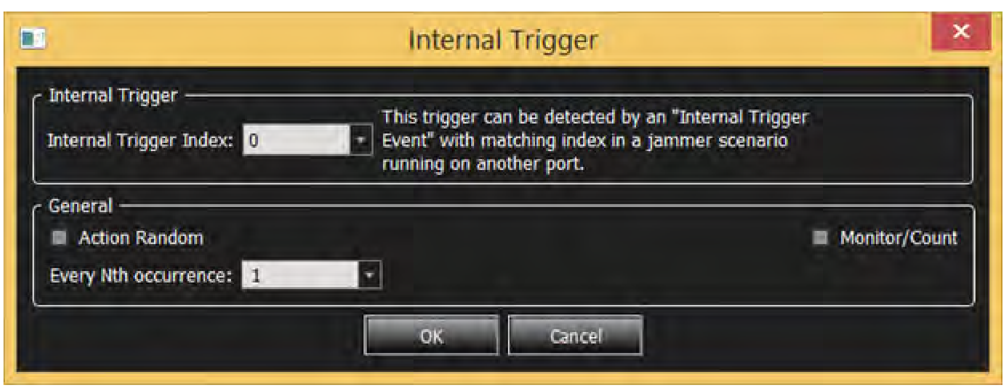


Figure 6.57: Internal Trigger Action Properties

Scenario 2

Figure 6.58: Scenario 2 using Jammer Internal Trigger Event

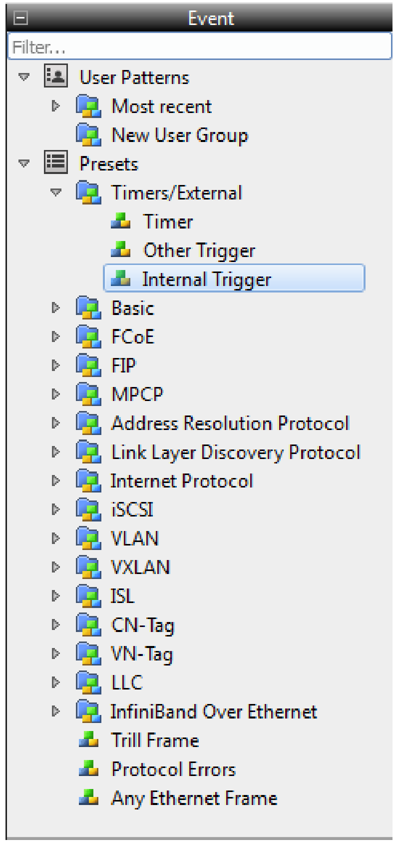


Figure 6.59: Internal Trigger Event in the Events Pane

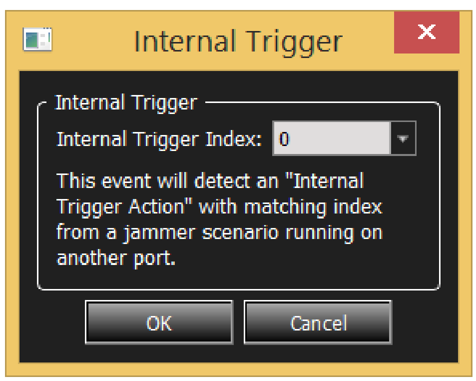


Figure 6.60: Internal Trigger Event Properties

6.5.19 Import/Export Jammer Libraries

Jammer libraries can be imported and exported. See Figure 6.61.

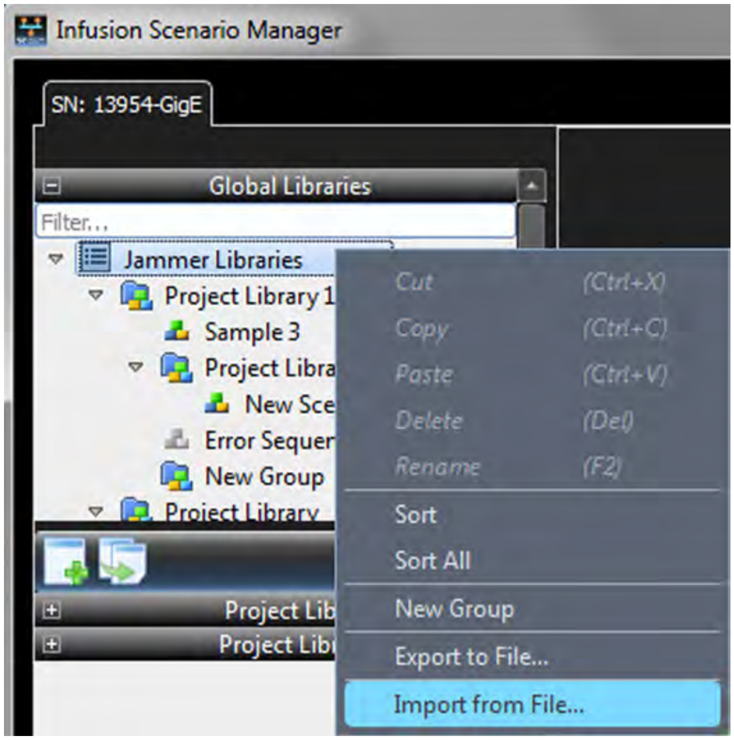


Figure 6.61: Import and Export Jammer Libraries to a File

To export a jammer file, click on Export to File and the following dialog pops up. See Figure 6.62.

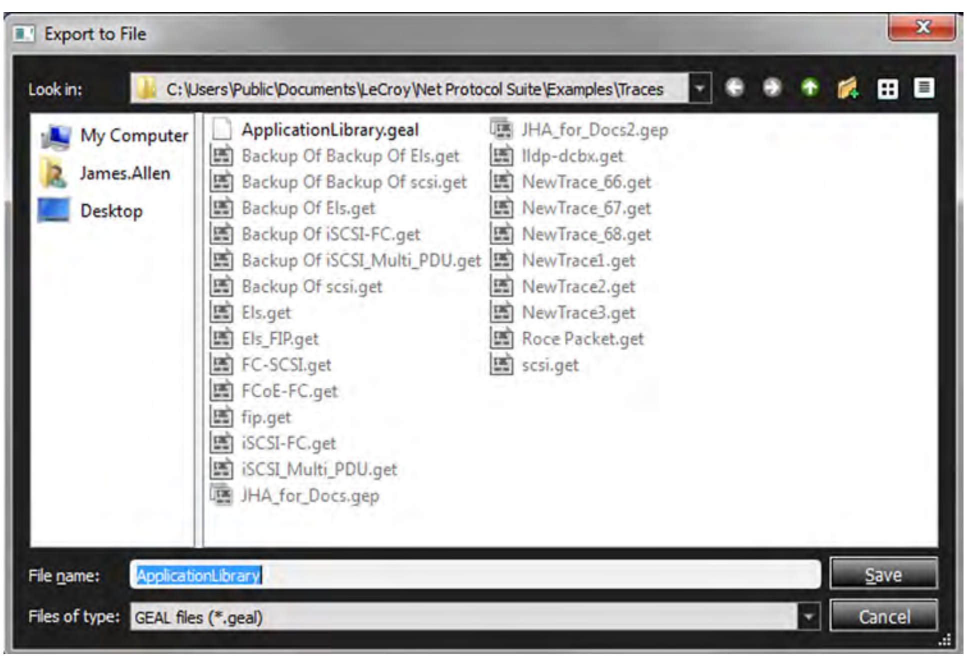


Figure 6.62: Export Jammer Library File

To import a jammer file, click on Import from File and the following dialog pops up. See Figure 6.63.

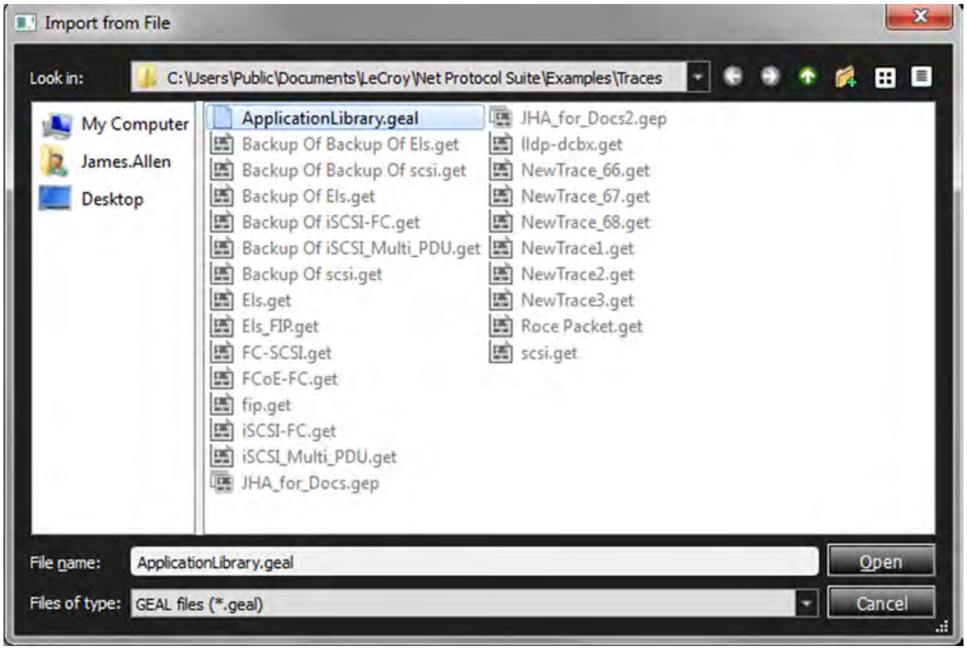


Figure 6.63: Import Jammer Library File

6.5.20 Infusion Error Messages/Corrective Action

TABLE 6.6: Detailed Error Message Descriptions/Corrective Action (Sheet 1 of 4)

Error Message	Detected Event/ Action	Reason	Corrective Action
Only Captured DWORD #4-#7 are allowed to be used with frame detector events	Capture DWORD Action	Invalid Parameter Setting	Change capture setting to Frame Detect
Only Captured DWORD #0-#3 are allowed to be used with non-frame detector events	Capture DWORD Action	Invalid Parameter Setting	Change capture setting to Non-Frame Detect
Capture DWORD action is not allowed when frame detection events are combined with other events	Capture DWORD Action	Operation Limitation	Remove Non-Frame OR Frame Detect according to Action Capture Setting
Too many Insert Actions	Insert Error/ Bytes/Symbol Action	Resource Limitation	Reduce Action Max is 8 for GE & FC
Too many Frame insert Actions	Frame Insert Actions	Resource Limitation	Reduce Action Max is 7 for GE & FC
Too many Frame Detection events	Frame Detect Event	Resource Limitation	Reduce Event, Max is 8 for GE10 & FC, 6 for GE40
Selected Action is only valid after Frame Detect Events.	Frame Jam Actions	Operation Limitation	Remove the Non-Frame Event or choose other action for the Non Frame Event

TABLE 6.6: Detailed Error Message Descriptions/Corrective Action (Sheet 2 of 4)

Error Message	Detected Event/ Action	Reason	Corrective Action
Frame Length in Frame Truncate Action cannot be less than 3.	Frame Truncate Action	Invalid Parameter Setting	Frame length setting should be more than 3
Selected Action is not valid after “Frame Detect” Events, Use “Frame Jam” action after Frame Detectors.	Non Frame Actions	Operation Limitation	Select actions from Frame Jam category
Events for this action are in different Directions.	Frame Actions	Operation Limitation	Change all Events to same direction
Direction of Events for this action should be same as Scenario Direction.	Frame Event	Parameter Setting	Change Scenario OR Frame Event direction
Selected Action is not valid after “Training Frame Detect” Events. Use “Training Frame Jam” action after Frame Detectors.	Training Sequence Event	Operation Limitation	Remove the incompatible Action
Selected Action is only valid after Training Frame Detect Events.	Training Frame Action	Operation Limitation	Use action only for Training Sequence Events
Selected Action is only valid after Auto Negotiation Detect Events.	Auto Negotiation Jam Action	Operation Limitation	Use action only for Auto Negotiation Events
Selected Action is not valid after Auto Negotiation Detect Event.	Auto Negotiation Events	Operation Limitation	Remove the incompatible Action
Selected Action is not valid after Both Link Up Event.	Both Link Up Event	Operation Limitation	Remove the incompatible Action
Selected Action is not valid after Link Speed.	Link Speed Event	Operation Limitation	Remove the incompatible Action
Too many Auto Negotiation Jam Actions	Auto Negotiation Jam Action	Resource Limitation	Reduce Action, Max is 4
Too many Frame Jam Action	Frame Jam Action	Resource Limitation	Reduce Action, Max is 8
“Insert Position” of Insert Action should be set to “Offset from frame start” for Frame Detect events.	Insert Symbol/ Bytes/Ordersets Action	Invalid Parameter Setting	Change the insert position to Offset from Frame
“Insert Position” of Insert Action should be set to “After Current Symbol\DWORD” for Non-Frame Detect events.	Insert Symbol/ Bytes/Ordersets Action	Invalid Parameter Setting	Change the insert position to after symbol/DWORD
Whether all or none of events should be Frame Detect	Insert Symbol Action	Operation Limitation	Remove all Frame Detect Patterns from Event
Variable Header is allowed for selected Action if and only if all Events are FCOE Frame Detect	Frame Actions	Operation Limitation	Uncheck Trigger on given pattern with Variable header length from the FCOE Frame Detector OR Remove the non-FCOE Frame Detect from Event

TABLE 6.6: Detailed Error Message Descriptions/Corrective Action (Sheet 3 of 4)

Error Message	Detected Event/ Action	Reason	Corrective Action
Combination of Variable and Fixed Header is only allowed when all Events are FCOE Frame Detect	Frame Events	Operation Limitation	Uncheck Trigger on given pattern with Variable header length from the FCOE Frame Detector OR Remove the non-FCOE Frame Detect from Event
Selected Action is only valid after Frame Detect Events with Same Direction	Frame Events	Invalid Parameter Setting	Change the Action direction setting to match Events
Selected Action is only valid after Auto Negotiation Detect Events with Same Direction	Auto Negotiation Events	Invalid Parameter Setting	Change the Action direction setting to match Events
Frame Delimiter OrderSet Can only Be Replaced By the Primitive Sequence OrderSet at the Speed of 8G or Less Than 8G.	Ordered Set Jam Action	Invalid Parameter Setting	User must select a compatible Primitive type
“Nth Occurrence” is not supported for Actions corresponding to Symbol Detect. Define the counter in event dialog instead.	Symbol Detect Event	Operation Limitation	Action counter Not supported when using this Pattern Event. Consider using pattern event counter.
“Nth Occurrence” is not supported for Actions corresponding to Ordered Set. Define the counter in event dialog instead.	Ordered Set Event	Operation Limitation	Action counter Not supported when using this Pattern Event. Consider using pattern event counter.
“Nth Occurrence” is not supported for Actions corresponding to DWORD Matcher. Define the counter in event dialog instead.	DWORD Matcher Event	Operation Limitation	Action counter Not supported when using this Pattern Event. Consider using pattern event counter.
Frame Detect Event with Variable Header is not valid for Replace Action.	Frame Jam Replace Action	Operation Limitation	Uncheck Trigger on given pattern with Variable header length from the FCOE Frame Detector.
Too many “Replace with Captured Data” Events.	Replace with Captured Data Action	Resource Limitation	Reduce Action placement, Max is 4.

TABLE 6.6: Detailed Error Message Descriptions/Corrective Action (Sheet 4 of 4)

Error Message	Detected Event/ Action	Reason	Corrective Action
Invalid parameters for “Replace with Captured Data”.	Frame Events	Invalid Parameter Setting	User must enable at least one byte mask.
Stop Scenario Action should be the only action in a condition of the state.	Stop Scenario Action	Operation Limitation	User must create a new condition for this action OR remove other actions from this condition.

6.6 Scenario Example

6.6.1 Example: Insert DWORD Matcher

In this example, the Global Rules panel of the Scenario waits for a Custom Frame then inserts a DWORD inside the frame. In Sequence 0 and State 0 it waits for an FCP SCSI Command, SBC3; inserts a DWORD inside the frame, beeps for a duration of 50 ms and stops the Scenario.

6.6.1.1 Creating Global Rules

This section describes using the Global Rules panel of the Scenario for this example. Recall that the Global Rules panel defines a single test state. The Global Rules do not have the capacity for multiple states, so that area of a Scenario cannot change state.

In terms of InFusion testing, a state defines test “behavior.” In this context, behavior is “waiting” for an Event and responding with an Action or set of Actions that happen simultaneously.

Keep in mind that a test state you implement with the Global Rules operates in parallel with the active test state of each sequence in the Scenario.

In effect, InFusion lets you do up to three line tests at the same time. You can do one test with the Global Rules and a separate test with each sequence you create. You can have up to two sequences in a Scenario.

1. Select Traffic Direction from the drop-down list to trigger on the defined event or trigger from InFusion Jammer (the default is **From P1/P3**, which is selected for this example).
2. In the Global Rules panel (see Figure 6.64).
3. Select **DWORD Matcher** in the Event panel and place it in the Global Rules panel (see Figure 6.65).

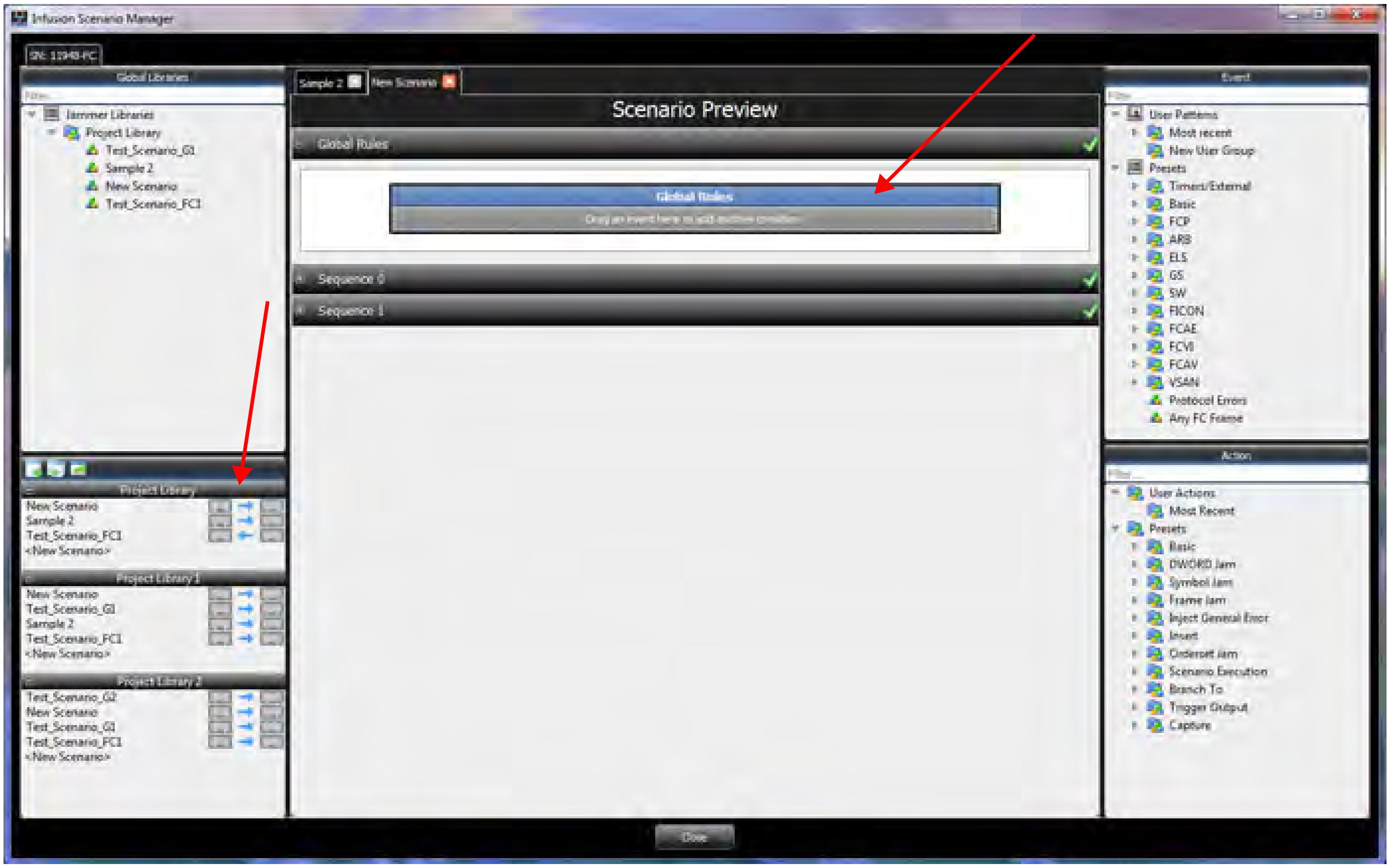


Figure 6.64: Global Rules Panel

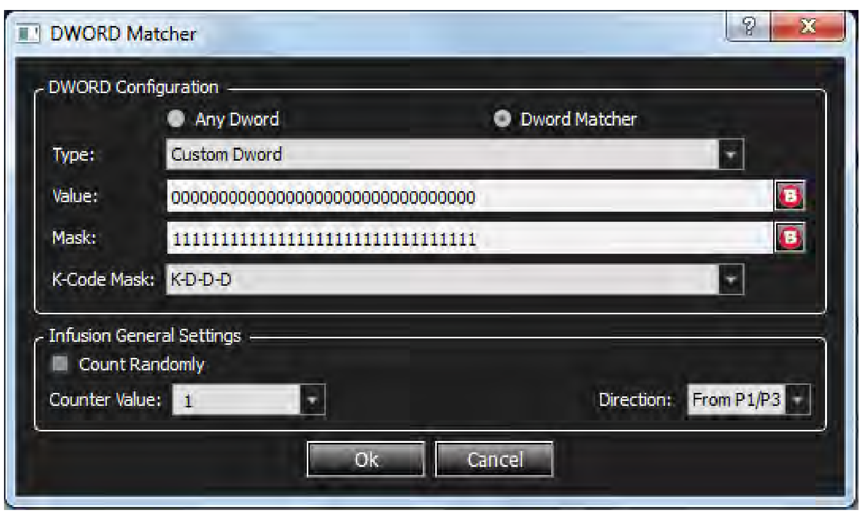


Figure 6.65: Adding an Event

4. The Event is added to the Global Rules panel (see Figure 6.66).
5. Select **Replace DWORD** in the Action panel and place it in the Global Rules panel (see Figure 6.66).
6. Right-click the New Scenario tab and select **Rename Scenario** and enter the name in the Library panel as shown in Figure 6.66.

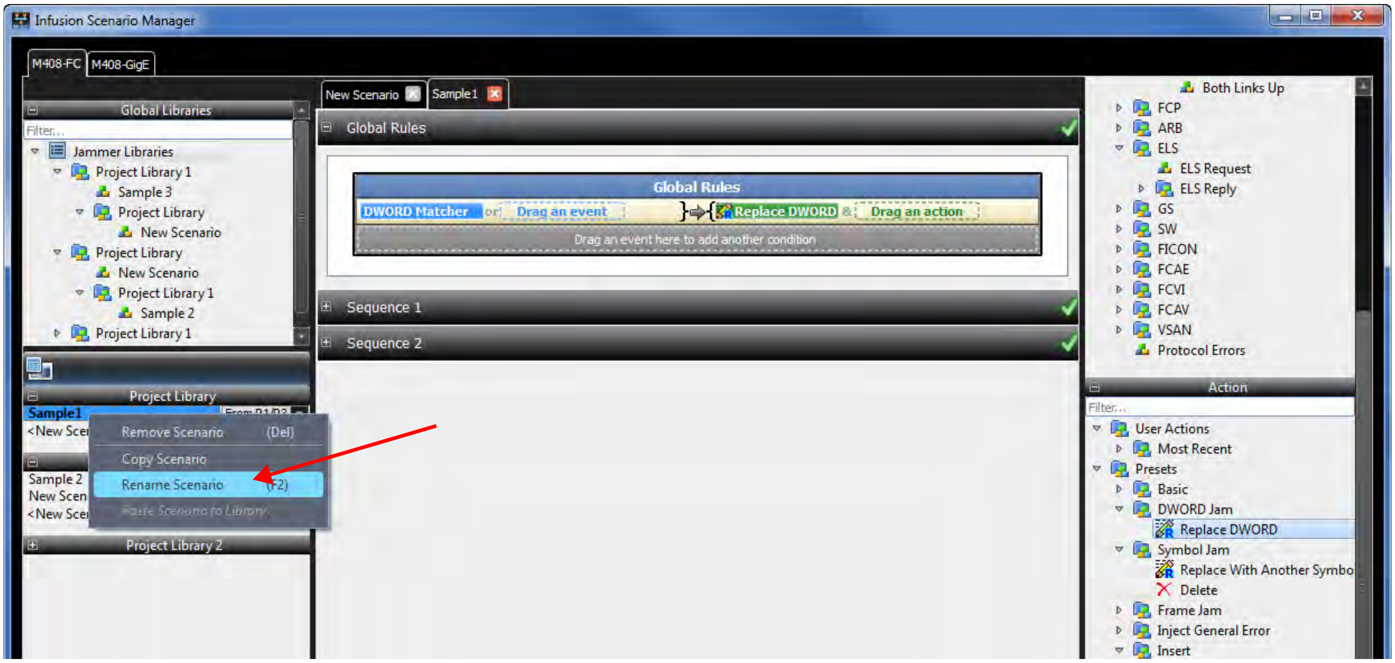


Figure 6.66: Global Rules – Naming a Scenario

6.6.1.2 Adding a Sequence

To add a Sequence click **Add State in the Sequence 1** panel.

You create a sequence one state at a time. The application numbers states consecutively from 0 up (1, 2, 3, and so on).

By default, the name of the first sequence in a Scenario is Sequence 1. The name of the first state is State 0. To change the name of a sequence or state, or to associate a description with it, click the name of the sequence or state.

1. Drag **6-Byte Any SCSI Command** under **FCP** as the Event to display the dialog.

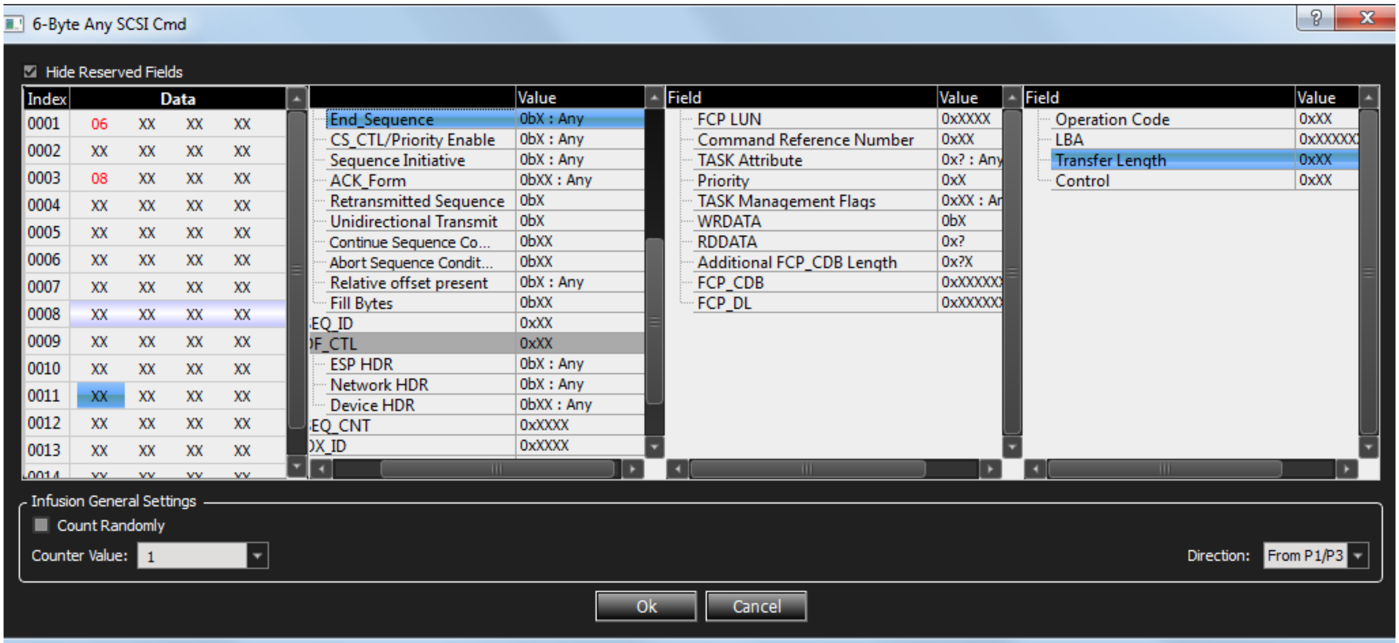


Figure 6.67: Adding an Event for Sequence 1

2. Click **OK** to close the 6-Byte Any SCSI Command dialog box.

3. After adding an Event, to add an Action in the Sequence 1 panel, drag and drop Monitor/Count.

   The Monitor/Count dialog box displays.

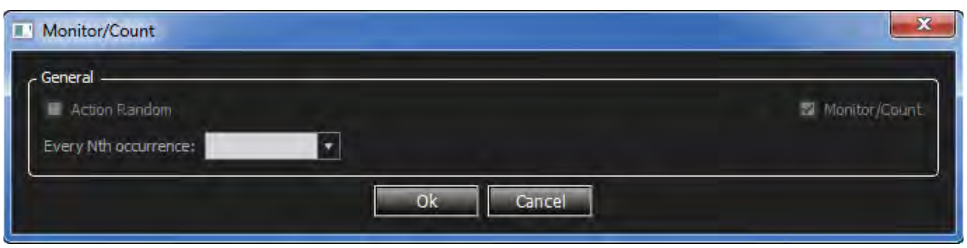


Figure 6.68: Adding Action Monitor/Count for Sequence 1

4. Click the **OK** button to close the Monitor/Count dialog box.

5. Repeat step 4 to add another Action (if desired).

   The completed Scenario is shown below.

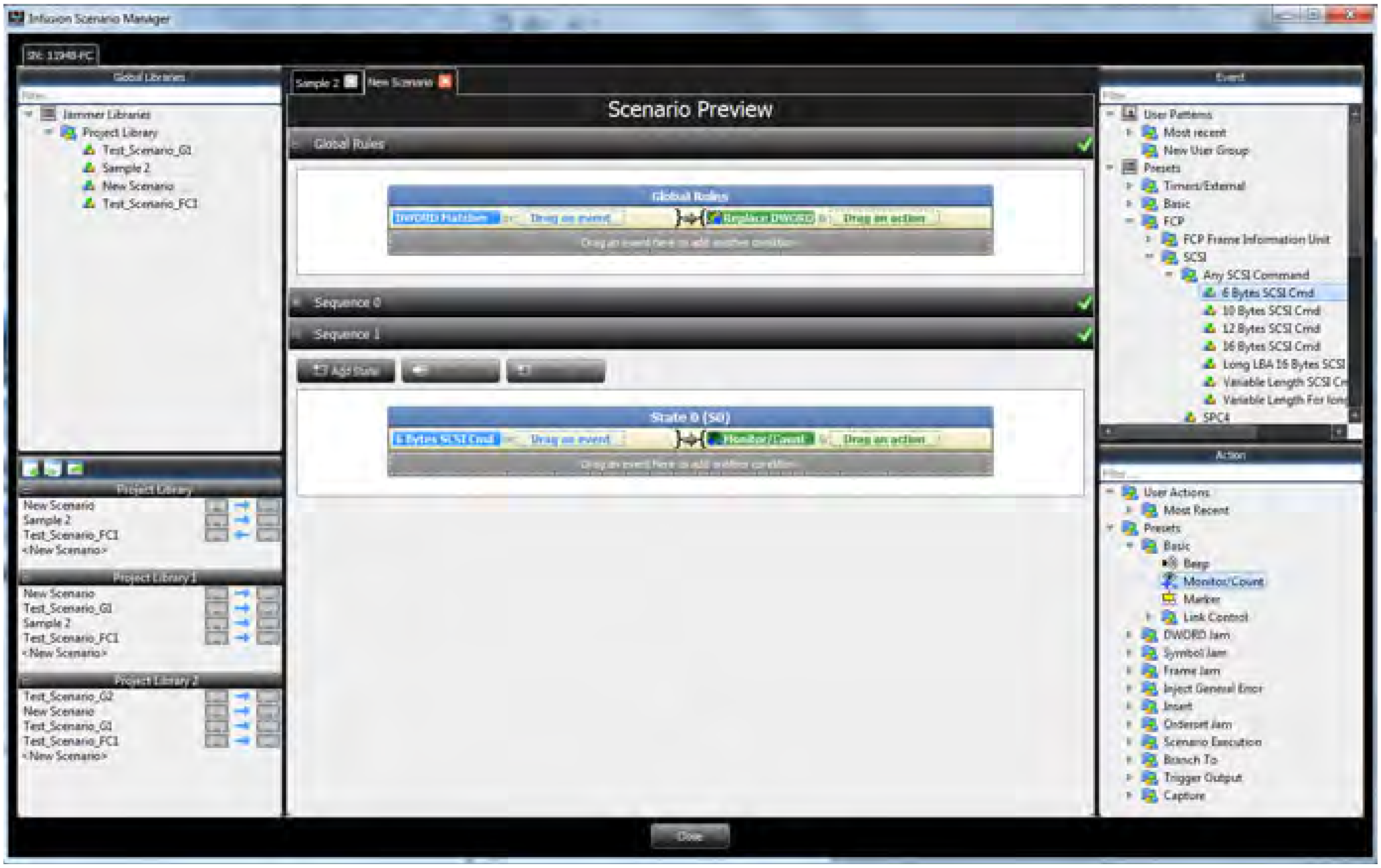


Figure 6.69: Complete Scenario of Insert DWORD Matcher

6.6.2 Sequence Creation

A sequence can have multiple states, but only one state is active at any time. In other words, at any point in time, a sequence “waits” for one Event (or Combined Event) and responds with the corresponding Action or set of Actions when the Event occurs.

A sequence is more powerful than Global Rules, because you can create branching or looping test logic with a sequence. You can include up to two sequences in a Scenario, but each is completely independent of the other. There is no branching or other interaction between the two, except through the Restart All Sequences Action.

You must follow some simple rules when creating sequences:

TABLE 6.7: Sequence Rules

Rule	Description
You can use only two branch Actions per state.	When you specify Actions for a state, you can only use two instances of **Branch to an Existing State** or **Branch to a New State**. If you try to use more than two, a red error message appears in the status area of the application that says “Too Many Actions.”
You can use only one restart sequence Action per state.	When you specify Actions for a state, you can only use one instance of **Restart Current Sequence** or **Restart All Sequences**. If you try to use more than one, a red error message appears in the status area of the application that says “Too Many Actions.”
You can use a maximum of 255 states per sequence.	If you try to use more than 255 states, a red error message appears in the status area of the application.

6.7 Summary of Scenario Creation

The suggested process of creating and executing a Scenario is as follows:

1. Create a Scenario in the library.
2. Drag and drop to create Global Rules Events and Actions and/or to create Sequence and State Events and Actions.
3. Complete the Scenario and Save it.
4. Select the Scenario in the Library that you want to run on the device.
5. To run the Scenario, click the **Start Session** (see 6.8.2, *Execute the Scenario from the Start/Stop Button*) button. The device starts to monitor/modify traffic.

6.8 Executing a Scenario

If you use a library as a Scenario archive, then the process of executing a Scenario is as follows:

6.8.1 Select a Scenario

Do one of the following:

- From the Project Library, click **File** → **Open** to open an existing File Library (Figure 6.70). The File Library displays all saved Scenarios in that library from which you can select a Scenario.

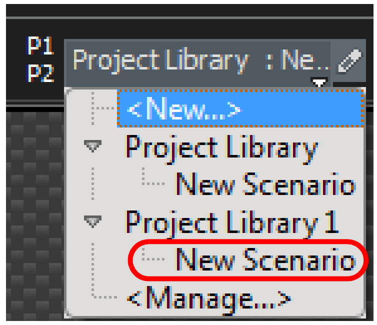


Figure 6.70: Project Library

- From a saved Scenario, select the desired Scenario from the drop-down list and click **Start Session** (Figure 6.71).

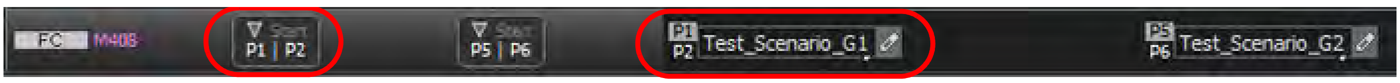


Figure 6.71: InFusion Control Interface Menu

The InFusion Control interface has the following controls:

Scenario drop-down list: . This is a drop-down list that lets you assign a scenario from the Project's library to the specified ports. Each port-pair has its own drop-down list and is assigned independently. The text on the left side of the drop-down list indicates the port-pair to which the scenario is assigned. The highlighted port label indicates the direction of jamming, which can be changed from the Scenario Manager interface (see section 6.5.10, *Traffic Modification Direction*).

6.8.2 Execute the Scenario from the Start/Stop Button

Start/Stop Session button: . This is a toggle button that starts or stops the session on the specified ports. Each port-pair has its own button and is controlled independently. The text on the bottom half of the button indicates the port-pair controlled by the button.

6.8.3 Log File of Scenario

Once the Scenario is complete or stopped the Output panel displays the Port, Time, Event, Action duration and value.

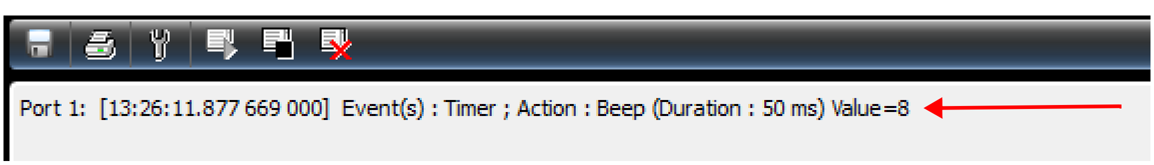


Figure 6.72: Output Panel Displaying Session Started and Stopped

Chapter 7

Infusion Batch Test Scenarios

7.1 Using the Batch Scenario Feature

You can run a sequence of executable scenarios to control both the Analyzer and the Jammer automatically. A Scenario Batch file is a a list of commands to run in sequence when you execute the file. A batch scenario can manage Jammer scenarios and Analyzer recordings and their assigned ports and hardware in sequence. The system checks for accuracy of inputs and commands.

Once a new Project is defined (see *3.1, Creating a New Project*), you can use the Batch Scenario feature: Select **File** → **Batch** to display the Batch Scenario Manager dialog (see Figure 7.1). Batch Scenarios are part of a Project and are saved as such. Each Project file can have a unique set of different Batch Scenarios.

A batch scenario can be repeated up to 10,000 times. To prevent infinite loops, branching to previous states is not permitted.

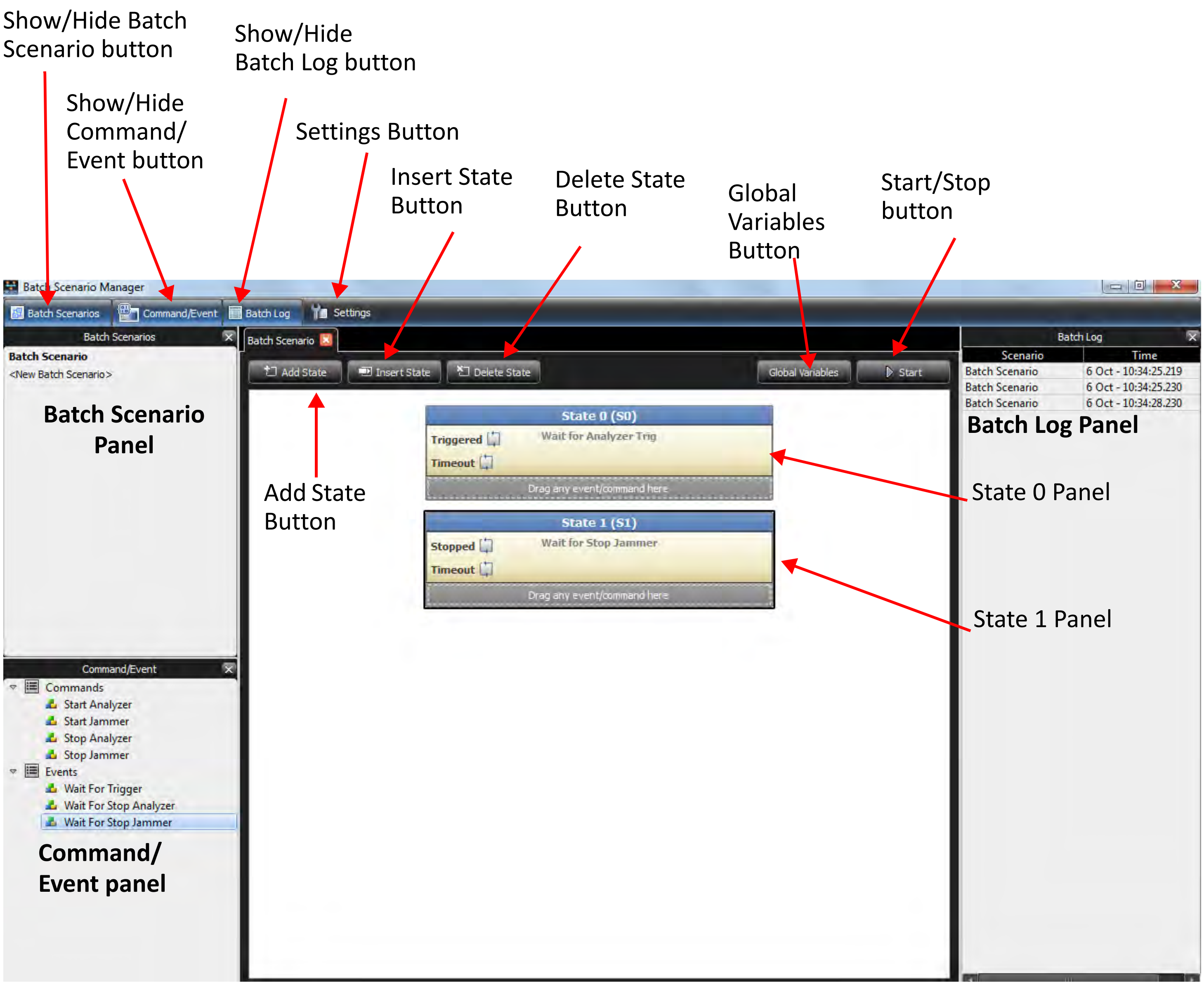


Figure 7.1: Batch Scenario Manager Window

7.1.1 Interface

The following buttons and panels are available to use the Batch Scenario functions:

- **Show/Hide Batch Scenario Button:** Toggles between showing/hiding the Batch Scenario pane.
- **Show/Hide Command/Event Button:** Toggles between showing/hiding the Command/ Event pane.
- **Show/Hide Batch Log Button:** Toggles between showing/hiding the Batch Log pane.
- **Add State Button:** Click to add a new state.
- **Insert State Button:** Click to insert a state after the selected state.
- **Delete State Button:** Click to delete the selected state.
- **Start Button:** Click to start the scenario.

- **Batch Scenario Panel:** Lists all the available Batch Scenarios. Double-click on <New Batch Scenario> to create a new scenario. The following operations are available through a right-click context menu:
  - Remove Scenario
  - Rename Scenario
  - Copy Scenario
  - Paste Scenario
- **Command/Event Panel:** Lists all the available Commands and Events.
- **Batch Log Panel:** Displays the scenario name, date and time run and description of the scenario.

NOTE: The log viewer reads up to 1000 entries, but when you save a batch log, it will contain the last 500,000 internal entries.

NOTE: To save the Jammer log from batch mode, enable "Automatic log" in the Jammer log settings.

7.2 Batch Scenario Overview

You create Batch Scenarios on a host machine running the Net Protocol Suite application. You then specify the Batch Scenarios for execution on a SierraNet platform.

The Net protocol Suite application provides a user friendly interface for building Batch Scenarios. The interface prompts you for simple decisions and choices using buttons and has a drag and drop interface. As you make your selections, the script takes shape automatically in the Batch Scenario window.

Click the **Add State** button, then drag and drop Commands and Events in the new State panels that get created. If invalid actions are assigned, then a red Invalid Session message displays in the Batch Log panel.

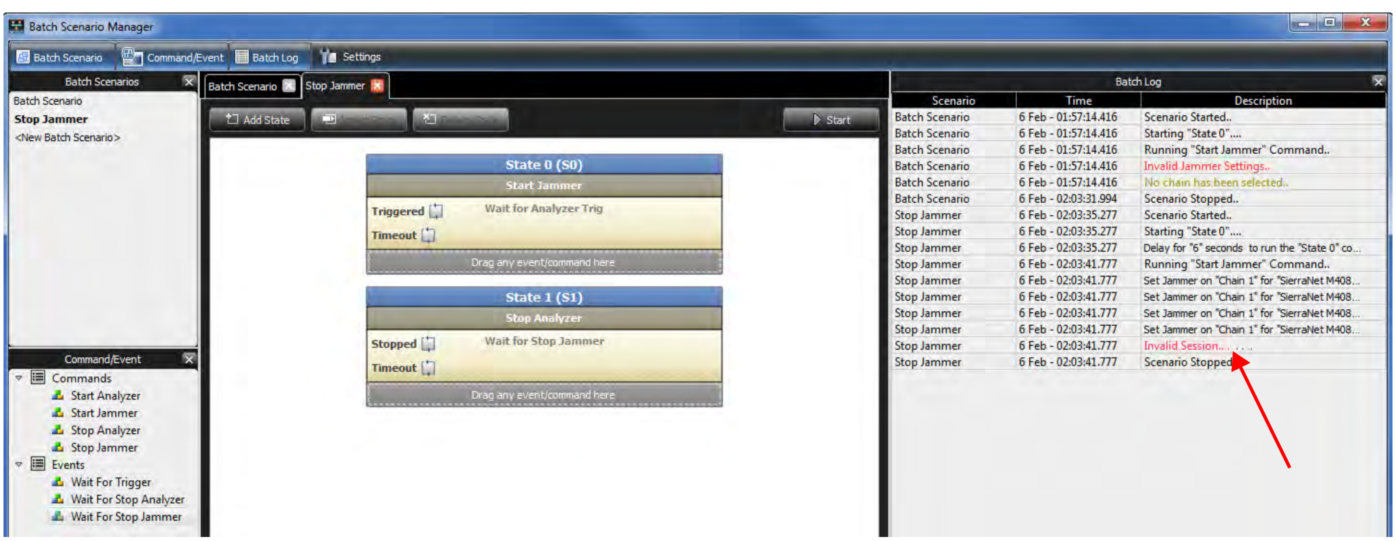


Figure 7.2: Add State Batch Scenario Manager

7.2.1 Adding Commands

Four types of commands are available:

7.2.1.1 Start Analyzer

Drag and drop the Start Analyzer command to display the Analyzer properties window.

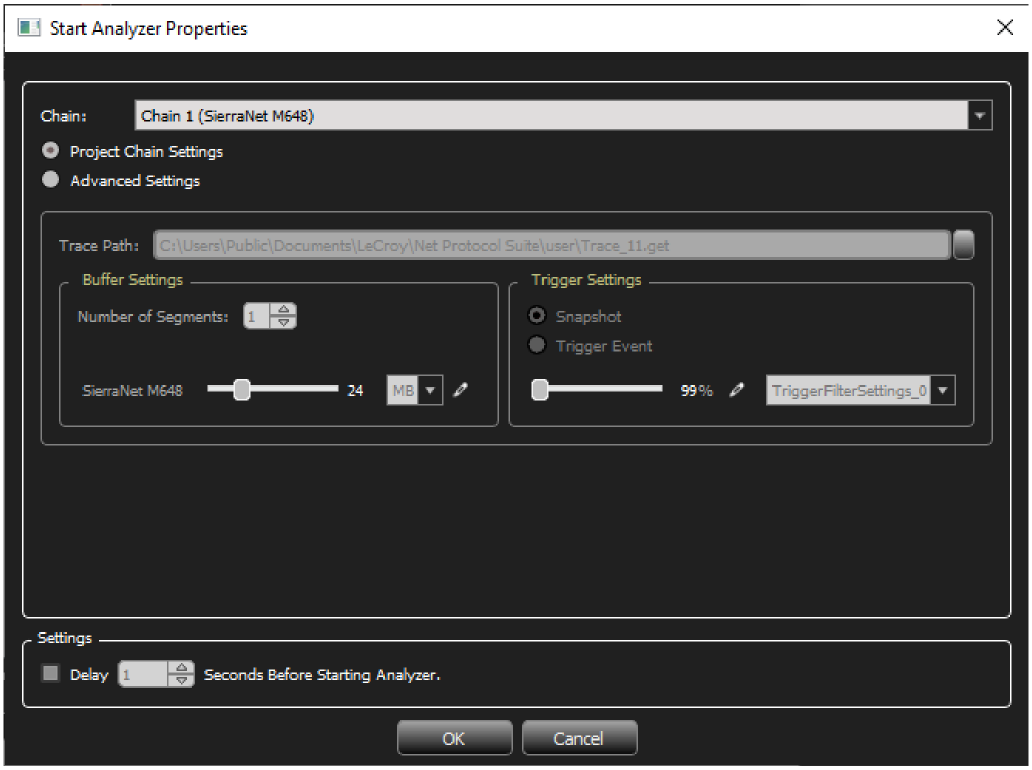


Figure 7.3: Start Analyzer Properties

Chain:	Select a Chain from the drop-down list.
Project Chain Settings:	Click this button to select Project Chain Settings.
Advanced Settings:	Click this button to select Project Chain Settings to activate the settings below:
Trace Path:	Click the ellipsis button to display the Select Trace File Name dialog to save the trace file.
Buffer Settings:	Set the number of segments and the buffer size.
Trigger Settings:	Select Snapshot or Trigger Event. Select the Trigger Filter Settings from the drop-down list and move the slider to the desired percentage.

7.2.1.2 Start Jammer

1. Drag and drop the **Start Jammer** command to display the *Start Jammer Properties* window (Figure 7.4).

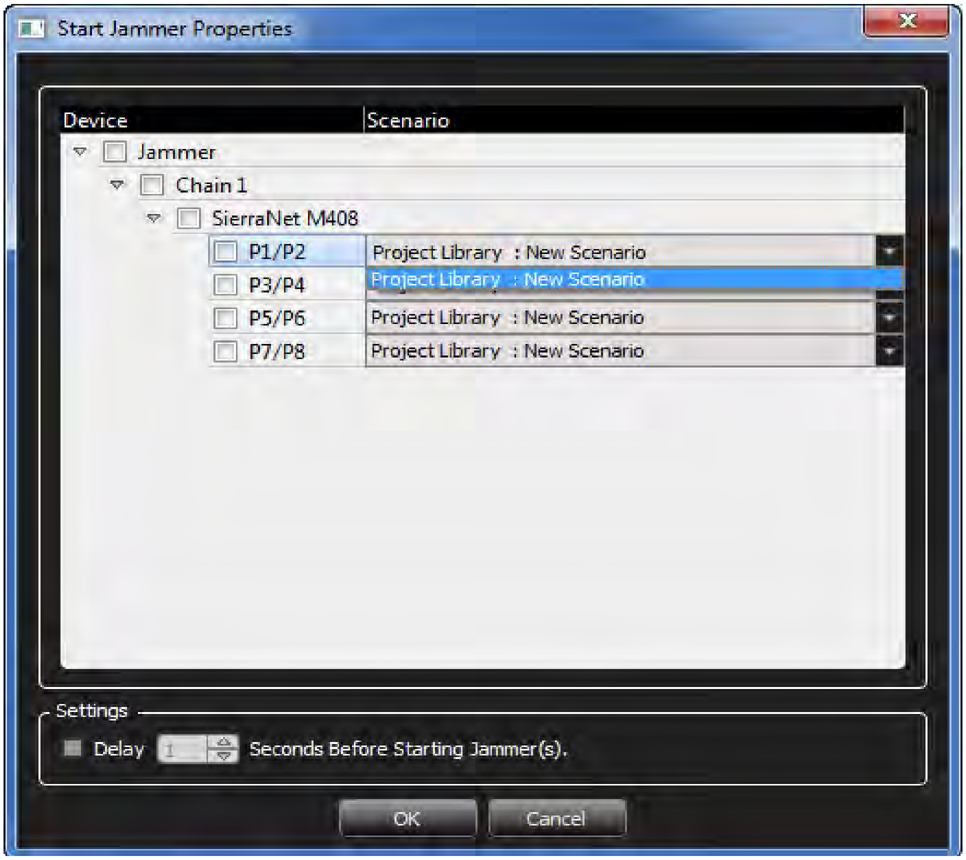


Figure 7.4: Start Jammer Properties

2. Select the **Jammer** check box to select all four port pairs, or select individual port pairs.

3. If a delay is needed after the command is executed, select the **Delay** check box and set the time in seconds.

7.2.1.3 Start Exerciser

Drag and drop the **Start Exerciser** command over the State Command tab to display the Start Exerciser Properties dialog ().

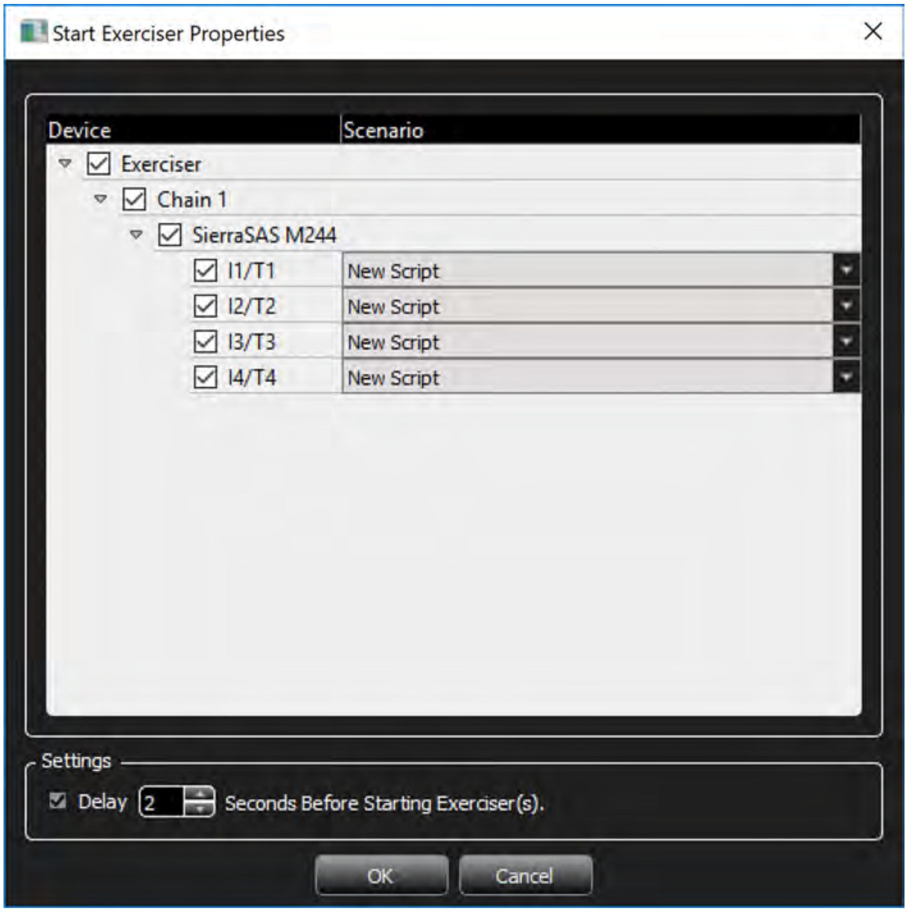


Figure 7.5: Start Exerciser Properties

7.2.1.4 Stop Analyzer

1. Drag and drop the **Stop Analyzer** command to display the *Stop Analyzer Properties* window (Figure 7.6).

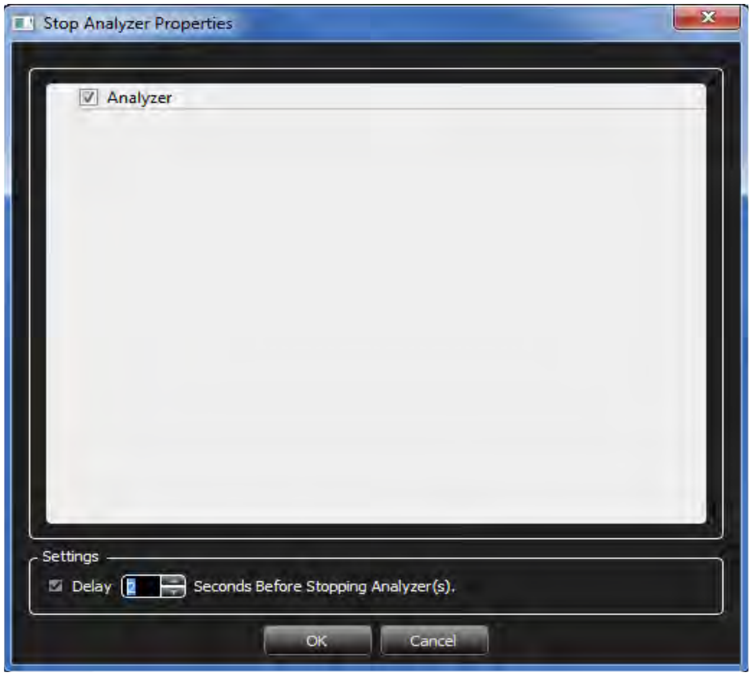


Figure 7.6: Stop Analyzer Properties

2. Select the **Analyzer** check box. If a delay is needed after the command is executed, check the **Delay** check box and set the time in seconds.

7.2.1.5 Stop Jammer

1. Drag and drop the **Stop Jammer** command to display the *Stop Jammer Properties* dialog window.

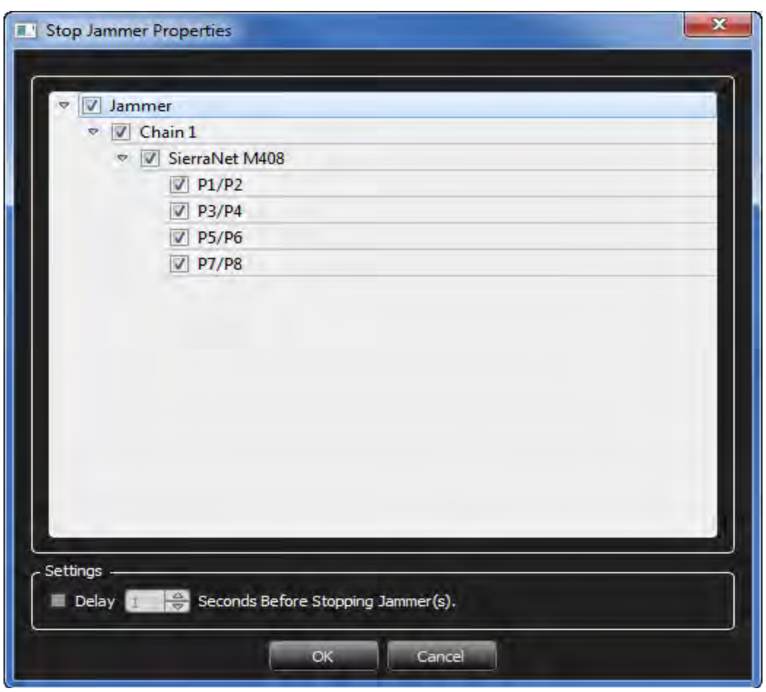


Figure 7.7: Stop Jammer Properties

2. Select the **Jammer** check box to select all four port pairs or select individual port pairs.

3. If a delay is needed after the command is executed, select the **Delay** check box and set the time in seconds.

7.2.1.6 Stop Exerciser

1. Drag and drop the **Stop Exerciser** command to display the *Stop Analyzer Properties* window (Figure 7.8).

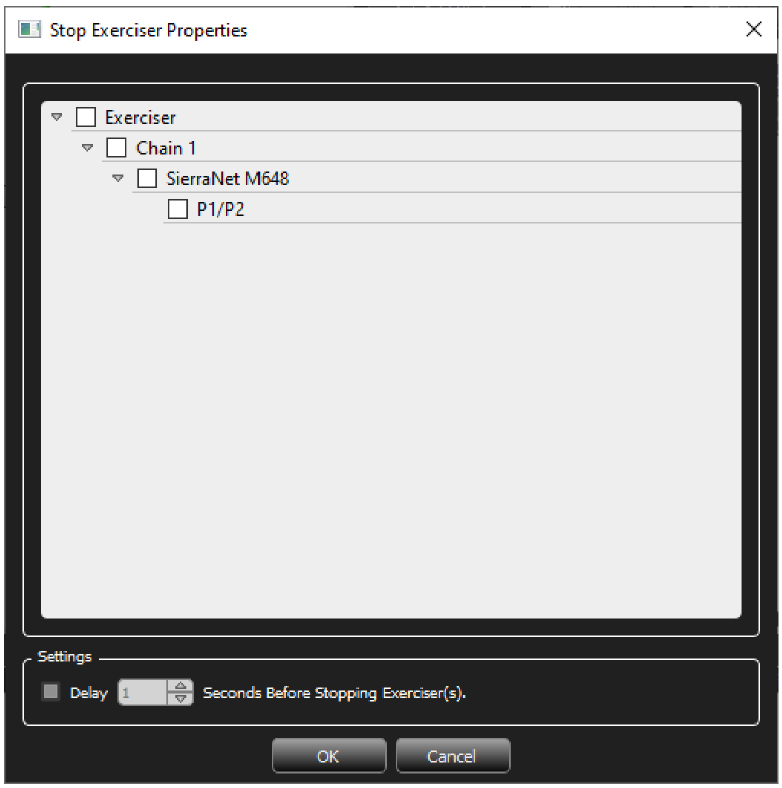


Figure 7.8: Stop Exerciser Properties

2. Click in the **Exerciser** check box to select all available port pairs or select individual port pairs.

3. If a delay is needed after the command is executed, select the **Delay** check box and set the time in seconds.

7.2.2 Adding Events

The four types of available events are described in this section:

- Wait for Trigger
- Wait For Stop Analyzer
- Wait For Stop Jammer
- Wait for Stop Exerciser

7.2.2.1 Wait for Trigger

1. Drag and drop the **Wait For Trigger** event to display the *Wait For Trigger Properties* window.

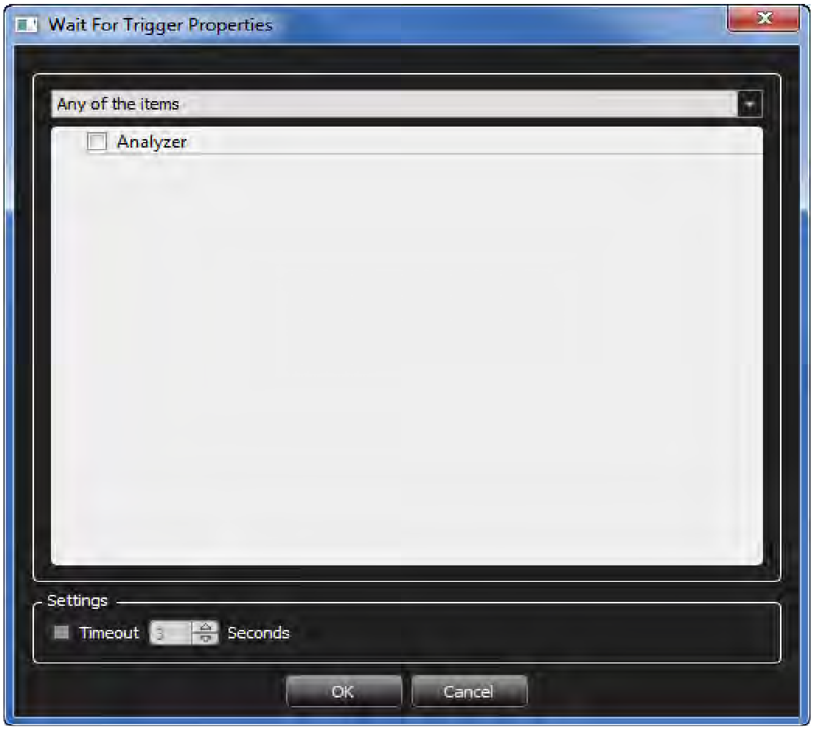


Figure 7.9: Wait For Trigger Properties

2. Select an option from the drop-down list.

3. To prevent an infinite Wait, you can select the **Timeout** check box and set the time in seconds.

7.2.2.2 Wait For Stop Analyzer

Drag and drop the **Wait For Stop Analyzer** event to display the *Wait For Stop Analyzer Properties* window (Figure 7.10).

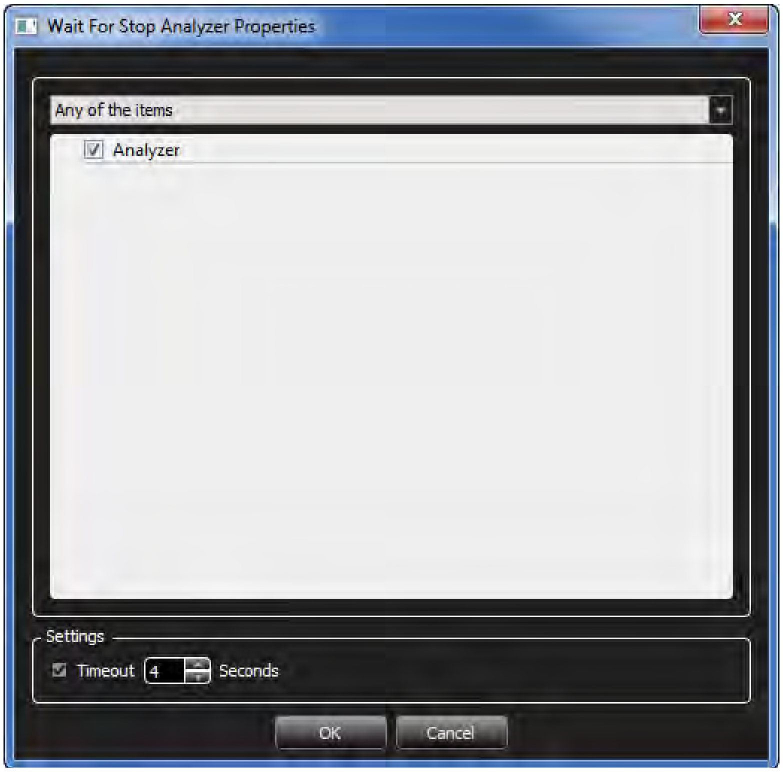


Figure 7.10: Wait for Stop Analyzer Properties

7.2.2.3 Wait For Stop Jammer

1. Drag and drop the **Wait For Stop Jammer** event to display the *Wait For Stop Jammer Properties* dialog window.

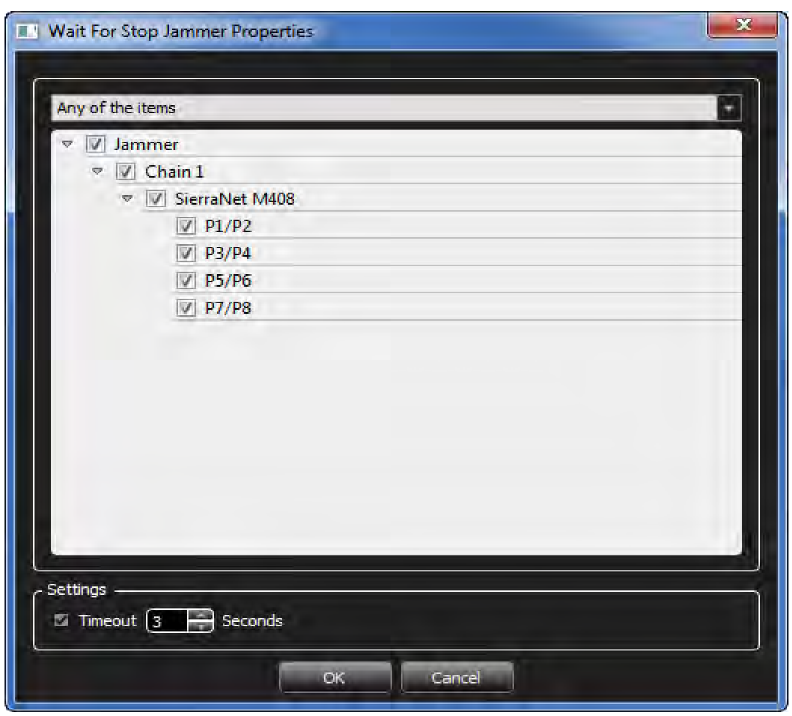


Figure 7.11: Wait For Stop Jammer Properties

2. Select the **Jammer** check box to select all four port pairs or select individual port pairs.

3. To prevent an infinite Wait, you can select the **Timeout** check box and set the time in seconds.

7.2.2.4 Wait for Stop Exerciser

1. Drag and drop the **Wait For Stop Exerciser** event to display the Wait For Stop Exerciser Properties dialog (Figure 7.12).

2. Click in the **Exerciser** check box to select all available port pairs or select individual port pairs.

3. To prevent an infinite Wait, select the **Timeout** check box and set the time in seconds.

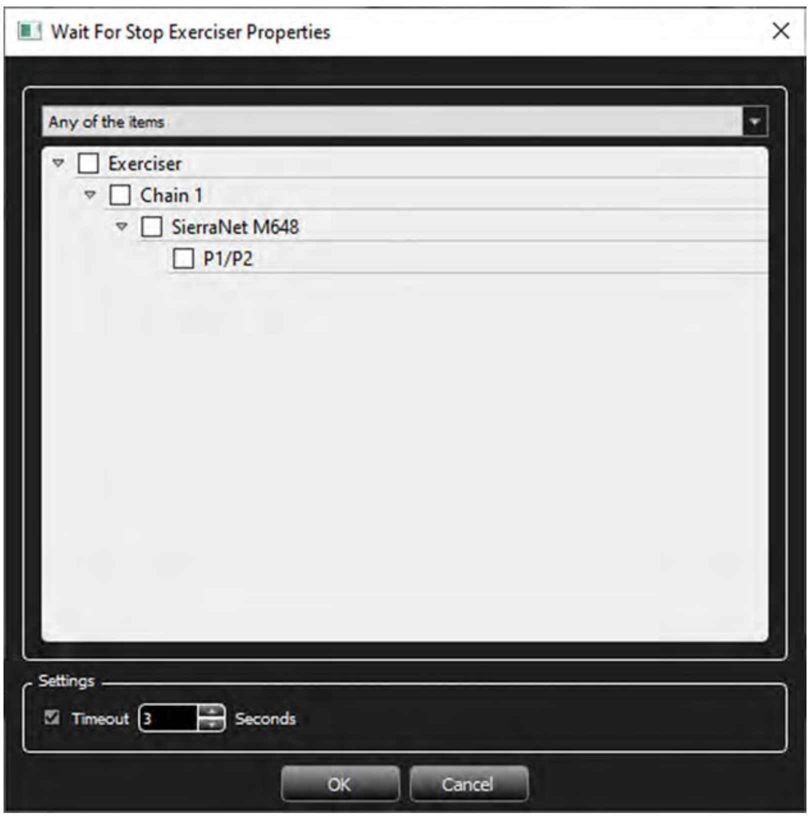


Figure 7.12: Wait For Stop Exerciser Properties

7.2.3 State Transition

1. Click the **State Transition**  icon to change the state to transition to.

2. Click the menu options to display as shown in Figure 7.13 and select the state to transition to.

3. To remove the state transition, select **No Jump**.

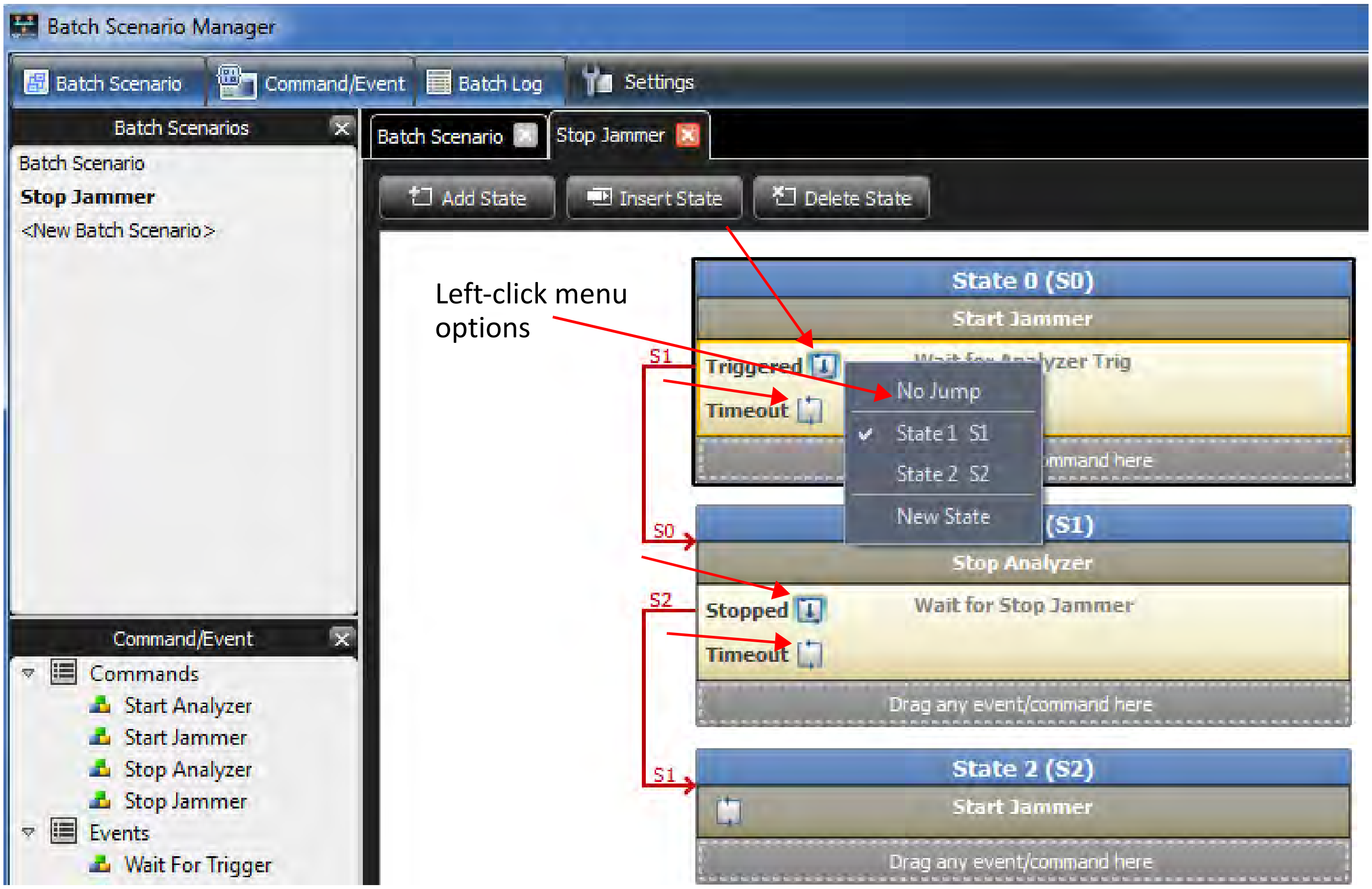


Figure 7.13: State Transition

7.2.4 Global Variables

Each batch scenario contains a list of global variables that allows you to set data for specific fields of frame events, or trigger setting patterns without editing them one by one. Global variables are automatically applied to all the trigger setting patterns that are selected in the *Start Analyzer* command immediately before you run the command.

If you select **Use Project Chain Settings** with the *Start Analyzer* command, global variables will be applied to the current trigger settings.

This also works for the Jammer. Global variables are applied automatically to all frame events of a Jammer scenario that are selected in the *Start Jammer* command, immediately before you run the command.

Global variables have no effect on any trigger settings or Jammer scenarios that are not used in the batch scenario.

Global variables provide dynamically changing event fields in runtime. You can add as many fields as you need to the global variable list and specify the value for them. When running batch mode, the software replaces the value in the specified field for any event in which that field is used. The software looks in all events for that field and replaces the value.

7.2.4.1 Global Variables Dialog Window

1. To change the definition of selected global variables, go to Batch Scenario Manager and click the **Global Variables** button. The Global Variables dialog window opens (Figure 7.15).

   This window consists of two panes: on the left, a tree of all available fields. On the right is a table of fields that can be selected.

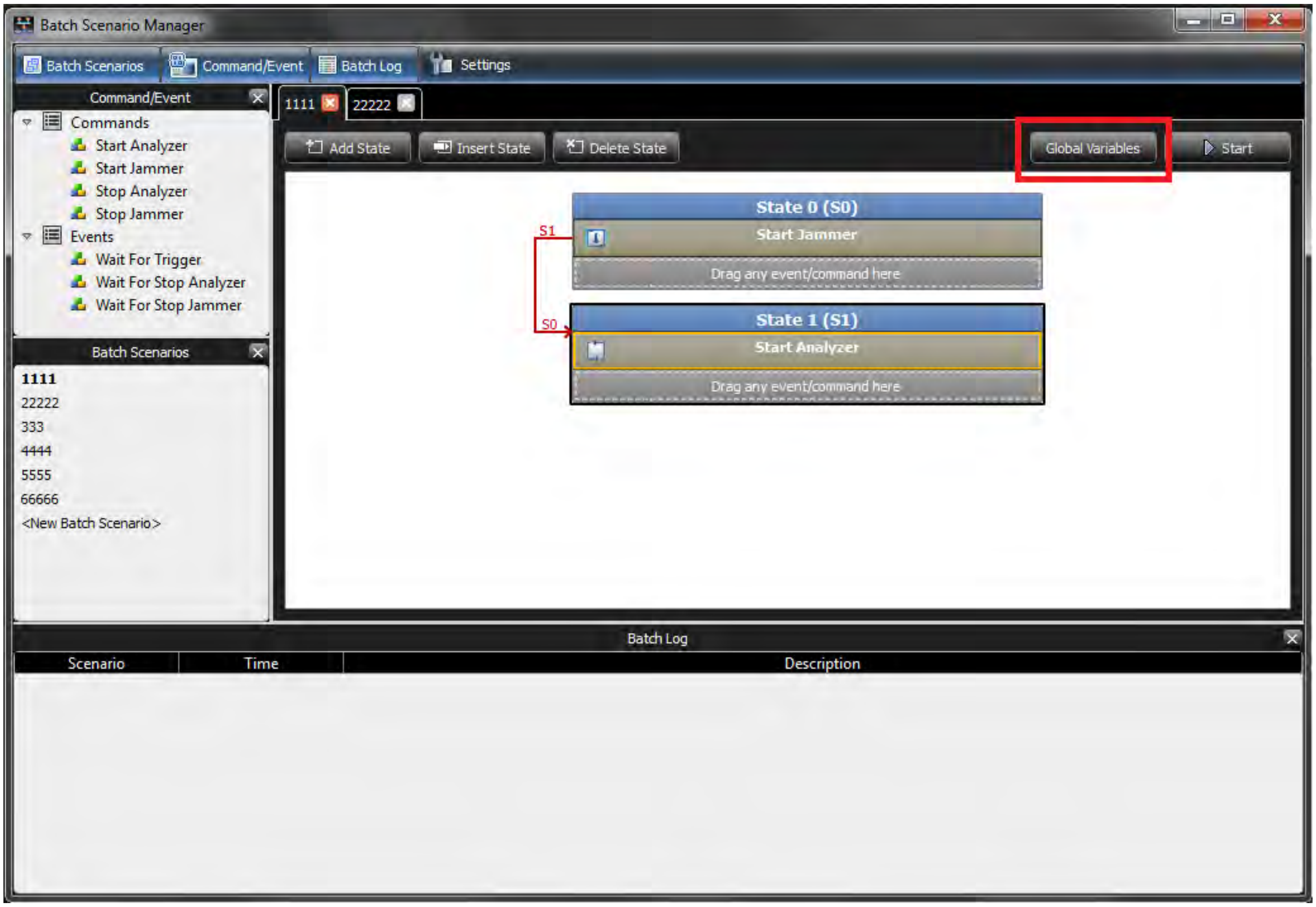


Figure 7.14: Batch Scenario Manager Window

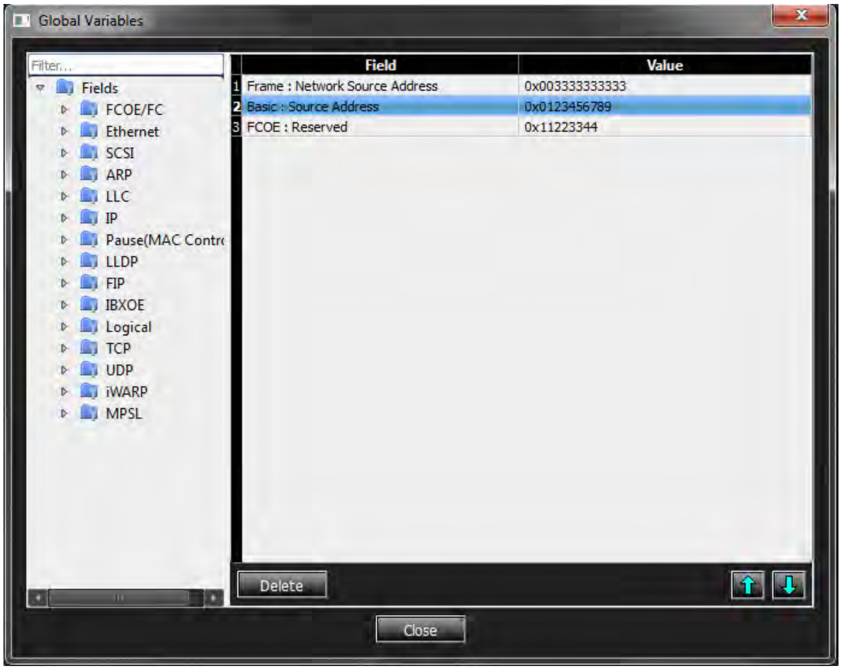


Figure 7.15: Global Variables Dialog Window

2. To add a global variable to the table, drag a field from the tree on the left and drop it into the table on the right. This adds the field to the table with an empty value.

3. To edit the value, double-click on the value cell.

   - A red "**H**" appears at the left of the value cell (Figure 7.16). This shows, by default, that the value is to be in hexadecimal format.
   - You can switch between binary and hexadecimal by simply clicking on the red H; it changes to a red "B" for binary. (See Figure 7.17.)

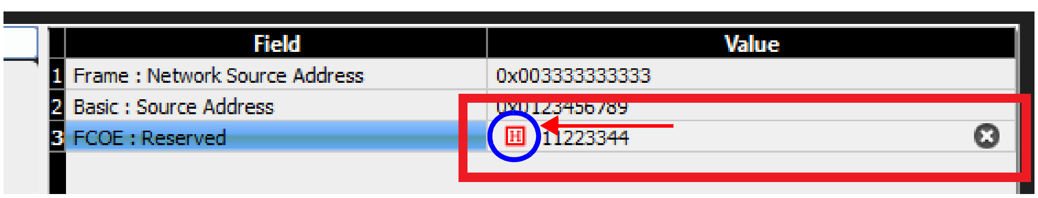


Figure 7.16: Hexadecimal Button

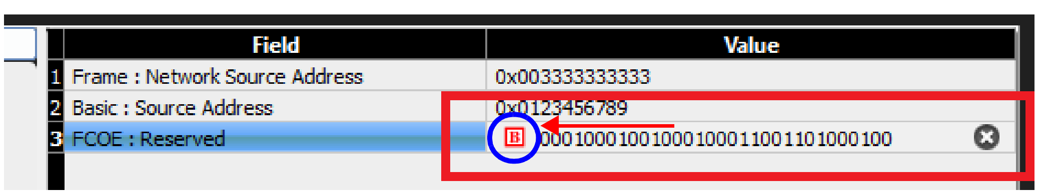


Figure 7.17: Binary Button

   - There is no length limit for the value, but it may trimmed according to field length when it is applied to a frame pattern or event.

4. To remove a global variable, simply select it on the table, then click **Delete**. The variable is removed from the right pane of the dialog.

The **Up** and **Down** arrows (Figure 7.18) let you rearrange the order of variable values that you wish to change, before Net Protocol Suite runs a scenario. For most fields, the order does not matter. However, for the fields that do change the format of events, this order becomes important.

For example:

Suppose you want to change the value of the field **Opcode** in a SCSI command, then change one of the other fields in that SCSI command:

- When you set Opcode fields, the event fields will be changed automatically; therefore, you must move the Opcode field to the top of the list. You can then change the value of another field.
- On the other hand, if you want to set the value of a field (e.g., **Originator S_ID**), changing its value has no effect on the format of other fields in an event. Therefore, you do not need to specify the order in which these fields are accessed.

Figure 7.18: Delete Button & Up/Down Arrows

NOTE: Replacing any value in a frame pattern or event may cause other fields values to reset. To avoid this, make sure you select the correct order of global variables.

For example:
Assume there is a batch scenario with one “Start Jammer” command and global variables as shown in Figure 7.19 and Figure 7.20.

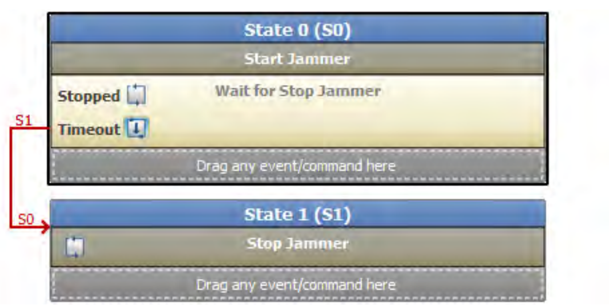


Figure 7.19: Example Batch Scenario

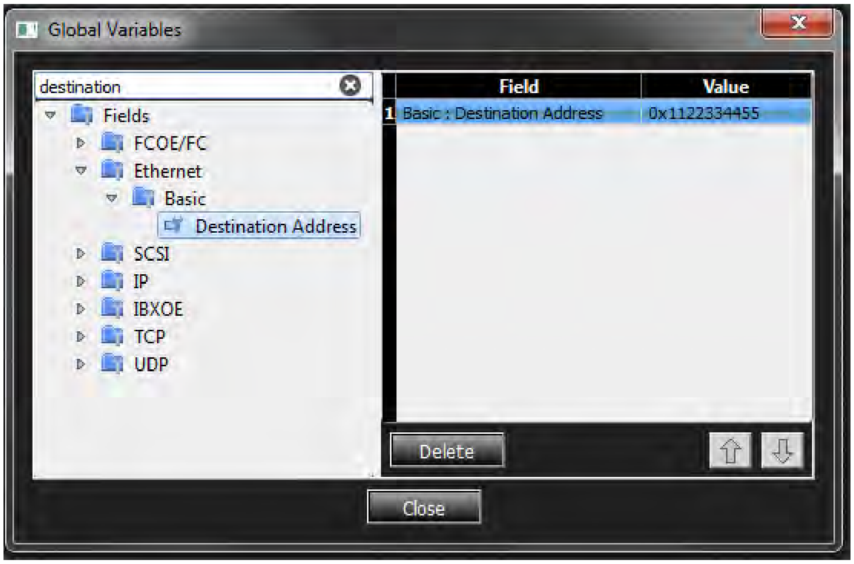


Figure 7.20: Selected Destination Address Field

A batch scenario such as this can run a Jammer scenario with a Frame Event. An example is shown in Figure 7.21.

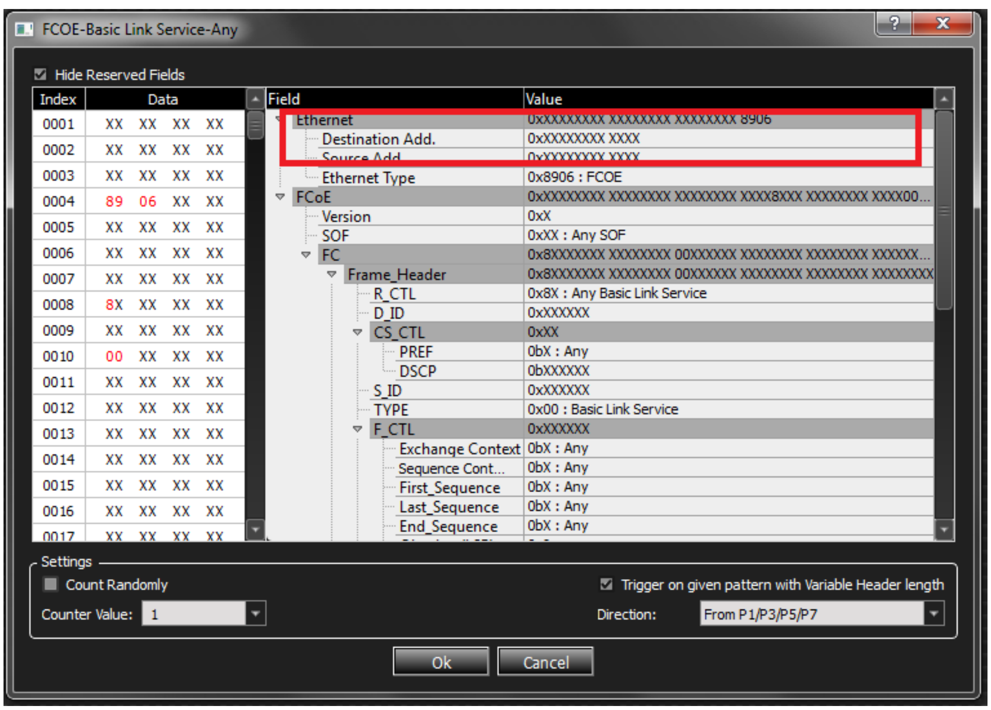


Figure 7.21: Destination Address Before Changes

As you see, the *Destination Address* field is 0xXXXXXXXX XXXX. After starting the batch scenario, the expected behavior is for the *Destination Address*" field to be replaced with the value 0x1122334455 from the defined global variable.

If you check the same Jammer Frame event after running the batch, the result will be as seen in Figure 7.22, which is the expected behavior.

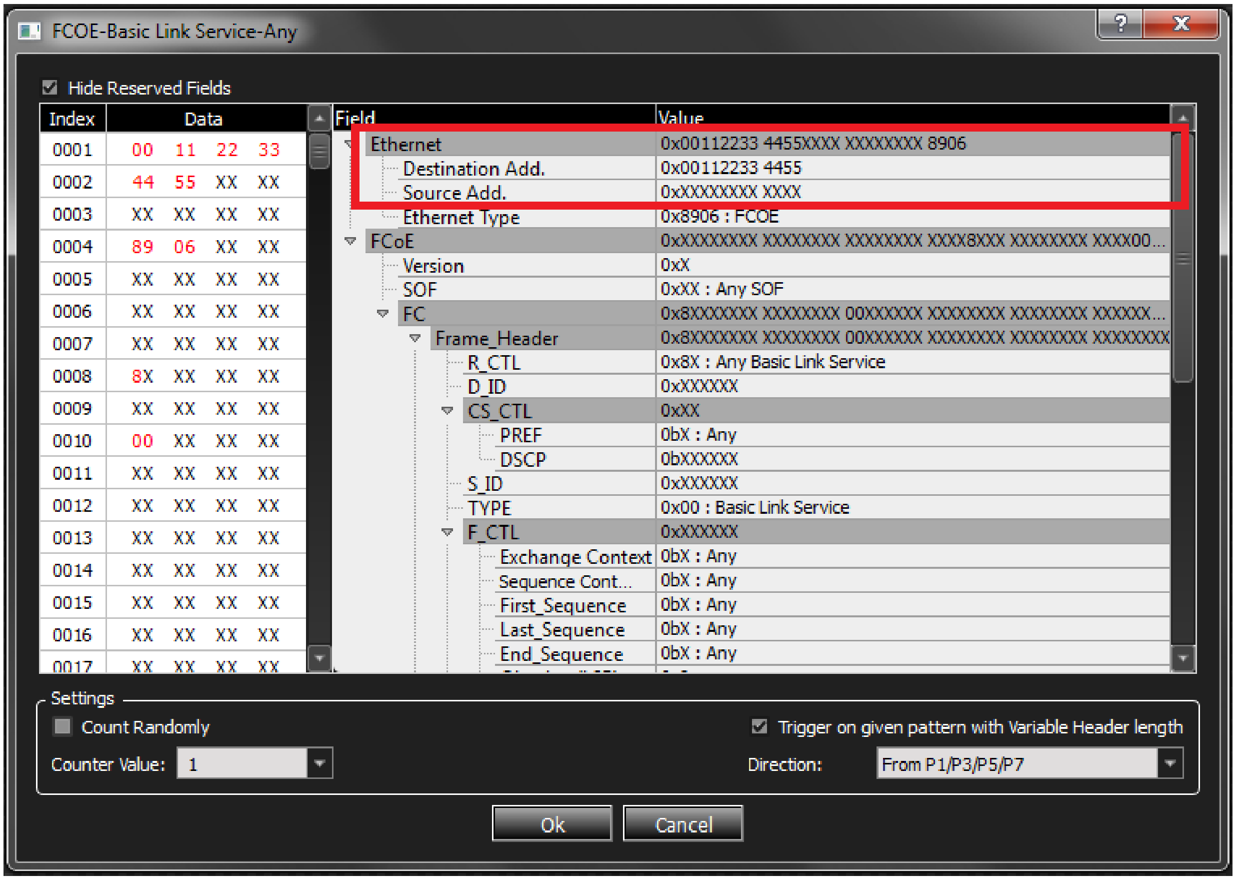


Figure 7.22: Destination Address After Changes

NOTE: This function makes changes in the actual frame pattern/event which will result in changes in your project.

Chapter 8

FC Exerciser

The Sierra Exerciser is a traffic generator that emulates FC Initiator/Targets. Traffic generation enables engineers to test designs under realistic conditions and to transmit known errors, allowing engineers to observe how devices handle faulty link conditions.

8.1 Setting Up for Generating Initiator Traffic

Connect the FC cable from the **Target** port of the Sierra Net Analyzer to the Target port on the unit under test. This transmits the Traffic Generator stream from the **Target** port to the Target-side port on the unit under test.

8.2 Setting Up for Generating Target Traffic

Connect the FC cable from the **Initiator** port of the Sierra Net Analyzer to the Initiator-side port on the unit under test. This transmits the Traffic Generator stream from the **Initiator** port to the Initiator-side port on the unit under test.

8.3 Traffic Generation

Traffic generation is performed via the execution of text-based scripts. These scripts contain statements about the types of traffic to be generated. These script files can be edited with the Script Editor utility provided by the application.

8.3.1 Launching the Exerciser Script Editor

To start the Exerciser:

1. Launch the NET Protocol Suite software. See Figure 8.1.

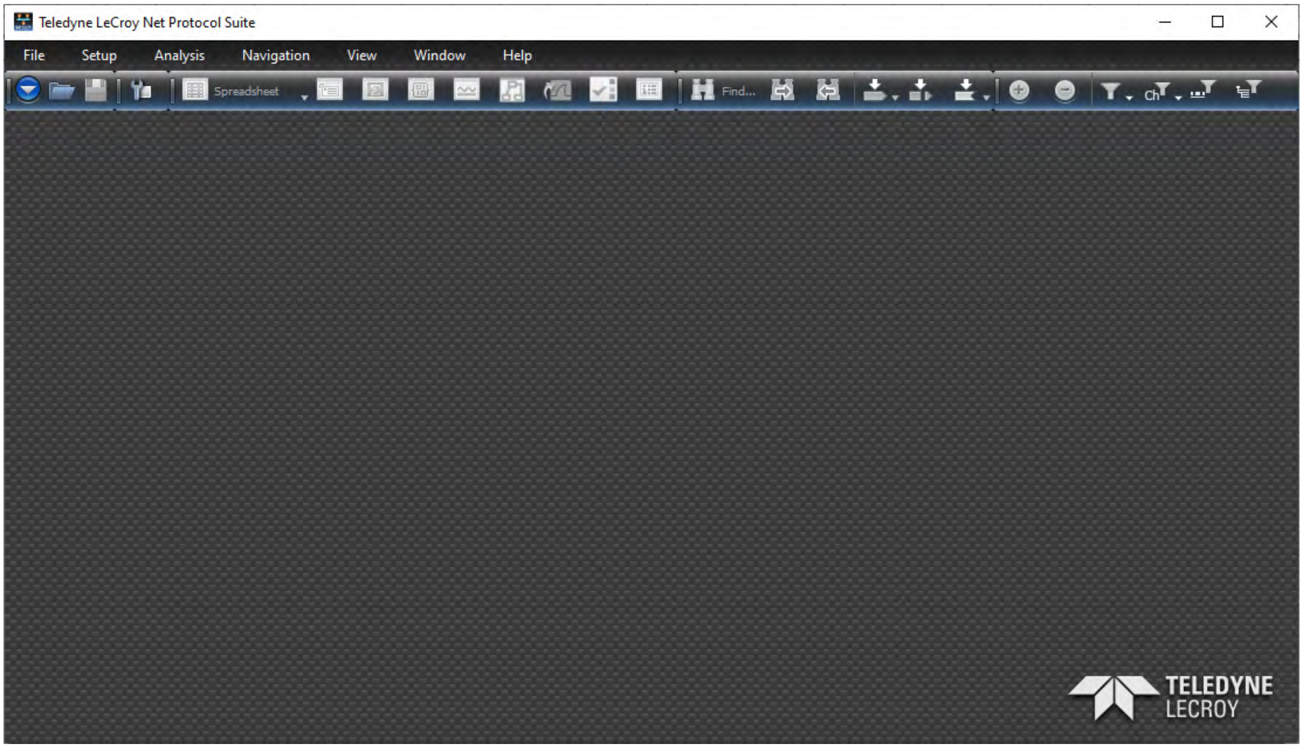


Figure 8.1: Net Protocol Suite Main Screen

2. Select **File → New Project**. See Figure 8.2.

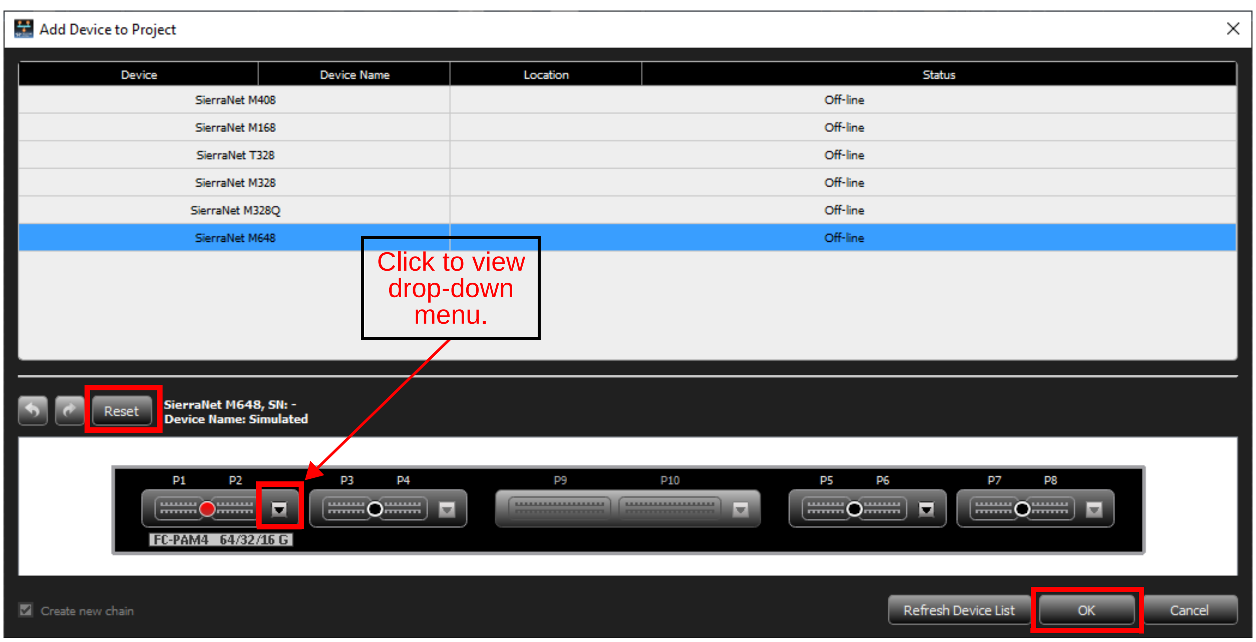


Figure 8.2: Add Device to Project

3. With the **SierraNet M648** selected, click Reset. This updates the port configurations and available speeds for the selected device.

4. To set up the port configuration:
   a. Click the drop down arrow next to the active ports to configure (Figure 8.3).
   b. Select an **Analyzer** or **Analyzer/Exerciser** configuration.
   c. Select an available FC speed.
   d. Click **OK**.

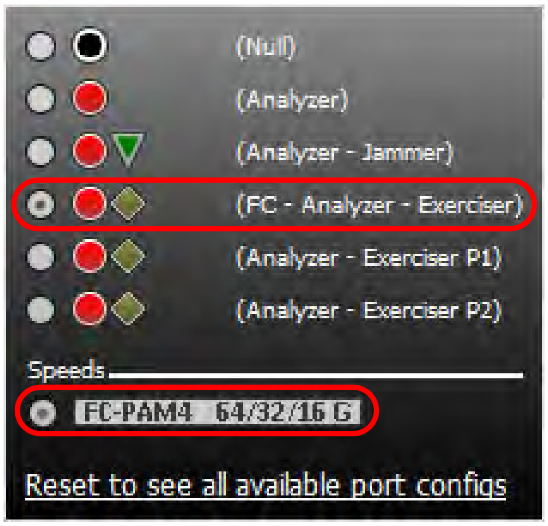


Figure 8.3: M648 P1/P2 Drop-Down Menu

The Main Screen appears with New Script Icons for each Initiator/Target pair. Figure 8.4.

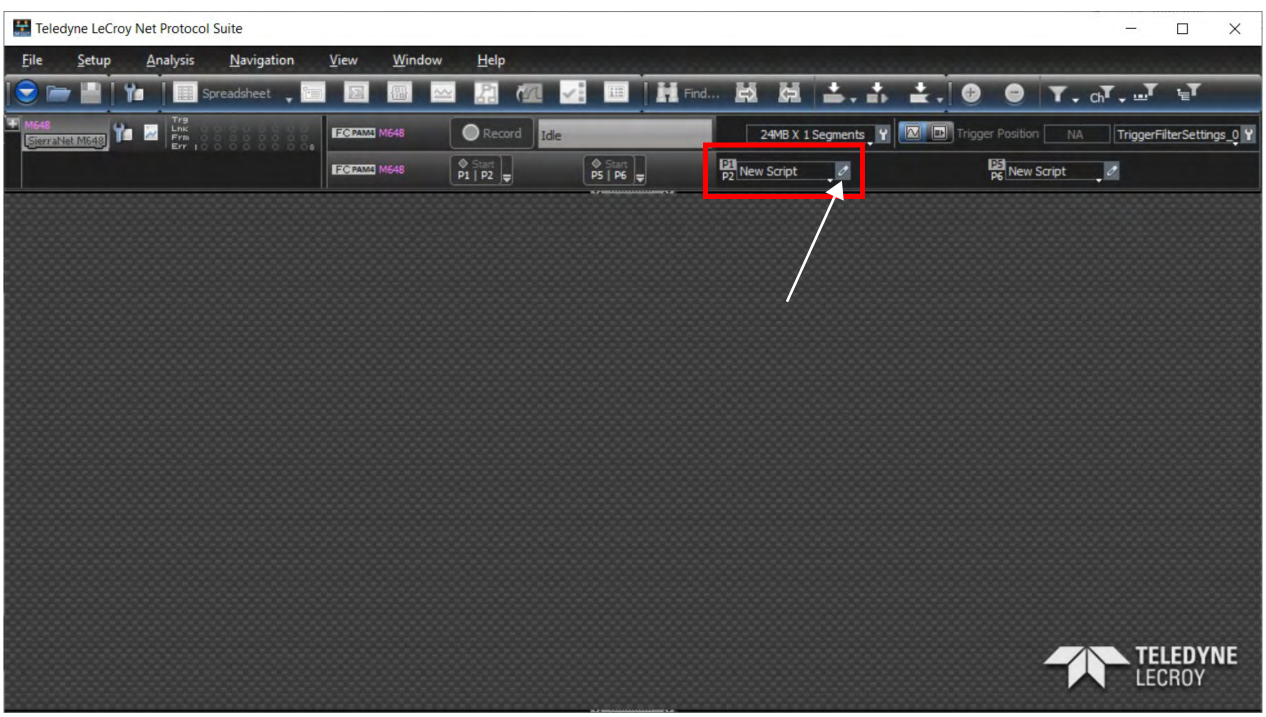


Figure 8.4: Main Screen with Script Icons for Target Ports

5. Click the small pencil icon next to the New Script tab to bring up the Exerciser Script Manager (Figure 8.5).

   For more information, see 8.3.2, *Exerciser Script Manager*, and 3.1.2, *Port Configuration*.

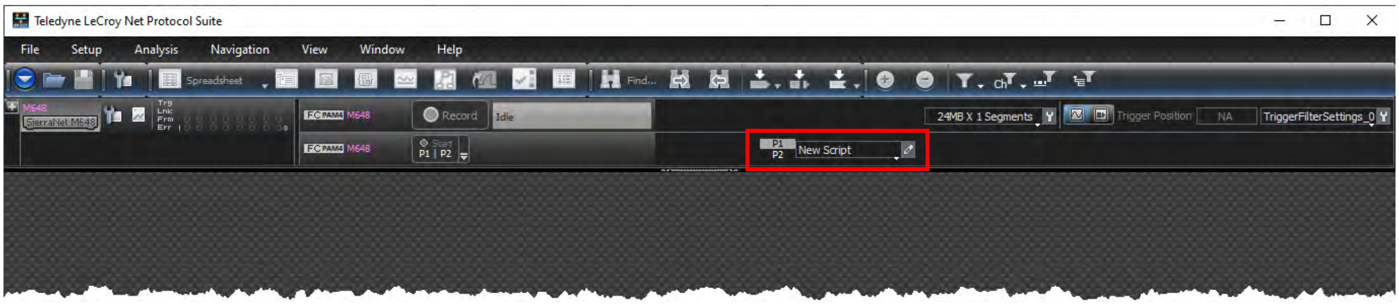


Figure 8.5: FC4 Main Menu with New Script Icons

8.3.2 Exerciser Script Manager

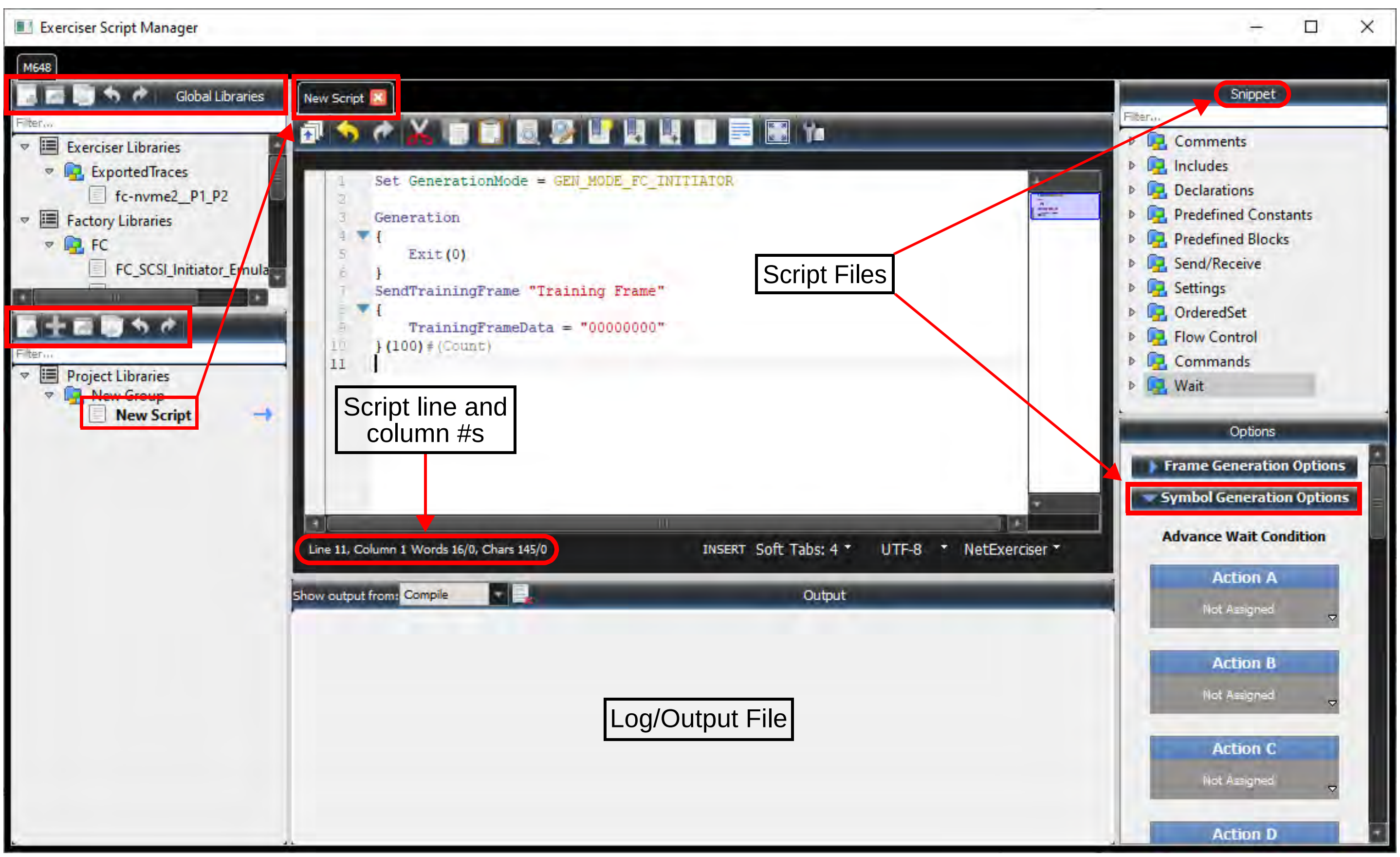


Figure 8.6: Exerciser Script Manager

The Exerciser Script Manager dialog has the following sections:

- Global Libraries (See 8.3.3, *Global Libraries Panel – Exerciser Libraries*.)
  - New Group (See 8.3.3.2, *Exerciser Libraries – New Group*.)
  - Export to File (See 8.3.3.3, *Exerciser Libraries – Export to File*.)
  - Import from File (See 8.3.3.4, *Exerciser Libraries – Import From Exerciser Script File*.)
- Project Libraries (See 8.3.4, *Project Library Panel*.)
  - New Group (See 8.3.4.2, *Add New Library Group Icon*.)
  - New Exerciser Script (See 8.3.4.3, *Add a New Exerciser Script to Project Library*.)
  - Export to File (See 8.3.4.4, *Export Exerciser Script Library to File*.)
  - Import from File (See 8.3.5.4, *Snippet Window*.)
- New Script Text Editing Window (See 8.3.5, *Script Text Editor Window*.)
  - Top: Toolbar (See 8.3.5.2, *Script Editor Toolbar*.)
  - Bottom: Status, Controls
- Output Log Window (See 8.3.5.3, *Exerciser Output Log Window*.)
- Snippet Window (Drag and drop a Snippet into the Scripting Editor to ensure the syntax is correct. See 8.3.5.4, *Snippet Window*.
- Generation Options Window: The Generation Options window is used when you want an “Advance Wait Condition”. See 8.3.5.5, *Generation Options (Advance Wait Conditions)*.

8.3.3 Global Libraries Panel – Exerciser Libraries

8.3.3.1 Global Library

The Global Library Panel keeps groups of scripts which can be used in other projects. This global library is saved in the preferences and not in the project.

The Main Library window (on the left) displays the available Exerciser Library Scripts. You can create a New Script, Open Containing Folder, Copy Container Folder Path, Add New Library, Rename Library or Remove Library. The Scripts saved on a specific platform in the Global Library are available in all projects for the same platform.

In the Global Libraries Panel at the Library Level (with a Right Click) you can:

- Cut a Library
- Copy a Library
- Paste a Library
- Delete a Library
- Rename a Library
- Sort Libraries
- Sort All Libraries
- Add a New Group
- Export Libraries to a File
- Import Libraries from a File

See Figure 8.7.

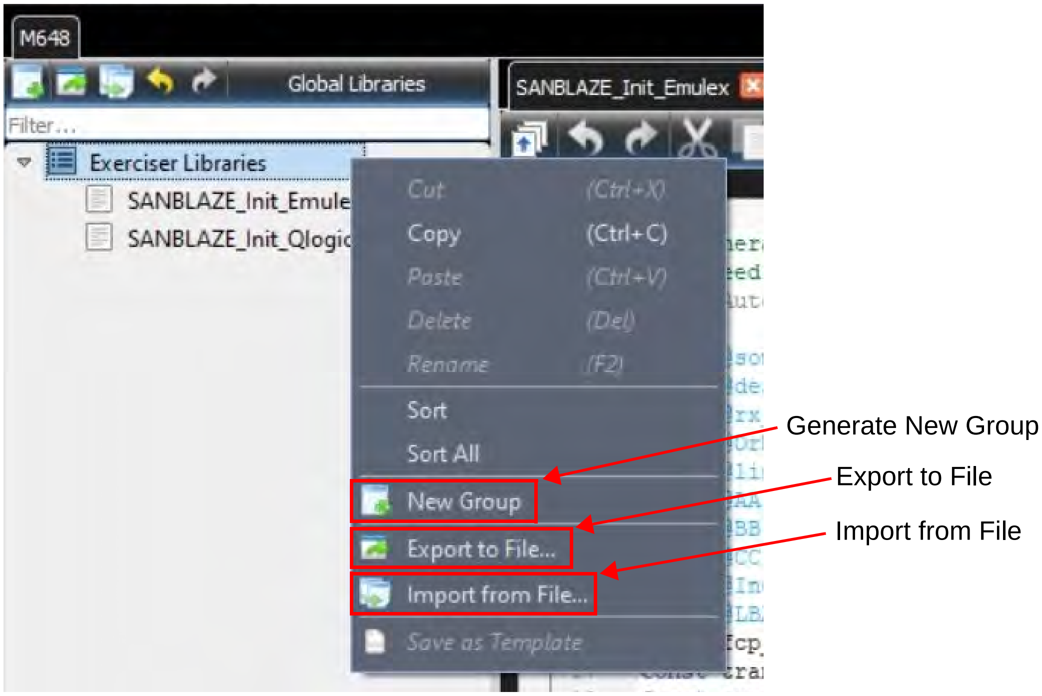


Figure 8.7: Operations Available from Global Libraries Panel (with Right Click)

8.3.3.2 Exerciser Libraries – New Group

The *New Group* icon has a number of functions depending on how it is used:

- If nothing in the tree list is selected, then *New Group* is disabled.
- If Exerciser Libraries is selected, then *New Group* will add a New Group folder underneath Exerciser Libraries.
- If a folder is selected, then *New Group* will add a New Group folder underneath the selected folder.

If you click on **New Group** a new Library called *New Group* will show up in the Global Libraries pane. You can rename it by right clicking on it and changing the name to something that makes sense for your testing. See Figure 8.8. Its primary function is to help you organize your Global Script Libraries.

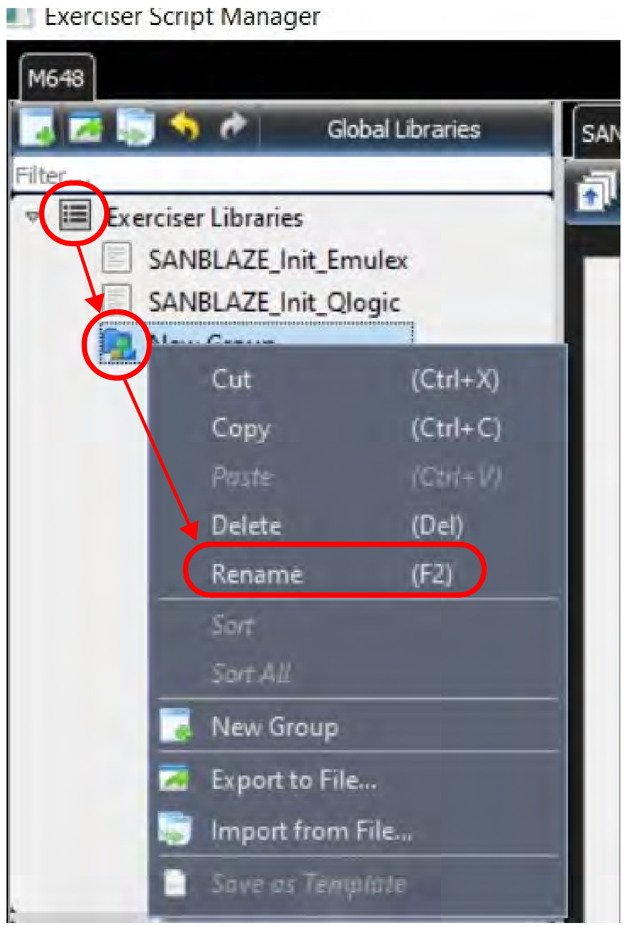


Figure 8.8: Global Libraries: Add a New Group → Rename

8.3.3.3 Exerciser Libraries – Export to File

If you select “Export to File” the following menu displays. Navigate to the Project folder to export your Project Library to a File. See Figure 8.9.

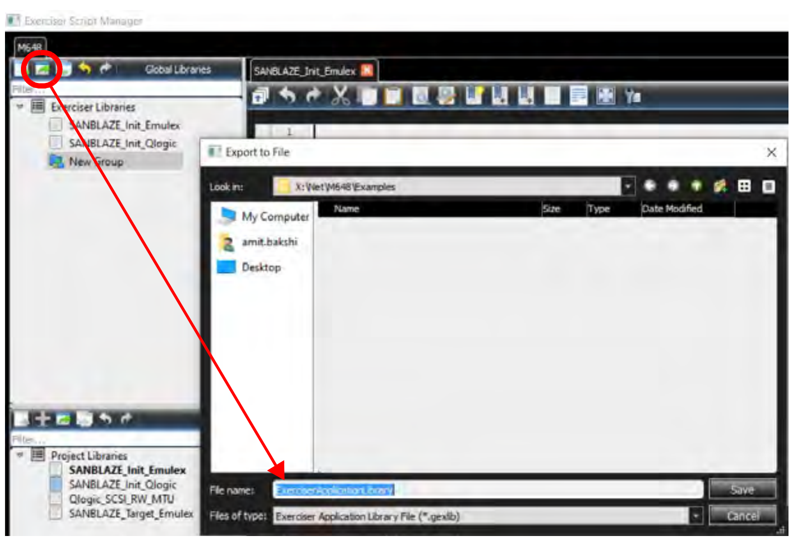


Figure 8.9: Export Script Library to a File

8.3.3.4 Exerciser Libraries – Import From Exerciser Script File

You can also Import Libraries from an Exerciser Script Library File. See Figure 8.10.

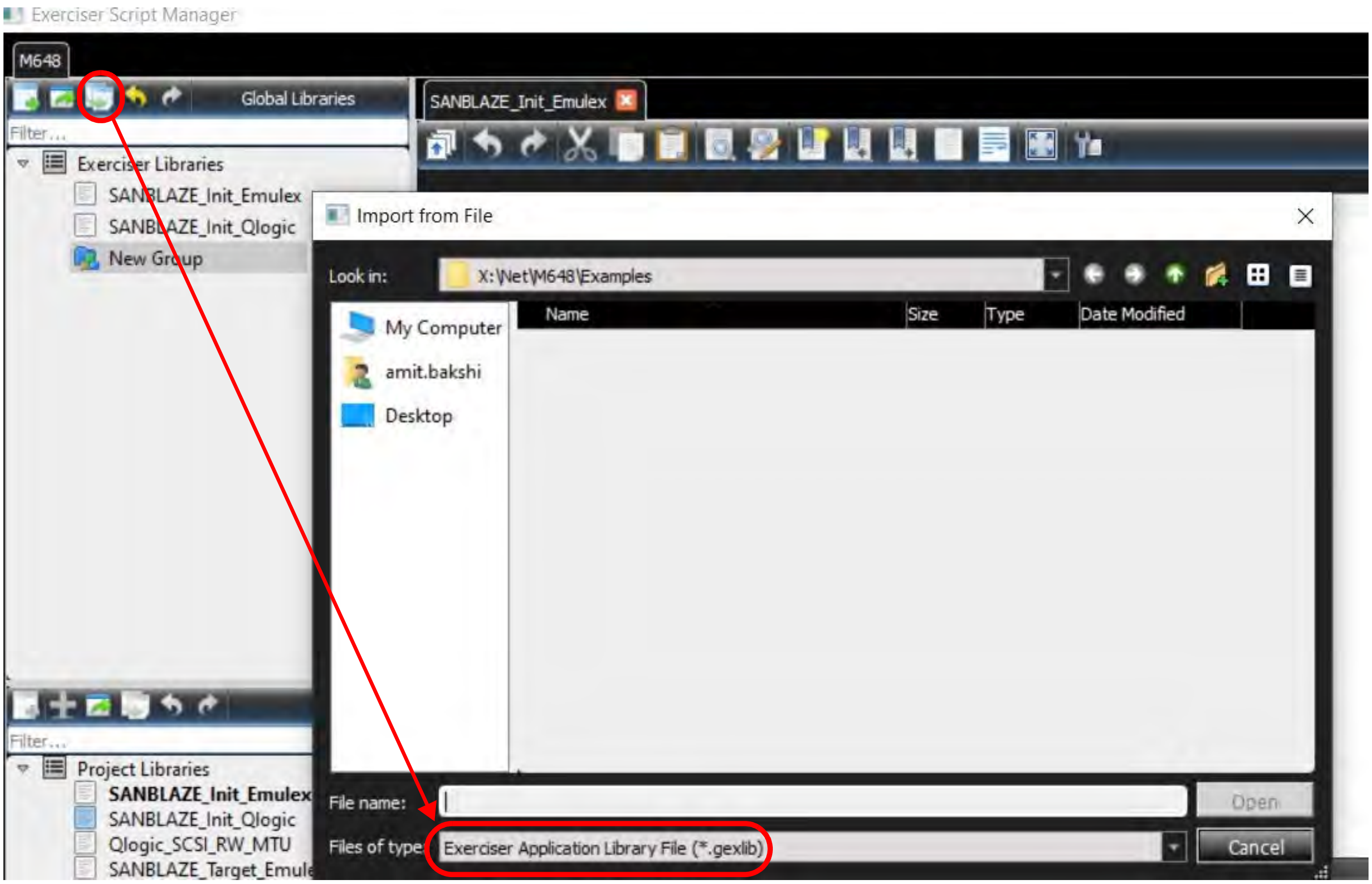


Figure 8.10: Import Script Library from File with .gexlib Extension

8.3.3.5 Import Exerciser Script from File

You can import an example file by clicking on that option and importing all of the scripts in the imported library (Figure 8.11).

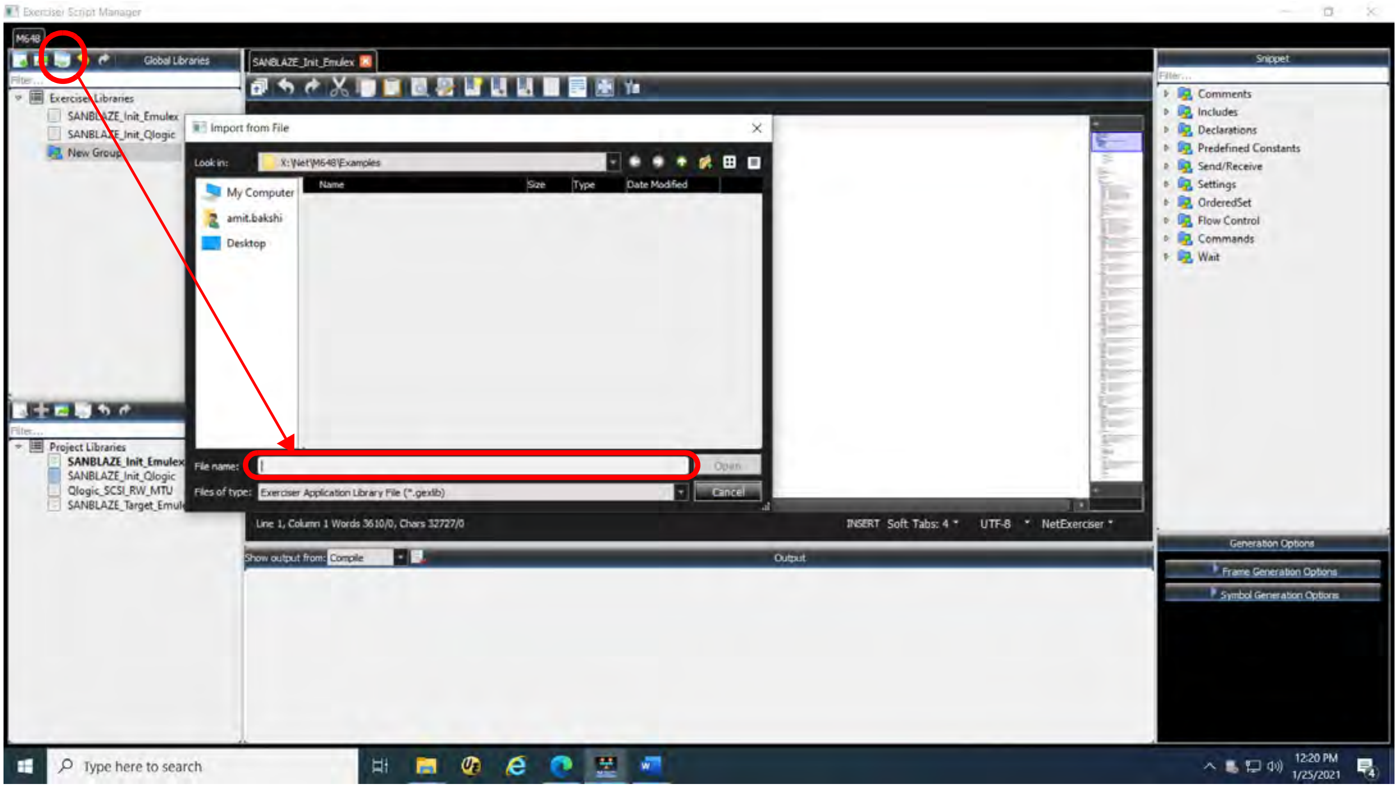


Figure 8.11: Import From File: Examples ➔ *.gexlib

8.3.3.6 Project

The Project is responsible to keep and persist defined scripts under the Project Library. To keep any script changes, either manually save the project or use “Auto Save” in the Exerciser settings dialog.

NOTE: Include files are not persistent in the project. So, they are saved automatically if any change is applied by the Exerciser Editor.

8.3.3.7 Session

The Exerciser session will have a three-state button to support Start, Stop and Continue:

- **Start**: To run a specific port Exerciser.
- **Stop**: To Stop currently running Exerciser in the port.
- **Continue**: Whenever the running script reaches a Pause command, it will be paused. The **Stop** button will be changed to **Cont.** and start blinking. Pressing **Cont.** will continue running the paused script.

8.3.3.8 Script Assignment

The Exerciser GUI will work the same way as the Jammer GUI, when configured as an Exerciser, it will show a drop-down list to choose an existing script from the Project Library or create a new one. See Figure 8.12.

Figure 8.12: Select a Script

8.3.3.9 Exerciser Status

NOTE: Based on the Script mode (Initiator/Target), it will highlight Ix or Tx icons in the left side of the Script Assignment.

The Exerciser Status and Exit code of each port will be shown in Device Output. See Figure 8.13.

Figure 8.13: Device Output: Exerciser Status

8.3.4 Project Library Panel

8.3.4.1 Project Library

The Project Library keeps scripts used in this project. It keeps scripts by saving the project library in the project. However, related include files won't be saved in the project.

NOTE: Discarding the Project will lose any changes in the exerciser script. To prevent this, enable "Auto Save Project" in the Exerciser Settings dialog.

Project Library Toolbar

- New Group: Creates a new group in project library.
- New Exerciser script: Makes a new script which is created from a default template script. Users can change the default script from the Exerciser Setting.
- Export: users can export the scrip or the whole library (*.gexlib).
- Import: users can import any FC Exerciser library (*.gexlib)

Project Library Tree

- Each item keeps a group or an Exerciser script.
- I or T will be shown in front of each script to identify the script generation mode (Initiator or Target).

The Project Library window (on the left) displays the project libraries. The Scripts saved in the Project Library are only available for the current project. See Figure 8.14.

In the Project Libraries Panel at the Script Level (with a Right Click) you can:

- Cut a Library
- Copy a Library
- Paste a Library
- Delete a Library
- Rename a Library
- Sort Libraries
- Sort All
- Add New Group (or add New Project Library)
- Add New Exerciser Script
- Export to a file
- Import from a File

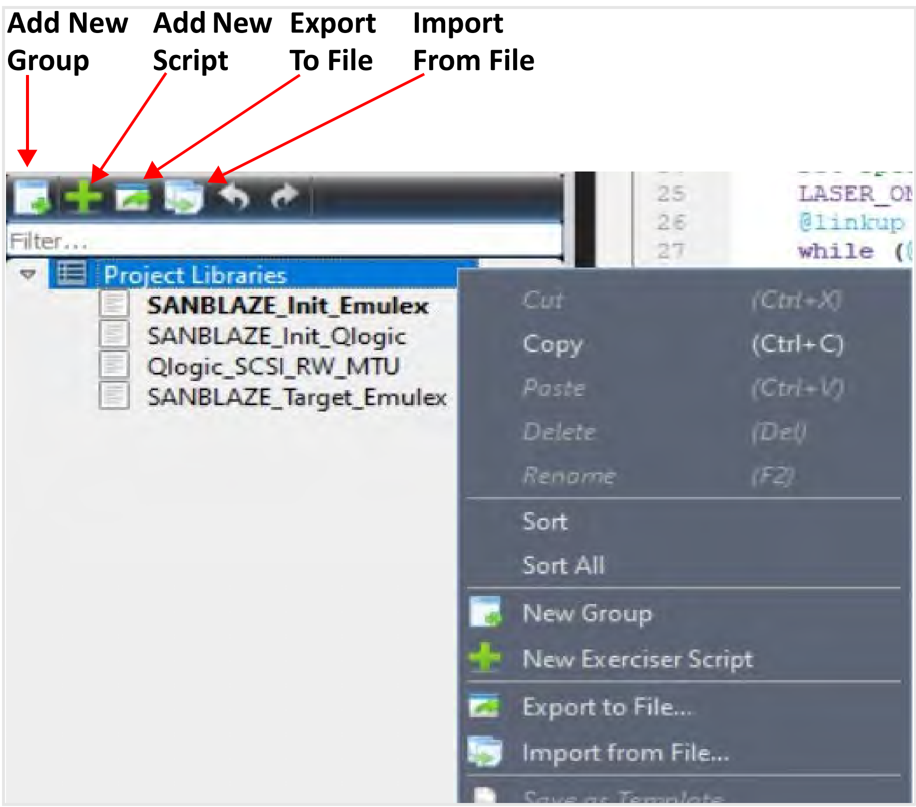


Figure 8.14: Operations Available from Project Library Pane (with Right Click)

8.3.4.2 Add New Library Group Icon

The New Group icon has a number of functions depending on how it is used:

- If nothing in the tree list is selected, then New Group will add a new Project Library folder.
- If a Project Library folder is selected, then New Group will add a New Group folder underneath that Project Library folder.

- If a folder is selected, then New Group will add a New Group folder underneath the selected folder.
- If a Script is selected, then New Group is disabled.

Selecting the Add New Library Group Icon will produce a new Project Library (see Figure 8.15). Its primary function is to help you organize your Scripts and Project Libraries.

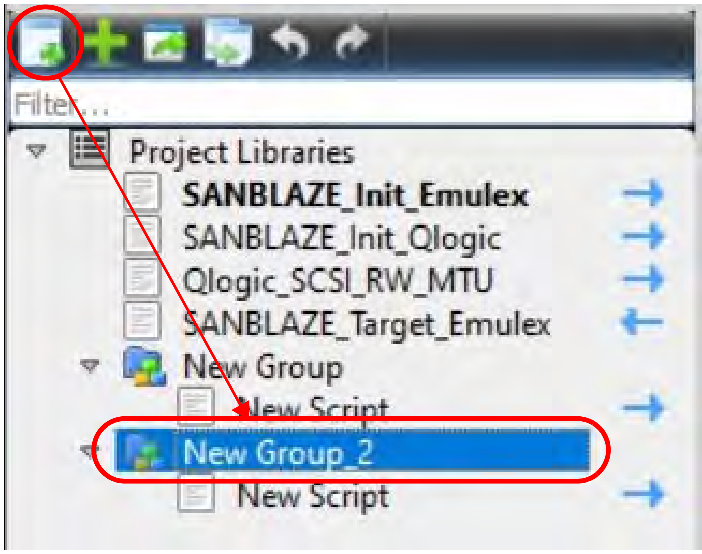


Figure 8.15: Add New Project Library

8.3.4.3 Add a New Exerciser Script to Project Library

To get a blank screen Script (to start writing a new Exerciser Script), click on the New Script icon and you'll get a script editor pane. See Figure 8.16.

NOTE: Teledyne LeCroy recommends loading an existing script and modifying it to suit your needs. Examples script are located as part of the installation of the NET Protocol Suite software. Typically these example scripts are located at:
C:\Users\Public\Documents\LeCroy\NET Protocol Suite\Generation\Samples

---

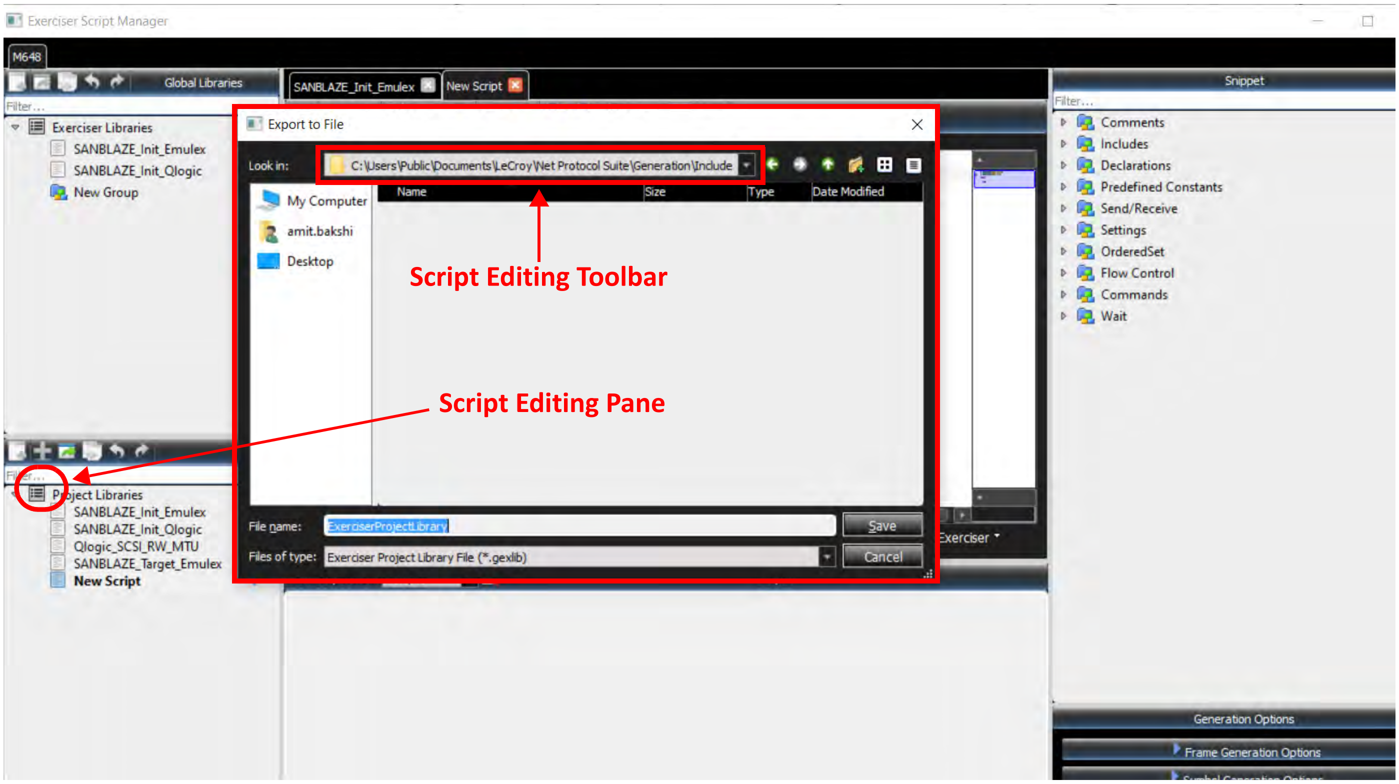


Figure 8.16: New Script Editing Pane

For details of the Script Editing Toolbar see 8.3.5.2, *Script Editor Toolbar*.

8.3.4.4 Export Exerciser Script Library to File

Selecting the Export Library Icon will pop up the following dialog, from which you can pick a library to Export. See Figure 8.17.

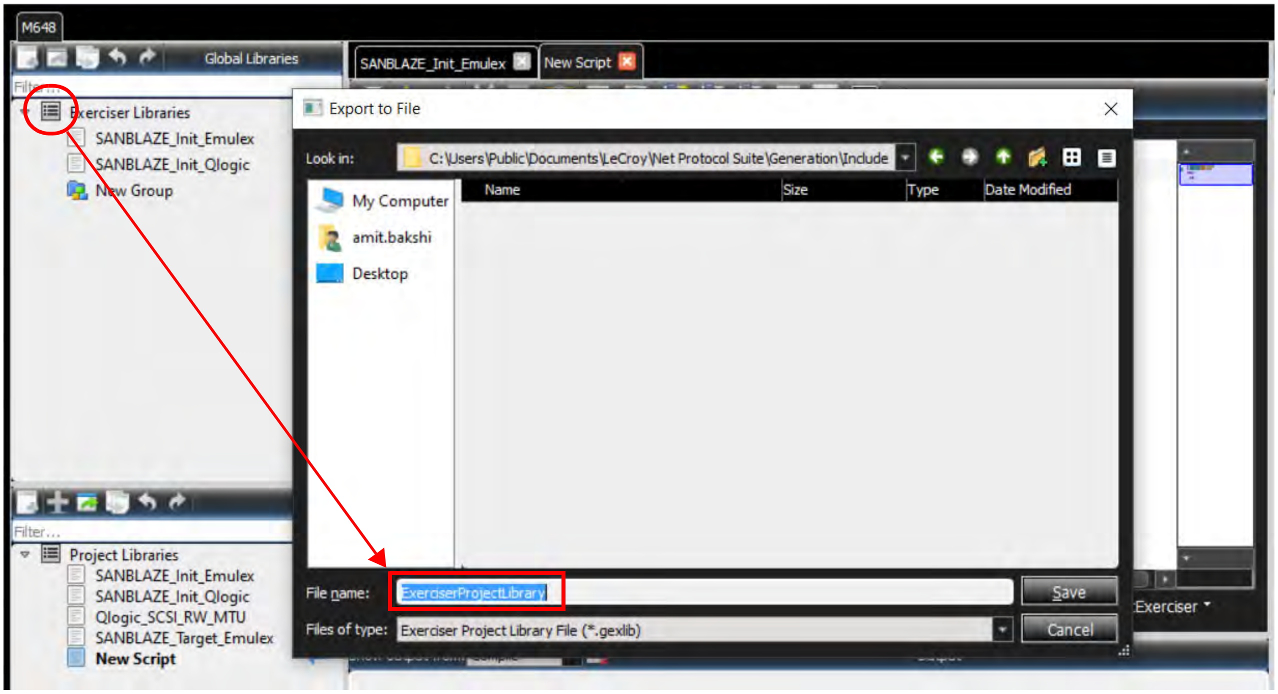


Figure 8.17: Export Exerciser Script to Project Library File

8.3.4.5 Import Project Library Icon

Selecting the Import Library Icon will pop up the following dialog (see Figure 8.18).

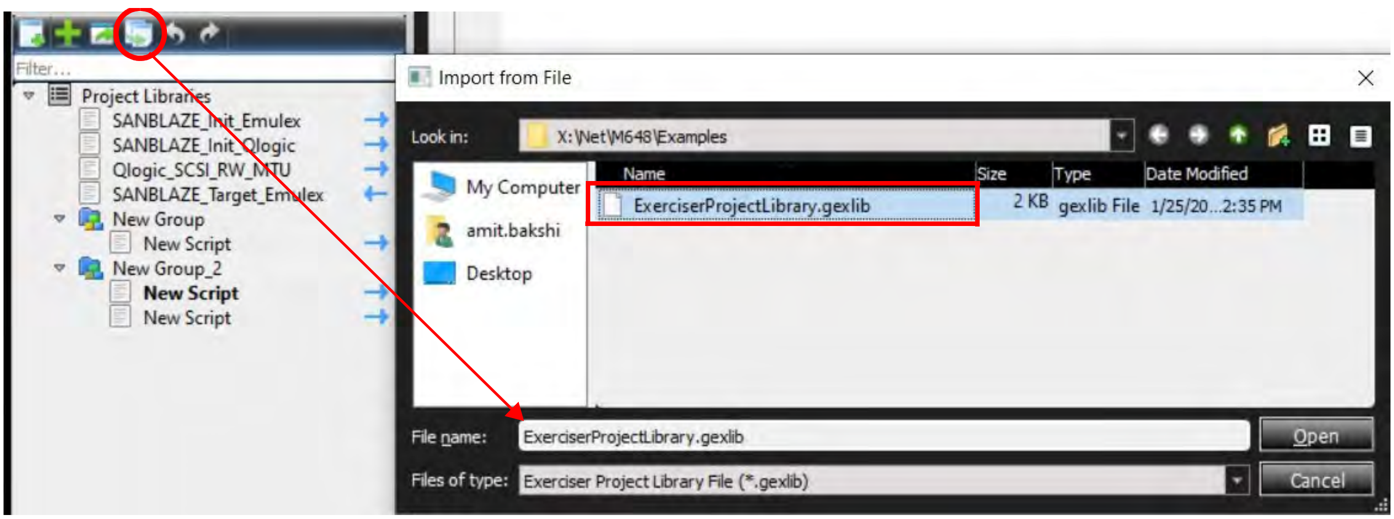


Figure 8.18: Import Project Library Dialog

8.3.4.6 Script Traffic Generation Mode

The Mode for traffic generation is shown on a global basis for the entire Script. In other words, the traffic will be generated as Initiator/Host or Target/Device based on defined “GenerationMode” in the script. The generation mode can be one of the following values:

- GEN_MODE_FC_INITIATOR
- GEN_MODE_FC_TARGET

See examples below: Figure 8.19 and Figure 8.20.

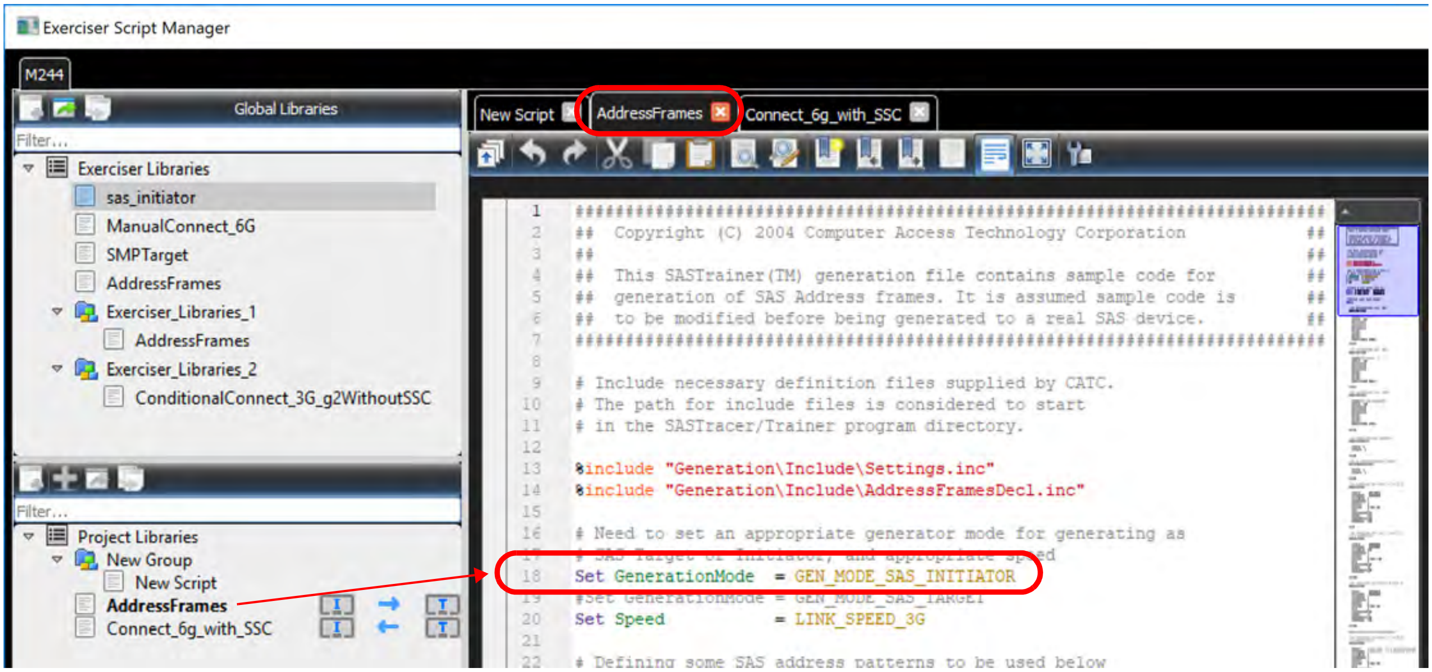


Figure 8.19: Script Traffic Generation from Initiator to Target

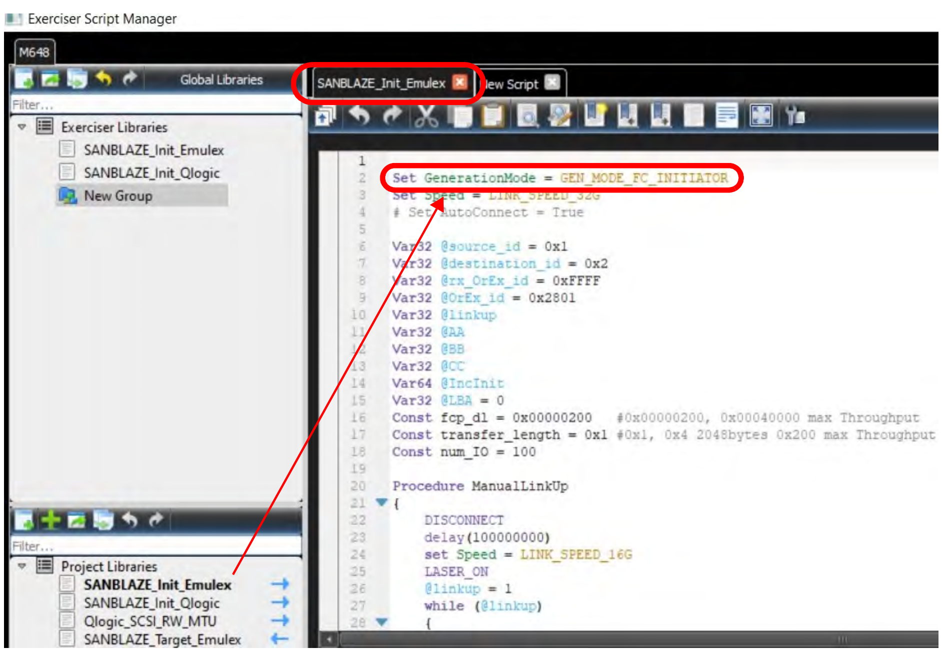


Figure 8.20: Script Traffic Generation from Target to Initiator

8.3.5 Script Text Editor Window

A typical script from the Exerciser library has been loaded into the script text editor. See Figure 8.21.

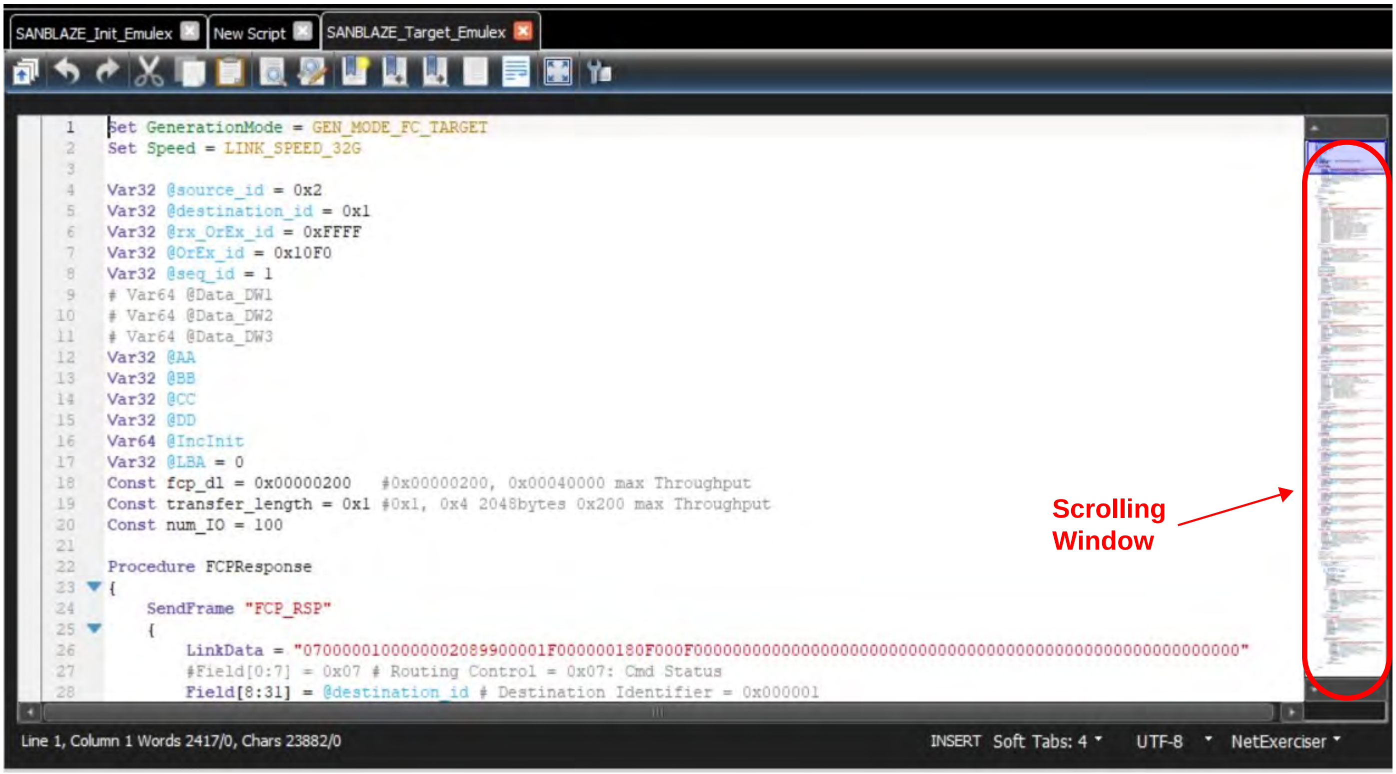


Figure 8.21: Script Editor: Script Loaded

8.3.5.1 Script Editor

The Script editor has the following functionalities:

- ❑ Code completion: Start typing in the script to get the suggestion list such as below (see Figure 8.22):

Figure 8.22: Code Completion Suggestions

- ❑ Syntax highlighting
- ❑ Code Folding
- ❑ Cut/Copy/Paste
- ❑ Multiple Undo/Redo
- ❑ Bracket Matching
- ❑ Bookmark
- ❑ Search/Replace

8.3.5.2 Script Editor Toolbar

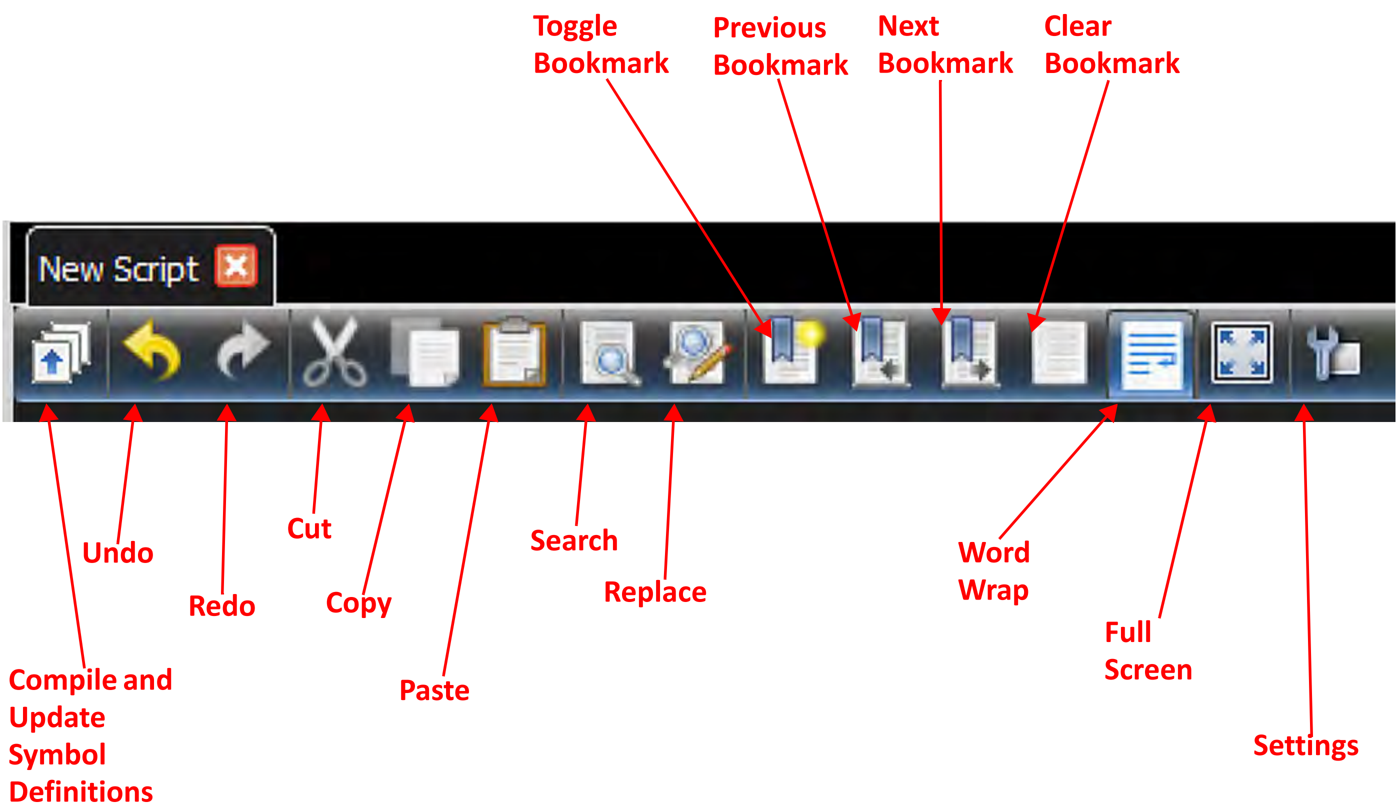


Figure 8.23: Exerciser Script Editor: Toolbar

- ❑ Compile and update symbol definitions: It will compile the current active script and update symbol definition for code completion.
- ❑ Settings (see Figure 8.24)

NOTE: The default include folder is "C:\Users\Public\Documents\LeCroy\NET Protocol Suite".

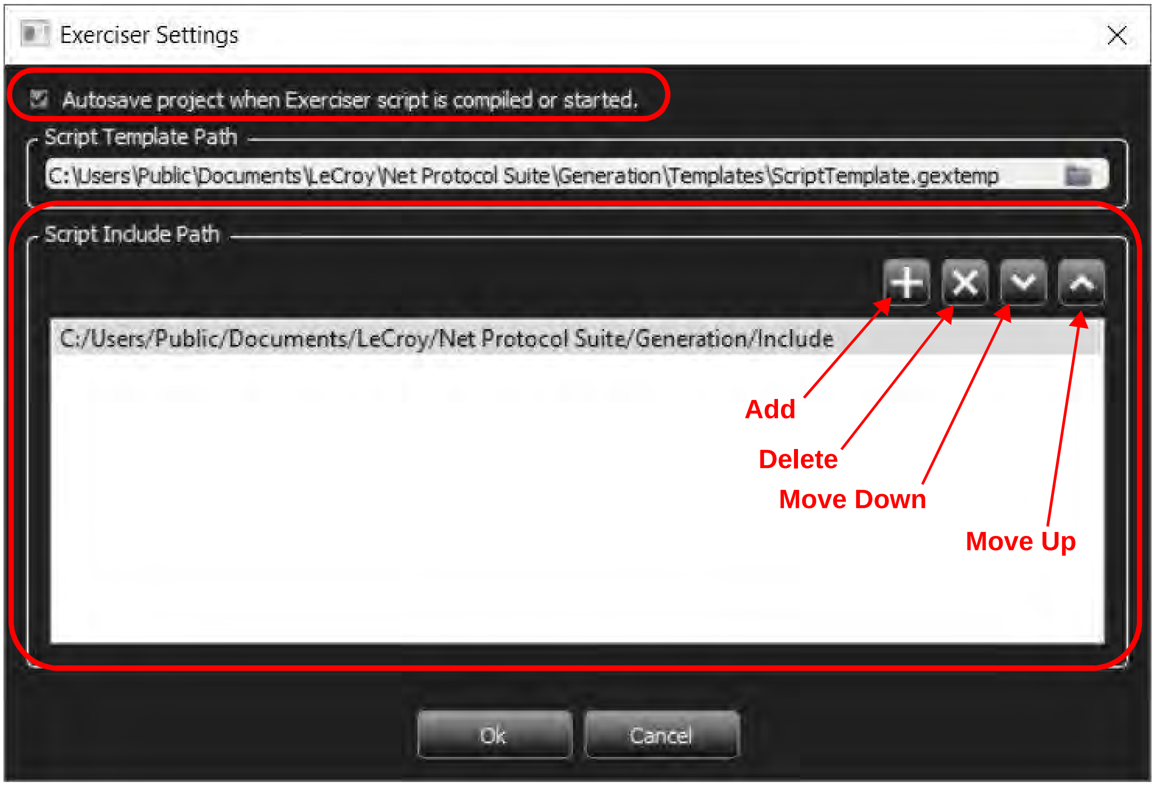


Figure 8.24: Exerciser Settings: User Include Path

- You can enable or disable the Autosave feature.
- You can set the User Template path to the installation path (as shown above)
- You can manipulate the Include files loaded with the software.

The Setting.inc file is described in more detail in 8.6.2, *Settings.inc File*.

8.3.5.3 Exerciser Output Log Window

Output window

The Output window shows any error after compiling the script. It has a goto feature that can be triggered by double click on an error to show the error line.

NOTE: If there is an error in an unopened include file, it opens it then goes to the error line.

An example of the output log window below shows the results of compiling a the sample script. See Figure 8.26 for details.

Errors in Script

If there is any error in the script, it will automatically switch to the Error output and shows all errors. By double click on any error, the script viewer will jump to the line and show the exact error point. See Figure 8.25.

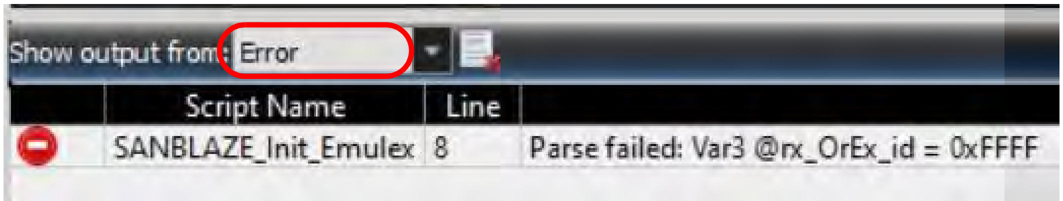


Figure 8.25: Compile Errors Shown in Output Window

8.3.5.4 Snippet Window

Code Snippet

All available keywords will be grouped in a tree and user can drag and drop them to the script and see a small snippet of how it can be used. Also, there is a tool tip that explains each keyword.

From the “Snippet Window” you can select an example and drag it into the Script Editor window and it will show you the exact syntax to implement that construct. See Figure 8.26.

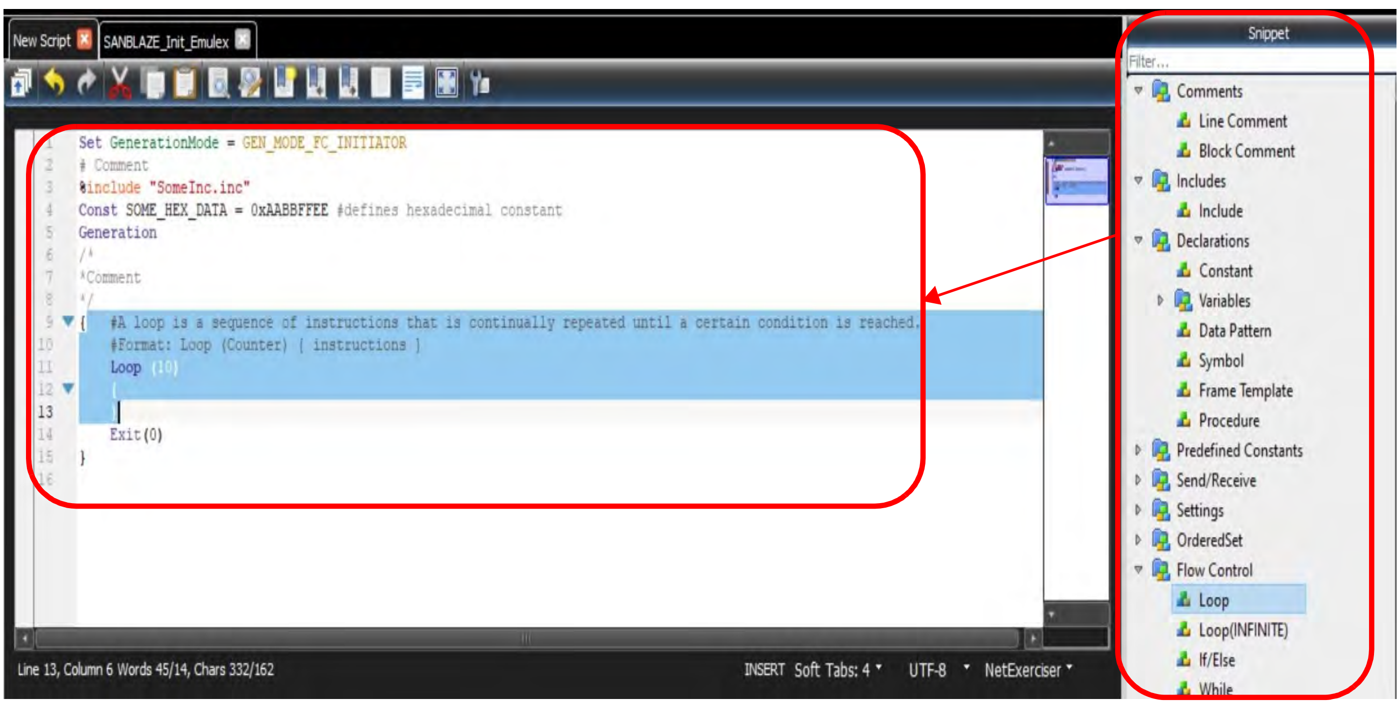


Figure 8.26: Snippet Window Example

8.3.5.5 Generation Options (Advance Wait Conditions)

Generation Options

You can predefine some events and bind them to 12 different actions (A – F in two categories). The Generation Options window is used if you want to use an “Advance Wait Condition”. There are twelve actions: 6 for frame events; 6 for symbol events.

Action A – Action F for both Frame and Symbol Events:

- In the example shown below, the “Snippet” window is used to add a Wait Command to the script. In this case, when the script gets to the `WF_FRAME_RESOURCES_OUTPUT_A`, the script pauses, waiting for `ELS_REPLY` frame, because that is the Advance Wait Condition defined for Action A. When the M648 finds the Frame, the script continues executing. See Figure 8.28 for details.

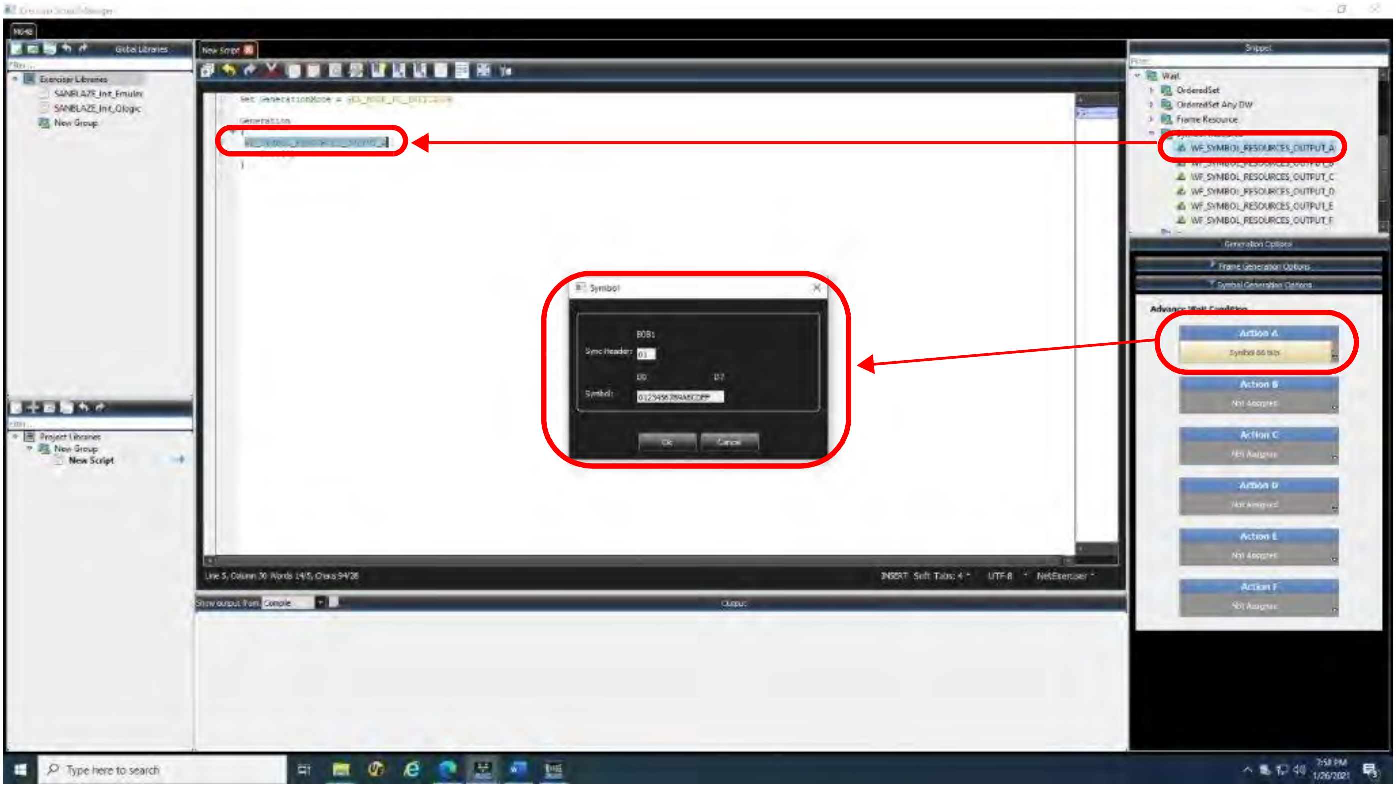


Figure 8.27: Generation Options: Advance Wait Condition

- If you select Action B as a Symbol Event, the following options display (Figure 8.28).

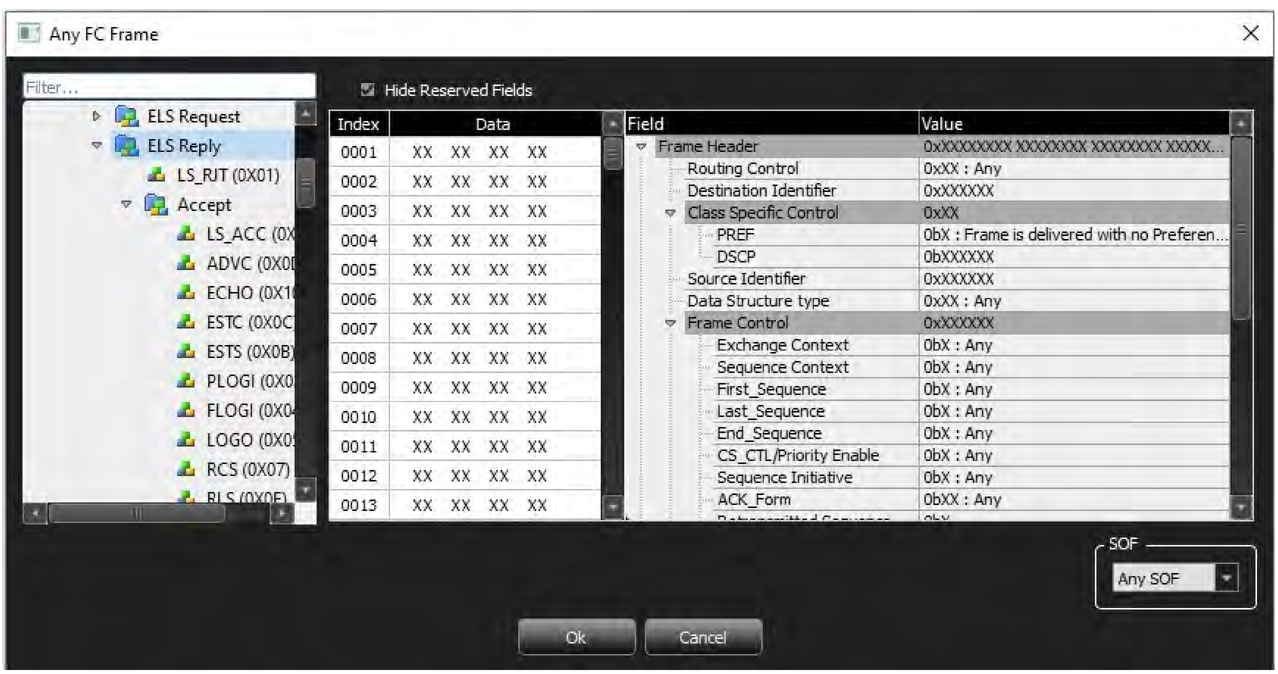


Figure 8.28: Options for Any Frame-Identify Any Frame

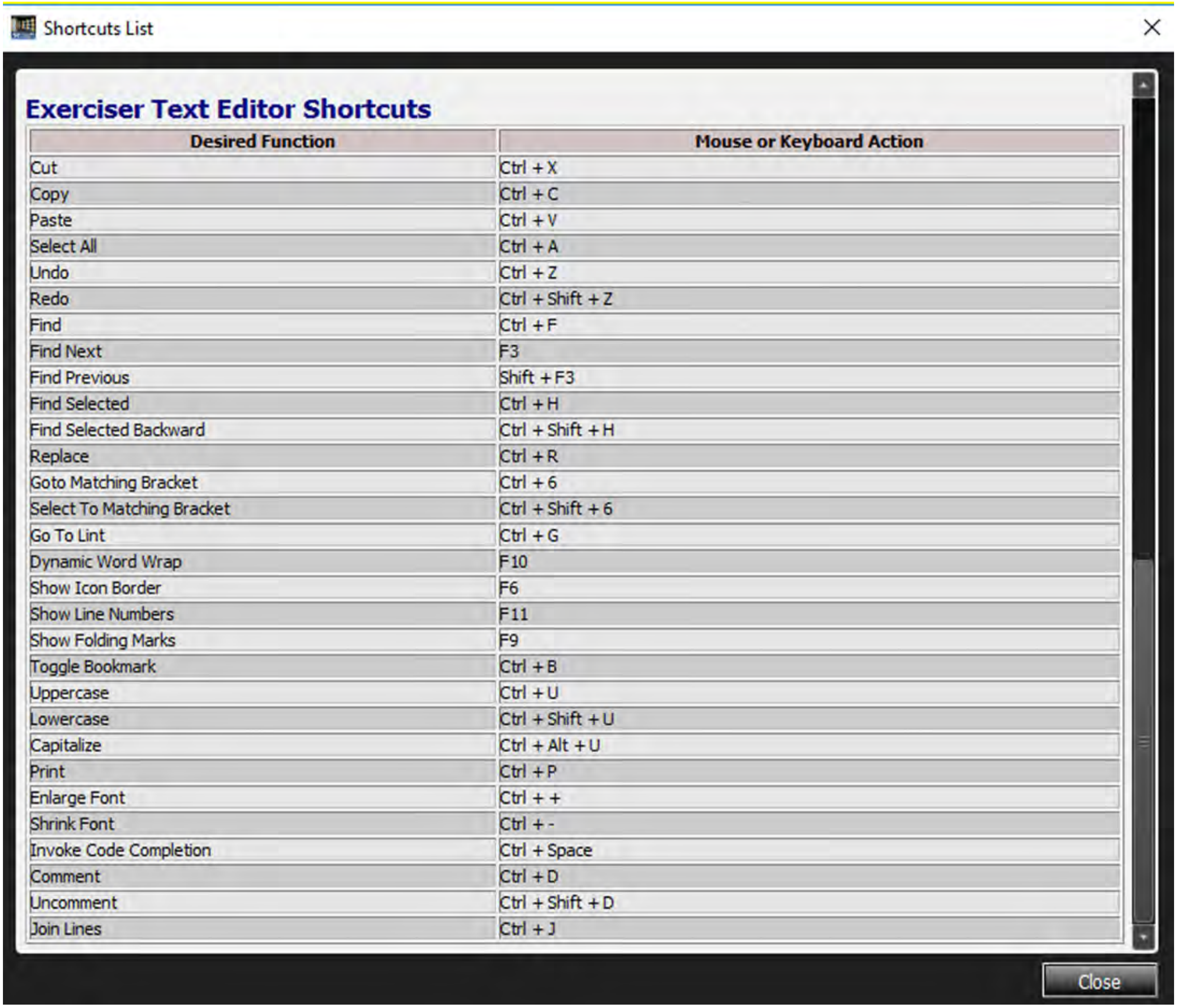
- ❑ From this menu, you can change the options to any Frame or any Command. Examples are shown in Figure 8.30 and Figure 8.31.

  These are the resource limitations for generation options:

  - **Frame**: Up to 32 DWORDs for each of the 6 resources.
  - **Symbols**: Up to 6 resources.

8.3.5.6 Exerciser Text Editor Shortcuts

The following list shows the Exerciser Text Editor Shortcuts. See Figure 8.29.



Shortcuts List

Exerciser Text Editor Shortcuts

Desired Function	Mouse or Keyboard Action
Cut	Ctrl + X
Copy	Ctrl + C
Paste	Ctrl + V
Select All	Ctrl + A
Undo	Ctrl + Z
Redo	Ctrl + Shift + Z
Find	Ctrl + F
Find Next	F3
Find Previous	Shift + F3
Find Selected	Ctrl + H
Find Selected Backward	Ctrl + Shift + H
Replace	Ctrl + R
Goto Matching Bracket	Ctrl + 6
Select To Matching Bracket	Ctrl + Shift + 6
Go To Lint	Ctrl + G
Dynamic Word Wrap	F10
Show Icon Border	F6
Show Line Numbers	F11
Show Folding Marks	F9
Toggle Bookmark	Ctrl + B
Uppercase	Ctrl + U
Lowercase	Ctrl + Shift + U
Capitalize	Ctrl + Alt + U
Print	Ctrl + P
Enlarge Font	Ctrl + +
Shrink Font	Ctrl + -
Invoke Code Completion	Ctrl + Space
Comment	Ctrl + D
Uncomment	Ctrl + Shift + D
Join Lines	Ctrl + J

Close

Figure 8.29: Short Cuts List

8.4 Launching an Exerciser Script

To launch an exerciser script:

1. From the Exerciser Script Editor, add some Sample scripts to your Project. See Figure 8.30.

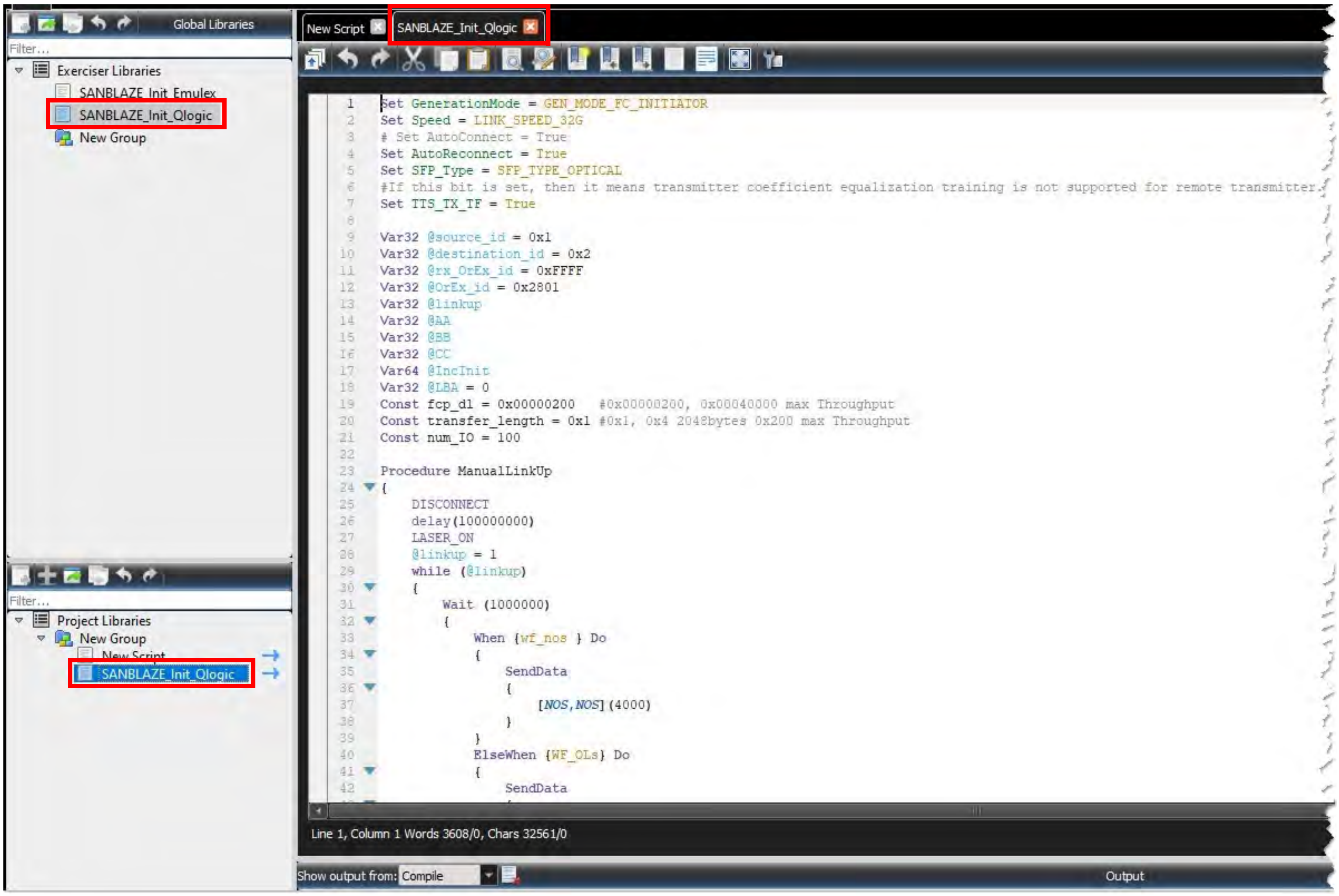


Figure 8.30: Scripts Added to Your Project

2. Close the editor and return to the NET Protocol Suite Main Menu, Figure 8.31.

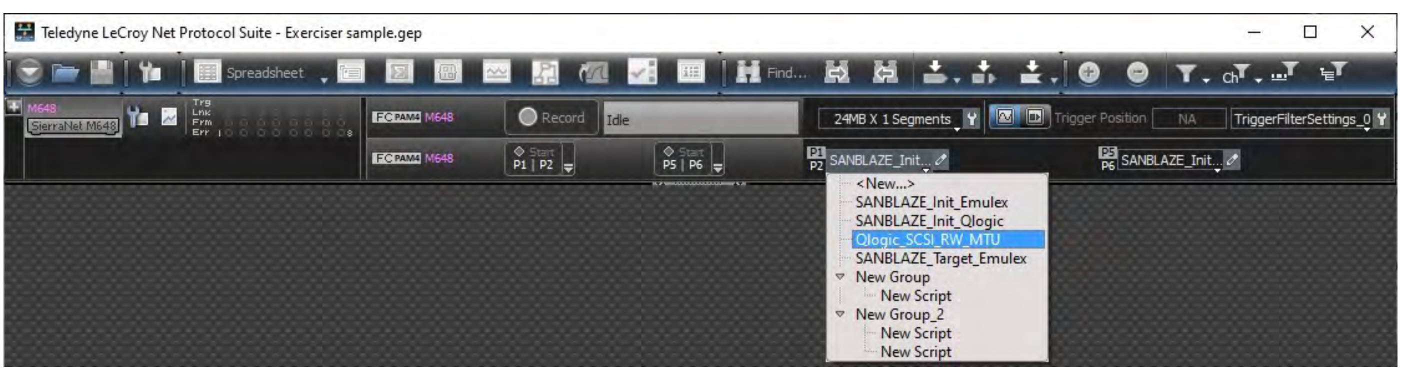


Figure 8.31: NET Protocol Suite: Main Menu – Available Scripts in Project

3. Select one of the available scripts, then click the respective port **Start** button to execute the script. See Figure 8.32.

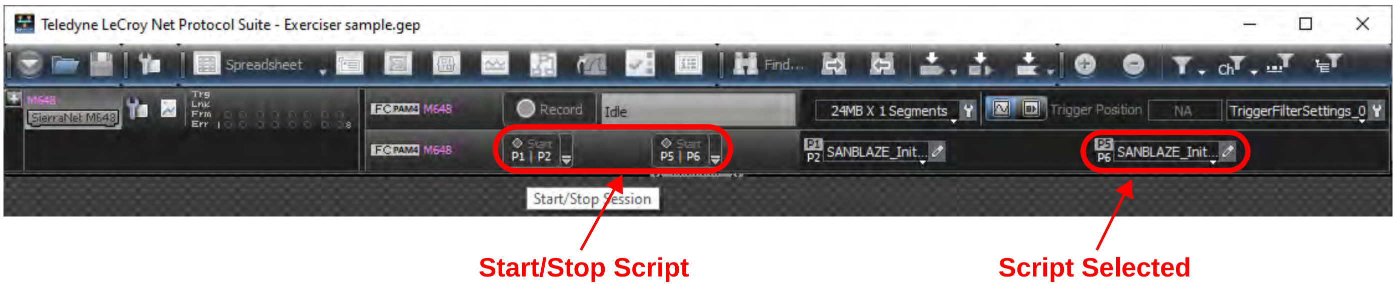


Figure 8.32: Script Selected

8.4.1 Connection Setting Button

If you select the small black down arrow next to the Start/Stop Session tab, you will see the Connection Settings for your analyzer. See Figure 8.33.

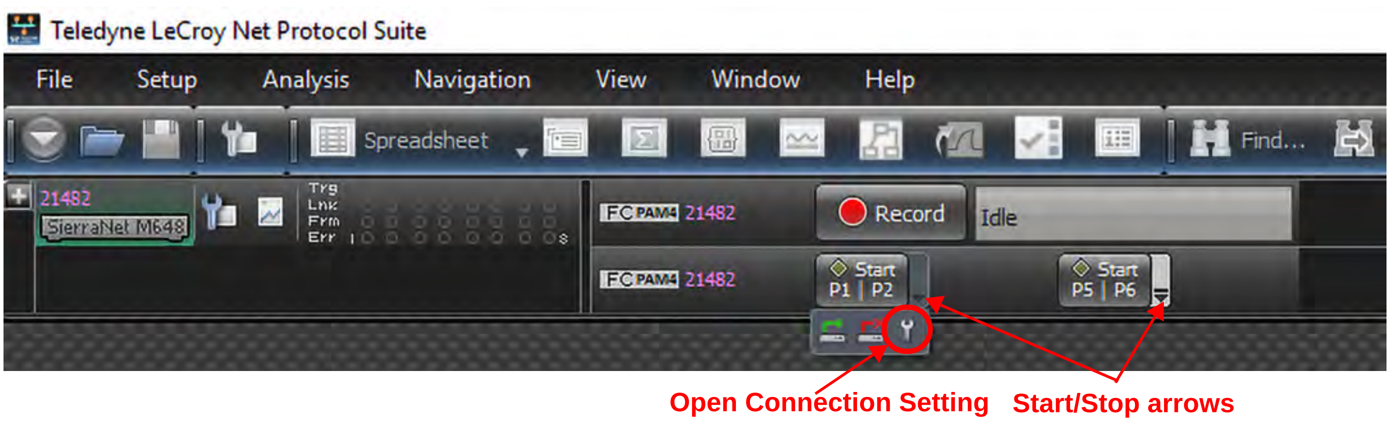


Figure 8.33: Connection Settings

To change the Connection setting, select the wrench icon. The Connection setting dialog displays, as shown in Figure 8.34.

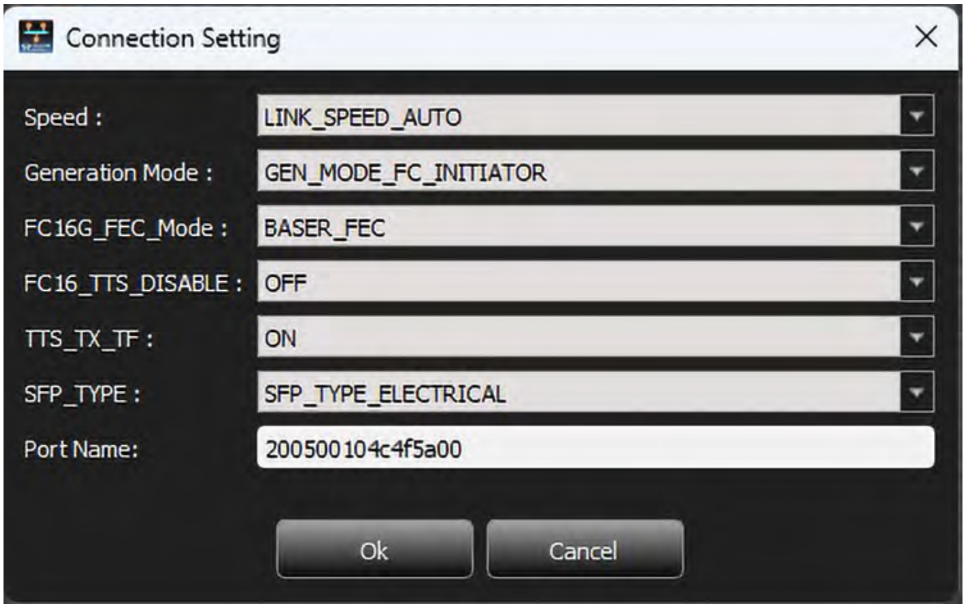


Figure 8.34: Connection Settings – Options – Generation Mode

Connection setting options are:

- Speed
- Generation Mode
- FC16G_FEC_Mode
- FC16_TTS_Disable
- TTS_TX_TF
- SFP_TYPE
- Port Name

Use the drop down arrows to choose the Connection Settings and click **OK**.

8.4.2 Connect/Disconnect

1. Click the small black down arrow to the right of Start P1|P2 to select from the following:
    - Connect icon to start the Exerciser executing the script (with the link up)
    - Disconnect icon to stop the Exerciser and take the link down. See Figure 8.35.

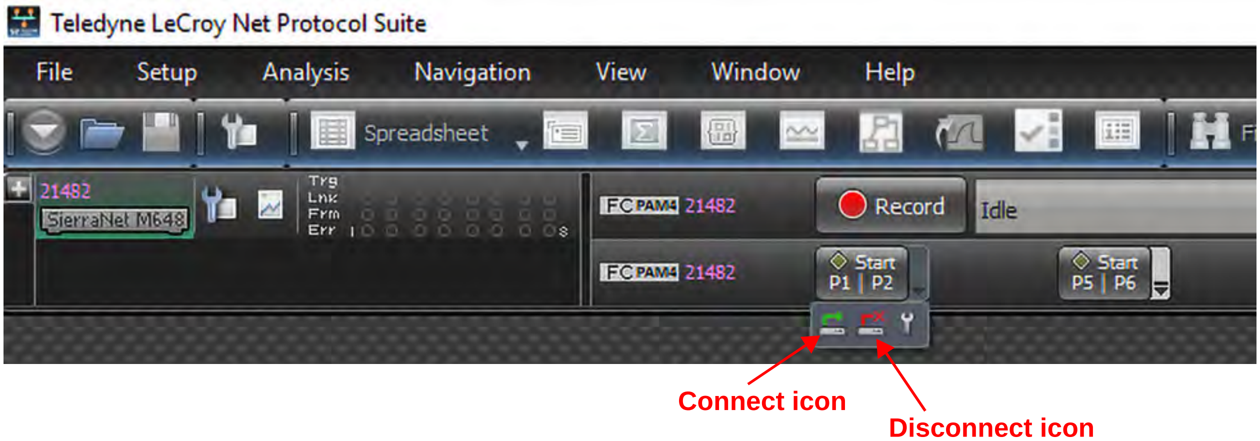


Figure 8.35: Start Script Running on Exerciser with Connect Button

2. If you connect both P1/P2 and P5/P6, both links are connected and linked up. See Figure 8.36 below.

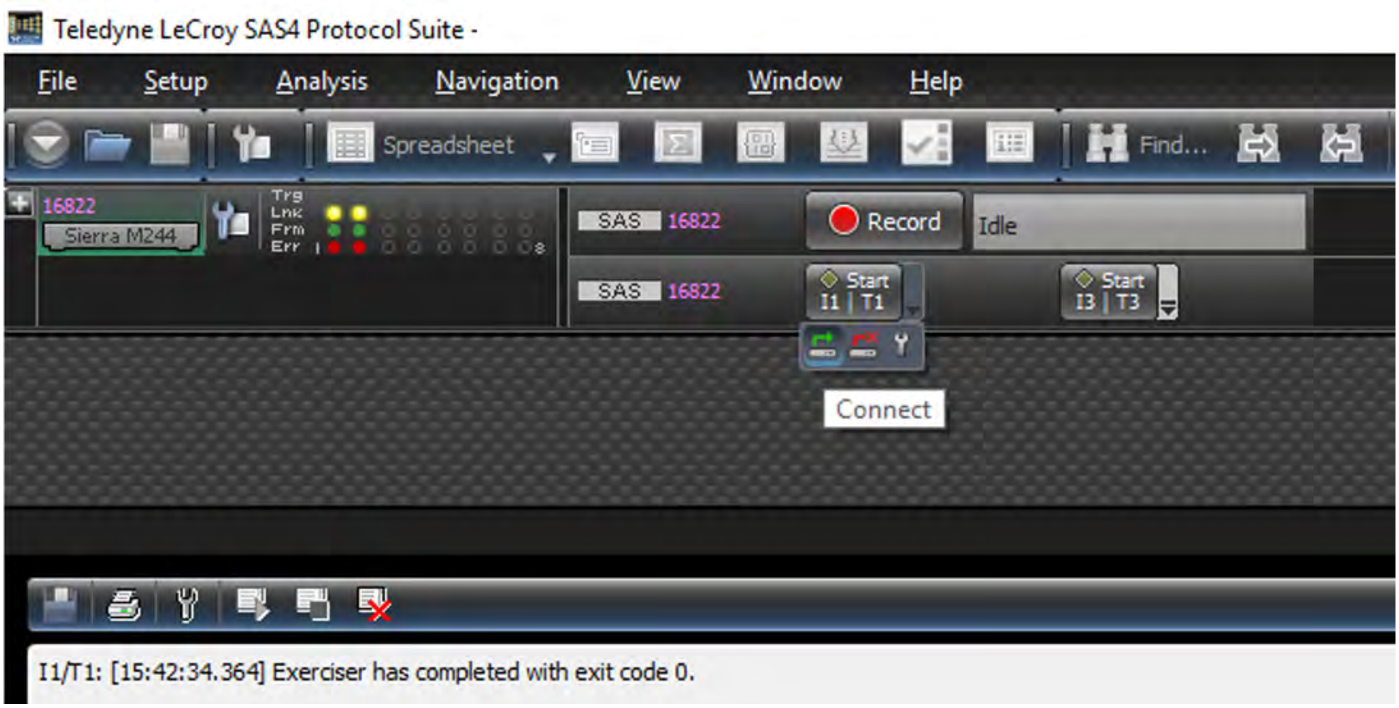


Figure 8.36: I1/T1 and I3/T3 Connected and Linked Up

3. If you select the **Disconnect** icon below the **Start/Stop** button, the link between the Initiator and Target will go down. See Figure 8.37.

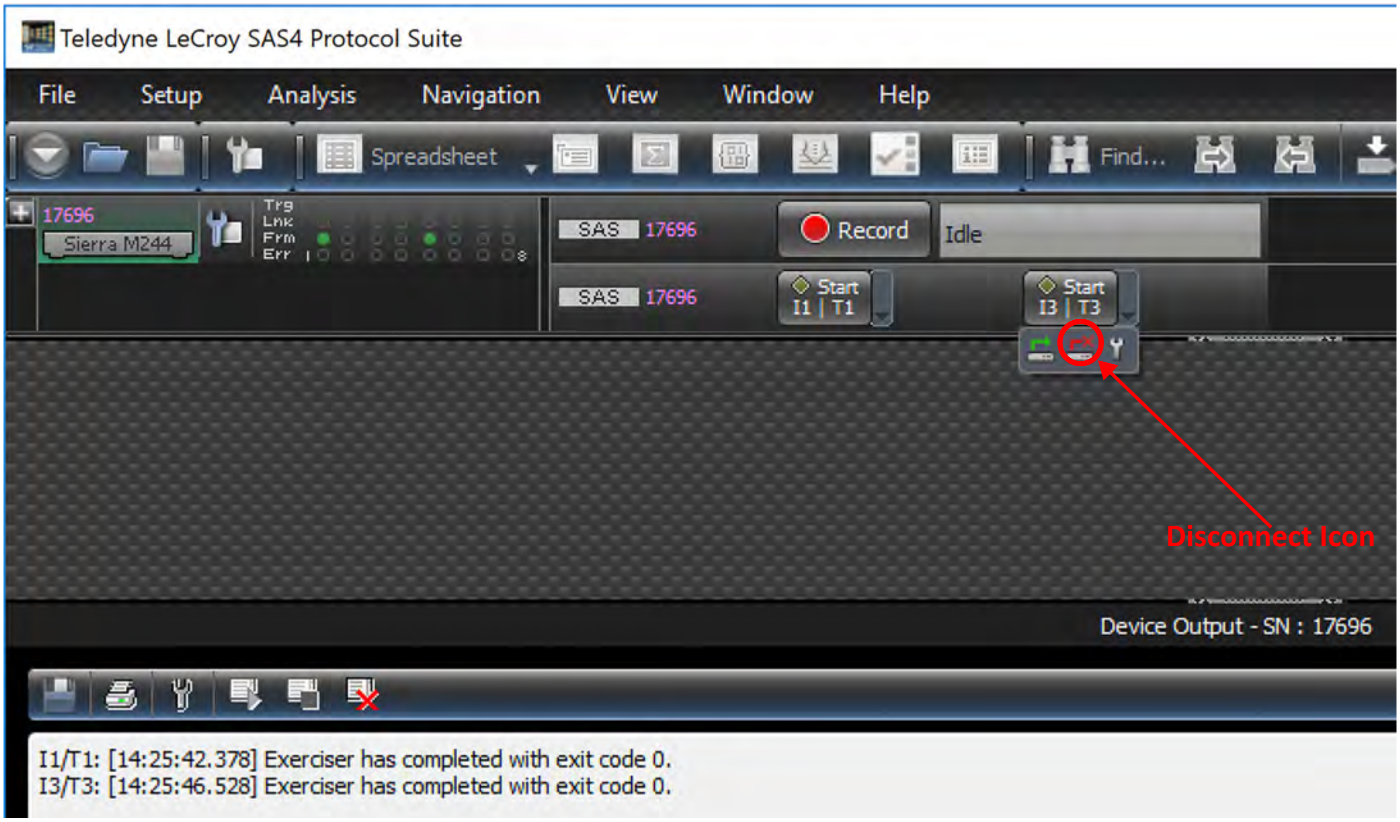


Figure 8.37: Disconnect Icon: Script Stopped and Link Disabled

8.5 Export to Exerciser Script

This feature enables the conversion of Traces to Exerciser scripts. It converts the FC Trace to a ready-to-run script that is a closer match to the original data.

Accuracy depends upon external factors such as drive behavior and the starting point of the exported frames. For example, if the capture is started with a wait for a response frame, it could be stuck at that point indefinitely.

NOTE:
- A memory limitation in bus engine (BE) limits the number of packets that can be exported.
- A few packets may be dropped at the beginning of the Trace before the first valid command packet.
- Underlying bandwidth issues may miss some **`wait_for`** commands.

To regenerate captured traffic in the Exerciser:

1. Open a Trace file.
2. Select **File → Export Trace → Export to Exerciser script**, as shown in Figure 8.38.

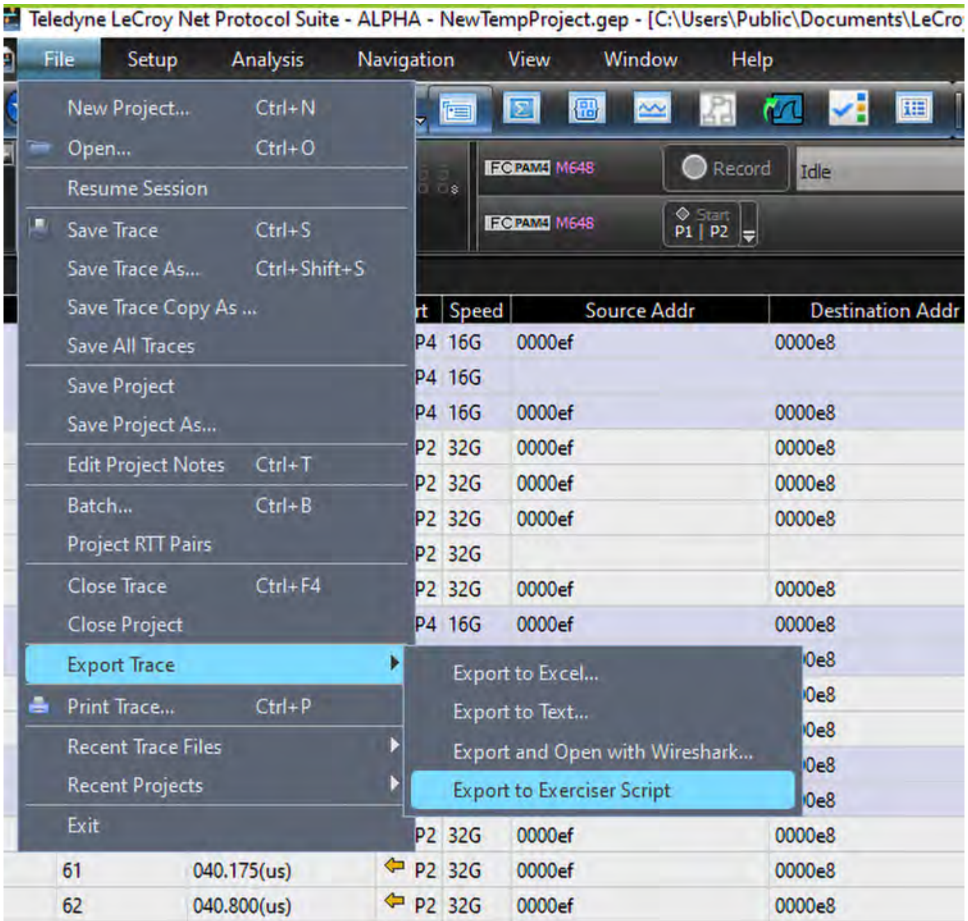


Figure 8.38: Export Trace to Exerciser Script

3. The Export to Exerciser Script Dialog displays, as shown in Figure 8.39.

.

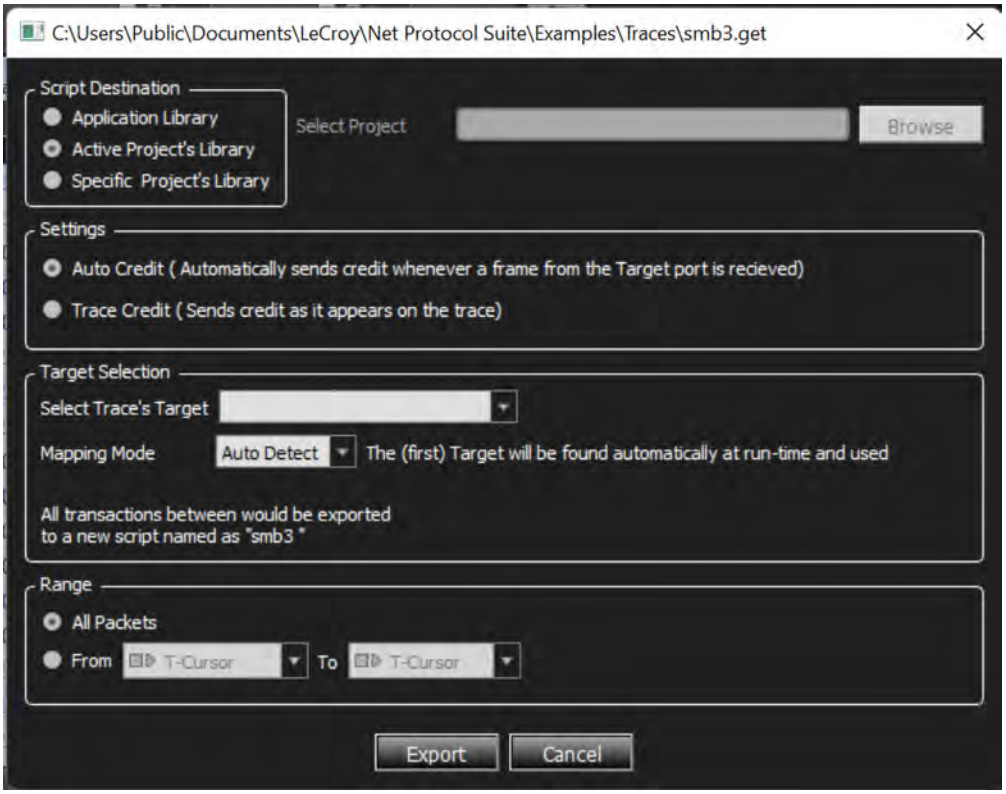


Figure 8.39: Export to Exerciser Script Dialog

4. To select the target, set the **Mapping Mode** to either Auto Detect or Wizard.

   a. Auto Detect: Exports the trace to an exerciser script without mapping to any specific target.

   b. Wizard: Allows you to choose a currently existing target to export the trace.

8.5.1 Auto Detect

If you choose Auto Detect, the system automatically detects a target and pre-fills the **Select Trace's Target** menu. Auto Detects returns the first detected targets. It detects targets on any topology, such as point to point/Fabric.

To execute the script, select the target from the **Select Trace's Target** menu and click **Export**. The system will create a script and open the

8.5.2 Wizard

Select this option to map the trace's target to a currently existing target:

1. From the Mapping Mode drop down, select **Wizard**. This open the **Select Target to Map** drop down menu. See Figure 8.40.

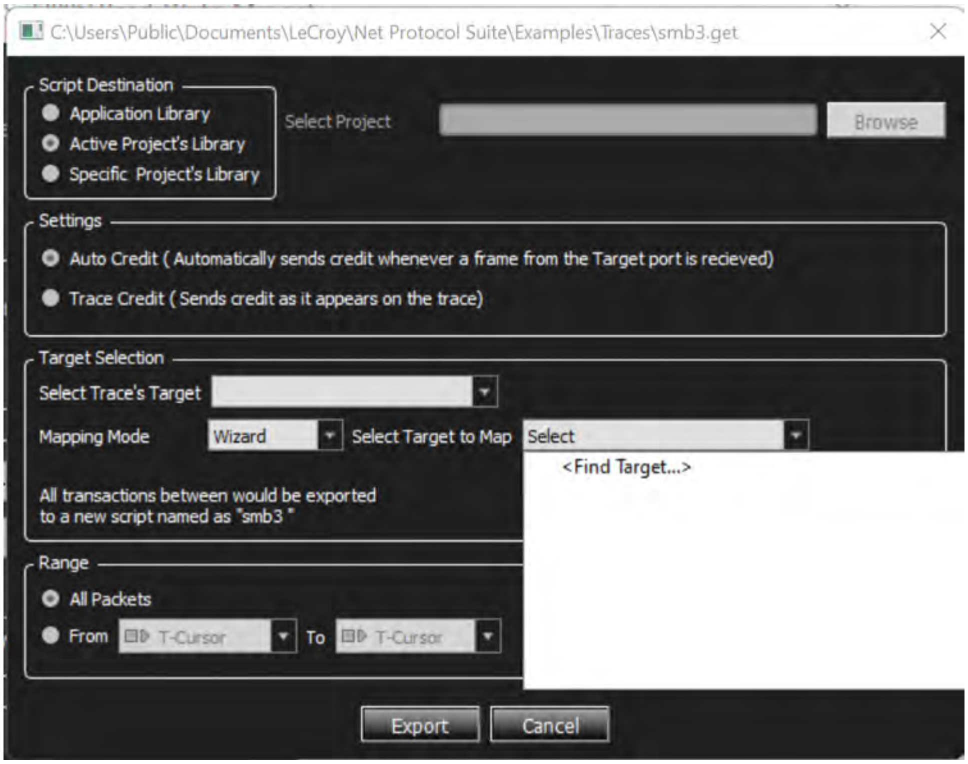


Figure 8.40: Wizard Mapping Mode

2. In the **Select Target to Map** drop down menu, click <Find Target...>. This opens the Find Target dialog box, as shown in Figure 8.41.

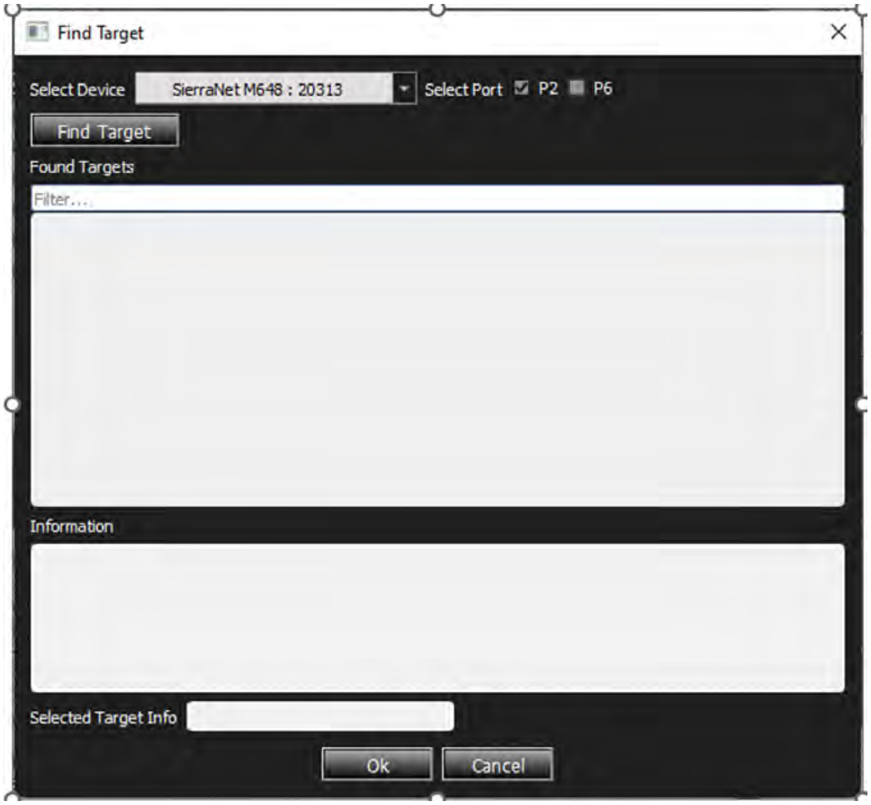


Figure 8.41: Find Target Dialog

3. **Select Device**: Choose the analyzer from the drop down list.

4. **Select Port:** Check the specific ports to find the targets. For example, Figure 8.41 shows P2 checked because there is a fabric connected only to P2.

5. Click **Find Target** to start the process.

An example of a compete fabric connected to the P2 port is shown in Figure 8.42. The P2 port is connected to a Fabric (Brocade) and 2 separate Targets (SANBlaze) are connected to the fabric with their own LUNs.

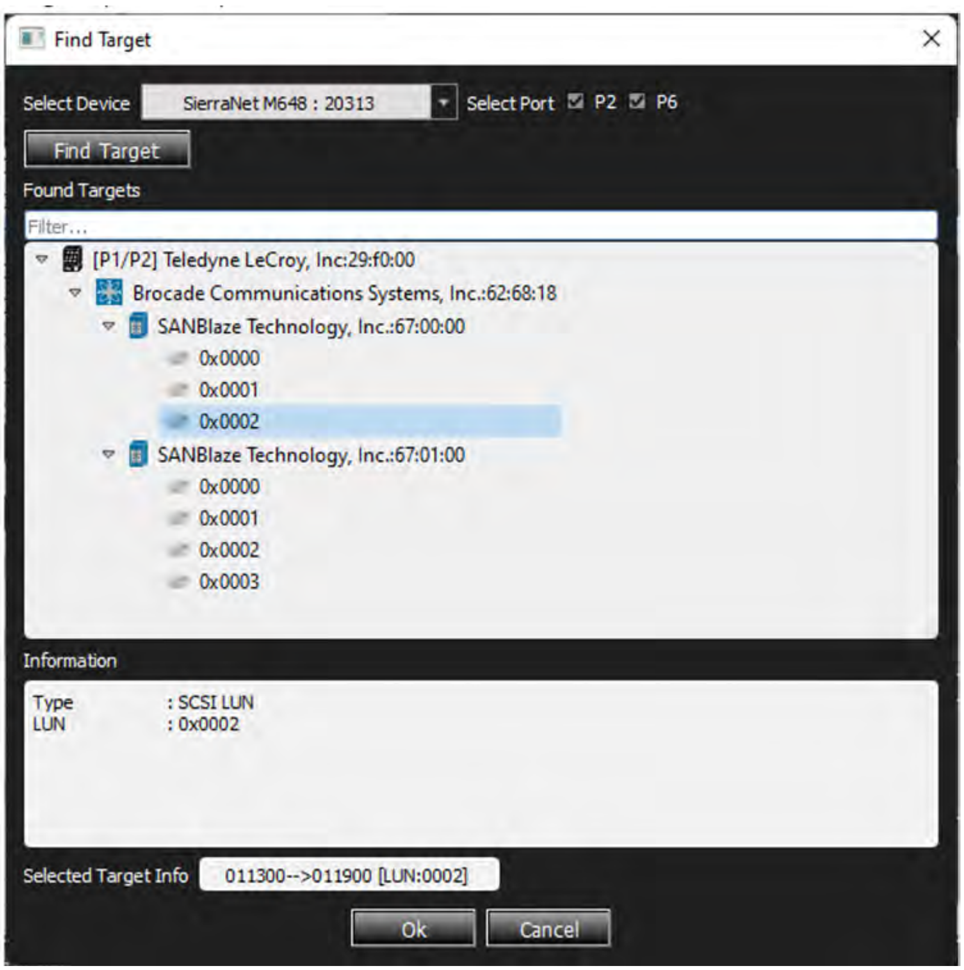


Figure 8.42: Sample Found Targets

6. Select the desired target from the list and click OK. The system will close this dialog and populate the Export to Script dialog with the chosen target information. See Figure 8.43.

8.5.3 Creating the Exerciser Script

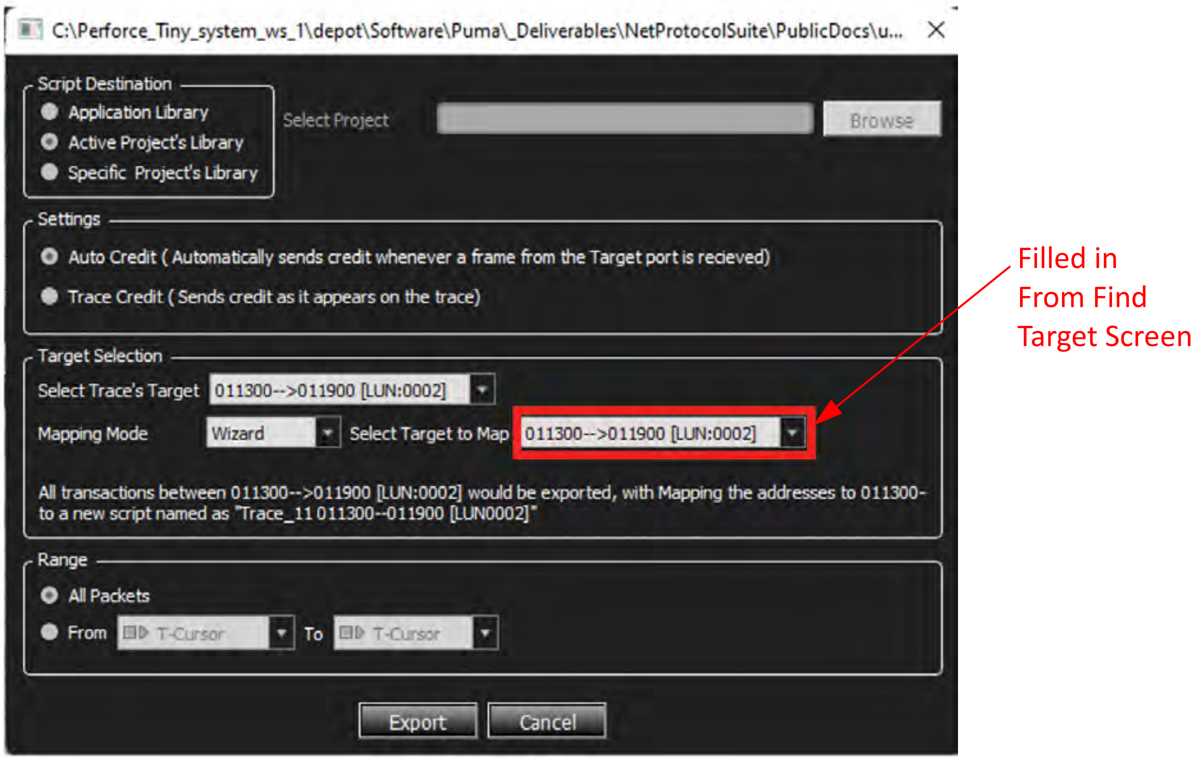


Figure 8.43: Export Script Dialog with Selected Target

1. Verify that the correct target is in the **Select Target to Map** field.
2. If desired, change the target using the drop down next to the **Select Trace's Target** and the **Select Target to Map** fields.
3. To export the target to the exerciser script, click **Export**.
4. The Exerciser Script Manager window displays containing the script information for the selected target. See Figure 8.44.

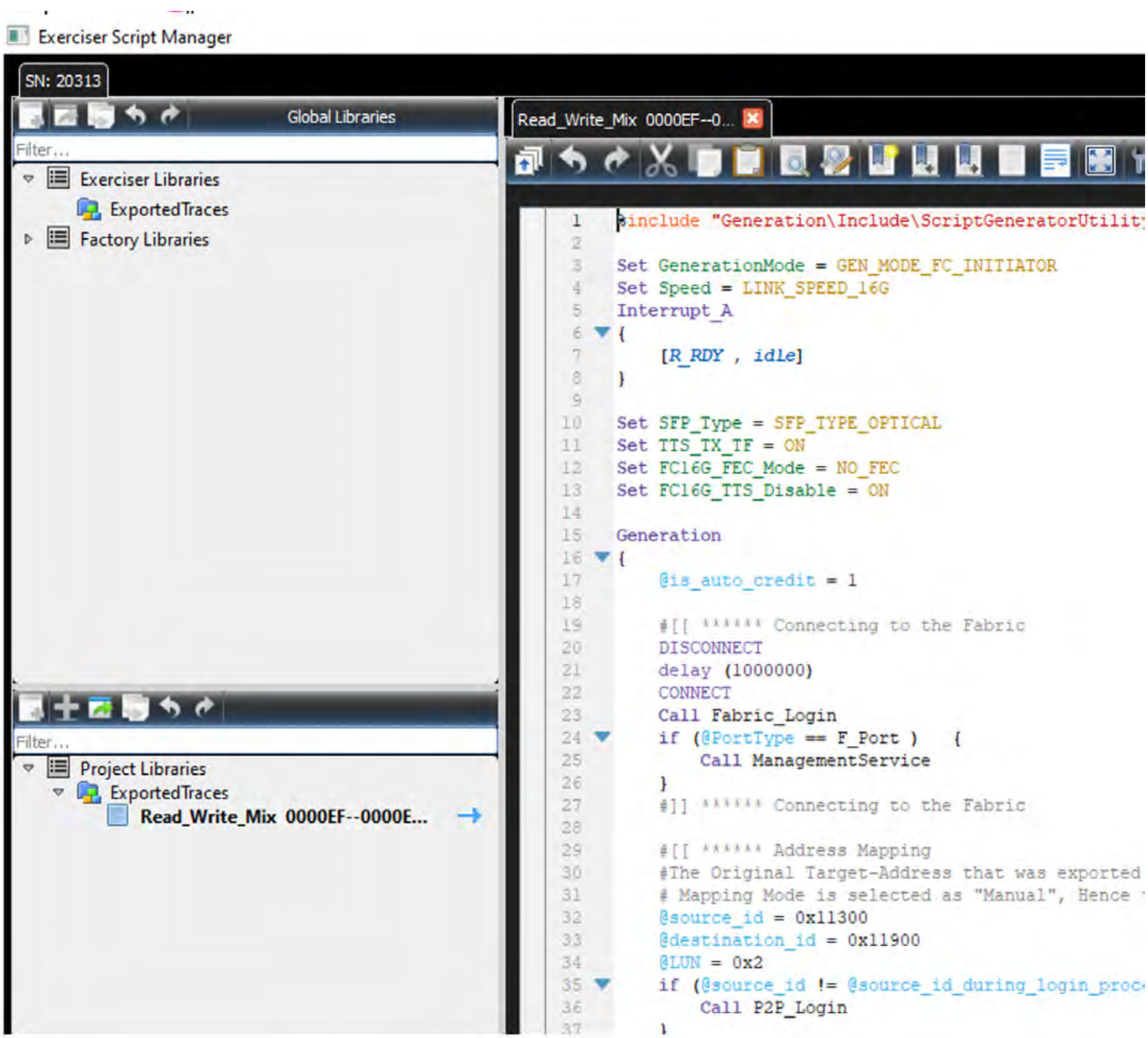


Figure 8.44: Exerciser Script Manager

5. The trace to exerciser script is complete. To create a trace, similar to the one shown in Figure 8.45, run the script and capture. The original trace's target is now mapped to the new target.

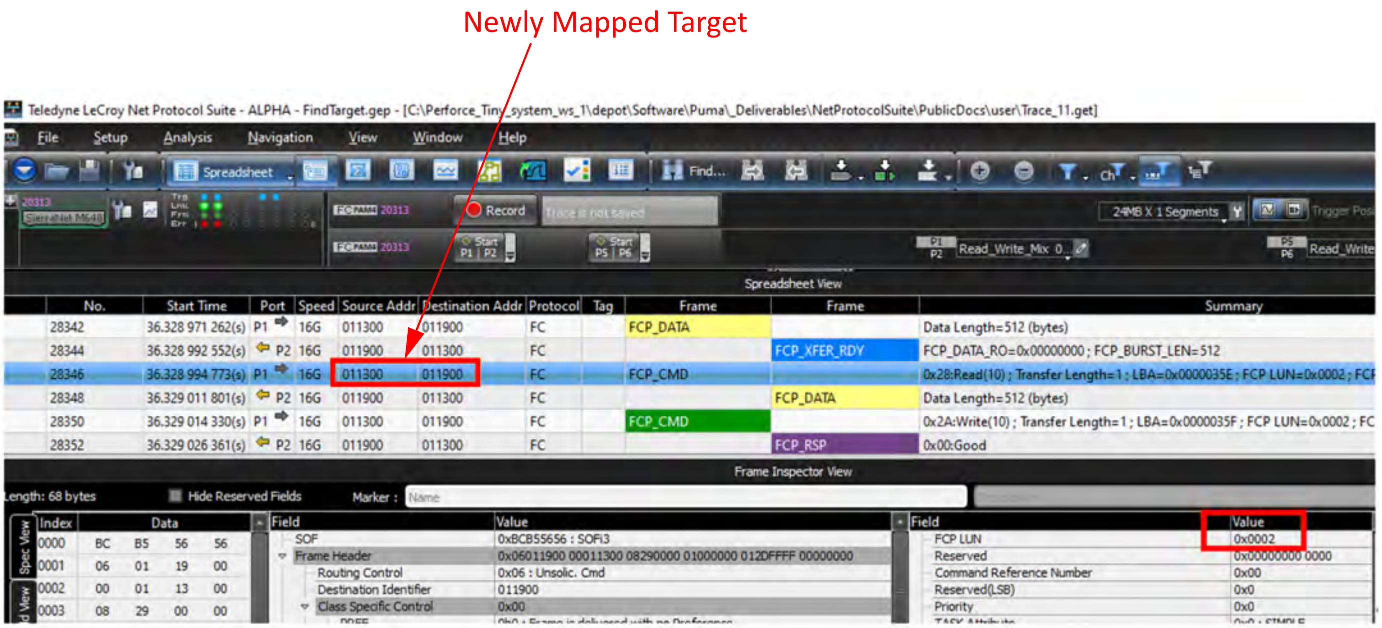


Figure 8.45: New Trace with new mapped target

8.5.4 Additional Information

Some additional features of the Sierra Net Protocol Suite are the following:

- There is a **Find Target** icon on the Exerciser Script Manager. Using it launches the Find Target dialog form which you can easily select different targets to add to the Exerciser Script Manager. See Figure 8.46.

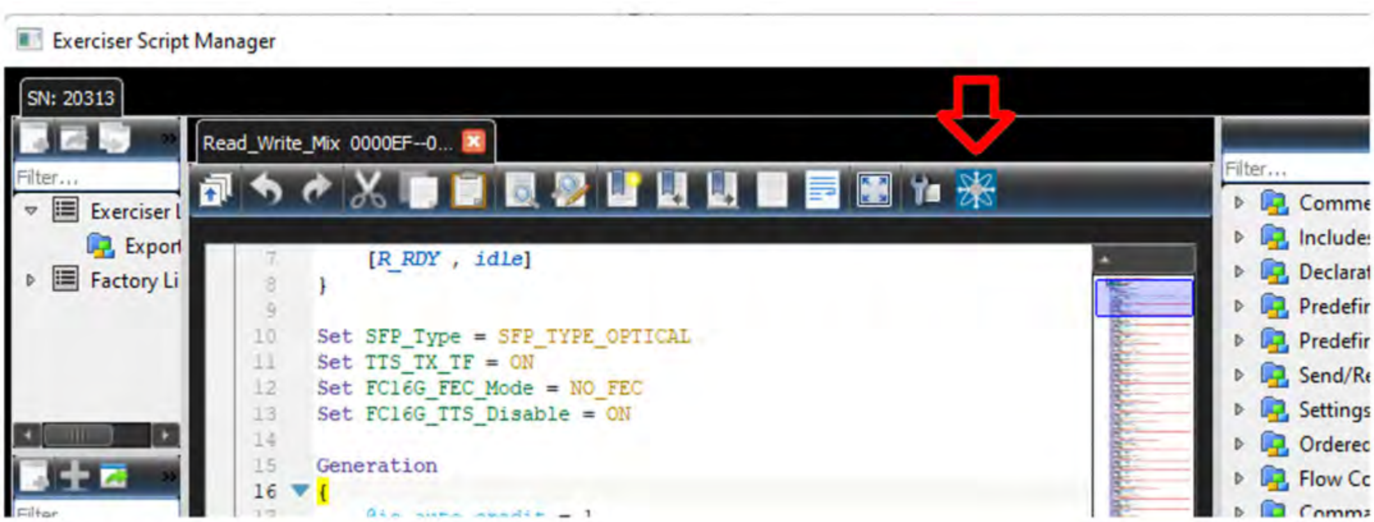


Figure 8.46: Find Target Icon on the Exerciser Script Manager Screen

- You can edit the target in the Exerciser Script, as shown in Figure 8.47. Simply change the variable's value with the newly mapped target. This feature helps to avoid exporting the trace again and again, if the intention is to just change the mapping of the target.

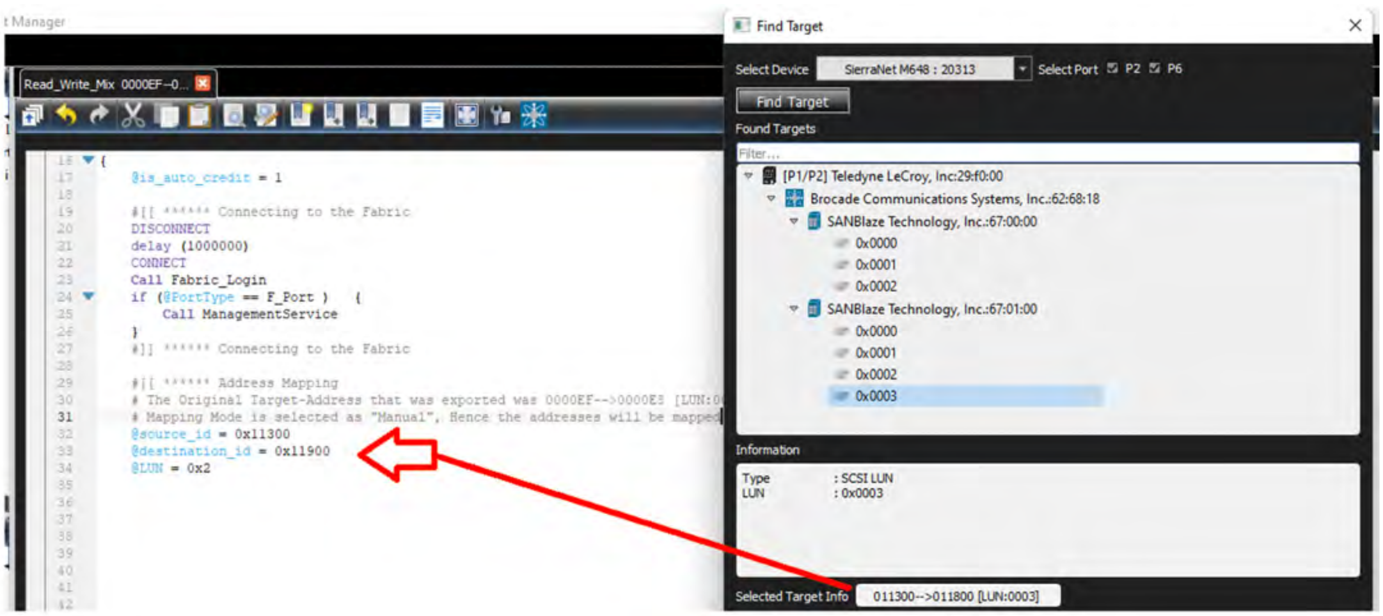


Figure 8.47: Script Changes

8.6 Overview of Generation and Global Settings Files

Example **.gexlib** files and **Include** files are in two directories called **\Samples** and **\Include** that are typically installed in:

C:\Users\Public\Documents\LeCroy\NET Protocol Suite\Generation\Samples and
C:\Users\Public\Documents\LeCroy\NET Protocol Suite\Generation\Include

8.6.1 Exerciser Script

The exerciser script consists of **include** statements, a Generation block, and optionally global statements.

The Generation block is the code responsible for the actual traffic generation. It is marked by the tag **Generation**. The composition and format of the Generation block is described later.

```
%include "Generation\Include\Settings.inc"

Generation
{

}
```

The **include** statements provide links to the **Include** files, which provide the definitions for primitives, frames and settings that hold for most or all of the generation session (global settings).

The exerciser settings and their default values are contained in the Teledyne LeCroy-provided Include file: Settings.inc

8.6.2 Settings.inc File

The **Settings.inc** file contains global statements about the link, the type of device being emulated, and other conditions that are to exist throughout part or all of the traffic generation.

This file may be included in the traffic generation file.

The Settings.inc is located at:

C:\Users\Public\Documents\LeCroy\NET Protocol Suite\Generation\Include

Editing Settings.inc

Text in the **Settings.inc** file can be edited directly or copied into the beginning of the traffic generation file and edited there.

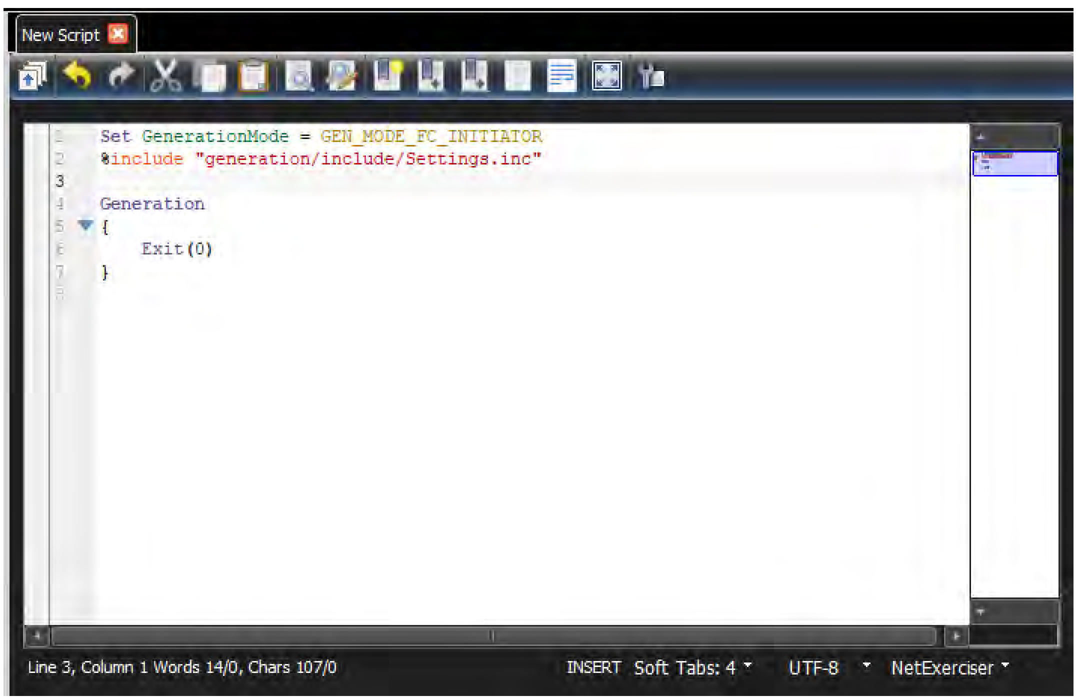


Figure 8.48: Edit Settings.inc File

When editing global settings, keep in mind the following rule:

The last line encountered before the Generation block takes precedence. Thus, if the following two lines about the device emulation were added just above the Generation block, the second would take effect:

- set GenerationMode = GEN_MODE_FC_TARGET
- set GenerationMode = GEN_MODE_FC_INITIATOR

8.6.2.1 Placing Global Settings in the Generation Block

Some global settings, such as AutoFillWordInsertion = On/Off can be set and reset in the Generation block. For example, you might want to set AutoFillWordInsertion = ON prior to traffic generation, and then change to OFF halfway through the generation session.

```
# Generation Block
Generation
{
      Set AutoFillWordInsertion = ON

#
      #  … some instructions here
      #

Set AutoFillWordInsertion = OFF

      #
      #  … some other instructions here
      #
}
```

When placed within the Generation block and viewed in the trace window, global settings appear as colored bars interspersed amidst the traffic.

The Following global settings cannot be placed within the Generation block:

- GenerationMode
- AutoConnect
- AutoReconnect

These commands should be configured either in the **Setting.inc** file or at the beginning of the traffic generation file as a global statement.

8.6.3 Symbol and Frame Definitions

The default value for all Frame fields are zero.

8.6.3.1 Special Conditions for Frames

CRC Calculations are calculated unless told otherwise - If the Cyclic Redundancy Check (CRC) is not explicitly set in the traffic generation file, the application assumes that you want it and calculates and displays it in front of the generated frames.

NOTE: CRC is a standard algorithm used by commonly available software to produce an eight-character, hexadecimal number using all the bytes in a Target file. This number, a “digital signature”, changes when any byte in the Target file changes. The digital signature does not change when the file name or creation date changes.

If you provide a CRC value, the application uses that value, even if it is incorrect. This gives you the option of configuring the generator to create CRC errors.

8.7 Sierra Exerciser Generation Language

The Sierra Exerciser File Generation Language is an API that allows you to separate traffic into text commands. These commands are used to construct primitives and frames that are sent to the Initiator or the Target.

8.7.1 File Structure

Exerciser scripts should have the following structure:

Declarations

- Global generation settings
- Constants
- Variables
- Data patterns
- FC Symbols

NOTE: Some declared objects could be used in further declarations as long as they are previously declared. No forward declarations are allowed at this time.

Generation Blocks

List of generation instructions

8.7.2 Language

8.7.2.1 Comments

is the Comment symbol. The line remainder after this symbol is ignored.

/* Something to be ignored */ is a Comment Block. All the text between **/*** and ***/** is ignored.

`AutoFillWordInsertion = ON #` This is an example of a line comment.

/*

This is an example of a block of comments.

***/**

8.7.2.2 Includes

The directive **%include "FileName.inc"** includes the file **FileName.inc**. This lets you add common definitions and templates into new scripts.

The language parser makes sure the same file is not included more than once.

Example:

```
%include "path_to_include\SomeInc.inc"
# This directive actually includes file 'path_to_include\SomeInc_1.inc'.
Absolute paths are also allowed:
%include "c:\absolute\path\to\include\SomeInc.inc"
```

NOTE: Default Path: "C:\Users\Public\Documents\LeCroy\NET Protocol Suite\"

8.7.2.3 Settings

The **`Set "Constant Name" = Value`** statement sets different constants/modes using the following value types:

- Predefined constants (TRUE, FALSE, ON, OFF, INFINITE)
- Numbers

Examples:

```
Set AutoFillWordInsertion = ON
Set WaitTimeOut = 239
```

See 8.7.8.11, *Generation Settings* for more details.

8.7.2.4 Constants

Only unsigned integers can be defined as constants. Some constants are predefined in Sierra Exerciser.

Examples:

```
Const SOME_HEX_DATA = 0xAABBFFEE #defines hexadecimal constant
Const SOME_DEC_DATA = 12     # defines decimal constant
```

8.7.2.5 Predefined Constants

- TRUE
- FALSE
- ON
- OFF
- INFINITE

8.7.2.6 Data Patterns

Data patterns are streams of hexadecimal values.

Examples:

- DataPattern MyPattern_1 = 11223344
- DataPattern MyPattern_2 = 11223344 AABBCCDD
- DataPattern MyPattern_3 = 11223344 AABBCCDD 10203040
- DataPattern MyPattern_Recursive_1 = 12345678 MyPattern_1 MyPattern_2

NOTE: Data Patterns can be used to implement some of the fields used in FC NVMe, which are very long, such as Host Identifier (128 bits), Host NVMe Qualified Name (2048 bits), and NVMe Subsystem NVMe Qualified Name (2048 bits).

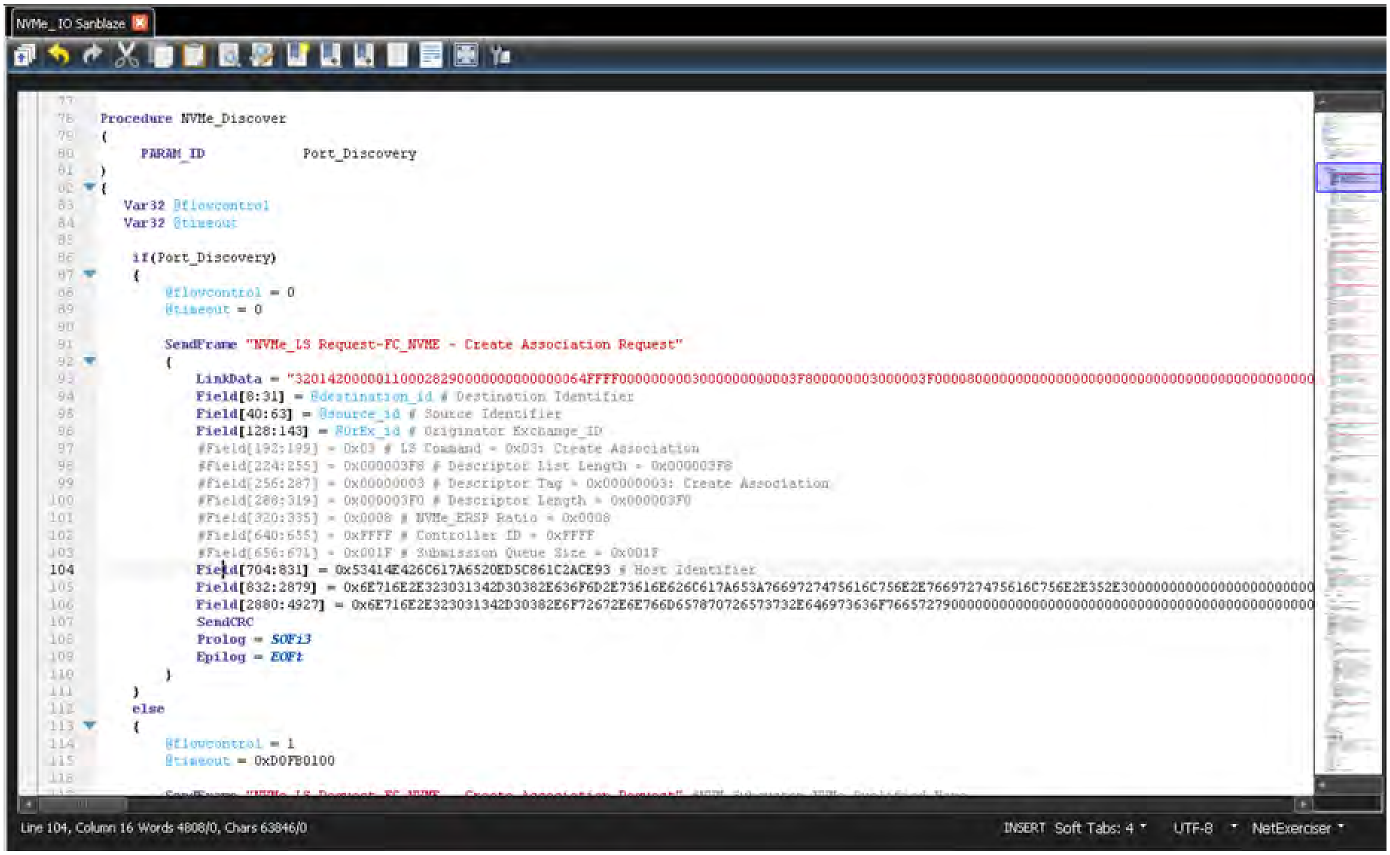


Figure 8.49: Example NVMe Port Discovery

The following formats are supported for hex data and can be used when the data size is more than 64-bits:

- Field[start_bit:end_bit] = "11111111222222223333333344444444"
- Field[start_bit:end_bit] = [aa aa aaaa bbbbbbbb cccccccc 6666666677777777 88888888]
- Field[start_bit:end_bit] = Hex("aaaaaaaabbbbbbbbcccccccc666666667777777788888888")
- This format can be used directly for ASCII strings:
  Field[start_bit:end_bit] = String("AAAAAAAAAAAAAAAB")

Features

For now, data pattern identifiers can be used for values longer than 64 bits. If you want to enter values as string or as data pattern values, add the following feature:

```
Set GenerationMode = GEN_MODE_FC_INITIATOR
Generation
{
  datapattern host_id = 11111111222222223333333344444444
  datapattern host_name =
aaaaaaaabbbbbbbbccccccccddddddddeeeeeeeeffffffff5555555566666666777777778888
8888
```

```
  SendFrame "CASS (Create Association)-NVMe_LS Request-FC_NVME - Create
Association Request" #InternalFrameType[0xef322803, 0x00000008]
  {
            LinkData =
"320000000000000028000000000000000000000000000000000300000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000111111112222222233333333444444440000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000A000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000B00000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000"
            #Field[0:7] = 0x32 # Routing Control = 0x32: NVMe_LS Request
            #Field[64:71] = 0x28 # Data Structure type = 0x28: NVMe over
Fibre Channel
            #Field[192:199] = 0x03 # LS Command = 0x03: Create Association
            Field[704:831] = host_id #0x11111111222222223333333344444444 #
Host Identifier = 0x11111111222222223333333344444444
            Field[832:2879] = host_name
#0x0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000A # Host NVMe
Qualified Name =
0x00000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000A
```

```
            #Field[2880:4927] =
0x00000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000B # NVM Subsystem
NVMe Qualified Name =
0x00000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000B
            SendCRC
            Prolog = SOFi2
            Epilog = EOFt
  }
  Exit(0)
}
```

If needed, you can add one or all of these features. For example:

```
Field[704:831] = String("DEVICE NAME")
```

OR

```
Field[832:2879] =
aaaaaaaabbbbbbbbccccccccddddddddeeeeeeeeffffffff5555555566666666777777778888
8888
```

OR

```
Field[832:2879] =
HEX("aaaaaaaabbbbbbbbccccccccddddddddeeeeeeeeffffffff555555556666666677777777
788888888")
```

8.7.2.7 Symbol Definitions

You can define named FC Symbols which contain two 32-bits DWORDS or one 64-bits QWORD. The last parameter in the parenthesis is the symbol count. These symbols can be used later for sending data.

Format:

```
Symbol symbol_name = [bb: value32_a, value32_b] (count)
Symbol symbol_name = [value32_a, value32_b]
Symbol symbol_name = bb: value32_a, value32_b (count)
Symbol symbol_name = bb: value32_a, value32_b
Symbol symbol_name = value32_a, value32_b (Count)
Symbol symbol_name = value32_a, value32_b
Symbol symbol_name = value64 (count)
Symbol symbol_name = value64
```

Here, “bb” is a two-bit symbol header value (10 by default for data and 01 for ordered sets). In case the user don’t provide header information, it would be calculated based on the symbol value types.

Value32_a and Value32_a are 32-bit DWORDs and Value64 is 64-bits Qword. Constants, variables and even variable expressions are also allowed to be used instead of values. For value64, 64-bits variables can be used.

Count is the number of symbols to send during SendData command. It can also be a constant (optional).

Examples:

```
var32 @a = 1
var64 @b = 2
const SOME_CONSTANT = 1
const COUNT = 2

Symbol symbol_1 = [10: 0x11224488, 0xaabb55dd](1)
Symbol symbol_2 = [10: @a, 0xaabb55dd](1)
Symbol symbol_3 = [10: 0x11224488, @a]    (1)
Symbol symbol_4 = [10: @b ]    (2)
Symbol symbol_5 = [10: 0x11224488aabb55dd ]    (2)
Symbol symbol_6 = [10: 0x11224488, 0xaabb55dd]
Symbol symbol_11 = 0x11224488, 0xaabb55dd (1)
Symbol symbol_12 = @a, 0xaabb55dd (1)
Symbol symbol_13 = 0x11224488, @a (1)
Symbol symbol_14 = @b (2)
Symbol symbol_15 = 0x11224488aabb55dd (2)
Symbol symbol_16 = 0x11224488, 0xaabb55dd
Symbol symbol_17 = SOME_CONSTANT, @a + 1 (COUNT)
Symbol symbol_18 = 10: @a, @a + 1
Symbol symbol_19 = R_RDY, R_RDY(100)
```

8.7.2.8 Send Data

This command sends data to the other side of the connection. SendData command is symbol-based and the format is like this:

```
SendData
{
Symbol_value
Symbol_name
SendData(value, mode, count)
}
```

Symbol value format is the same as format used to define symbols:

```
[bb: value1, value2](count)
[value1, value2]
bb: value1, value2
value1, value2 (count)
value1, value2
expression_1, expression_2
ordered_set1, ordered_set2
```

```
CRC, ordered_set (suppose to use an EOF ordered_set here)
```

NOTE: You can use 32-bit variables instead of each value (value1 or value2) or a 64-bits variable instead of both values or mix of values and variables:

```
[bb:@first_var32, @second_var32](count)
[bb:@var32,  value1](count)
[bb: @var64](count)
```

NOTE: When OrderedSets are used, you should comply with Spec rules, or use the raw format and calculate the symbol values manually.

```
@dword1 = 0x01000010
    SendData
    {
        [R_RDY        , R_RDY     ]
        [SOFi3     , @dword1   ]
        [0x00000000, 0x08000000]
        [10:0x00000000, 0x00000000]
        [10:0x00000000, 0x00000000]
        [10:0x00000000, 0x00000000]
        [10:0x00000000, 0x00000000]
        [10:0x00000000, 0x00000000]
        [10:0x00000000, 0x2BCBEC78]
        #[ 0x00000000, CRC]
        [01:EOFt ,Idle]
    }
```

* CRC can be inserted manually or calculated automatically with the CRC keyword as a Symbol value.

SendCRC/CRC

SendCRC will calculate CRC of a SendData/SendFrame. When there are variable values in SendData, you must include SendCRC command instead of last DWORD. Otherwise, wrong CRC value will be sent.

The constraints are SendCRC is only supported on last DWORD before end of frame.

Send

To instruct the Exerciser to send a bigger volume of data inside a SendData frame, you may use the following commands:

```
Send(@varName, SEND_FIXED, repeat_count)
Send(value64, SEND_FIXED, repeat_count)
```

This command sends the value in the 64-bit variable for 'repeat' number of times. If a 32-bit variable is used here, lower DW would be used for Send command.

```
Send(@varName, SEND_PRBS_11, repeat_count)
Send(value64, SEND_PRBS_11, repeat_count)
```

This command sends the value in the 64-bit variable for ‘repeat’ number of times, by incrementing the variable by 1 in each iteration.

```
Send(@varName, SEND_PRBS_11, repeat_count)
Send(value64, SEND_PRBS_11, repeat_count)
```

This command sends the PRBS_11 value with the initial seed from the 64-bit variable for 'repeat' number of times.

Example:

```
SendData
{
[R_RDY , R_RDY ](100)
[SOFi3 , 0x01000010]
```

NOTE: When OrderedSets are used, you should comply with Spec rules, or use the raw format and calculate the symbol values manually.

```
Send(0x00000000, SEND_FIXED, 6)
[0x00000000, CRC]
[EOFt ,Idle]
}
@dword1 = 0x00000100
SendData
{
R_RDY, R_RDY(100)
SOFi3, 0x01000010
Send(@dword1, SEND_INCREMENTAL, 6)
0x00000000, SendCRC
EOFt ,Idle
}
```

Field Definition

- Field length is in bits. '*' means that the length is variable and is set based on the assigned value.
- Field starting offset is calculated from frame start based on the length of the previous fields.

Examples:

```
Field32      : 32 = 0xAABBFFEE
FrameType    : 8  = 12
HashedDest   : 24 = HEX_DATA
Reserved1    : 8  = 0xDA
Field16      : 16 = 0xAAAA
Reserved2    : 8  = 0xAD
CRC          : 32
```

Data field Definition

- **Data = { pattern }**: Pattern is assigned to Data.
- **Data = count, value**: A pattern of "count" times "value" is assigned to Data.

  Data = count, start value, step: A pattern of values starting with "start value" with steps of "step" and a length of "count" is assigned to Data.

8.7.2.9 Frames

Using the “Frame” or “Packet” keyword, you can define a frame of traffic you frequently use outside the Generation block. Then, you can use the defined Frame in the Generation block stream multiple times. If you try to define a Frame inside the Generation block, you will get a compilation error.

Declarations of prologue and epilogue may be mixed with field declarations.

```
Frame "name" : "parent name"
{
Field Definition 0: "Field Name : Field Length = Default Value"
…
Field Definition n: "Field Name : Field Length = Default Value"
Symbol Definition 0: "Symbol name, offset, count"
…
Symbol Definition m: "Symbol name, offset, count"
Prolog = "ordered_set name"
Epilog = "ordered_set name"
}
```

8.7.2.10 Prologue and Epilogue

Prologue and epilogue are primitive chains to be used at the beginning and end of the frame.

Examples:

```
PProlog = SOFi2 # For this frame ordered set 'SOFi2' is a Prolog.
Epilog = EOFt # For this frame ordered set 'EOFt' is an Epilog.
```

8.7.2.11 Inserting Symbols

Additional symbols can be inserted inside frames with the following format:

Symbol: Symbol_name, offset, count

- **symbol_name** is the name of a symbol which is already defined.
- **offset** is a symbol offset is the position to insert the symbol. For example, value 1 means insert the symbol after the first symbol (2-DWORDs) in the Frame, which would be the third and forth DWORDs (if the count is 1). This value is optional and 0 by default.
- **Count** is the count of symbol to be inserted inside the frame. This value is optional and 1 by default.
- **Symbol*** This command can be used to clear all the previously inserted symbols inside a frame. The user can insert new symbols after this command or just remove all of them in the inherited Frame.

Examples:

```
Symbol : *
Symbol : symbol1, 2, 100
```

NOTE: If the offset value is more than the count of symbols in the frame, the Symbol command would be ignored.

8.7.2.12 Inheriting Frames

Inheriting Frames can be derived from other Frames, therefore inheriting the layout of the parent Frame. In this case, the user may:

- Change Prolog and Epilog
- Change default field values
- Add new fields

Frame Examples

```
Frame Some_Frame
{
    Field32 : 32 = 0xAABBFFEE
    FrameType : 8 = 12
    HashedDest : 24 = HEX_DATA
    Reserved1 : 8 = 0xDA
    Field16 : 16 = 0xAAAA
    Reserved2 : 8 = 0xAD
    Data : * = PATTERN_1
    CRC : 32
    Symbol : *
    Symbol : symbol1, 36, 5
    Prolog = SOFi2
    Epilog = EOFt
}
Frame Some_Frame_1 : Some_Frame
{
    Field32 = "Some Hex Data"
    Data = { 11111111 22222222 33333333 44444444 55555555 }
    Opcode : 128, 8, 0x2A
    LBA : 64
    Symbol : *
    Symbol : symbol1, 24, 48
    Prolog = SOFi3
}
```

8.7.3 Generation Block

Generation block is the starting point of exerciser script.

```
Generation
{
}
```

8.7.4 Preprocessor Integer Arithmetic

Examples:

```
x = (3 * 2 ) / 6
x = x + 2
y =>> 2
y = x & 0x000000FF | 0x0000FF00
x = 10
++x
while(x > 1)
{
 x -= 1
}
Y = 10
```

8.7.5 Loops

Loops can be used in two modes:

1. Using an integer number, loop a specified number of loops. This number has to be smaller than 67,000,000.
2. Using the word “infinite”, loops forever.

```
Loop(credits)
{
 Wait_For{WF_FRAME_RESOURCES_OUTPUT_C}
 senddata{[r_rdy ,idle]}
 credits--
}
```

NOTE: The Exerciser can support up to 4 levels of nested loops.

8.7.6 Controlling Connection Speed

When you use the **Autoconnect** feature, the Exerciser always tries to connect to the DUT with the highest possible speed. In this case, the **Set Speed** command is not used.

If you want to connect to the DUT with a specific speed, you may set the Autoconnect feature to OFF, and set/hardcode the desired speed, using the Set Speed command

8.7.7 Exerciser Script Important Features

The Exerciser script language can already produce FC Symbol Sequences and Frames.

The Exerciser script enhancements described in this section allow generation of Commands and Application Layer sequences (as in the Exerciser), by processing received frames, making complex decisions, and generating the contents of frames in run-time, for both RX and TX. Variables can keep the run-time state of the bus. Low-level commands can manipulate variables and use variables to create patterns.

The features and commands include:

- Variable Operations/Identifier
- Functions
- Commands
- Wait
- SendData
- Generation Options
- Orderset
- Flow control
- Procedures

The Exerciser can be programmed to act as FC Initiator, or FC Target.

NOTE: An Example Project, which includes scripts implementing UNH tests (Exerciser UNH example.gep), can be found under the Examples/ Projects folder in the installation.

8.7.7.1 FC Initiator

As an Initiator, Exerciser can send commands and interact with its peer to complete the command in normal conditions and some popular error conditions. Limitations are:

- Uses only one command at a time.
- Sends only limited Write data patterns.
- Has tight flow control, due to limited RX frame processing.

8.7.7.2 FC Target

As a Target, Exerciser can receive commands in all protocols and respond to them in normal conditions or some popular error conditions. Limitations are:

- Uses only one command at a time. Command queuing is not supported.
- Has tight flow control, due to limited RX frame processing.

8.7.7.3 Variable Definition

Variable definition is similar to definitions in programming languages. You can define up to 250 32-bit or 125 64-bit variables. There is no constraint on variable names, except that you cannot use keywords.

Variable scopes are general and you should define them in the script header before the Generation block.

The syntax of variable definition is:

```
VAR32 @VariableName1, @VariableName2, ...
VAR64 @VariableName
```

VAR64 holds field values greater than 32 bits, such as FCAddress.

NOTE: Variable names should start with @.

8.7.7.4 Assigning Variable Values

You can set variable values in different ways:

Constant Value

```
@varName1 = 1234
```

Other Variable Value

```
@varName1 = @varName2
```

Result of Expression on Other Variables

```
@varName1 = @varName1 + @varName2
```

Fields of Last Received Frame

```
@varName1 = (FCFrame)LRF::FrameType
```

...where LRF is Last Received Frame.

NOTE: Specifying packet type (FCFrame) before LRF causes last received frame to be this packet type, and field start-bit position is calculated according to the packet-type definition.

Part of Last Received Frame

```
@varName1 = LRF[startBitOffset:endBitOffset],
where offsets are bit based
```

Example:

```
@varName1 = LRF[32:39]
SendFcFrameCommand_Initiator
{
 Data = LRF[startBitOffset:endBitOffset]
 Tag = 0x101
}
```

The constraints are:

- Length bigger than 64 bit is not supported
- Offsets (StartBitOffset and EndBitOffset) should be in same DWORD, or adjacent DWORDS

Random Values

```
@varName1 = Random
```

8.7.7.5 Expression on Variables

Mathematical expressions, such as sum, subtract, and shift:

```
@varName1 + @varName2
@varName1 - @ varName2
@varName1 & @varName2
@varName1 | @varName2
@varName1 ^ @varName2
@varName1 << 2
@varName1 >> 1
```

Logical expressions, such as compare, equal, not, and, and or:

```
@varName1 > @varName2
@varName1 < @ varName2
@varName1 == @varName2
@varName1 != @ varName2
!@varName1
(logical expression1) && (logical expression2)
(logical expression1) || (logical expression2)
```

Complex expressions (combination of different operators) with prioritizing supported:

```
(@varName1 + @varName2) > @varName3
```

Extended Variable Operations (Multiply, Divide, Remainder, none-numeric shift):

Multiplication Operations

```
var32 @a = @b * 3
@a *= 2
@c = @a * @b
```

Division Operations

```
var32 @a = @b / 3
@a /= 2
@c = @a / @b
```

Remainder Operations

```
var32 @a = @b % 3
@a %= 2
@c = @a % @b
```

Shift Operations

```
@a = @b >> @c
@a = @b << @c
```

NOTE: In order to use extended variable operations like *, /, % and shift (<<' >>) with variables, this include file must be added before Generation block: `%include "Generation/Include/VariableOperations.inc"`

8.7.7.6 Reserved Constants

Reserved constants are predefined values that can be assigned to variables and their values changes during program execution. The following reserved constants are defined in the software:

```
      Training_ERROR_COUNT
LRT
      Local_Tx_status_word
-B_B_Credi
```

Example:

```
Var32 @a = B_B_Credit
```

8.7.7.7 Variable Domains

Variable domains can be either global (outside Generation block) or local (inside a Generation block or a procedure).

Local and Global Domains

Variables can be either defined outside the Generation block which makes them global variables or inside Generation block or procedures. Global variables are visible everywhere after they are defined.

Variables that are defined in the Generation block are valid after they are defined, and also inside inline procedures, or procedures with parameters (which are also inline).

Variables that are defined inside the procedures are valid only inside the procedure and all the inline procedures that are called after the variable definition (inside the same procedure).

If a variable is defined inside a domain that has already a variable with the same name in the higher domain, the variable defined in the same domain will override the previous variable and the previous variable would no longer be visible in the current domain but it value won't be updated by changing the newly defined variable.

NOTE: This Domain concept also applies to Constants, Identifiers, DataPatterns and Symbols.

Examples:

```
var32 @a = 1 # Global::@a

Procedure Proc2
{
   var32 @var1_proc2 = @a # on the first call, @a is Global::@a and equals to
1
      # on the second call, @a is Proc1::@a and equals to 2
    var32 @a = 3 # Proc2::@a
    var32 @var2_proc2 = @a # @var2_proc2 == 3, here @a is overrided by
      #local variable and its value is 3
    @a = 4        #only update Proc2::@a to 4
}

Procedure Proc1
{
    var32 @var1_proc1 = @a # valid operation: @var1_proc1 == 1,
# Here @a (Global::@a) is valid and equal to 1
    Call Proc2
    #Proc2::@a is no longer visible here, so @a here is Generation::@a

    var32 @var2_proc1 = @a # valid operation: @var2_proc1 == 1,
#Here @a (Global::@a) is valid and equal to 1

    var32 @a = 2 # proc1::@a
```

```
        Call Proc2
        #value of @a is still 2 here (Proc1::@a)
    }

    Generation
    {
        var32 @var1_gen = @a # valid operation: @var1_gen == 1
        Call Proc1
        var32 @var2_gen = @a # valid operation: @var2_gen == 1, here @a is still
    Global::@a

        var32 @a = 5 # Generation::@a
        var32 @var3_gen = @a # valid operation: @var3_gen == 5 as
    # Generation::@a would override the Global::@a
        exit(@a)      # exits with the code 5
    }
```

8.7.7.8 If/While in Logical Expressions

Like programming languages, scripts allow conditional statements.
The **if/while** syntaxes are:

```
If (expression)
{
   …
}
ElseIf (expression 2)
{
   …
}
.
.
.
ElseIf (expression n)
{
   …
}
else
{
   …
}

While(expression)
{
   …
   If (condition 1) { BreakWhile }
   …
   If (condition 2) { ContinueWhile }
   …
}
```

BreakWhile

If it's called inside a While loop block, program execution point would jump to the next instruction after the While block.

ContinueWhile

If it's called inside a While loop block, program execution point would jump to the first instruction inside the While block.

Example for if, then else:

```
@HT_RxFISType = LRF[0:7]
#LRF_SATA_FIS_TYPE_START_BIT:LRF_SATA_FIS_TYPE_END_BIT
if  (@HT_RxFISType == SATA_FIS_TYPE_DMA_ACTIVATE)   then  {…}
 else { if (@HT_RxFISType == SATA_FIS_TYPE_DATA) then  {…}
             else { if (@HT_RxFISType == SATA_FIS_TYPE_RD2H)  then  {…} } }

Example for while:
while (@NCQ_Temp0)   {
            @NCQ_Temp1= @NCQ_Temp1 >> 1
            If (@NCQ_Temp1 != 0) then { … }
            @NCQ_Temp0 = @NCQ_Temp1 & 0x00000001     }
```

NOTE:
- Nested **while** and **if** are supported.
- The keyword **then** is optional.

Wait/When/Do in Logical Expressions

The **wait/when/do** syntaxes are:

```
wait (time)
{
    When {exp} do
    {
        …
    }
    Elsewhen {exp}do
    {
        …
    }
    on_timeout
    {
        …
    }
}
Example:
wait { #no timeout use global WaitTimeout value default 1000 useconds (1 ms)
    when {WF_R_RDY} do
    { … }
    elsewhen {WF_VC_RDY} do
    { … }
    on_timeout
    { … }
}
```

NOTE: Nested wait should not exceed two deep. Use a procedure call to extend wait logic sequence.

```
Example:
wait_for (100000) { WF_R_RDY WF_TIMEOUT} { … } # (100 ms)

      "Wait_For (1000) { WF_SOFi3 WF_R_RDY WF_TIMEOUT }
      "Wait_For (1000) { WF_SOFi3 WF_R_RDY }
      "Wait_For { WF_SOFi3 WF_R_RDY WF_TIMEOUT }
Also these three are the same and just wait for 1ms
      "Wait_For { WF_TIMEOUT }
      "Wait_For (1000)
      "Wait_For (1000) { WF_TIMEOUT }
```

NOTE: Using the `WF_TIMEOUT` condition is optional when a timeout value is defined. `Wait + Wait_For` is OK. So these three expressions are the same (default timeout value is 1ms).

8.7.7.9 Using Variable Values in Creating Patterns on Bus

In creating patterns to send on bus, the Exerciser script allows using variables. In these cases, because the created pattern is dynamic, it is not possible to do scrambling and calculating in the software code. These tasks are done in the hardware Bus Engine. To activate, set “Auto scramble mode” to “on”.

The following examples show uses of variables in creating patterns.

Use Variable for Field Value

```
SendELSReqPLOGI
{
    OriginatorExchageId = 0x1
    DestinationIdentifier = @variableName1
    ...
}
```

The constraint is that **Field Length** bigger than 64 bit is not supported.

Use LRF Directly for Field Value

```
Send_FCPData
{
    Data = LRF[startBitOffset:endBitOffset]
    SourceIdentifier = 0x101
}
```

The constraints are:

- Length bigger than 64 bit is not supported and
- Offsets (StartBitOffset and EndBitOffset) should be in same DWORD, or adjacent Dwords

```
Wait_For{WF_R_RDY}
SendData
{
    [01: Idle, SOFn3]
    [10:@AA, @BB]
    [10:0x08090008, @DD]
```

```
    [10:@CC, @frame_count]
    send(@IncInit, SEND_INCREMENTAL, last_size/8) #(fcp_dl-max_mtu)
    [01:CRC ,EOFt]
}
```

When there are variable values in SendData, you must include SendCRC command instead of last DWORD. Otherwise, wrong CRC value will be sent.

The constraint is that **SendCRC** is only supported on last DWORD before end of frame.

8.7.7.10 Timer

Exerciser script syntax allows using some timers. You can start a timer anywhere. The timer current value is loadable on variable to be used in expressions and conditions on this expression. There are four timers, named A, B, C, and D.

Starting Timer (setting timer value to zero)

```
CLEAR_TIMER_A
CLEAR_TIMER_B
CLEAR_TIMER_C
CLEAR_TIMER_D
```

Loading Timer Current Value in Variables

```
@varName1 =TIMER_A
@varName1 =TIMER_B
@varName1 =TIMER_C
@varName1 =TIMER_D
```

Example:

```
      CLEAR_TIMER_A
While(@Counter < MaxPeriodCount) {
                  … @Counter = TIMER_A … }
```

8.7.7.11 Frame and Symbol Resources A-F

There are six Recording Resources as defined in 8.3.5.5, *Generation Options (Advance Wait Conditions)*. Details on their use is described below in 8.7.8.7, *Wait Commands*.

8.7.7.12 PATTERN Counter

Exerciser script syntax allows you to use counters on a number of defined events in generation settings.

Syntax for loading counters in variables is:

```
@varName1 = COUNT_FRAME_RESOURCE_OUTPUT_A
…
@varName1 = COUNT_FRAME_RESOURCE_OUTPUT_F
@varName1 = COUNT_SYMBOL_RESOURCE_OUTPUT_A
…
@varName1 = COUNT_SYMBOL_RESOURCE_OUTPUT_F
```

Syntax for clearing (resetting) counters is:

```
CLEAR_FRAME_RESOURCE_OUTPUT_A
…
```

```
CLEAR_FRAME_RESOURCE_OUTPUT_F
CLEAR_SYMBOL_RESOURCE_OUTPUT_A
…
CLEAR_SYMBOL_RESOURCE_OUTPUT_F
Example:
CLEAR_FRAME_RESOURCE_OUTPUT_A
While(@Counter < MaxReceivedFrameCount)
{
    …
    @Counter = COUNT_FRAME_RESOURCE_OUTPUT_A
    …
}
```

8.7.7.13 Procedure Definition

Procedures allow creating simple syntaxes for complex reusable parts in scripts. You can write such code once as a procedure and use everywhere required.

Inline procedures are the same as procedures by they increase the compiled assembly size but they can use local variables which are defined after them (before call instruction).Procedure definition syntax is:

```
procedure procedureName
{
...
}

Or
Procedure_Inline procedureName
{
    ...
}
```

Calling procedure syntax is `Call procedureName`.

NOTE:
- Recursive calls are not allowed and are not flagged.
- The user can define up to 256 none-inline different procedures including those inside the include files. Defining each procedure uses one resource only if that procedure is referenced in the script more than once.
- Procedure with parameters are also inline and also defining a local variable inside a procedure would make it inline.

Hint: To pass parameters to procedures or return values from them, global variables or parameters can be used.

8.7.7.14 Procedure with Parameters

For passing a parameter to a procedure, you can define different of parameters:

PARAM_ID: Value parameters are defined with the keyword PARAM_ID and can be constants, identifiers, numbers and any numeric expression that is supported.

PARAM_VAR32 / PARAM_VAR64: For sending variables you can use either 32-bit variables using PARAM_VAR32 or 64-bit variables using PARAM_VAR64. Variable expressions also can be used to send the result to the procedure as a parameter.

PARAM_ID_REF: For returning a numeric value from a procedure, PARAM_ID_REF can be used and an identifier name should be passed as parameter during calling the procedure.

PARAM_VAR32_REF / PARAM_VAR64_REF: For returning a 32/64 bit Variable, PARAM_VAR32_REF / PARAM_VAR64_REF can be used and a variable name with the same size should be passed as parameter during calling the procedure.

Parameter Types

PARAM_ID: can be used for sending numeric values to procedures

PARAM_ID_REF: can be used for sending and receiving numeric values to/from procedures

PARAM_VAR32: can be used for sending 32-bit variables values to procedures

PARAM_VAR32_REF: can be used for sending and receiving 32-bit variables values to/from procedures

PARAM_VAR64: can be used for sending 64-bit variables values to procedures

PARAM_VAR64_REF: can be used for sending and receiving 32-bit variables values to/from procedures

Calling functions with parameters

For calling parameter with parameters, valid expressions must be used for each type of parameters which are as the following:

PARAM_ID: numeric expressions like values, constants or identifier expressions can be used (e.g. 12, i, i + 1)

PARAM_ID_REF: only identifiers can be used. For using an identifier it should be defined already by assigning a default value like 0 to it before passing it to a procedure. (e.g. i, j)

PARAM_VAR32: numeric and 32-bit variable expressions like values, constants or identifier expressions and 32-variables and 32-bit variable expressions can be used (e.g. 12, i, i + 1, @a, @a + i + 1, @a + @b)

PARAM_VAR32_REF: only 32-bit variables can be used. For using a variable it should be defined already before call instruction. (e.g. @a, @j)

PARAM_VAR64: numeric and 32/64-bit variable expressions like values, constants or identifier expressions and variables and variable expressions can be used (e.g. 12, i, i + 1, @a, @a + i + 1, @a + @b)

PARAM_VAR64_REF: only 64-bit variables can be used. For using a variable it should be defined already before call instruction. (e.g. @a_64, @j_64)

Procedure definition with parameters syntax is:

```
procedure procedureName(Param_Type1 Param1, Param_Type2 Param2, … ,
Param_Type_n Param_n)
```

```
{
    ...
}

#    Parameter Types
#    - PARAM_ID: for sending numeric values to procedures
#    - PARAM_ID_REF: for sending and receiveing numeric values to/from
procedures
#    - PARAM_VAR32: for sending 32-bit variables values to procedures
#    - PARAM_VAR32_REF: for sending and receiveing 32-bit variables values
to/from procedures
#    - PARAM_VAR64: for sending 64-bit variables values to procedures
#    - PARAM_VAR64_REF: for sending and receiveing 32-bit variables values
to/from procedures
Procedure ProcedureName3
(
    PARAM_ID            param1,  #e.g. 1, 2 + i, i
    PARAM_ID_REF        param2,  #e.g. i
    PARAM_VAR32         @param3, #e.g. @a, @a + @b, 2
    PARAM_VAR32_REF     @param4, #e.g. @a
    PARAM_VAR64         @param5, #e.g. @a, @a + @b, 2
    PARAM_VAR64_REF     @param6  #e.g. @a
)
{
    #You can access procedure parameters here inside procedure block ...
}
```

Calling procedure syntax is:

```
Call procedureName(Param1, Param2, … , Param_n)
```

Flow Control Expressions

Return: Return is used for returning from Procedures and continues the program from the next instruction after the call. If return is used inside the Generation Block, it would work the same as the exit(0) instruction.

8.7.8 Sierra Exerciser Generation Commands

8.7.8.1 General Commands

LASER_ON

Enables exerciser to send traffic without the Link-Up process.

LINK_RESET_PROT

BE initiates link reset protocol sequence

LINK_FAILURE_PROT

BE initiates link Failure protocol sequence

EXIT_MANUAL_TRAINING

When a manual training frame command Is used, Exerciser moves to a state where it continuously sends Training frames until this command is executed.

Example:

When a wait command is written after a `SendTrainingFrame` command, the Exerciser keeps sending the last training frame instead of idles. This command is used to exit from manual training command and move on to normal data.

Send_NOS

Exerciser sends NOS for the time specified in `NOS_Transmit_time` speed neg settings.

Send_OLS

Exerciser sends OLS for the time specified in `OLS_Transmit_time` speed neg settings.

Send_LR

Exerciser sends LR for the time specified in `LR_Transmit_time` speed neg settings.

Send_LRR

Exerciser sends LRR for the time specified in `LRR_Transmit_Time` speed neg settings.

SendTrainingFrame

Transmits a specific Training Frame.

SendRawTrainingFrame

Transmits user specified 32+256 bits of Manchester encoded data.

SendAlignmentMarkerError

Indicates which index of Alignment Marker (AM) to be corrupted.(ex: 64G FC has 4 AMs. Each index0-3 indicates 4 AMs respectively).

Format:

```
SendAlignmentMarkerError(Index_Mask, Replace Index Mask, Count)
```

where:

- `Index_Mask` (Index_0..index_3): Indicates which index of AM to be corrupted (e.g., 64G FC has 4 AMs. Each index0-3 indicates 4 AMs, respectively).
- `Replace Index Mask` (0-3) with User-defined value: When this bit is set User defined value specified in speed neg settings will be Placed in the corresponding Alignment marker for no. of times specified in count.
- Count: Number of AMs to be corrupted.

Example:

```
SendAlignmentMarkerError (INDEX_0 | INDEX_1 | INDEX_2,  REPLACE_INDEX_1 |
REPLACE_INDEX_2, 1024)
```

SetAMIndexValue

Sets alignment marker default values for Index0..Index3. These values can be used later in the `SendAlignmentMarkerError` command to inject alignment marker error.

`AM_INDEX0_VALUE` - User defined value for the 1st Alignment Marker

AM_INDEX1_VALUE - User defined value for the 2nd Alignment Marker

AM_INDEX2_VALUE - User defined value for the 3rd Alignment Marker

AM_INDEX3_VALUE - User defined value for the 4th Alignment Marker

WaitForTrainingFrame

Wait for specified Training Frame.

Format:

```
WaitForTrainingFrame(Training_Sequence, Mask, Change/*TRUE or FALSE*/})
```

Example: (waiting for SN, 64G)

```
WaitForTrainingFrame(0x80004000, 0xC0004000, FALSE)
```

Analyzer Trigger

SET_ANALYZER_TRIGGER - Call this command to set Analyzer Trigger.

SET_EXTERNAL_TRIGGER - Call this command to set External Trigger Out. Settings and External Trigger In Type to High Active, Low Active, Toggle and set External TrigOut pulse width.

Clear Timers

CLEAR_TIMER_A - Clears timer resource A

CLEAR_TIMER_B - Clears timer resource B

CLEAR_TIMER_C - Clears timer resource C

CLEAR_TIMER_D - Clears timer resource D

Error Injection

InjectRSFECError (RSFEC error type) - Injects correctable and uncorrectable FEC errors. Only works for 32G and 64G speeds.

InjectSyncHeaderError(count) - Sync header error command injects idle-idle symbols with wrong sync header error on the link.

Clear Resources

CLEAR_FRAME_RESOURCE_OUTPUT_A - Clears Frame Resource Counter A

CLEAR_FRAME_RESOURCE_OUTPUT_B - Clears Frame Resource Counter B

CLEAR_FRAME_RESOURCE_OUTPUT_C - Clears Frame Resource Counter C

CLEAR_FRAME_RESOURCE_OUTPUT_D - Clears Frame Resource Counter D

CLEAR_FRAME_RESOURCE_OUTPUT_E - Clears Frame Resource Counter E

CLEAR_FRAME_RESOURCE_OUTPUT_F - Clears Frame Resource Counter F

CLEAR_SYMBOL_RESOURCE_OUTPUT_A - Clears Symbol Resource Counter A

CLEAR_SYMBOL_RESOURCE_OUTPUT_B - Clears Symbol Resource Counter B

CLEAR_SYMBOL_RESOURCE_OUTPUT_C - Clears Symbol Resource Counter C

CLEAR_SYMBOL_RESOURCE_OUTPUT_D - Clears Symbol Resource Counter D

CLEAR_SYMBOL_RESOURCE_OUTPUT_E - Clears Symbol Resource Counter E

CLEAR_SYMBOL_RESOURCE_OUTPUT_F - Clears Symbol Resource Counter F

Speed Settings

SET_SPEED_16G - Changes the speed of exerciser to 16G

SET_SPEED_32G - Changes the speed of exerciser to 32G

SET_SPEED_64G - Changes the speed of exerciser to 64G

SET_RX_SPEED_16G - Allow Wait_For on specific 16G speed Rx Traffic

SET_RX_SPEED_32G - Allow Wait_For on specific 32G speed Rx Traffic

SET_RX_SPEED_64G - Allow Wait_For on specific 64G speed Rx Traffic

SET_RX_SPEED_AUTO - Allow Wait_For on any speed Rx Traffic

Link Protocol Sequences

LINK_RESET_PROT - BE initiate link reset protocol sequence

LINK_FAILURE_PROT - BE initiate link Failure protocol sequence

Delays

Delay() - Generate a 1-microsecond delay

Random Delay() - Generate a random delay (between 1 microsecond and 20 microseconds)

8.7.8.2 Speed Negotiation Settings

TABLE 8.1: Speed Negotiation Settings (Sheet 1 of 2)

Command	Value	Description
AM_Remote_Degrade	OFF	When this bit set to high, Remote Degrade bit for Alignment marker is calculated according to the degrade counters specified inside Speed Neg parameter block—When disabled Zero is placed in RD bit of AM.
FEC_Degrade_interval	0	This is a 32 bit register that specifies the number of RS-FEC code words that make up a Degrade interval.
Degrade_Activate_threshold	0	This is a 32 bit register that specifies a symbol error count. If error count is more than this value, then RD bit gets high.

TABLE 8.1: Speed Negotiation Settings (Sheet 2 of 2)

Command	Value	Description
Degrade_Deactivate_Threshold	0	This is a 32 bit register that specifies a symbol error count. The value here controls the threshold used to deactivate RD. **NOTE**: The Reed Solomon Decoder counts the number of symbol errors detected in all the code words within the FEC_Degrade_interval. If a codeword is uncorrectable, the number of symbol errors detected is incremented by 16. When the number of symbol errors detected within a FEC_Degrade_interval exceeds the Degrade_Activate_Threshold, RD will be signaled to the remote link partner using a bit in the Alignment Marker. At the end of an interval, if the number of symbol errors is less than the Degrade_Activate_Threshold, RD will be signaled to the remote link partner using a bit in the Alignment Marker. At the end of an interval, if the number of symbol errors is less than the Degrade_Deactivate_Threshold, RD will be de-asserted in the Alignment Marker.

8.7.8.3 FC Manual Speed Negotiation Timers

TABLE 8.2: FC Manual Speed Negotiation Timers

Command	Value	Description
NOS_Trasmit_Time_us	45000	Primitive is transmitted for specified time. User entered time value to be converted in to no. of clock cycles and programmed in to settings
OLS_Transmit_Time_us	5000	OLS primitive is transmitted for specified period of time. User entered time value to be converted in to no. of clock cycles and programmed in to settings.
LR_Transmit_Time_us	10	LR primitive is transmitted for specified period of time. User entered time value to be converted in to no. of clock cycles and programmed in to settings.
LRR_Transmit_Time_us	10	LRR primitive is transmitted for specified period of time. User entered time value to be converted in to no. of clock cycles and programmed in to settings.

8.7.8.4 Wait Commands

TABLE 8.3: Wait Commands

Wait Command Name	Description
WF_ELS_Request_Frame	Waits for a ELS Request Frame
WF_ELS_Reply_ACC_Frame	Waits for a ELS Reply ACC_Frame
WF_ELS_Reply_RJT_Frame	Waits for a ELS Reply RJT Frame

TABLE 8.3: Wait Commands

WF_B_B_Credit_Available	Waits until a BB_Credit is available

8.7.8.5 InjectRSFECError Command Values (Sheet ? of ?)

Table 8.4 contains the possible values for the InjectRSFECError command:

TABLE 8.4: InjectRSFECError Command Values

Error Type	RS-FEC	Parameter
Correctable	1 symbol at Data	FEC_CORRECTABLE_1_DATA
Correctable	1 symbol at Parity	FEC_CORRECTABLE_1_PARITY
Correctable	4 symbols at Data, 3 symbols at Parity	FEC_CORRECTABLE_4_DATA_3_PARITY
Correctable	1 symbol at Data, 6 symbols at Parity	FEC_CORRECTABLE_1_DATA_6_PARITY
Correctable	7 symbols at Data	FEC_CORRECTABLE_7_DATA
Correctable	7 symbols at Parity	FEC_CORRECTABLE_7_PARITY
Uncorrectable	4 symbols at Data, 4 symbols at Parity	FEC_UNCORRECTABLE_4_DATA_4_PARITY
Uncorrectable	8 symbols at Data	FEC_UNCORRECTABLE_8_DATA
Uncorrectable	8 symbols at Data(only one bit in each symbol)	FEC_UNCORRECTABLE_8_DATA_1_BIT
Uncorrectable	8 symbols at Parity	FEC_UNCORRECTABLE_8_PARITY
Uncorrectable	1 symbol at Data, 7 symbols at Parity (only one bit in each symbol)	FEC_UNCORRECTABLE_1_DATA_7_PARITY_1_BIT
Uncorrectable	1 symbol at Data(only one bit in each symbol), 7 Parity symbols	FEC_UNCORRECTABLE_1_DATA_1_BIT_7_PARITY
Uncorrectable	7 symbols at Data, 1 symbol at Parity	FEC_UNCORRECTABLE_7_DATA_1_PARITY
Uncorrectable	all Parity symbols	FEC_UNCORRECTABLE_ALL_PARITY
Error Type	RS-FEC for PAM4	PAM4 Parameter
Correctable	1 symbol at Data	FEC_CORRECTABLE_1_DATA
Correctable	1 symbol at Parity	FEC_CORRECTABLE_1_PARITY
Correctable	8 symbols at Data, 7 symbols at Parity	FEC_CORRECTABLE_8_DATA_7_PARITY
Correctable	1 symbol at Data, 14 symbols at Parity	FEC_CORRECTABLE_1_DATA_14_PARITY
Correctable	15 symbols at Data	FEC_CORRECTABLE_15_DATA
Correctable	15 symbols at Parity	FEC_CORRECTABLE_15_PARITY
Uncorrectable	8 symbols at Data, 8 symbols at Parity	FEC_UNCORRECTABLE_8_DATA_8_PARITY
Uncorrectable	16 symbols at Data	FEC_UNCORRECTABLE_16_DATA
Uncorrectable	16 symbols at Data (only one bit in each symbol)	FEC_UNCORRECTABLE_16_DATA_1_BIT
Uncorrectable	16 symbols at Parity	FEC_UNCORRECTABLE_16_PARITY
Uncorrectable	1 symbol at Data, 15 symbols at Parity (only one bit in each symbol)	FEC_UNCORRECTABLE_1_DATA_15_PARITY_1_BIT
Uncorrectable	1 symbol at Data(only one bit in each symbol), 15 Parity symbols	FEC_UNCORRECTABLE_1_DATA_1_BIT_15_PARITY
Uncorrectable	15 symbols at Data, 1 symbol at Parity	FEC_UNCORRECTABLE_15_DATA_1_PARITY
Uncorrectable	all Parity symbols	FEC_UNCORRECTABLE_ALL_PARITY

8.7.8.6 Predefined Ordered Sets

The following ordered sets are defined by default in the FC Exerciser. They can be used inside SendData, SendFrame and Frame commands.

- Idle
- LPI
- SOFi2
- SOFn2
- SOFi3
- SOFn3
- SOFf
- EOFt
- EOFa
- EOFn
- EOFni
- R_RDY
- VC_RDY(a, b)
- BB_SCs
- BB_SCr
- NOS
- OLS
- LR
- LRR

NOTE: VC_RDY parameters are optional and can be numbers, constants or variables. When using VC_RDY with no parameters, a and b are assumed to be zero.

8.7.8.7 Wait Commands

After using Wait/Wait_for commands, the exerciser will wait until the specified timeout has elapsed (default value if not specified) or any of the defined conditions are satisfied e.g. SOF ordered set is received from the DUT.

Syntax:

```
WAIT_FOR { <command1> <command2> ... <group1> <group2> ... }
```

Table 8.5 shows all the possible conditions for `wait` and `wait_for` commands:

TABLE 8.5: Wait & Wait_For Commands (Sheet 1 of 2)

Wait Command Name	Description
WF_TIMEOUT	Timeout Credit Available When WF_TIMEOUT is requested in WAIT_FOR command, the wait session will be released after timeout has elapsed. See 8.7.8.8, *WHEN / ELSEWHEN / ON_TIMEOUT Commands* for more detailed explanation. The Timeout value can be set two different ways: 1. Through the global WaitTimeout setting that can appear anywhere in generation. Default value is 1000 microseconds. Syntax: Set WaitTimeout = <value> (in microseconds) 2. Through local WaitTimeout value for this specific wait session. Syntax: WAIT_FOR (<number_of_microseconds>){WF_TIMEOUT <other_wait_commands>} In this case wait for other commands will be released no later than after number_of_microseconds, but global WaitTimeout value remains unchanged for future use.
WF_SOFi2_DW1	Wait for the SOFi2 OrderedSet in the first DWORD
WF_SOFi2_DW2	Wait for the SOFi2 OrderedSet in the second DWORD
WF_SOFi2	Wait for the SOFi2 OrderedSet in any DWORD
WF_SOFn2_DW1	Wait for the SOFn2 OrderedSet in the first DWORD
WF_SOFn2_DW2	Wait for the SOFn2 OrderedSet in the second DWORD
WF_SOFn2	Wait for the SOFn2 OrderedSet in any DWORD
WF_SOFi3_DW1	Wait for the SOFi3 OrderedSet in the first DWORD
WF_SOFi3_DW2	Wait for the SOFi3 OrderedSet in the second DWORD
WF_SOFi3	Wait for the SOFi3 OrderedSet in any DWORD
WF_SOFn3_DW1	Wait for the SOFn3 OrderedSet in the first DWORD
WF_SOFn3_DW2	Wait for the SOFn3 OrderedSet in the second DWORD
WF_SOFn3	Wait for the SOFn3 OrderedSet in any DWORD
WF_SOFf_DW1	Wait for the SOFf OrderedSet in the first DWORD
WF_SOFf_DW2	Wait for the SOFf OrderedSet in the second DWORD
WF_SOFf	Wait for the SOFf OrderedSet in any DWORD
WF_ALL_SOF	Wait for any SOF OrderedSet in any DWORD
WF_EOFt_DW1	Wait for the EOFt OrderedSet in the first DWORD
WF_EOFt_DW2	Wait for the EOFt OrderedSet in the second DWORD
WF_EOFt	Wait for the EOFt OrderedSet in any DWORD
WF_EOFa_DW1	Wait for the EOFa OrderedSet in the first DWORD
WF_EOFa_DW2	Wait for the EOFa OrderedSet in the second DWORD
WF_EOFa	Wait for the EOFa OrderedSet in any DWORD
WF_EOFn_DW1	Wait for the EOFn OrderedSet in the first DWORD

TABLE 8.5: Wait & Wait_For Commands (Sheet 2 of 2)

Wait Command Name	Description
WF_EOFn_DW2	Wait for the EOFn OrderedSet in the second DWORD
WF_EOFn	Wait for the EOFn OrderedSet in any DWORD
WF_EOFni_DW1	Wait for the EOFni OrderedSet in the first DWORD
WF_EOFni_DW2	Wait for the EOFni OrderedSet in the second DWORD
WF_EOFni	Wait for the EOFni OrderedSet in any DWORD
WF_ALL_EOF	Wait for any EOF OrderedSet in any DWORD
WF_IDLE_DW1	Wait for the IDLE OrderedSet in the first DWORD
WF_IDLE_DW2	Wait for the IDLE OrderedSet in the second DWORD
WF_IDLE	Wait for the IDLE OrderedSet in any DWORD
WF_R_RDY_DW1	Wait for the R_RDY OrderedSet in the first DWORD
WF_R_RDY_DW2	Wait for the R_RDY OrderedSet in the second DWORD
WF_R_RDY	Wait for the R_RDY OrderedSet in any DWORD
WF_VC_RDY_DW1	Wait for the VC_RDY OrderedSet in the first DWORD
WF_VC_RDY_DW2	Wait for the VC_RDY OrderedSet in the second DWORD
WF_VC_RDY	Wait for the VC_RDY OrderedSet in any DWORD
WF_ER_RDY_DW1	Wait for the ER_RDY OrderedSet in the first DWORD
WF_ER_RDY_DW2	Wait for the ER_RDY OrderedSet in the second DWORD
WF_ER_RDY	Wait for the ER_RDY OrderedSet in any DWORD
WF_BB_SCs_DW1	Wait for the BB_SCs OrderedSet in the first DWORD
WF_BB_SCs_DW2	Wait for the BB_SCs OrderedSet in the second DWORD
WF_BB_SCs	Wait for the BB_SCs OrderedSet in any DWORD
WF_BB_SCr_DW1	Wait for the BB_SCr OrderedSet in the first DWORD
WF_BB_SCr_DW2	Wait for the BB_SCr OrderedSet in the second DWORD
WF_BB_SCr	Wait for the BB_SCr OrderedSet in any DWORD
WF_MRKtx_DW1	Wait for the MRKtx OrderedSet in the first DWORD
WF_MRKtx_DW2	Wait for the MRKtx OrderedSet in the second DWORD
WF_MRKtx	Wait for the MRKtx OrderedSet in any DWORD
WF_NOS_DW1	Wait for the NOS OrderedSet in the first DWORD
WF_NOS_DW2	Wait for the NOS OrderedSet in the second DWORD
WF_NOS	Wait for the NOS OrderedSet in any DWORD
WF_OLS_DW1	Wait for the OLS OrderedSet in the first DWORD
WF_OLS_DW2	Wait for the OLS OrderedSet in the second DWORD
WF_OLS	Wait for the OLS OrderedSet in any DWORD

8.7.8.8 WHEN / ELSEWHEN / ON_TIMEOUT Commands

The “on_timeout” command is related to the “wait-condition” command. The user can specify the statements that have to happen when the time (which is mentioned in the “wait-condition”) elapses (without any of the “when” statement taking place). Typical syntax would be:

```
wait (time)
{
```

```
        When {exp} do
        {
            #Some statements
        }
        elsewhen {exp} do
        {
            #Some statements
        }
        on_timeout
        {
            #Some statements, which would get executed when time-out happens
    (“time”)
        }
    }
```

8.7.8.9 WF_TIMEOUT Parameter

WF_TIMEOUT is a parameter within “wait_for” command. When the user specifies it in the “wait_for” command, the wait session will be released after the timeout has elapsed. Typical syntax would be as follows:

```
wait_for (time) { WF_R_RDY WF_TIMEOUT }
```

Note that “wait_for” command can be also defined without mentioning time-out as well. Following is an example for it:

```
wait_for {WF_OLS}
```

In this case, the Exerciser waits indefinitely for the WF_OLS parameter to become true. If the user doesn’t want to get blocked indefinitely, the WF_TIMEOUT parameter can be used.

8.7.8.10 Predefined Constants

Predefined Constant

- TRUE
- FALSE
- ON
- OFF
- INFINITE

TRUE or ON values are equal to 1 and FALSE or OFF values are equal to 0. INFINITE constant is only used in the infinite loop expressions.

```
Loop (INFINITE) { … }
```

8.7.8.11 Generation Settings

To change the default values of FC exerciser settings you can use SET command before and inside Generation block. If a setting value is updated outside Generation block multiple files (e.g. in different header files) the latest value would be used and applied only once to the Exerciser but inside Generation block, all the set commands would be applied, even if they are used back to back.

```
Set setting_name = setting_value
```

All the generation settings are applied before Generation block with their default values unless they are defined by the user or inside the "`Settings.inc`" in case it's included in the script.

The following settings are only valid before Generation block:

- GenerationMode
- AutoConnect
- AutoReconnect

TABLE 8.6: Generation Settings (Sheet 1 of 4)

Setting	Default Value	Description
GenerationMode	GEN_MODE_FC_INITIATOR	Generation Mode - must be defined or no generation will take place. Possible Values: • GEN_MODE_FC_INITIATOR • GEN_MODE_FC_TARGET
AutoMode Settings		
AutoConnect	OFF	When this bit is set, exerciser Engine automatically detects the maximum commonly supported speed and links up. Possible Values: ON / OFF
AutoReconnect	OFF	When this bit is set, exerciser automatically tries to reconnect whenever the link is dropped after the initial linkup without a connect command.
Fill Words		
AutoFillWordInsertion	OFF	When this bit is set, exerciser inserts fill words specified in IPG_count automatically after each frame. Possible Values: ON/OFF
IPG_count	6	When AutoFillWordInsertion is ON, This would be the number of fill Dword inserted after each frame.
FC 16G FEC Setting		
FC16G_FEC_Mode	NO_FEC	This command is only valid for 16G. When this bit is high, BASER_FEC mode is enabled. When zero no fec is enabled. Possible Values: • NO_FEC • BASER_FEC

TABLE 8.6: Generation Settings (Sheet 2 of 4)

Setting	Default Value	Description
Delimiter Settings		
ClassSupport	CLASS3_DATAGRAM	When auto mode is enabled, the exerciser automatically replaces the Delimiters with the required class. When a fixed class is selected, it supports Specified class only. Possible Values: • CLASS3_DATAGRAM • CLASS2_MULTIPLEX • CLASS_SUPPORT_AUTO
Link Speed Settings		
Speed	LINK_SPEED_16G	Default speed setting specified from board license minimum speed. Possible Values: • LINK_SPEED_16G • LINK_SPEED_32G • LINK_SPEED_64G
RX_Speed	LINK_SPEED_AUTO	Default Rx speed setting specified from board license minimum speed. Possible Values: • LINK_SPEED_16G • LINK_SPEED_32G • LINK_SPEED_64G • LINK_SPEED_AUTO
Wait Settings		
WaitTimeout	1000	Default timeout value (when not specified) in Wait_For and Wait commands. (in ms)
Speed Negotiation Settings		
FC16G_TTS_Disable	OFF	Disable training: When this bit is set, exerciser uses NOS/OLS/LIP commands to get the link up instead of training. Possible Values: ON / OFF
SFP_Type	SFP_TYPE_ELECTRICAL	Indicates the type of SFP used. Possible Values: • SFP_TYPE_ELECTRICAL • SFP_TYPE_OPTICAL

TABLE 8.6: Generation Settings (Sheet 3 of 4)

Setting	Default Value	Description
LSN_Speed_Supported	LSN_SUPPORTED_SPEED_16GB | LSN_SUPPORTED_SPEED_32GB | LSN_SUPPORTED_SPEED_64GB	Indicates which speeds are enabled during LSN. Default is supporting all the speed available in the license. Possible Values: • LSN_SUPPORTED_SPEED_16GB • LSN_SUPPORTED_SPEED_32GB • LSN_SUPPORTED_SPEED_64GB #or any mix of these values like: • LSN_SUPPORTED_SPEED_32GB • LSN_SUPPORTED_SPEED_64GB By default all the speeds are supported regarding the speed license and if user adds the support for a speed without having the required license, an error would be generated during execution.
TTS_Precoding_Req_FC64	OFF	Enable or disable precoding request. Possible Values: ON / OFF
TTS_PRESET_REQ_FC32	OFF	When this bit is set to high, preset bit of control field in training frame will be set to high. Possible Values: ON / OFF
TTS_INITIALIZE_REQ_FC32	OFF	When this bit set to high, initialize bit of control field in training frame will be set to high. Possible Values: ON / OFF
TTS_INITIAL_PRESET_REQ_FC64	TTS_INITIAL_PRESET_NO_REQ	Sets the preset bits of control field in PAM4 training frame. Possible Values: • TTS_INITIAL_PRESET_NO_REQ • TTS_INITIAL_PRESET_PRESET_1 • TTS_INITIAL_PRESET_PRESET_2 • TTS_INITIAL_PRESET_PRESET_3
FC Manual Speed Negotiation Counters		
PASS_SYNC_TEST_COUNT_64B_66B	1000	Pass sync_test decision blocks requires that 64B/66B Word Synchronization be maintained for a monitoring period that shall equal or exceed receiving the pass sync_test count.
PASS_SYNC_TEST_COUNT_TTS	300	Pass sync_test decision blocks requires that Transmission Training signal Synchronization be maintained for a monitoring period that shall equal or exceed receiving the pass sync_test count.

TABLE 8.6: Generation Settings (Sheet 4 of 4)

Setting	Default Value	Description
FC Manual Speed Negotiation Timers		
LSN_TX_CYCLE_TIMER_ms	154	Transmission time of a particular speed in the Wait_for_signal, Negotiate_master stages during LSN.
LSN_FAIL_TIMER_ms	1620	Watchdog timer threshold (ms) Time allowed for the algorithm to continue without passing the Pass sync_test at any supported speed.
LSN_END_WAIT_TIMER_us	2048	This timer is started after LSN sequence completion. The link sends additional TTS frames until this timer expires to ensure that the remote link partner receives a sufficient number of training frames to detect the link state.
LSN_END_TRAINING_START_TIMER_us	2000	This timer is started after LSN sequence completion. The link starts switching its Host Electrical Transceiver to transmit the TTS frames for 64GFC transmitter training after meeting the requirements specified in lsn_end_wait_timer and must complete this switch before lsn_end_training_start_timer expires.
MAX_WAIT_TIMER_ms	1500	A timer that limits the duration of active training. This timer sets the limit on how long transmitter training is allowed to operate to find the optimal transmit coefficients and receiver adaptive equalization values for reliable link operation.
LINKUP_WATCHDOG_TIMER_ms	10000	This timer is started upon LSN sequence completion. This timer sets the maximum amount of time from LSN complete to transmitter training complete.
LINK_WAIT_TIMER_us	32	A timer that limits the duration in which the transmitter will transmit the Transmitter Training Signal at fixed settings after the remote FC_Port indicates training complete to ensure that remote FC_Port correctly detects the local interface state.
LINK_TEST_TIMER_ms	45	A timer that determines the delay in the LINK_TEST state before sampling of the link quality
RECEIVER_TRANSMITTER_TIMEOUT_ms	100	Used by the receiver logic to detect Loss-of-Synchronization

8.7.9 Interrupts

Interrupt routines are blocks of script (like procedures with no parameters) that run simultaneously with the main script and are triggered (called) automatically. When any of those predefined events inside the Interrupt option happen, the corresponding Interrupt routines are called by the Script Engine and run simultaneously with the main script.

Interrupt routines should be relatively small in size and short in duration in to avoid disruptions in running the main script. Therefore, the number of instructions is limited and only a few commands are supported inside Interrupts. Because of the way the Interrupts are executed and to avoid memory corrupts, Global variable updates are not allowed. They can, however, be used inside Interrupts, but care must be taken as their value may change inside the Generation block during the execution of the Interrupt routine.

8.7.9.1 Interrupt Events

Three different types of events are supported for Interrupts. All of these resources can be used for any Interrupt routine. If more than one event type is used for an Interrupt, it will be called when either of those events occur.

- **Frame Events**: Frame events can be used to trigger an Interrupt routine when a Frame pattern is received (similar to Frame event in GenOptions).
- **Symbol**: Symbol events can be used to trigger an Interrupt routine when a special Symbol is received (similar to Symbol event in GenOptions).
- **Orderedset Mask**: Orderedset Mask events can be used to trigger an Interrupt routine when any ordered set in the selected list on the specified DWORD is received.

Interrupt Syntax

Any of the Interrupt routines can be defined after (or before) Generation block in any order.

```
Generation {
      # Generation Block here
}

Interrupt_A {
# Interrupt Routine A can be defined here
}

Interrupt_B {
# Interrupt Routine B can be defined here
}

Interrupt_C {
# Interrupt Routine C can be defined here
}

Interrupt_D {
# Interrupt Routine D can be defined here
}
```

8.7.9.2 Valid Commands Inside Interrupts

Send Commands

- SendData (Including Send and SendCRC commands)
- Send Symbol
- Frame
- SendFrame
- LRF statements

- Local Variable Definition/Assignment
- Local Variable Operations
- Global Variable Operations (Read-Only)
- Following Functions:
  - InjectSyncHeaderError
  - InjectRSFECError
  - ReverseByteOrder
  - Exit
- If-Else expressions

8.7.9.3 Interrupts Known Limitations

Limited Commands:

Only the specified commands in *8.7.9.2, Valid Commands Inside Interrupts* are allowed to be used inside Interrupts. Interrupt routines should also be as minimal as possible, with no complex logic, to avoid interference with the main script logic.

Using Variables:

Each Interrupt has its own resources for temporary and local variables and they cannot be shared between different Interrupts or Generation block.

To avoid memory corrupts, Global variable updates are not allowed, but they can be used inside Interrupts. However, this not encouraged as their value might change anytime inside the Generation block during the execution of the Interrupt routine; thus making its behavior unpredictable.

Limited number of resources:

The Block size and temporary variable resources are much more limited for Interrupts compared to generation script. Using large blocks or complex logic is discouraged as it may interfere with the execution of Generation block.

Send/Receive Buffer:

The send buffer, if prioritized based on the Interrupt ID (from A to D), and Generation block have the lowest priority for sending data on the line.

Receive buffer is accessible to Interrupts and Generation block simultaneously (when using LRF expressions).

8.7.10 Fabric Login

As of release 6.10, all Initiator example scripts have been updated to use “wait timeout” into a centralized include file “LoginUtility.inc”, which handles most FC P2P/Fabric login processes on both SCSI and NVMe.

Users can add this line to their script to start (or refer it for their own setup):

```
%include "Generation\Include\LoginUtility.inc"
```

For NVMe, users will still need to update NVMe_Subsystem_Target manually in the file LoginUtility.inc

8.7.11 IO Write/Read Function

For the IO Write/Read Function, you must create a script for the first LOGIN process. When the command is used, the Bus Engine starts a Write/Read process using the defined settings.

To start a Write/Read process, define the following parameters:

- **IO_AutoCredit**—This gets following values:
  - **ON**: The BE sends one R_RDY as soon as it receives a SOF.
  - **OFF**: The user must define an interrupt to handle credit.
- **IO_ThreadCount**—This is the number of threads to be enabled in the BE. It gets values from 1 to 8 (default is 4).
- **IO_ReadWriteType**—This can get following values:
  - **RW_100_READ** – Logic sends only READ commands.
  - **RW_100_WRITE** – BE sends only Write commands.
  - **RW_10_WRITE_90_READ** – BE sends 10% Write commands and 90% READ commands.
  - **RW_25_WRITE_75_READ** – BE sends 25% Write commands and 75% READ commands.
  - **RW_50_WRITE_50_READ** – BE sends 50% Write commands and 50% READ commands.
  - **RW_75_WRITE_25_READ** – BE sends 75% Write commands and 25% READ commands.
  - **RW_90_WRITE_10_READ** – BE sends 90% Write commands and 10% READ commands.

Once you have defined the above parameters, the IO_Write Function is ready to run.

The prototype is as follows:

IO_Write(initial value, Send Type, Transfer Length, Max Payload size)

- **Initial Value**—This is a 64-bit initial value (initial seed) for the payload type.
- **Send Type**—Defines the type of payload to be send. The following values can be set:
  - SEND_FIXED
  - SEND_INCREMENTAL
  - SEND_PRBS11
- **Transfer Length**—Defines the length of the data transfer for each command. The following values can be set:
  - IO_SIZE_256KB
  - IO_SIZE_32KB
  - IO_SIZE_4KB

- IO_SIZE_512B

- **Maximum Payload Size**—Defines the maximum allowed payload size in bytes.

8.7.11.1 Exerciser as Initiator

This section contains some examples for getting maximum data throughput and maximum IOPS when Exerciser acts as an Initiator.

Maximum Data Throughput

For getting maximum data throughput, maximum payload size must be set to 2112. The maximum possible transfer length, which is 256KB, must also be used.

The following examples illustrate **Maximum Data Throughput** for **Write** and **Read** commands:

INPUT: Maximum Data—Write

Set IO_AutoCredit = ON
Set IO_ThreadCount = 8
Set IO_ReadWriteType = RW_100_WRITE
IO_Write(0x1, SEND_INCREMENTAL, IO_SIZE_512B)

RESULTS: Maximum Data—Write

I/O Performance	
Reads per second	0 IOPS
Writes per second	11882 IOPS
Total I/Os per second	11882 IOPS
Read Rate	0.00 MB/s (0%)
Write Rate	2970.51 MB/s (93%)
Total Throughput	2970.51 MB/s (46%)

INPUT: Maximum Data Throughput—Read

Set IO_AutoCredit = ON
Set IO_ThreadCount = 8
Set IO_ReadWriteType = RW_100_READ
IO_Write(0x1, SEND_INCREMENTAL, IO_SIZE_256KB, 2112)

RESULTS: Maximum Data Throughput—Read

I/O Performance	
Reads per second	12573 IOPS
Writes per second	0 IOPS
Total I/Os per second	12573 IOPS
Read Rate	3143.44 MB/s (98%)
Write Rate	2970.51 MB/s (0%)
Total Throughput	3143.44 MB/s (49%)

Maximum IOPS

For getting maximum IOPS, the minimum possible transfer length, which it is 512B, must be used. Below is an example of maximum IOPS for write and read commands.

The following examples illustrate **Maximum IOPS** for **Write** and **Read** commands:

INPUT: Maximum IOPS—Write

```
Set IO_AutoCredit     =  ON
Set IO_ThreadCount    =  8
Set IO_ReadWriteType  =  RW_100_WRITE
IO_Write(0x1, SEND_INCREMENTAL, IO_SIZE_512B)
```

RESULTS: Maximum IOPS—Write

I/O Performance	
Reads per second	0 IOPS
Writes per second	102941 IOPS
Total I/Os per second	102941 IOPS
Read Rate	0.00 MB/s (0%)
Write Rate	50.26 MB/s (2%)
Total Throughput	50.26 MB/s (1%)

INPUT: Maximum IOPS—Read

```
Set IO_AutoCredit     =  ON
Set IO_ThreadCount    =  8
Set IO_ReadWriteType  =  RW_100_READ
IO_Write(0x1, SEND_INCREMENTAL, IO_SIZE_512B)
```

RESULTS: Maximum IOPS—Read

I/O Performance	
Reads per second	575240 IOPS
Writes per second	0 IOPS
Total I/Os per second	575240 IOPS
Read Rate	280.97 MB/s (9%)
Write Rate	0.00 MB/s (0%)
Total Throughput	280.97 MB/s (4%)

8.7.11.2 Exerciser as Target

When the Exerciser acts as the Target, the following settings must be entered prior to running the first test:

- IO_AutoCredit
- IO_ThreadCount
- Maximum Payload size

Once the script has run, with SANBlaze as the initiator, the above settings are only entered once per session. Therefore, each time a new test scenario is run in SANBlaze and when that test is completed, a new test can be performed without rerunning the script.

Below are some examples for getting maximum data throughput and maximum IOPS when the Exerciser acts as the Target. For all of these example tests, the script is same as following and it needs to be run once at beginning.

- set IO_AutoCredit = ON
- Set IO_ThreadCount = 8
- IO_Write(0x1, SEND_INCREMENTAL, IO_SIZE_256KB, 2112)

8.8 Frame Decoding

This section describes the use of internal decoding for sending packets and getting fields from LRF.

8.8.1 SendFrame

You can define a SendFrame and send it without defining its Frame template. It uses internal decoding for sending packets.

To invoke SendFrame, do one of the following:

- Drag the **SendFrame Keyword** to open the pop-up menu, then click **Insert Frame**.

  OR

- Drag and drop **SendFrame** from code snippets, then click **Insert Frame**.

Once **Insert Frame** is selected, the following code is added to the script:

```
RawFrame "Frame_Name"
{
      LinkData = "Raw Data String"
      #Field[start:end] = field value #Field Name1 = Field1 value/option
      value
      #Field[start:end] #Field Name2 = Field2 value/option value
      #SendCRC
      Prolog = SOFi3 #(any SOF)
      Epilog = EOFn #(any EOF)
}
```

- **SendFrame**—This Keyword is used to identify the packet Decoding.
- **Frame_Name**—Shows the protocol stack and frame name, which is needed for the inserted Packet to decode. For example, for FCP Data Frame, it will be “FCP Frame Information Unit(Data)-FCP_DATA”.

NOTE: You must not change this value; otherwise, it will not produce the expected result.

- **LinkData**—Frame raw data.

NOTE: You must not change this value; otherwise, it will not produce the expected result.

- **Fields**—All fields that have been changed in the frame are shown with their value/ Option, but they are commented. If you to assign new values by a constant or a variable, you must update each individual field with the following format:

  `Field[Start:End] = field value` (while Field value can be a constant or a variable)

- **Send** – Use this to Send a pattern (Fixed/Incremental or PRBS11) after the LinkData and before CRC. The format is the same as the Send command inside SendData Block and has the same format:

```
Send(@var64_name, SEND_INCREMENTAL, repeat_count)
```

NOTE: When using this command inside the SendFrame, an idle is inserted before the Prolog to avoid padding LinkData with trailing zeros (before the pattern) when it is QWORD aligned.

- **SendCRC**—If **Recalculate CRC** is checked, SendCRC will be sent.
- **Prolog**—You can assign any predefined orderedset.
- **Epilog**—You can assign any predefined orderedset.

This an example related to FCP Data frame:

```
SendFrame "FCP Frame Information Unit(Data)-FCP_DATA"
{
    LinkData =
"010000000000001F080000000000000000000000000000000000000000000000"
    #Field[0:7] = 0x01 # Routing Control = 0x01: Solic. Data
    #Field[40:63] = 0x00001F # Source Identifier = 0x00001F
    #Field[64:71] = 0x08 # Data Structure type = 0x08: SCSI-FCP
    SendCRC
    Prolog = SOFi2
    Epilog = EOFa
}
```

8.8.2 LRF Fields

You can select a LRF field visually using built-in decode.

1. To select a field, drag the **LRF** to the script body in the middle pane. This opens the dialog window (Figure 8.50).

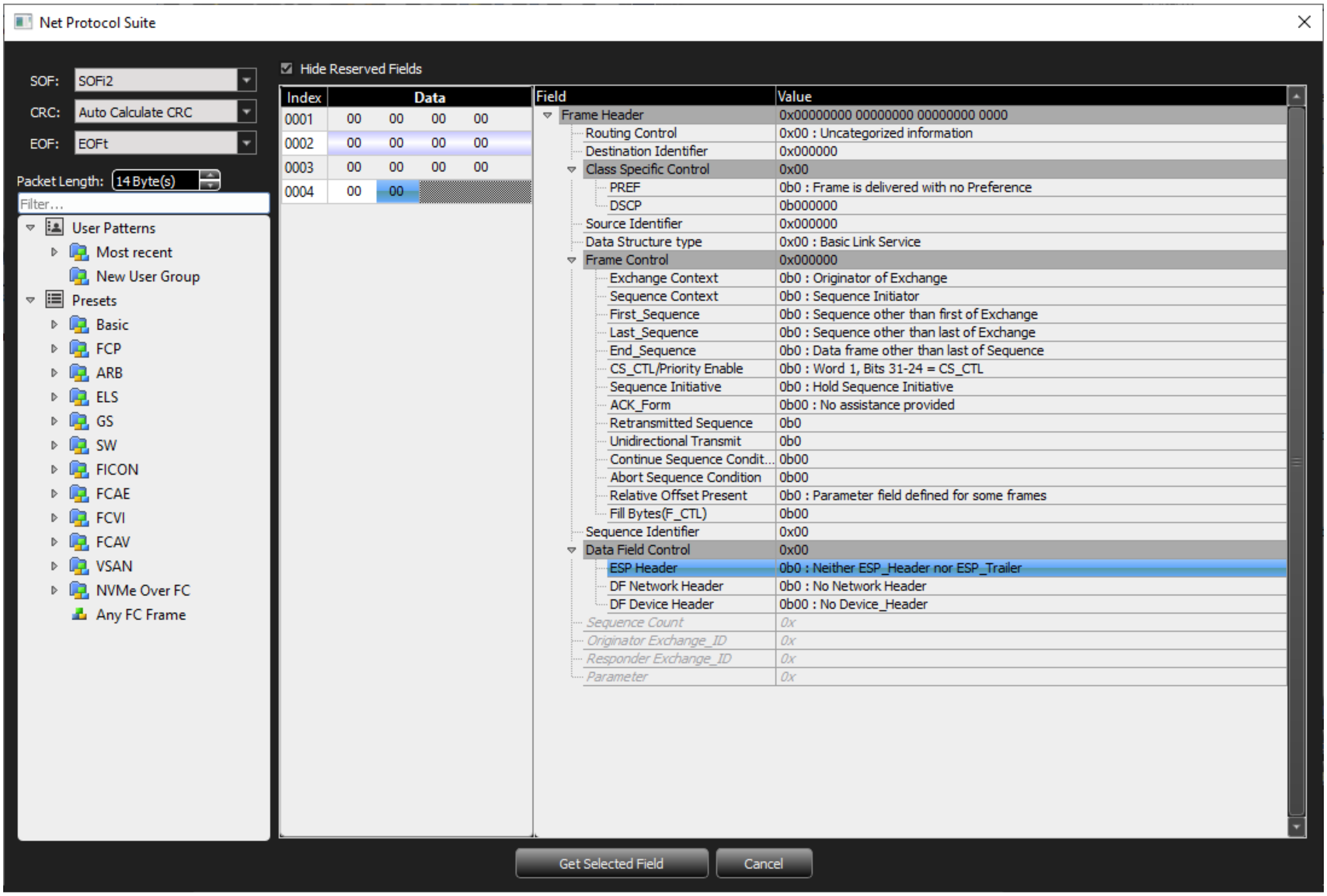


Figure 8.50: LRF Field Dialog Window

2. Select any field to get the value from LRF. When you choose the **Get Selected** field, the following is added to the LRF position:

```
LRF[Start bit offset: End bit offset] #Field Name (Commented)
```

Therefore, for the above example it will be:

```
@OpCode= LRF[40:48] # Operation Code
```

NOTE: LRF needs a left side variable to be assigned, otherwise it will generate compile error.

Hint: To find the start bit and end bit of a field, you can use LRF or SendFrame dialogues by typing them into the script (anywhere); then right-click and choose the **insert frame** option for the *SendFrame* keyword, or **GetField** for the *LRF* keyword; then choose the intended field or update its value with a none-zero value (e.g., with FFFFFF).

8.8.2.1 Rearrange Byte Order

When a Word value is received from LRF that you wish to use, the byte order is reversed; therefore, it must be rotated manually. Because the Word value cannot be used directly in the defined `frame_template`, it needs to be swapped.

Two other functions also can be used to reverse byte order of identifiers. ReverseByteOrder32 can be used for 32-bit values and ReverseByteOrder64 for 64-bit values.

Reverse Byte Order

To get the value from the Last Received Frame in a reversed byte order, `LRF_BYTE_REV` can be used:

```
LRF_BYTE_REV[Start bit offset: End bit offset] #Field Name (Commented)
```

NOTE: `LRF_BYTE_REV` can only be used when the field size (`end_bit_offset - start_bit_offset + 1`) is dividable by 8 (8, 16, 24 or 32 for 32-bit variables).

Reversing byte order can also be performed later using the `ReverseByteOrder` command as shown in the following example:

```
Var32 @OrEx_id = LRF[128:143]# Originator Exchange_ID
ReverseByteOrder(@Rx_id, 16)
```

In the `ReverseByteOrder` function, the first parameter is the variable needed to reverse the bytes, and the second parameter is the size of data inside variable in bits (16 bits here). If the size is 32 bits, a second parameter is not needed:

```
Var32 @OrEx_id = LRF[128:143]# Originator Exchange_ID
ReverseByteOrder(@Rx_id)
```

So, the following expressions are the same:

1
```
@OrEx_id = LRF[128:143] << 16# Originator Exchange_ID
ReverseByteOrder(@OrEx_id)
@rx_OrEx_id = LRF[144:159] << 16 # Responder Exchange_ID
ReverseByteOrder(@rx_OrEx_id
```

2
```
@OrEx_id = LRF_BYTE_REV[128:143]# Originator Exchange_ID
@rx_OrEx_id = LRF_BYTE_REV[144:159] # Responder Exchange_ID
```

3
```
@OrEx_id = LRF[128:143]# Originator Exchange_ID
ReverseByteOrder(@OrEx_id, 16) # = 32 - length
@rx_OrEx_id = LRF[144:159] # Responder Exchange_ID
ReverseByteOrder(@rx_OrEx_id, 16)
```

ReverseByteOrder32

Call this function to reverse the byte order of a 32-bit identifier.

```
param32 = 0x11223344
```

`call ReverseByteOrder32(param32) # param` would be `0x44332211` after this call.

ReverseByteOrder64

Call this function to reverse the byte order of a 64-bit identifier.

```
param64 = 0x1122334455667788
```

`call ReverseByteOrder64(param64) # param` would be `0x8877665544332211` after this call.

NOTE:
- Constants cannot be used in `ReverseByteOrder32` and `ReverseByteOrder64` functions.
- The "generation/include/utilities.inc" file needs to be included to use `ReverseByteOrder32` and `ReverseByteOrder64` functions:

  %include "generation/include/utilities.inc"

8.8.3 Copy/Paste Frame

FC Exerciser script supports copy-paste frame feature by copying a frame from trace view and right-click anywhere in the script and choose the "Paste Frame" option to add a SendFrame snippet based on the values of the copied frame.

This feature can make filling required values for a specific frame much easier as user can copy a similar frame from a trace and paste it inside the script and only update the required values.

8.9 Known limitations

8.9.1 Points to be Noted

1. Due to symbol rearrangement, there might be some extra fills words inserted in the traffic in some cases.
2. When exerciser is waiting to receive or doing some variable, Arithmetic operations, fill words are put on the line.
3. When no frames or primitives are transmitted fill words are put on the line as per spec.

8.9.2 Limitations

1. Generation memory is limited to 16k memory blocks.
2. Back to back wait statement might miss the valid event if the gap between two successive event points are very minimal.
3. Loops, Jumps, If, else, while, when statements, variable operations will insert idles on the line during execution.

Chapter 9

Ethernet Exerciser

The SierraNet Ethernet Exerciser is a traffic generator that enables engineers to test designs under realistic conditions and to transmit known errors, thus allowing observation of how devices handle faulty link conditions.

The Ethernet Exerciser supports two modes of operation:

- Easy Mode is GUI driven, and facilitates creating upper layer scripts in a quick and easy way. This is described in “Port Settings - Easy Mode” on page 595.
- Script Mode allows much more control over all layers, but requires spelling out the desired Exerciser behavior in detailed scripts. This is described in “Port Settings - Script Mode” on page 602.

9.1 Hardware Setup for Generating Traffic

Connect the Ethernet cable from the Digital re-timed port (P1, P2, P5 or P6) of the Sierra Net Analyzer to an available port on the device under test.

9.2 Software Setup for Traffic Generation

To start the Exerciser and set it up, do the following:

1. Launch the Net Protocol Suite software (Figure 9.1).

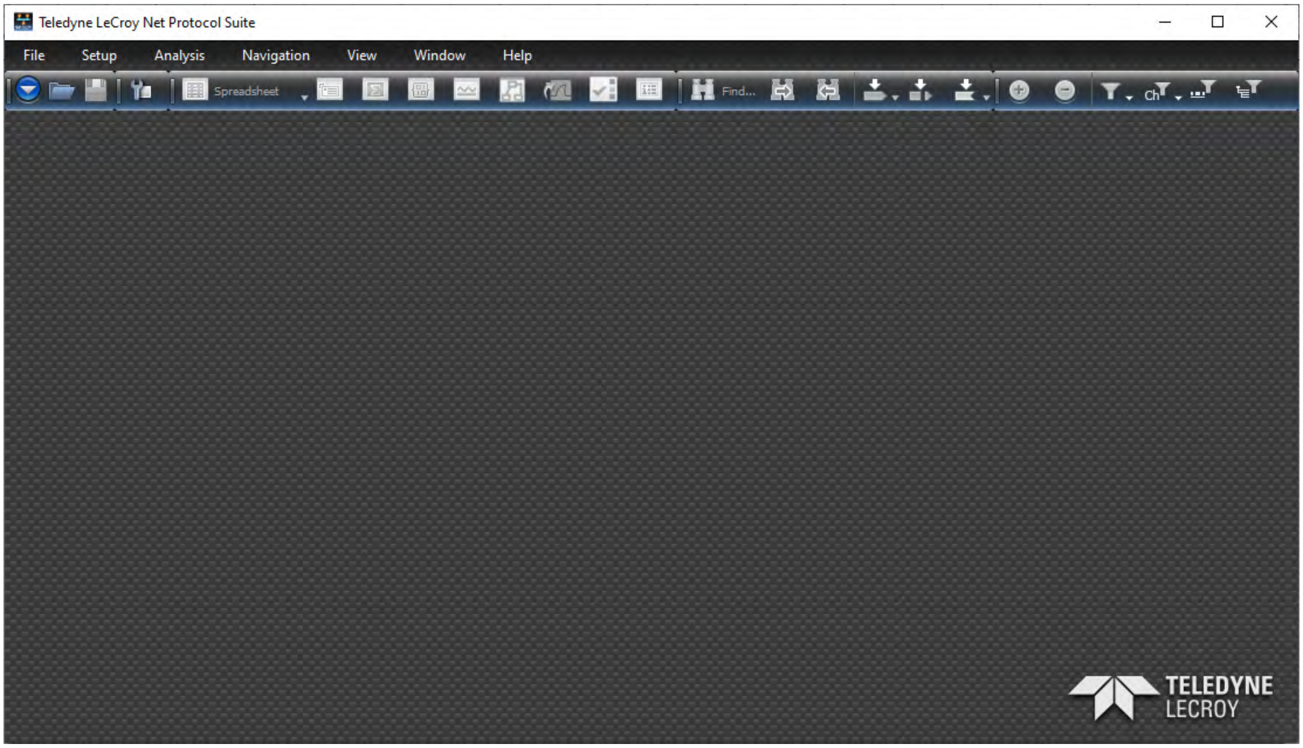


Figure 9.1: Net Protocol Suite Main Screen

2. Select **File** → **New Project**. The Add Device to Project dialog appears with the list of devices and available ports for the selected device (Figure 9.2).

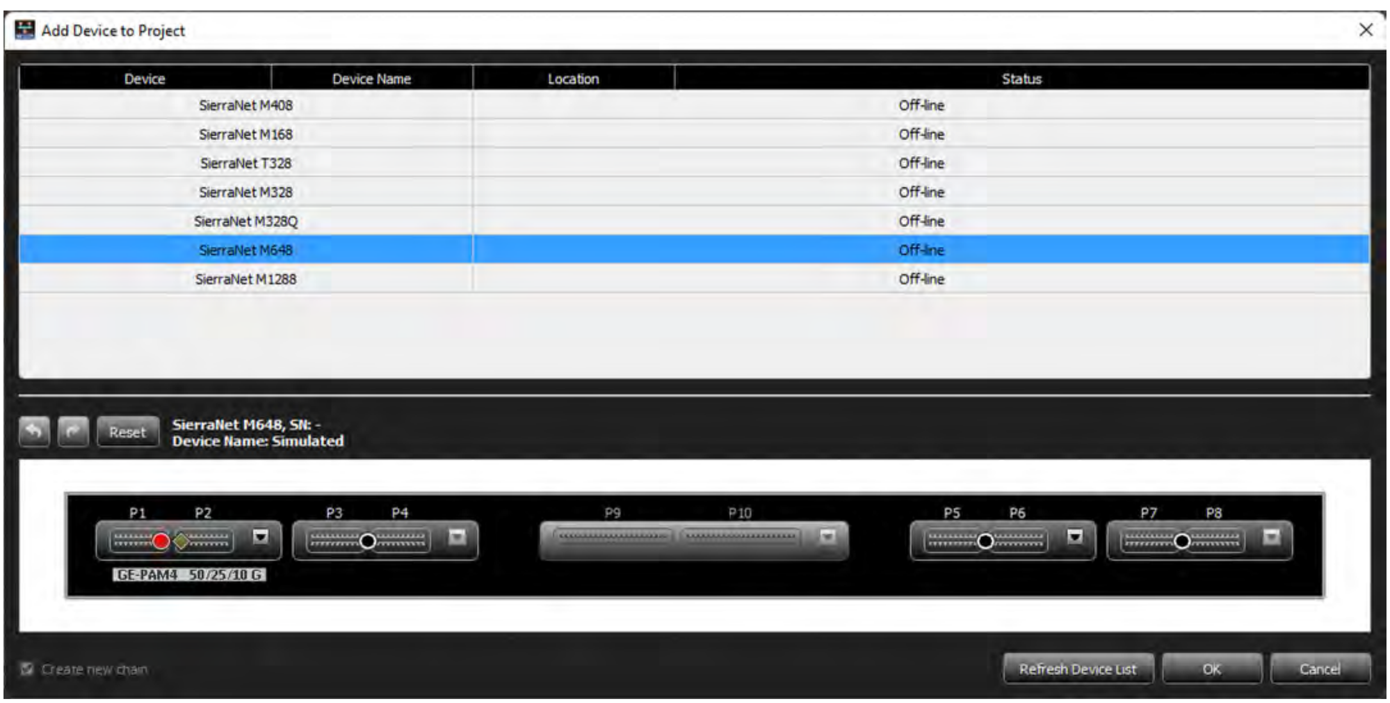


Figure 9.2: Add Device to Project

3. From the *Add Device to Project* window, click once on the device to highlight it.

NOTE: If the device you want to use is not on the list, click the Refresh Device List button to refresh the list at any time. A progress bar displays and, once the system finds all devices, the list updates. See Figure 9.3.

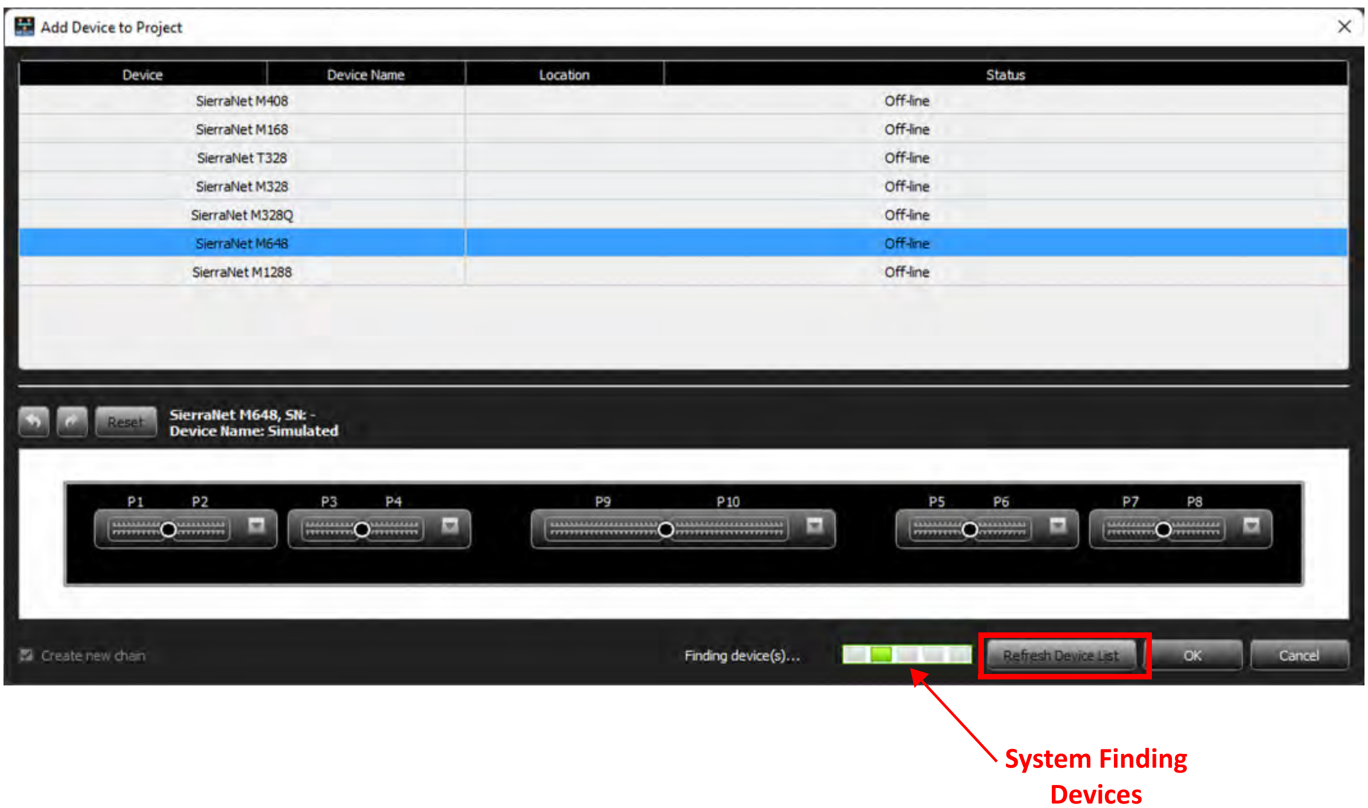


Figure 9.3: Refresh Device List

4. To configure a port pair (shown with SierraNet M648 selected), do the following:

   a. If needed, click Reset to reset the port configuration settings. This shows all available port configurations and speeds for the selected device.

   b. Click the down arrow for P5/P6 (as shown in the example) to open the drop-down menu (Figure 9.4).

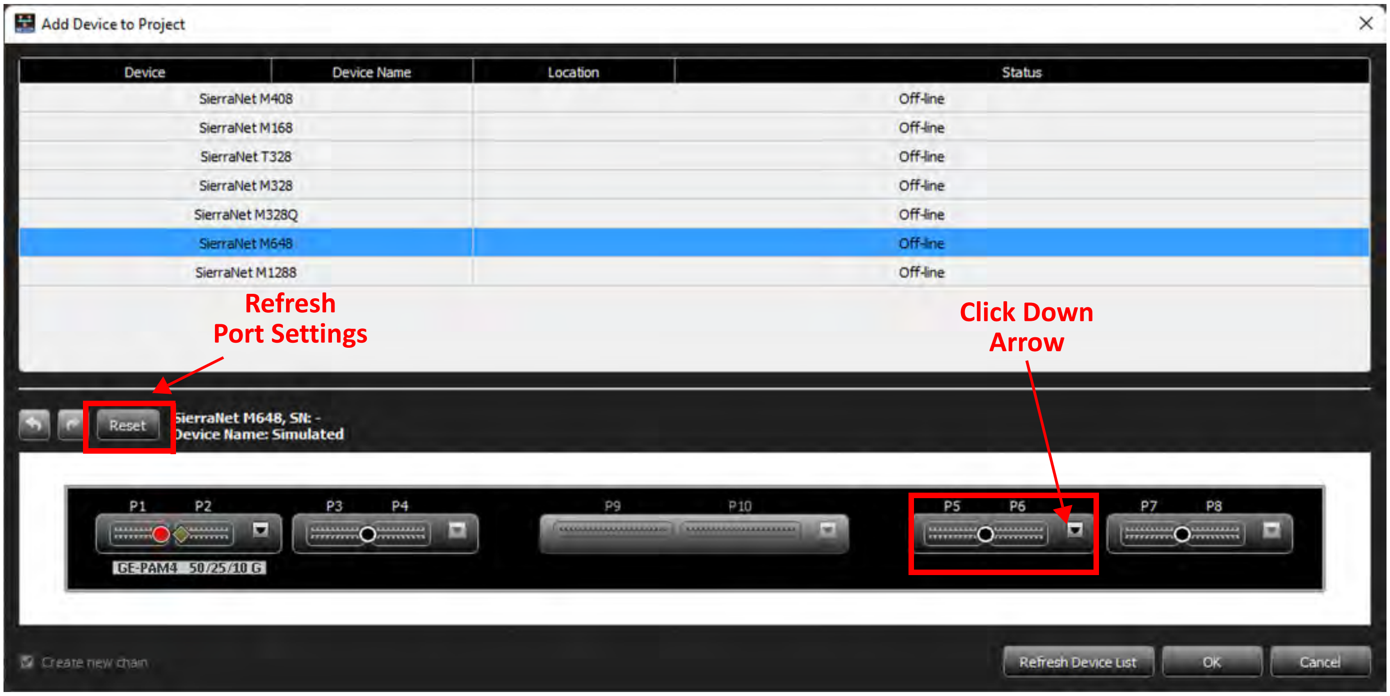


Figure 9.4: M648 Port Pairs

c. From the drop down menu (Figure 9.5), click the radio buttons for an **Analyzer – Exerciser** on the desired port.

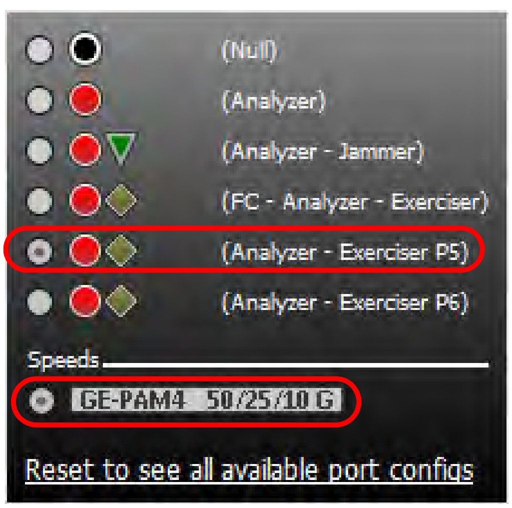


Figure 9.5: M648 Port Pair Drop-Down Menu

d. Select the **Speed**.

e. Once all options are selected in the port pair drop-down menu, the menu closes.

f. Click **OK** in the *Add Device to Project* dialog to save your selections.

The Main Screen (Figure 9.6) now shows the configured ports as ready to be started.

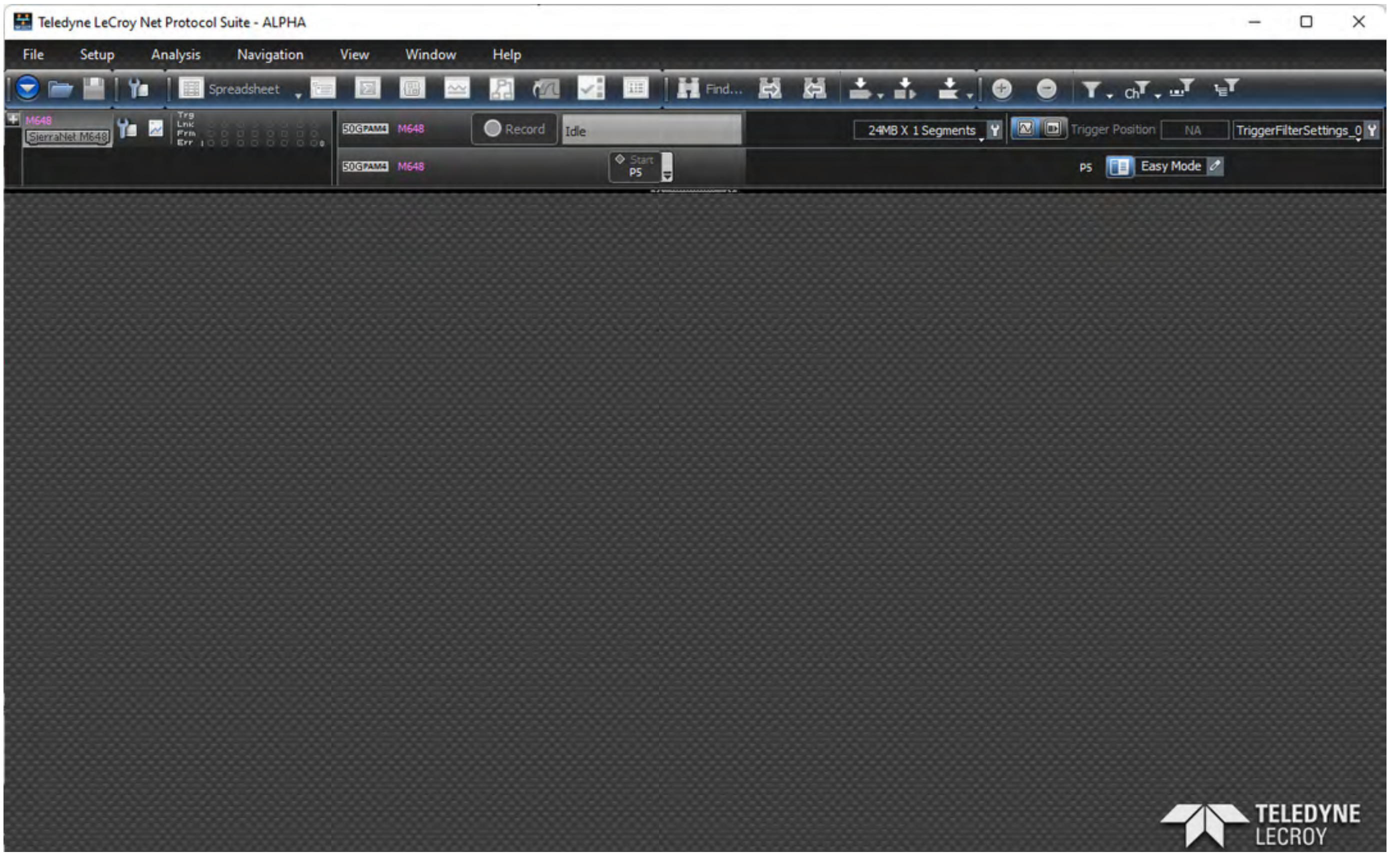


Figure 9.6: Main Screen with Port P5

9.3 Port Settings

To define the Port Activation Settings, click the down arrow for the **Start/Stop Session** button for the desired port then click the wrench icon. The Port Activation Settings dialog box displays (Figure 9.7 and Figure 9.8).

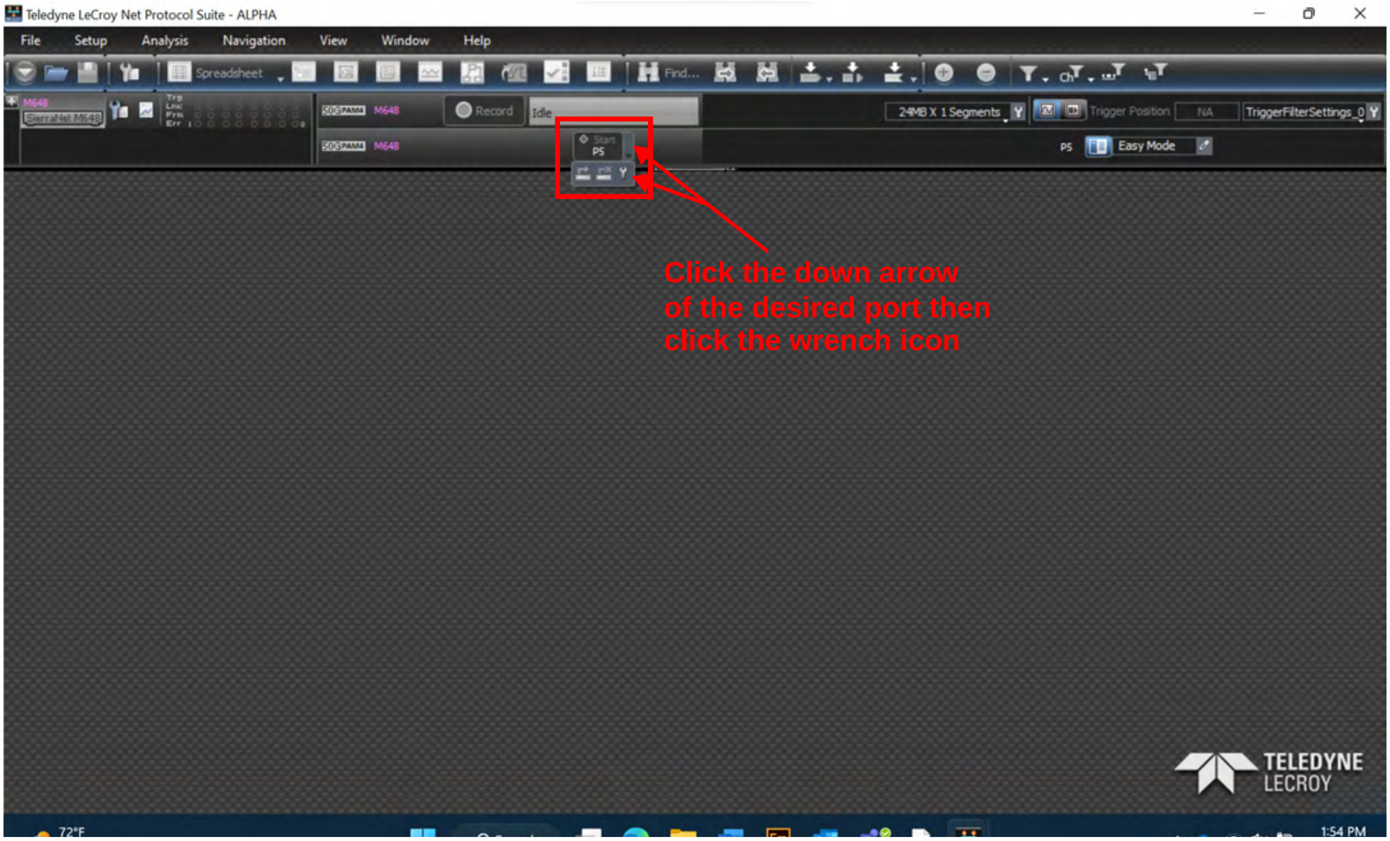


Figure 9.7: Example Main Screen with P5 Active for M648

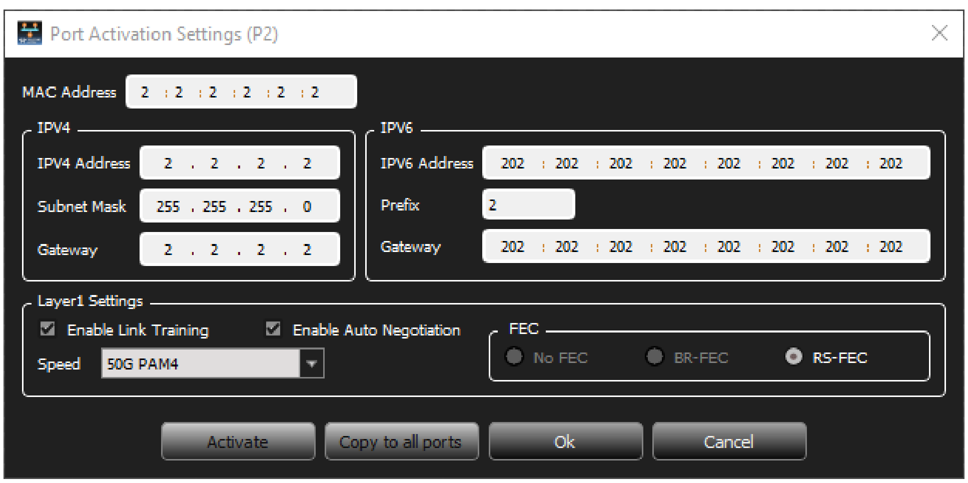


Figure 9.8: Port Activation Settings Dialog Box

1. Fill out all addresses.
2. Set the desired traffic generation speed.
3. Enter Layer1 settings.
4. When finished, click **Ok**.

9.4 Port Settings - Easy Mode

To access the Easy Mode Port Settings, Click the pencil on the Easy Mode/ Script Mode icon (located to the right of the M648 ports). The *Easy Mode Port Settings* screen appears (Figure 9.9).

NOTE: If the icon says "New Script" instead of "Easy Mode", then click to switch to "Easy Mode."

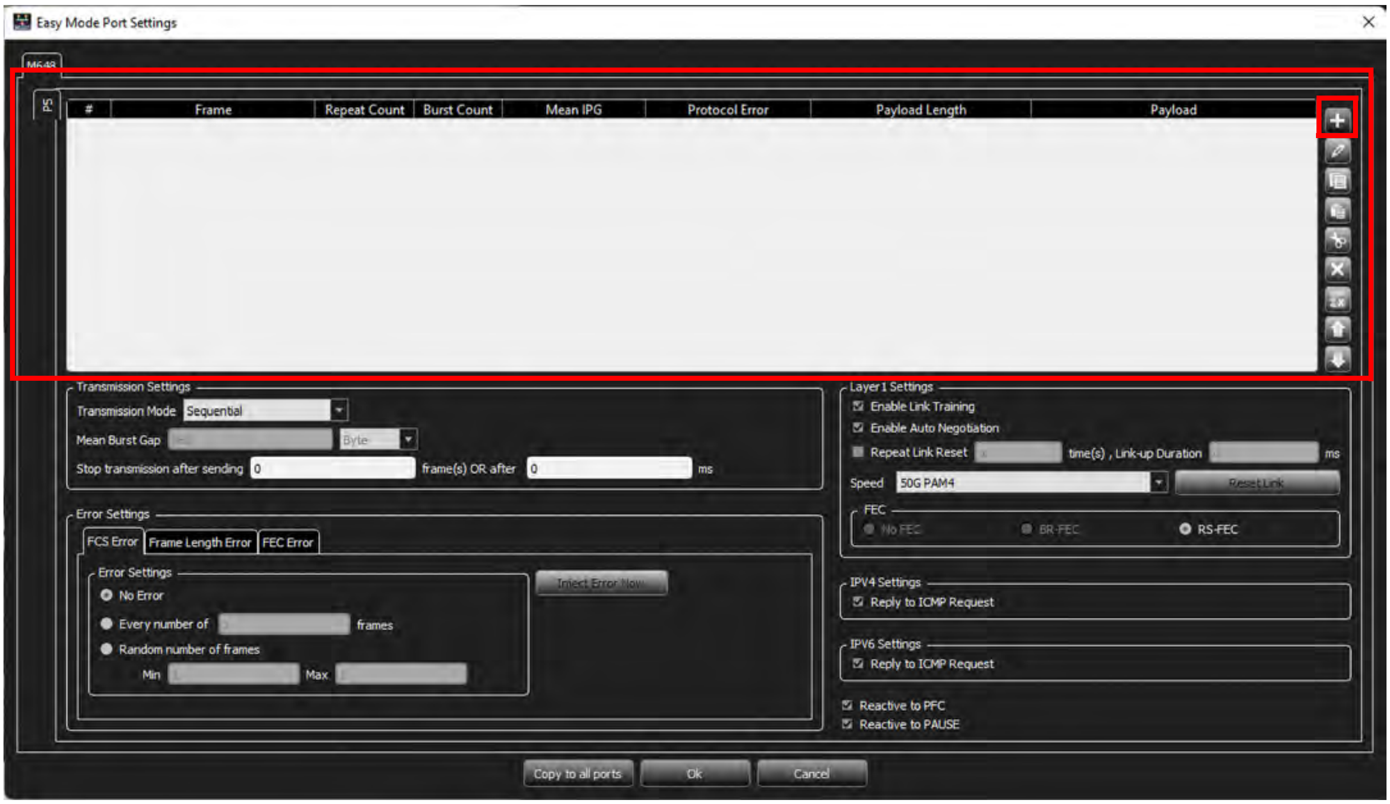


Figure 9.9: Easy Mode Port Settings Screen

1. Define the Frame(s) to be sent:

   a. Click the on the right.

   b. Expand the Preset or Pattern to display the desired frames (Figure 9.10).

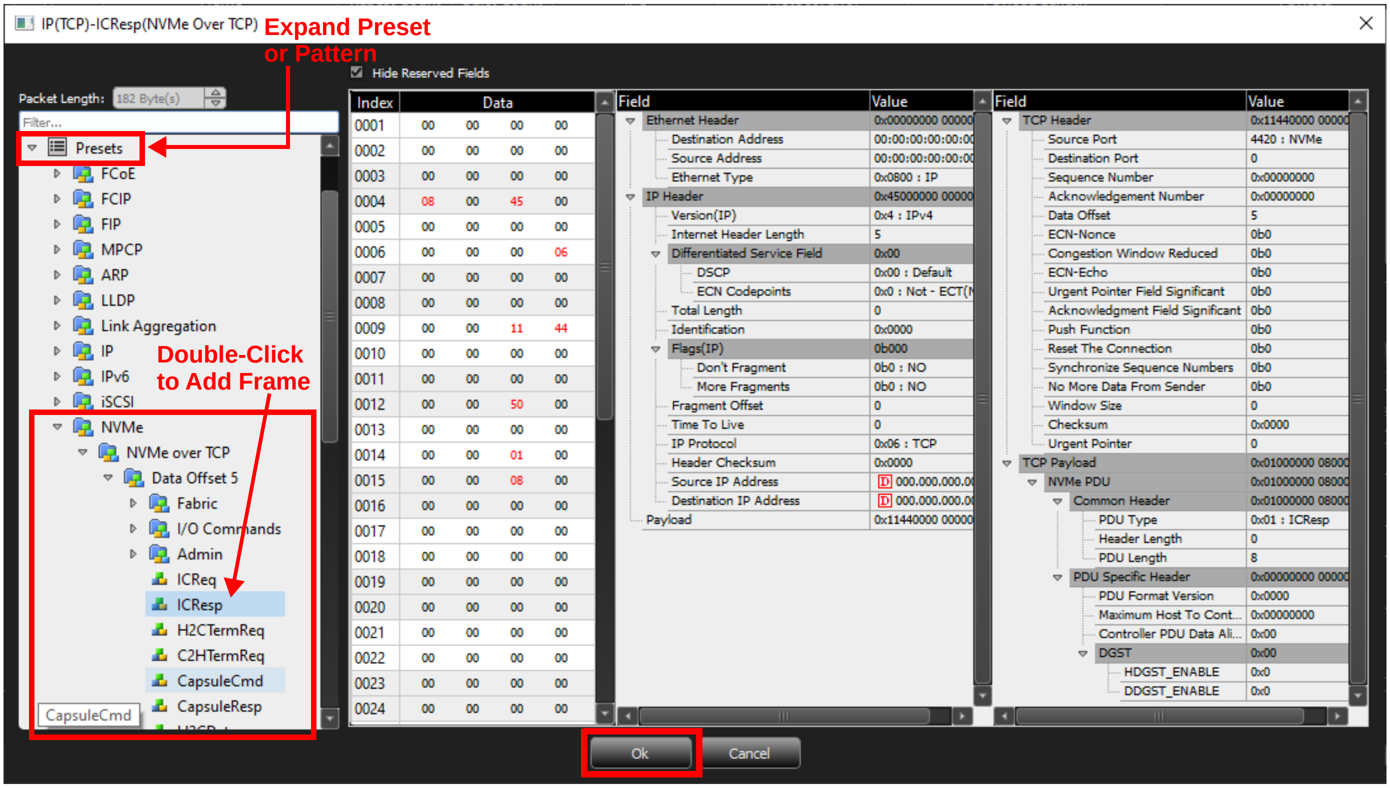


Figure 9.10: Add Frame

c. Double-click on the frame you want.

d. When you are finished adding frames, click **Ok**. The added frame(s) appears in the Frame Display Area (Figure 9.11).

NOTE: The Length field gets calculated and updated automatically.

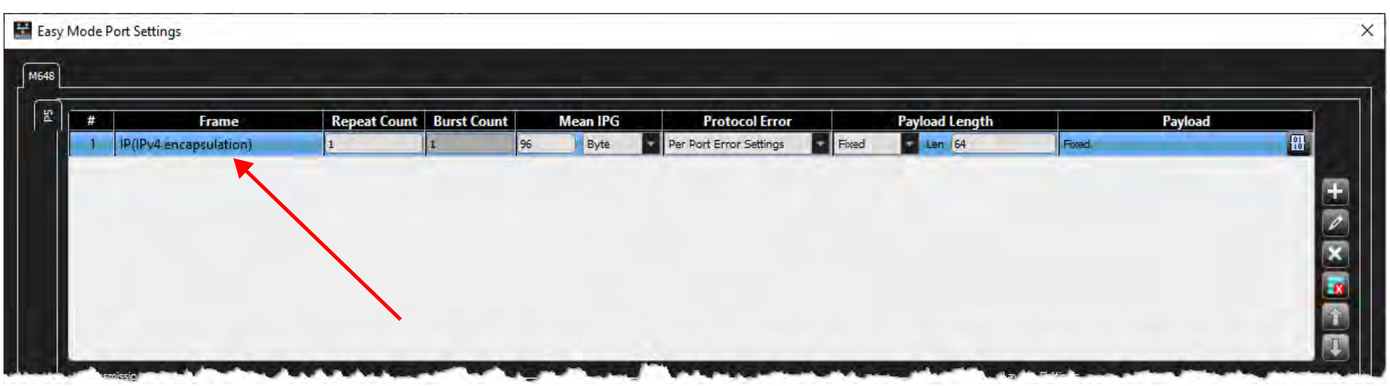


Figure 9.11: Frame Added to Port Settings

9.4.1 Frame Display Area

TABLE 9.1: Easy Mode Window – Frame Display Area (Sheet 1 of 2)

Setting/Control	Description
Frame number	Counts the number of frames from 1 through total
Frame	Name of selected frame
Repeat Count	Number of times to repeat each frame
Burst Count	Number of bursts for the Repeat Count. This field is only active in Burst-Interleave Transmission Mode. **NOTE:** Repeat Count must be a Multiple of the Burst Count.
Mean IPG	Interpacket Gap—You can set the IPG in bytes or nanoseconds. **NOTE:** The minimal IPG is speed-dependent and automatically set by the software.
Protocol Error	You can inject errors from the drop-down menu. The default is Per Port Error Settings, as defined in the bottom pane of the dialog.
Payload Length	Length of data to be included in the frame: • Fixed • Random – Enter range from minimum to maximum) • Incremental – Min, Max, and Step
	NOTE: The payload length field gets calculated and updated automatically. The payload length is only incremented for frames that are repeated when the Repeat Counter is used. The payload length is limited to 1999 bytes.
Payload	Define the Payload: Select the Pattern Type, then select the Payload Pattern Size and specify the Payload Pattern that will be repeated up to the Payload Length. • Fixed – Always sends the same thing. • Incremental – Increments the Payload Pattern by the Step. • Random – Creates a random pattern the size of Payload Length.
Custom	Define exactly what you want the pattern to be, or you can import a file.

TABLE 9.1: Easy Mode Window – Frame Display Area (Sheet 2 of 2)

Setting/Control	Description
Controls	
	Add frames
	Edit the selected frame
	Delete selection
	Removes all frames
	Move Up—Moves selected frame up
	Move Down—Moves selected frame down
Copy to all ports	Copies all settings to other ports (if available in selected port configuration).
Ok	Confirms settings
Cancel	Cancels all changes

9.4.2 Transmission Settings

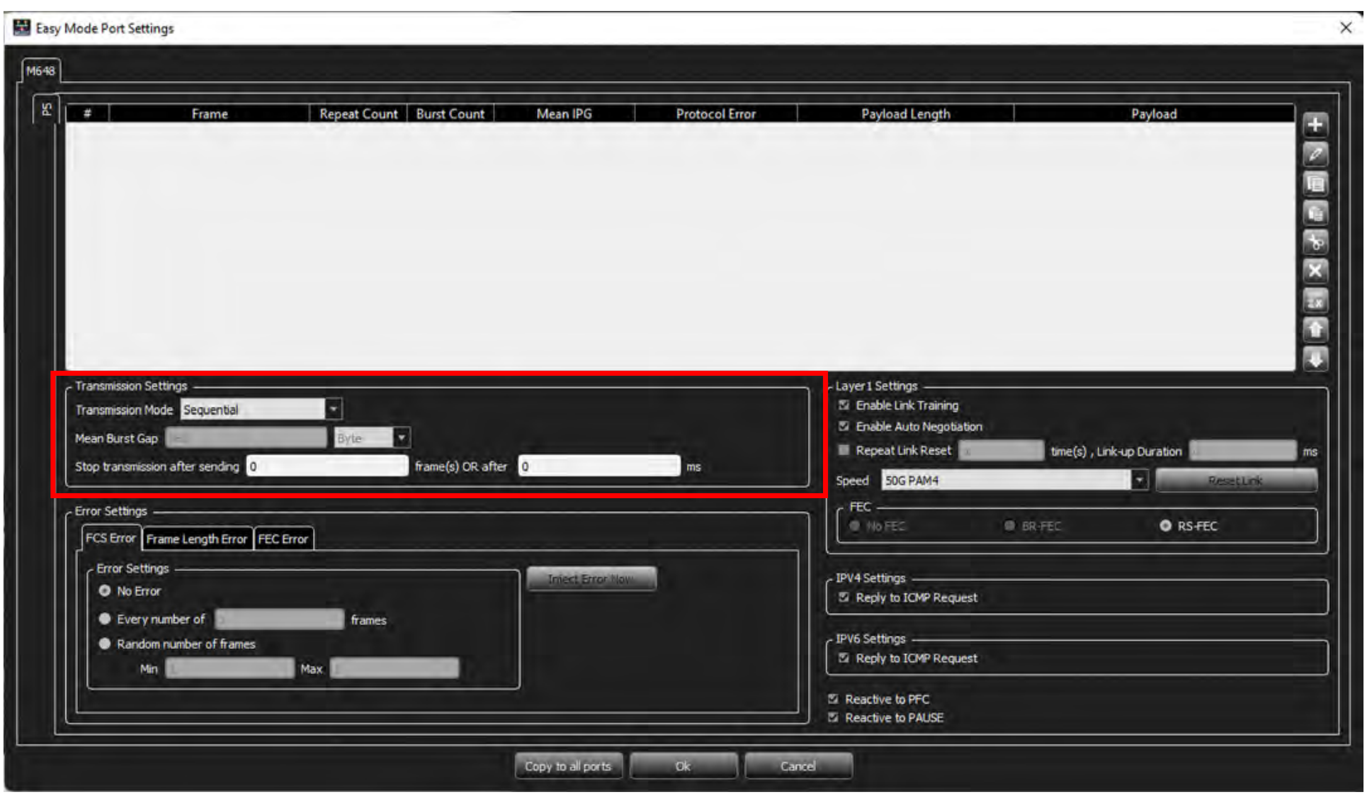


Figure 9.12: Easy Mode Transmission Settings

TABLE 9.2: Easy Mode Window – Transmission Settings

Setting	Description
Transmission Mode	**Sequential**—Frames are sent out according to the order defined in the top pane. Each frame is repeated as many times as specified in “Repeat Count” settings for that frame. **Interleave**—One frame is sent from each row in the top pane, until each one reaches “Repeat Count” settings. An example can be found in Table 9.3. **Burst-Interleave**—“Burst Count” bursts, each of “Repeat Count” frames, are sent from each frame defined in the top pane. An example can be found in Table 9.3.
Mean Burst Gap	Only applicable in Burst-Interleave Mode. This is the gap (defined in either bytes or nanoseconds) between consecutive bursts of frames (between each frame in the burst, the defined IPG will remain).
Stop transmission after sending	Stop sending frames after a set number of frames or milliseconds

TABLE 9.3: Example Transmission Mode

Option	Example
Interleave	For example, if 3 frames have been defined: • A (Repeat Count=3) • B (Repeat Count=2) • C (Repeat Count=1) The sequence of sending frames is: • A, B, C • A, B • A • A, B, C • A, B ... then the above sequence repeats. (Sequence repeats until the “Stop transmission” conditions have been met.)
Burst-Interleave	For example, if 3 frames have been defined: • A (Repeat Count=9, Burst Count=3) • B (Repeat Count=6, Burst Count=3) • C (Repeat Count=3, Burst Count=3) The sequence of sending frames is: • A, A, A • B, B, B • C, C, C • A, A, A • B, B, B • A, A, A ... then the above sequence repeats. (Sequence repeats until the “Stop transmission” conditions have been met.)

9.4.3 Error Settings

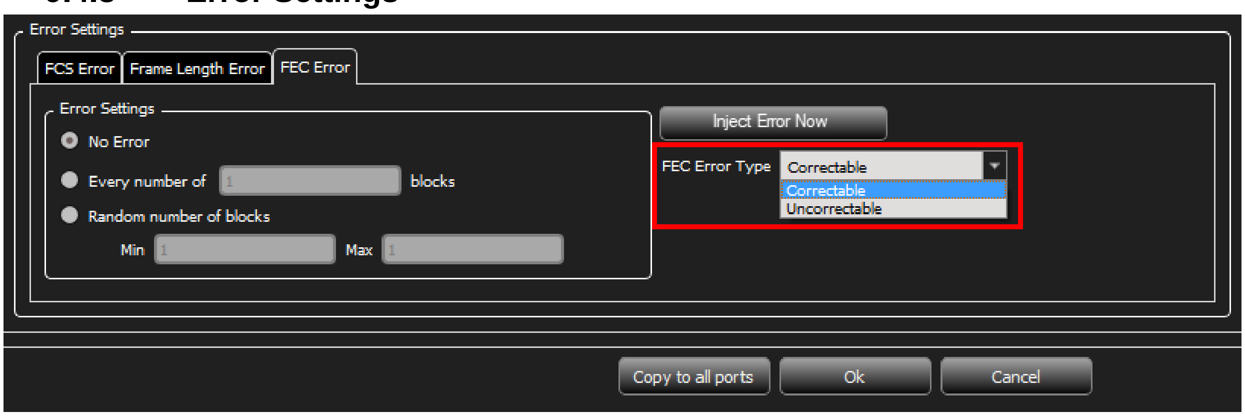


Figure 9.13: FEC Error Type Options

TABLE 9.4: Easy Mode Window – Error Settings

Setting	Description
FCS Error	• No Error • Every number of [#] frames • Random number of frames – Min to Max.
Frame Length Error	• No Error • Every number of [#] frames • Random number of frames – Min to Max
FEC Error	• No Error • Every number of [#] blocks • Random number of blocks – Min to Max Select FEC Error Type, **Correctable** or **Uncorrectable**, from the drop-down list (Figure 9.4.4).
	Press the **Inject Error Now** button to inject the errors defined in Error Settings instantaneously.

9.4.4 Layer1 Settings

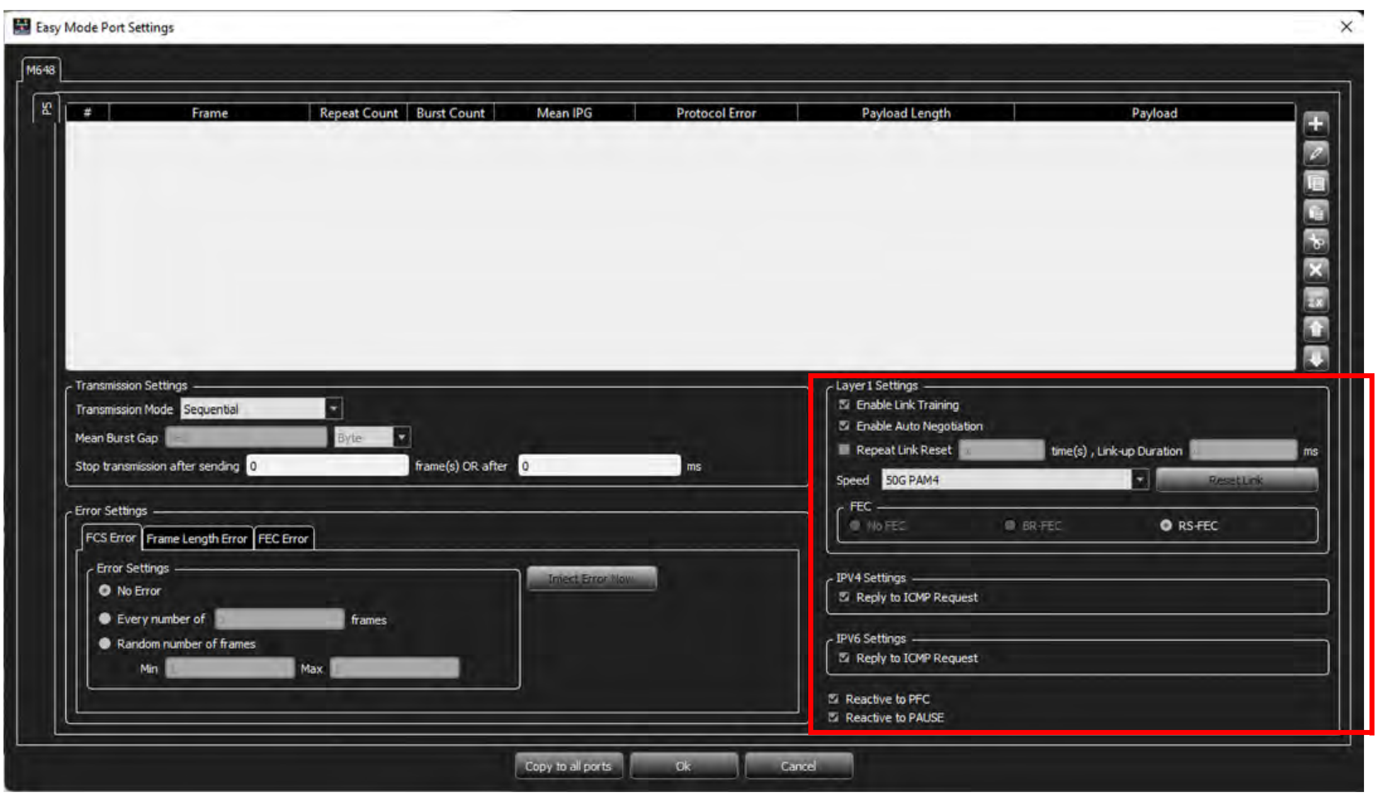
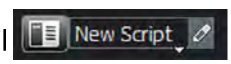


TABLE 9.5: Layer1 Settings

Setting	Description
Enable Link Training	Enable/disable Link Training
Enable Auto Negotiation	Enable/disable Auto Negotiation
Repeat Link Reset	The number of time to execute link bring up cycles.
Link-up Duration (ms)	The time (in ms) to keep the link up between Link Reset cycles.
Speed	Select the desired generation speed: 10G, 25G or 50G PAM4.
	Reset the link per the Port Activation Settings (Figure 9.8).
FEC	• No FEC (applicable only in 10G and 25G Speeds) • BR-FEC (applicable only in 25G Speed) • RS-FEC (applicable only in 50G PAM4 Speed)
IPV4 Settings	Enable/disable Reply to ICMP Request
IPV6 Settings	Reply to ICMP Request
Reactive to PFC	Enable/disable listening and responding to PFC
Reactive to PAUSE	Enable/disable listening and responding to PAUSE

9.5 Port Settings - Script Mode

To access the Script Mode Port Settings, Click the pencil 

on the Easy Mode/ Script Mode icon (located to the right of the M648 ports). The *Exerciser Script Manager* screen appears (Figure 9.14).

NOTE: If the icon says "Easy Mode" instead of "New Script", then click  to switch to "New Script."

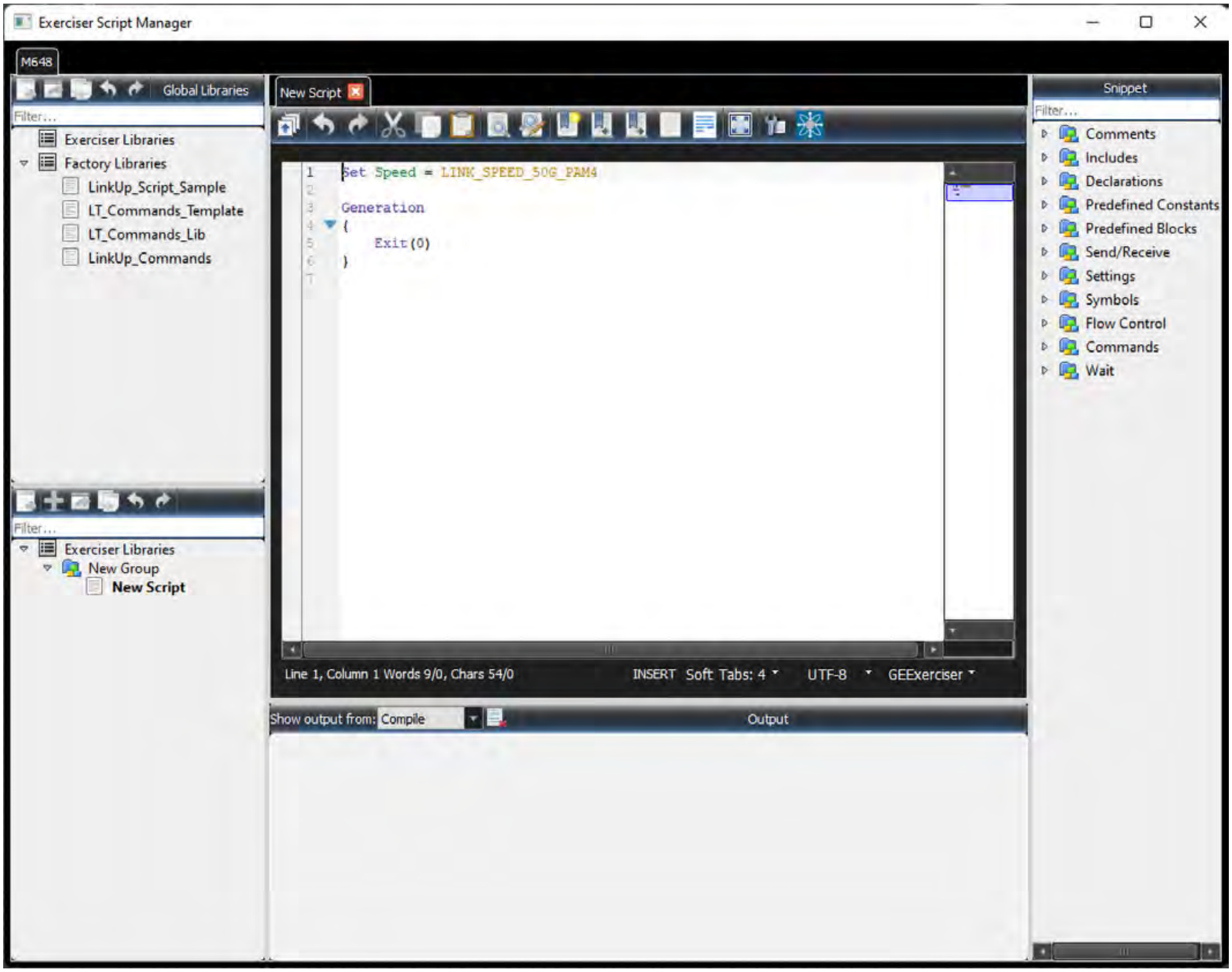


Figure 9.14: Exerciser Script Manager

9.5.1 Commands

Easily add commands to the *New Script* window by dragging and dropping commands from the *Snippet* area into the *New Script* window. The commands are organized into folders. Some folders also have sub-folders. The following sections describe the commands in more detail.

NOTE: The installation now contains the following files, which include examples for using the AN/LT Ethernet Exerciser:

- LT_Commands_Lib, LT_Commands_Template,
- LinkUp_Script_Sample, and
- LinkUp_Commands.

9.5.1.1 Comments

Line Comment

is the Comment symbol for a line comment. Anything on the line after the # symbol is ignored.

Example:

```
AutoFillWordInsertion = ON # This is an example of a line comment.
```

Block Comment

All the text between /* and */ is ignored.

Example:

```
/*
This is an example of a block of comments.
*/
```

9.5.1.2 Includes

The directive `%include` "FileName.inc" includes the file FileName.inc. This lets you add common definitions and templates into new scripts.

The language parser makes sure the same file is not included more than once.

Example:

```
%include "path_to_include\SomeInc.inc"
# This directive actually includes file 'path_to_include\SomeInc_1.inc'.
Absolute paths are also allowed:
%include "c:\absolute\path\to\include\SomeInc.inc"
```

NOTE: Default Path: "C:\Users\Public\Documents\LeCroy\NET Protocol Suite\"

9.5.1.3 Declarations

Constant

Only unsigned integers are defined as constants. Some constants are predefined in the Sierra Exerciser.

Examples:

```
Const SOME_HEX_DATA = 0xAABBFFEE #defines hexadecimal constant
Const SOME_DEC_DATA = 12     # defines decimal constant
```

Data Pattern

Data patterns are streams of hexadecimal values. Data Patterns are used to implement some of the fields used in FC NVMe, which are very long, such as:

- Host Identifier (128 bits),
- Host NVMe Qualified Name (2048 bits), and
- NVMe Subsystem NVMe Qualified Name (2048 bits).

Examples:

```
DataPattern MyPattern_1 = 11223344
DataPattern MyPattern_2 = 11223344 AABBCCDD
DataPattern MyPattern_3 = 11223344 AABBCCDD 10203040
DataPattern MyPattern_Recursive_1 = 12345678  MyPattern_1   MyPattern_2
```

Variables

Variables are similar to definitions in programming languages. Define up to 250 32-bit or 125 64-bit variables. There are no constraints on variable names, except that you cannot use keywords. The available variables are:

- Var32
- Var64
- Var32_Ref
- Var64_Ref

Variable scopes are general and defined in the script header before the Generation block. Start variable names with @.

Example:

```
VAR32 @VariableName1, @VariableName2, ...
VAR64 @VariableName
```

NOTE: VAR64 holds field values greater than 32 bits, such as FCAddress.

Global

Global scripts define a procedure. Procedures allow creating simple syntaxes for complex reusable parts in scripts. You can write such code once as a procedure and use it anywhere required. Along with the Procedure script command, you can define procedures with:

- Procedure(params...), and
- Procedure_Inline

NOTE: Place Global scripts outside of the generation block.

Procedure(params...)

Define a procedure with parameters.

Parameter Types:

- PARAM_ID: for sending numeric values to procedures
- PARAM_ID_REF: for sending and receiveing numeric values to/from procedures
- PARAM_VAR32: for sending 32-bit variables values to procedures
- PARAM_VAR32_REF: for sending and receiveing 32-bit variables values to/from procedures

- PARAM_VAR64: for sending 64-bit variables values to procedures
- PARAM_VAR64_REF: for sending and receiveing 32-bit variables values to/from procedures

Example:

```
Procedure ProcedureName
(
    PARAM_ID            param1,  #e.g. 1, 2 + i, i
    PARAM_ID_REF        param2,  #e.g. i
    PARAM_VAR32         @param3, #e.g. @a, @a + @b, 2
    PARAM_VAR32_REF     @param4, #e.g. @a
    PARAM_VAR64         @param5, #e.g. @a, @a + @b, 2
    PARAM_VAR64_REF     @param6  #e.g. @a
```

Procedure_Inline

Define an inline procedure.

Example:

```
Procedure_Inline ProcedureName
```

9.5.1.4 Predefined Constants

The Predefined Constants are:

- TRUE - TRUE values are equal to 1
- FALSE - FALSE values are equal to 0
- ON - ON values are equal to 1
- OFF - OFF values are equal to 0
- INFINITE - Used in Loop or Wait instructions

Example:

```
Loop(INFINITE) {}
Wait(INFINITE) { when {WF_LINK_UP} do {} }
```

FEC Type

- FEC_Disabled
- BR_FEC_Enabled
- RS_FEC_Enabled

Link Speed

- Link_Speed_10G
- Link_Speed_25G
- Link_Speed_50G_PAM4
- Link_Speed_Auto

Reserved Variables

- LRAN - Last Received Auto Negotiation
- LRLT - Last Received Link Training
- Random - Loads the variable with a random value (Generated at runtime)

Example:

```
Var32 @some_var = Random
```

9.5.1.5 Predefined Blocks

Generation Block

The Generation block is the starting point of script execution. The following settings are only valid before Generation block:

- GenerationMode
- AutoConnect
- AutoReconnect

Example:

```
Generation
{
      #implementation here ...
}
```

9.5.1.6 Send/Receive

Send Symbol

Send Predefined GIGE symbols. Format:

```
SendSymbol (SYMBOL_NAME, MINIMUM_COUNT)
```

Supported symbol names are:

- Idle_Idle
- Idle_LocalFault
- Idle_RemoteFault
- Idle_LinkInterrupt
- LocalFault_Idle
- LinkInterrupt_Idle
- RemoteFault_Idle
- LocalFault_LocalFault
- RemoteFault_RemoteFault
- LinkInterrupt_LinkInterrupt

The 'MINIMUM_COUNT' value is considered as a lower minimum: if no other 'Send' instruction or 'EXIT_SEND_SYMBOL' instruction is executed the exerciser will continue to repeat the last data on the line.

SendTrainingFrame

Transmits a specific Training Frame. Two options are available: PAM2(default) and PAM4. See Figure 9.15 and Figure 9.16.

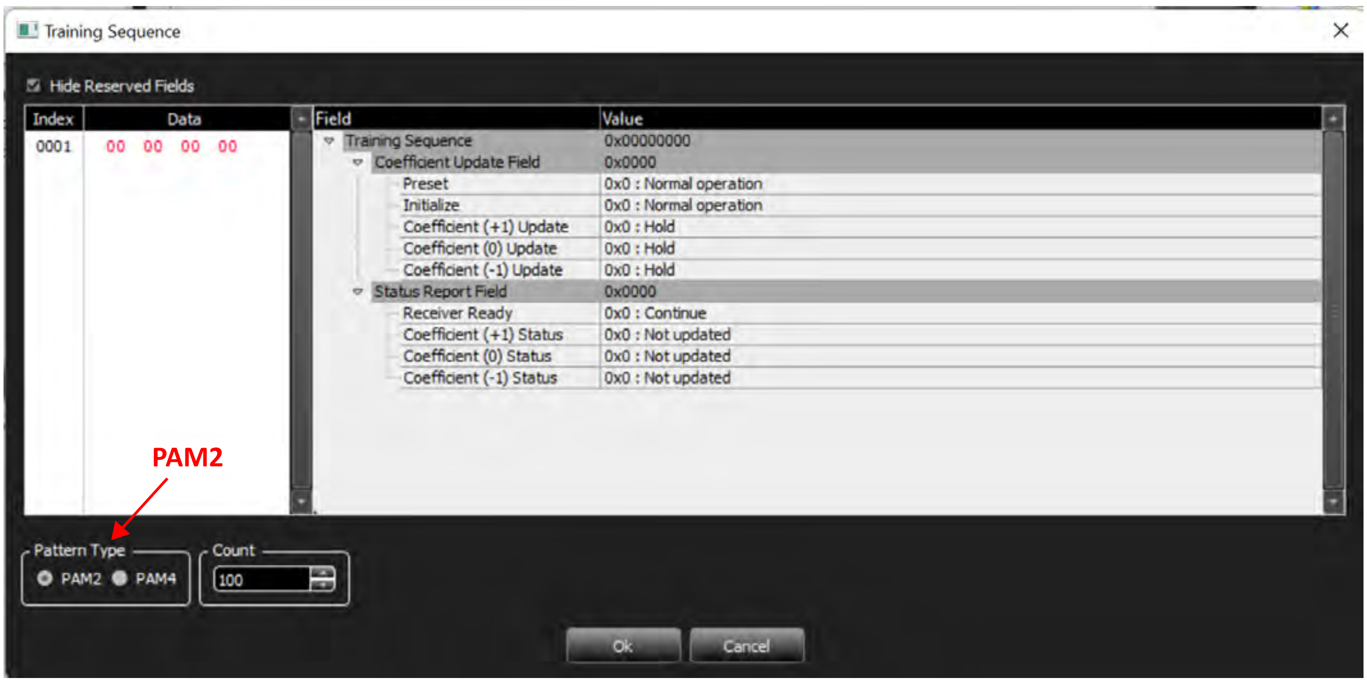


Figure 9.15: SendTrainingFrame Training Sequence Screen: PAM2

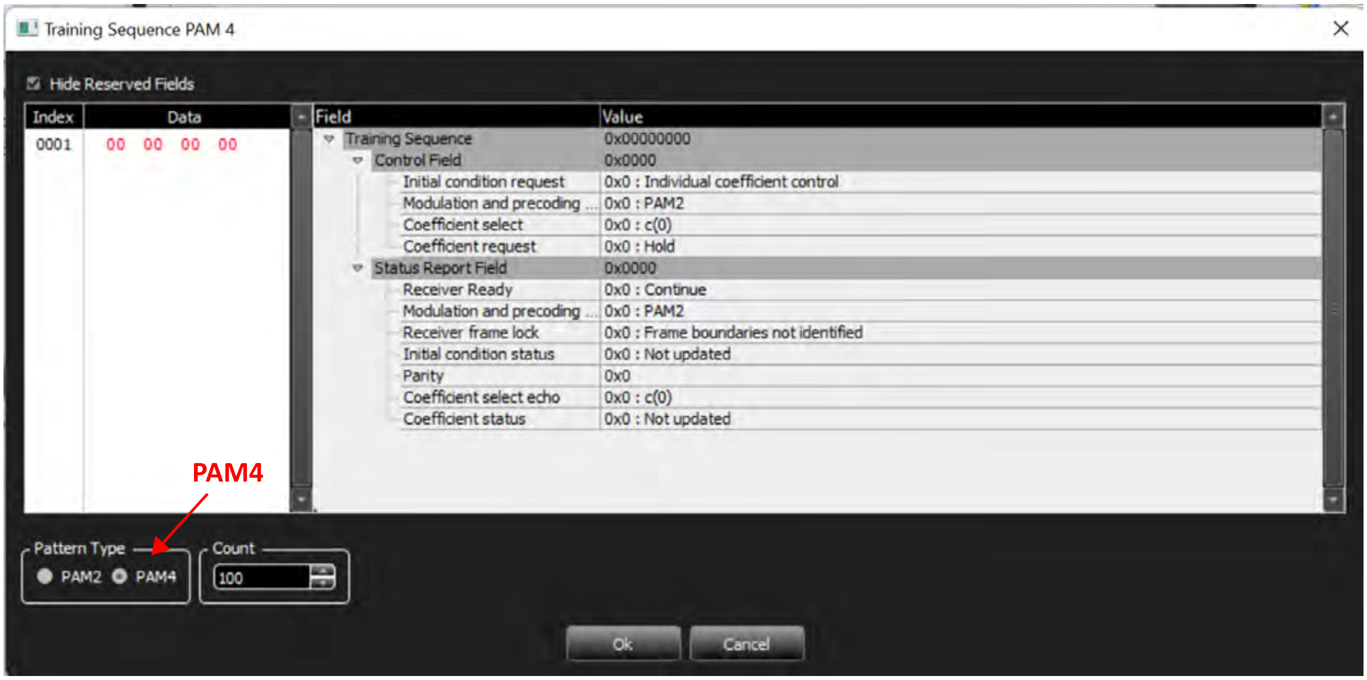


Figure 9.16: SendTrainingFrame Training Sequence Screen: PAM4

Format:

```
SendTrainingFrame "Training Frame"
{
    TrainingFrameData = "32bit_Hex_Data"
    #field value overwriting [optional]:
    Field[start_bit:end_bit] = value
    Field[start_bit:end_bit] = value
    Field[start_bit:end_bit] = value
    ...
}(Minimum_Count)
```

Example:

```
SendTrainingFrame "Training Frame"
{
    TrainingFrameData = "00000010"
    Field[4:5] = 0x1
}(100)
```

The 'MINIMUM_COUNT' value is considered as a lower minimum: if no other 'Send' instruction or 'EXIT_MANUAL_TRAINING' instruction is executed, the exerciser continues to repeat the last data on the line.

SendAutoNegFrame

Transmits a specific Auto-Negotiation Frame. Format:

```
SendAutoNegFrame "Frame Name"
{
    AutoNegFrameData = "48bit_Hex_Data"
```

```
    #field value overwriting [optional]:
    Field[start_bit:end_bit] = value
    Field[start_bit:end_bit] = value
    Field[start_bit:end_bit] = value
    ...
}(Minimum_Count)
```

Example:

```
SendAutoNegFrame "Auto Negotiation IEEE.std 802.3"
{
    AutoNegFrameData = "000000080000"
    Field[19:19] = 0x1
}(100)
```

The 'MINIMUM_COUNT' value is considered as a lower minimum. That is, if no other 'Send' instruction or 'EXIT_MANUAL_AUTONEG' instruction is executed the exerciser will continue to repeat the last data on the line.

SendRawAutoNegFrame

Transmits user specified 106 bits of Manchester encoded data. Format:

```
SendRawAutoNegFrame(FrameMarker_8bit, AN_Data_96bits, RandomBit_2bits,
Minimum_Count)
```

Example:

```
SendRawAutoNegFrame(0xF0, CCCCCCCC CCCCCCCC CCCCCCCC, 0b10, 200)
```

NOTE: The MINIMUM_COUNT value is considered as a lower minimum. If no other Send instruction or EXIT_MANUAL_AUTONEG instruction is executed the exerciser will continue to repeat the last data on the line.

9.5.1.7 Settings

FECEnabled

Possible values are:

- FEC_DISABLED (default)
- RS_FEC_ENABLED
- BR_FEC_ENABLED

Supported FEC values based on speed:

- 10G -> Only FEC_DISABLED
- 25G -> All 3 values are supported.
- 50G -> Only RS_FEC_ENABLED

NOTE: Using unsupported FEC type for the specified speed will result in undefined behavior.

Example:

```
Set FecEnabled = RS_FEC_ENABLED
```

Speed Settings

Two possible scripts are available: `Speed` and `Rx_Speed`.

Speed

Default speed setting specified from unit license. Values are:

- LINK_SPEED_10G
- LINK_SPEED_25G
- LINK_SPEED_50G_PAM4 (default)

Example:

```
Set Speed = LINK_SPEED_50G_PAM4
```

Rx_Speed

Default Rx speed setting specified from unit license. Values are:

- LINK_SPEED_10G
- LINK_SPEED_25G
- LINK_SPEED_50G_PAM4
- LINK_SPEED_AUTO (default)

Example:

```
Set Rx_Speed = LINK_SPEED_AUTO
```

Wait Settings

WaitTimeout

Set the default timeout value (us) when it's not specified in the `wait` and `wait_for` commands. Accepts Any integer between 0 to 1,206,323,052,078.

Example:

```
Set WaitTimeout = 1000
```

9.5.1.8 Symbols

The Symbols folder contains the following commands:

- Idle_Idle
- LocalFault_Idle
- RemoteFault_Idle
- LinkInterrupt_Idle
- Idle_LocalFault
- Idle_RemoteFault

- ❑ Idle_LinkInterrupt
- ❑ LocalFault_LocalFault
- ❑ RemoteFault_RemoteFault
- ❑ LinkInterrupt_LinkInterrrupt

The following is an example of coding using these commands:

```
SendSymbol(Idle_Idle, 10000)
```

9.5.1.9 Flow Contro

Loop

Loop for a certain number of times.

Format:

```
Loop (Counter) { instructions }
```

Example:

```
Loop (10)
```

Loop(INFINITE)

Infinite Loop.

#Format:

```
Loop (Counter) { instructions }
```

Example:

```
Loop (INFINITE) #Never ending loop. You can only use exit to finish the
script
```

If/Elself/Else

Example for if, then else:

```
@lt_mp_response         = @received_link_training & LT_MP_Req
    if (@lt_mp_response == LT_MP_Resp_PAM4)
    {
        @mp_response    =   LT_MP_PAM4
    }
    elseif (@lt_mp_response == LT_MP_Resp_PAM4_Pre)
    {
        @mp_response    =   LT_MP_PAM4_Precoding
    }
    else
    {
        @mp_response =   LT_MP_PAM2
    }
```

While

Example for while:

```
while (@NCQ_Temp0)   {
@NCQ_Temp1= @NCQ_Temp1 >> 1
If (@NCQ_Temp1 != 0) then { … }
@NCQ_Temp0 = @NCQ_Temp1 & 0x00000001     }
```

BreakWhile

If it’s called inside a While loop block, program execution point would jump to the next instruction after the While block.

ContinueWhile

If it's called inside a While loop block, program execution point would jump to the first instruction inside the While block. Nested while and if are supported, the keyword then is optional.

Wait/When/ElseWhen

Waits for conditions with a timeout. If the timeout is not defined, `WaitTimeout value (us)` will be used.

Format:

```
Wait [(timeout value us)] {When {conditions} Do{instructions} [ElseWhen
{conditions} Do{instructions}] [On_Timeout{instructions}] }
```

Example:

```
Wait (1000)
{
When { WF_LINK_UP } Do
{}
ElseWhen { WF_TIMEOUT } Do
{
}
On_Timeout
{
}
```

Wait_For

Waits for conditions until a `timeout(us)`. If the timeout is not defined, it waits until one of the conditions is fulfilled.

If timeout is not defined and `WF_TIMEOUT` condition is added, the default timeout value (1 ms) is used for timeout.

#Format:

```
Wait_For [(timeout value)] { list of conditions }
```

Example:

```
Wait_For (100) { WF_LINK_UP }
```

WaitForTrainingFrame

Wait for a specified Training Frame.

Format:

```
WaitForTrainingFrame(Training_Sequence, Mask)
```

Example:

```
WaitForTrainingFrame(0x80004000, 0xC0004000)
```

WaitForAutoNegFrame

Wait for a specified Auto-Negotiation Frame.

Format:

```
WaitForAutoNegFrame(AutoNeg_pattern, Mask)
```

Example:

```
WaitForAutoNegFrame(0x400000000000, 0xFF0000000000)
```

Return

Return from procedure to the caller.

Exit

Call this command in any branch of the Exerciser program to stop execution. The Exit code can be specified either with a constant or a variable. When the variable name is recognized, the exerciser reads the data in the specified variable and considers it as the exit code.

NOTE: The maximum value that is allowed for the exit code is 255 (0xFF).After exit, the Port Status dialog displays the exit code.

Format:

```
Exit [(code value)];
Exit = Exit(0)
```

Example:

```
Exit (1)
```

Call

This command moves the execution point to the calling procedure and comes back after the procedure is finished.

Example:

```
Call procedure_name
```

9.5.1.10 Commands

LinkUp

The exerciser will go through connection sequence using the current settings. Generation will not resume until the connection is established. If the program is manually stopped before this command finishes, the exerciser will remain in the state in which it tries to linkup with the specified settings.

Format:

```
LinkUp([AN_Enabled/An_Disabled], [LT_Enabled/LT_Disabled])
```

Example:

```
LinkUp(AN_Enabled, LT_Enabled)
LinkUp(AN_Disabled, LT_Disabled)
```

LinkDown

The exerciser will break the existing connection to DUT.

EXIT_MANUAL_TRAINING

After sending a manual training frame, the exerciser moves to a state in which it continuously sends training frames until this command is executed. For example, when a wait command is written after a `send_training_frame` instruction, the exerciser keeps sending the last training frame instead of idles. In that case, this command is used to exit from manual training and move on to normal data.

EXIT_MANUAL_AUTONEG

After sending a manual auto-neg frame, the exerciser moves to a state in which it continuously sends auto-neg frames until this command is executed. For example, when a wait command is written after a `send_autoneg_frame` instruction, the exerciser keeps sending the last auto-neg frame instead of idles. In that case, this command is used to exit from manual training and move on to normal data.

EXIT_SEND_SYMBOL

After using `SendSymbol` instruction, the exerciser moves to a state in which it continuously sends the symbol until this command is executed. For example, when a wait command is written after a `SendSymbol` instruction, the exerciser keeps sending the last symbol instead of idles. In that case, this command is used to exit from Symbol state and move on to normal data.

Delay

The exerciser will wait for the specified time (ns) before executing the next command.

Format:

```
Delay [(value_in_ns)]
```

Example:

```
Delay (1)
```

9.5.1.11 Wait

WF_LINK_UP

Waits for the link up

WF_TIMEOUT

Waits until the specified timeout

9.6 Start Generation Session

Each defined Exerciser port has a **Start/Stop Session** button (Figure 9.17), with a three-option drop down menu. Pressing **Start** automatically activates the Exerciser and starts the traffic defined in the Port Settings.

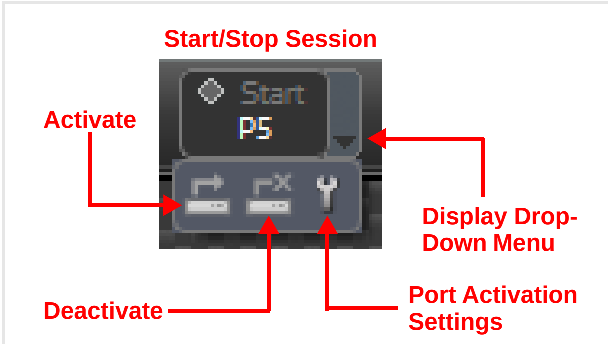


Figure 9.17: Start/Stop Generation Session Button

The three options are as follows:

- **Activate**—Brings the link up, based on the Port Activation Settings (see below). Once activated, the Exerciser will respond to Ethernet requests if/as defined in the Port Settings
- **Deactivate**—Link goes down.
- **Port Activation Settings**—Defines the parameters for the port. See Figure 9.8 in Section 9.3, *Port Settings*.

Chapter 10

Side-Band Command Channel

10.1 Using the Side-Band Command Channel Feature

NOTE: This section only applies to the SierraNet T328, M328, and M328Q models.

TCP Port 4004 of the analyzer Ethernet host interface is defined for exclusive use as a side-band command channel. Any client may send commands to this port. There are no responses defined for these commands. The structure of a command sent on this channel is an ASCII-encoded text string with length 1-256 bytes. Commands are case-sensitive. The last character of each command must be '!'—the receiving port expects this character as a command delimiter.

It is the sender's responsibility to ensure the analyzer is in the proper state for its issued command to have the expected result.

The commands defined for this channel are:

TABLE 10.1: Side-Band Commands

Command (ASCII text)	Description
TRIGGER_ANALYZER!	**Assuming the analyzer is in the waiting-for-trigger state, this command will cause it to trigger. Otherwise, the command has no effect.**
STOP_ANALYZER!	Assuming the analyzer is in the recording state, this command will stop the recording immediately and enable uploading to begin. Otherwise, the command has no effect.

Example 1 – Python:

```
import socket

HOST = '1.2.3.4' # The analyzer's IP address
PORT = 4004      # The message port used by the analyzer

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((HOST, PORT))
s.sendall(b'TRIGGER_ANALYZER!')
```

Example 2 – Linux shell:

```
echo TRIGGER_ANALYZER! | netcat 1.2.3.4 4004
```

Appendix A

How to Contact Teledyne LeCroy

Send e-mail to Support	psgsupport@teledyne.com
Contact support	teledynelecroy.com/support/contact
Visit Teledyne LeCroy's web site	teledynelecroy.com
Tell Teledyne LeCroy	Report a problem to Teledyne LeCroy Support via e-mail by selecting **Help > Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.

Appendix B

China Restriction of Hazardous Substances Table

The following tables are supplied in compliance with China’s Restriction of Hazardous Substances (China RoHS) requirements:

部件名称	有毒有害物质和元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
PCBAs	X	O	X	X	X	X
机械硬件	O	O	X	O	O	O
金属片	O	O	X	O	O	O
塑料部件	O	O	O	O	X	X
电源	X	X	X	O	X	X
电源线	X	O	X	O	X	X
保护外壳(如有)	O	O	O	O	X	X
电缆组件(如有)	X	O	X	O	X	X
风扇(如有)	X	O	X	O	X	X
交流滤波器和熔丝组件(如有)	X	O	X	O	O	O
外部电源(如有)	X	X	X	O	X	X
探头(如有)	X	O	X	O	X	X
O: 表明该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求之下。						
X: 表明该有毒有害物质至少在该部件的某一均质材料中的含量超过 SJ/T11363-2006 标准规定的限量要求。						

EFUP (对环境友好的使用时间) 使用条件：
温度：5摄氏度到40摄氏度
湿度：5% - 95%最大相对湿度 (无冷凝)
高度：最高2000米

Part Name	Toxic or Hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr^{6+})	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCBAs	X	O	X	X	X	X
Mechanical Hardware	O	O	X	O	O	O
Sheet Metal	O	O	X	O	O	O
Plastic Parts	O	O	O	O	X	X
Power Supply	X	X	X	O	X	X
Power Cord	X	O	X	O	X	X
Protective Case (if present)	O	O	O	O	X	X
Cable Assemblies (if present)	X	O	X	O	X	X
Fans (if present)	X	O	X	O	X	X
AC Filter/Fuse Assy (if present)	X	O	X	O	O	O
Ext Power Supply (if present)	X	X	X	O	X	X
Probes (if present)	X	O	X	O	X	X
O: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement specified in SJ/T11363-2006.						
X: Indicates that this toxic or hazardous substance contained in at least one of the homogenous materials used for this part is above the limit requirement specified in SJ/T11363-2006.						

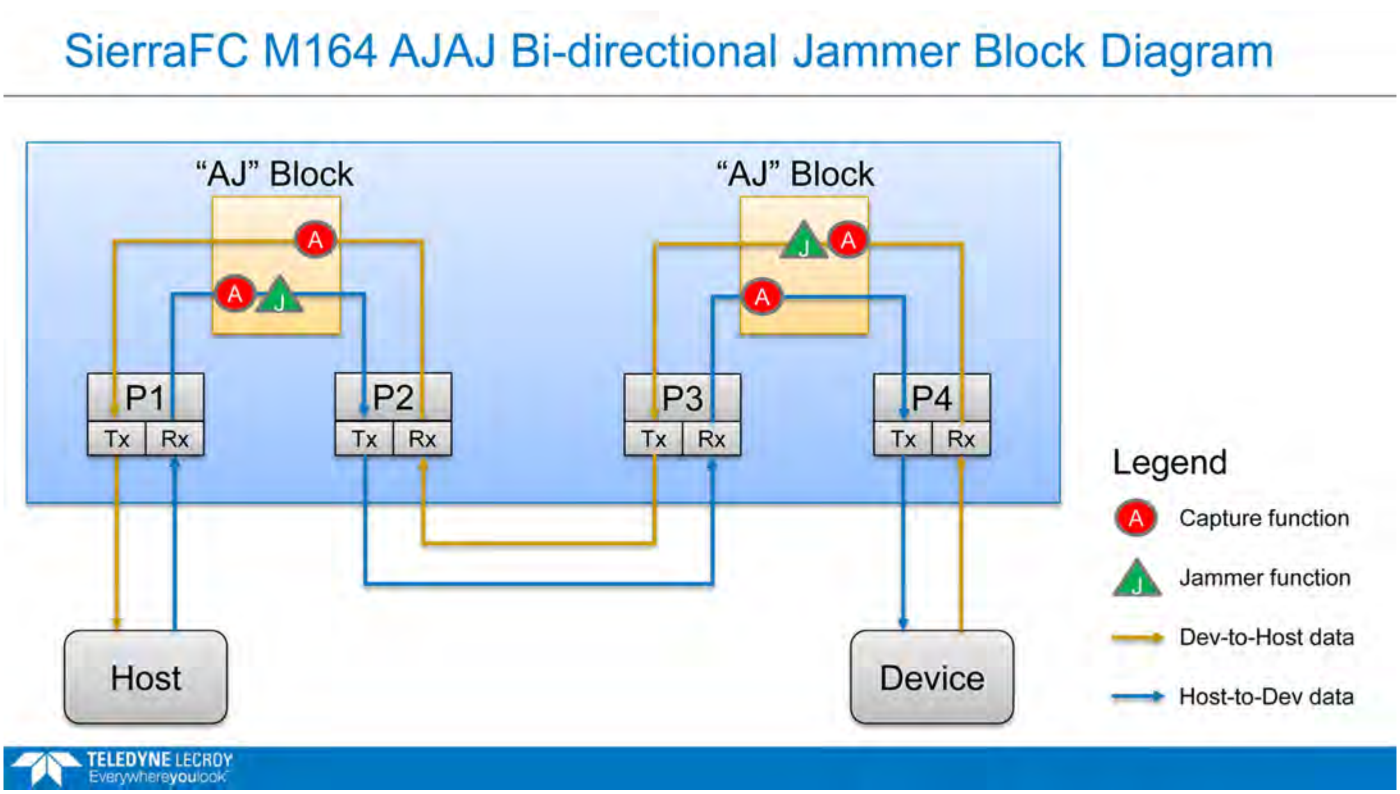
EFUP (Environmental Friendly Use Period) Use Conditions:

Temperature	5C to 40C
Humidity	5% to 95% max RH (non-condensing)
Altitude	Up to 2000 meters

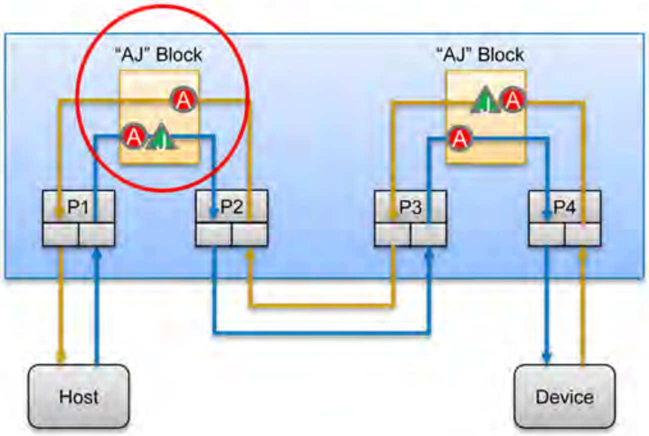
Appendix C

AJAJ – Bidirectional Jamming Operation

NOTE: Though this section specifically discusses the SierraFC M164 product, the same principles also apply to SierraNet M408/M168 and to SierraNet M648.

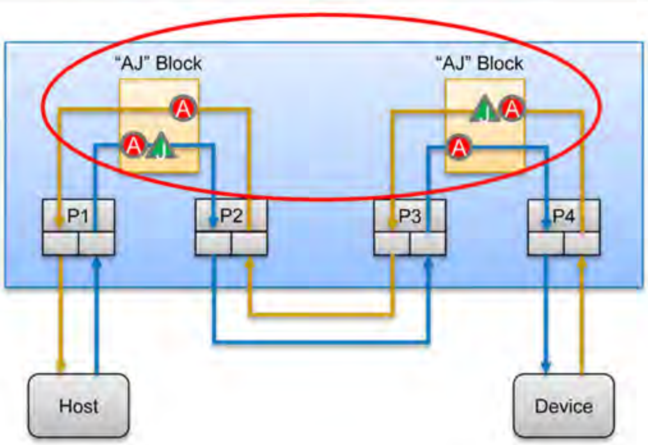


SierraFC M164 AJAJ Bi-directional Jammer Block Diagram



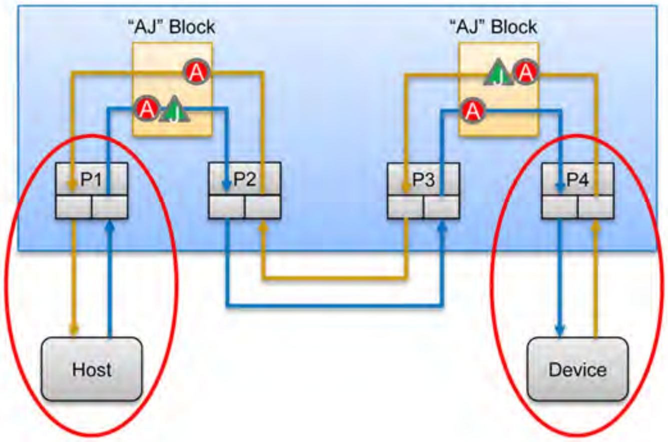
- Functionality of a single "AJ" Block
  - Monitors both directions of a single link
  - Captures traffic in both directions
  - Jams traffic in one direction, specified through scenario
  - In the direction where jam is applied, captured data will be pre-jam

SierraFC M164 AJAJ Bi-directional Jammer Block Diagram



- Two "AJ" Blocks can be configured back-to-back on a single link to create a bi-directional jamming configuration
  - Jam in both directions simultaneously
  - Capture pre- and post-jam data in both directions

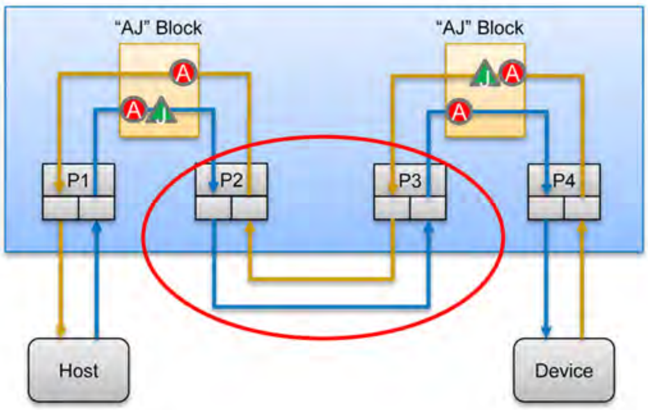
Bi-Directional Jamming Setup and Configuration instructions



- Connect P1 to the Host and P4 to the Device
- Connect P2 to P3 with a jumper cable
- Set the Jammer scenario running on P1/P2 to jam direction "From P1/P3"
- Set the Jammer scenario running on P3/P4 to jam direction "From P2/P4"

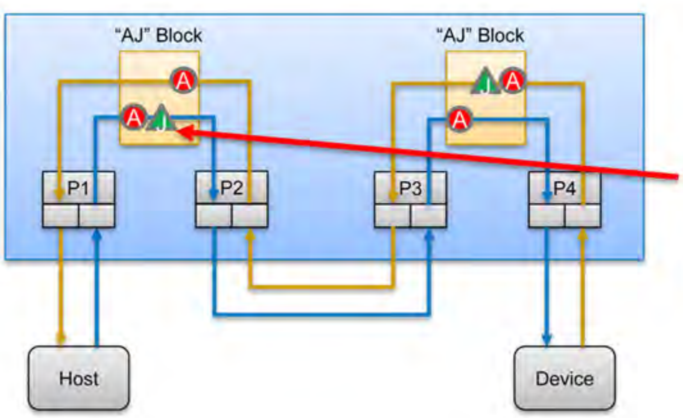
TELEDYNE LECROY
Everywhereyoulook

Bi-Directional Jamming Setup and Configuration instructions



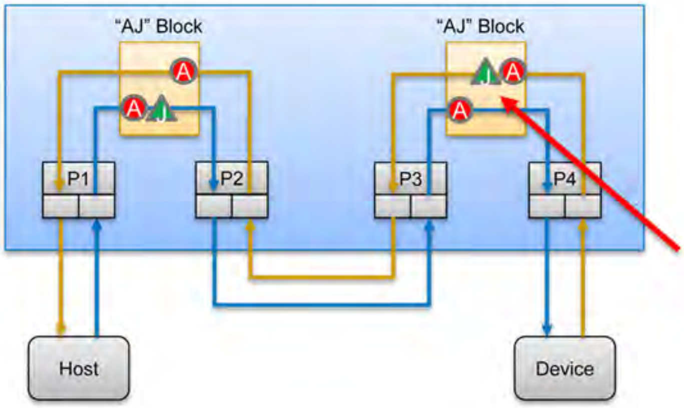
- Connect P1 to the Host and P4 to the Device
- Connect P2 to P3 with a jumper cable
- Set the Jammer scenario running on P1/P2 to jam direction "From P1/P3"
- Set the Jammer scenario running on P3/P4 to jam direction "From P2/P4"

Bi-Directional Jamming Setup and Configuration instructions



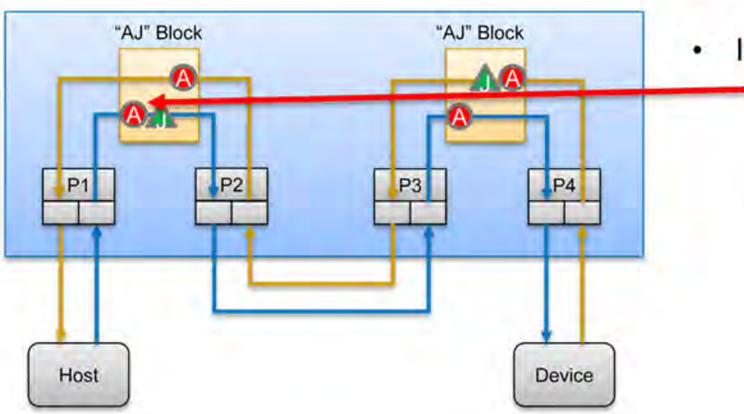
- Connect P1 to the Host and P4 to the Device
- Connect P2 to P3 with a jumper cable
- Set the Jammer scenario running on P1/P2 to jam direction "From P1/P3"
- Set the Jammer scenario running on P3/P4 to jam direction "From P2/P4"

Bi-Directional Jamming Setup and Configuration instructions



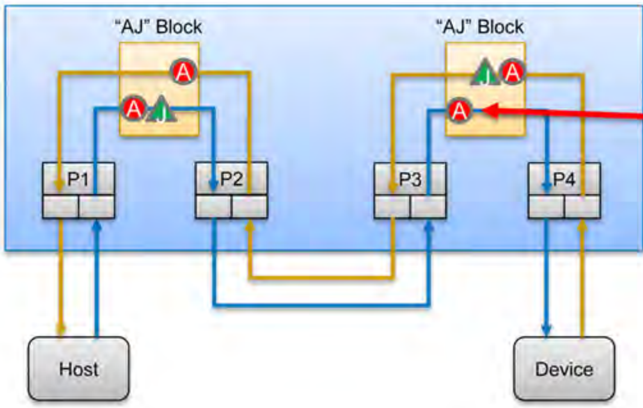
- Connect P1 to the Host and P4 to the Device
- Connect P2 to P3 with a jumper cable
- Set the Jammer scenario running on P1/P2 to jam direction "From P1/P3"
- Set the Jammer scenario running on P3/P4 to jam direction "From P2/P4"

Interpreting the Trace



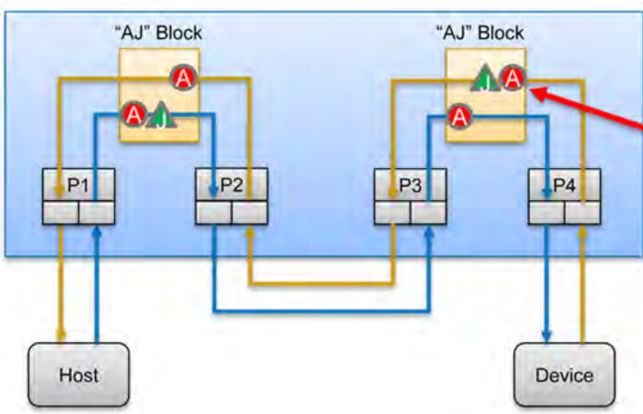
- Items/events in the trace:
  - P1 – from the Host before jamming
  - P3 – from the Host after jamming
  - P4 – from the Device before jamming
  - P2 – from the Device after jamming

Interpreting the Trace

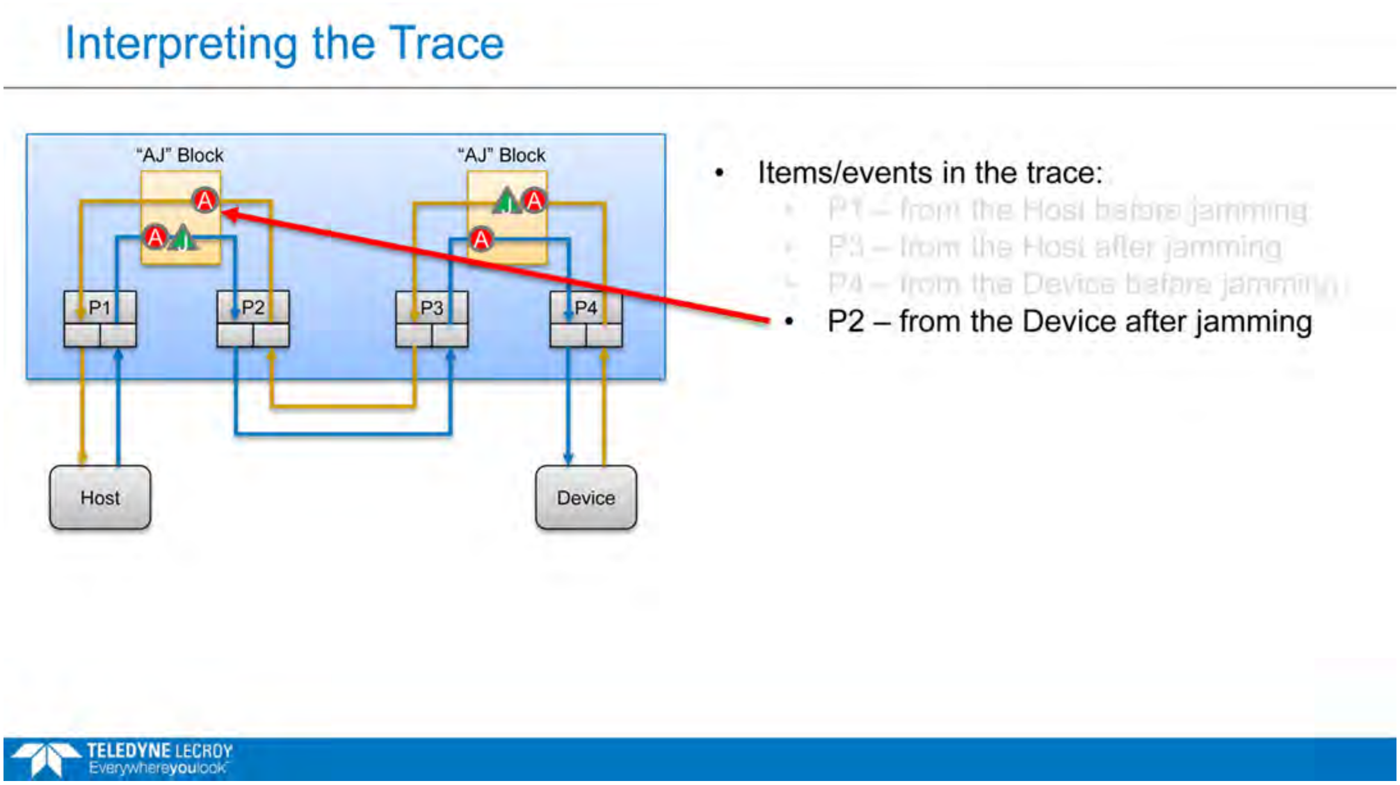


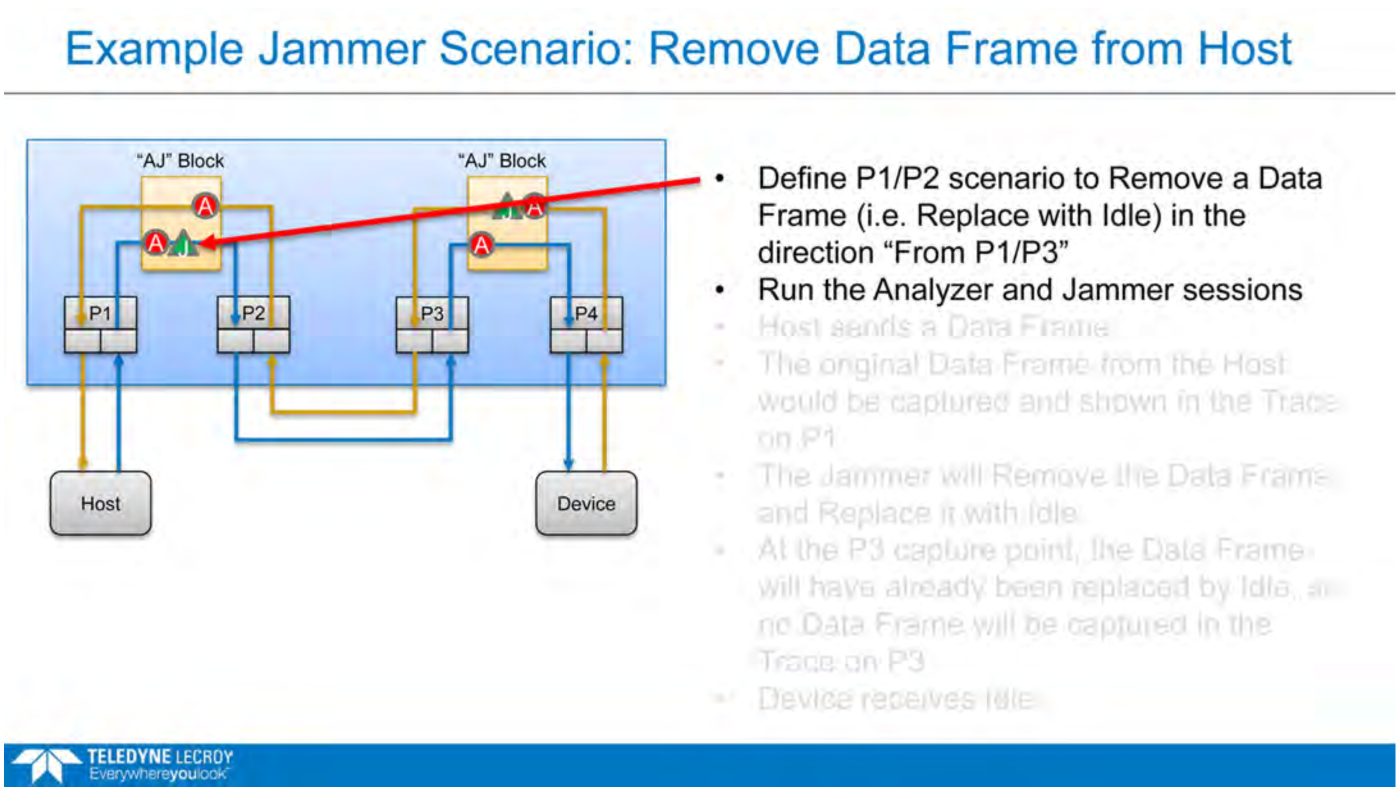
- Items/events in the trace:
  - P1 – from the Host before jamming
  - P3 – from the Host after jamming
  - P4 – from the Device before jamming
  - P2 – from the Device after jamming

Interpreting the Trace

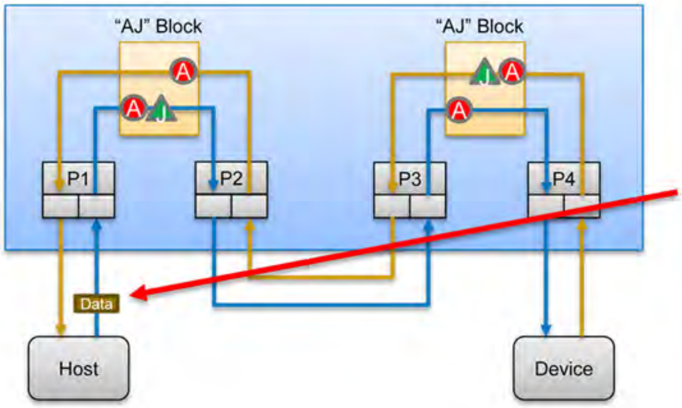


- Items/events in the trace:
  - P1 – from the Host before jamming
  - P3 – from the Host after jamming
  - P4 – from the Device before jamming
  - P2 – from the Device after jamming


Interpreting the Trace
"AJ" Block
"AJ" Block
P1
P2
P3
P4
Host
Device
Items/events in the trace:
P1 – from the Host before jamming
P3 – from the Host after jamming
P4 – from the Device before jamming
P2 – from the Device after jamming
TELEDYNE LECROY
Everywhereyoulook


Example Jammer Scenario: Remove Data Frame from Host
"AJ" Block
"AJ" Block
P1
P2
P3
P4
Host
Device
Define P1/P2 scenario to Remove a Data Frame (i.e. Replace with Idle) in the direction "From P1/P3"
Run the Analyzer and Jammer sessions
Host sends a Data Frame
The original Data Frame from the Host would be captured and shown in the Trace on P1
The Jammer will Remove the Data Frame and Replace it with Idle
At the P3 capture point, the Data Frame will have already been replaced by Idle, so no Data Frame will be captured in the Trace on P3
Device receives Idle
TELEDYNE LECROY
Everywhereyoulook

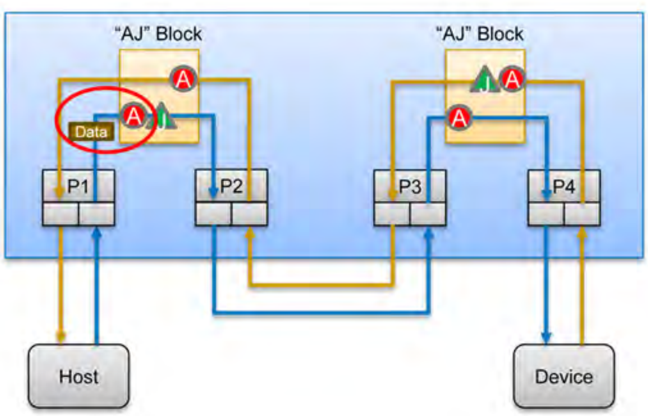
Example Jammer Scenario: Remove Data Frame from Host



- Define P1/P2 scenario to Remove a Data Frame (i.e. Replace with Idle) in the direction "From P1/P3"
- Run the Analyzer and Jammer sessions
- Host sends a Data Frame
- The original Data Frame from the Host would be captured and shown in the Trace on P1
- The Jammer will Remove the Data Frame and Replace it with Idle
- At the P3 capture point, the Data Frame will have already been replaced by Idle, so no Data Frame will be captured in the Trace on P3
- Device receives Idle

TELEDYNE LECROY
Everywhereyoulook™

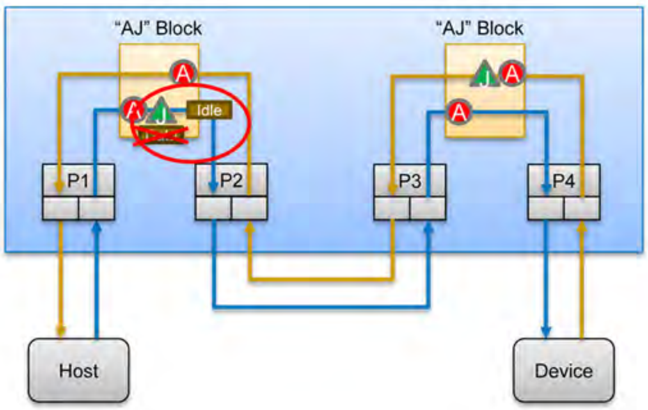
Example Jammer Scenario: Remove Data Frame from Host



- Define P1/P2 scenario to Remove a Data Frame (i.e. Replace with Idle) in the direction "From P1/P3"
- Run the Analyzer and Jammer sessions
- Host sends a Data Frame
- The original Data Frame from the Host would be captured and shown in the Trace on P1
- The Jammer will Remove the Data Frame and Replace it with Idle
- At the P3 capture point, the Data Frame will have already been replaced by Idle, so no Data Frame will be captured in the Trace on P3
- Device receives Idle

TELEDYNE LECROY
Everywhereyoulook™

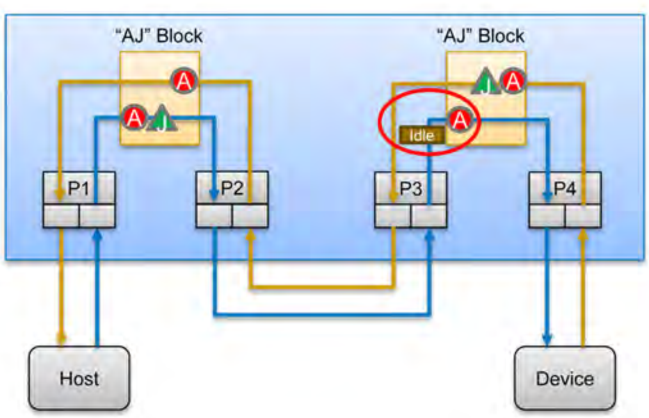
Example Jammer Scenario: Remove Data Frame from Host



- Define P1/P2 scenario to Remove a Data Frame (i.e. Replace with Idle) in the direction "From P1/P3"
- Run the Analyzer and Jammer sessions
- Host sends a Data Frame
- The original Data Frame from the Host would be captured and shown in the Trace on P1
- The Jammer will Remove the Data Frame and Replace it with Idle
- At the P3 capture point, the Data Frame will have already been replaced by Idle, so no Data Frame will be captured in the Trace on P3
- Device receives Idle

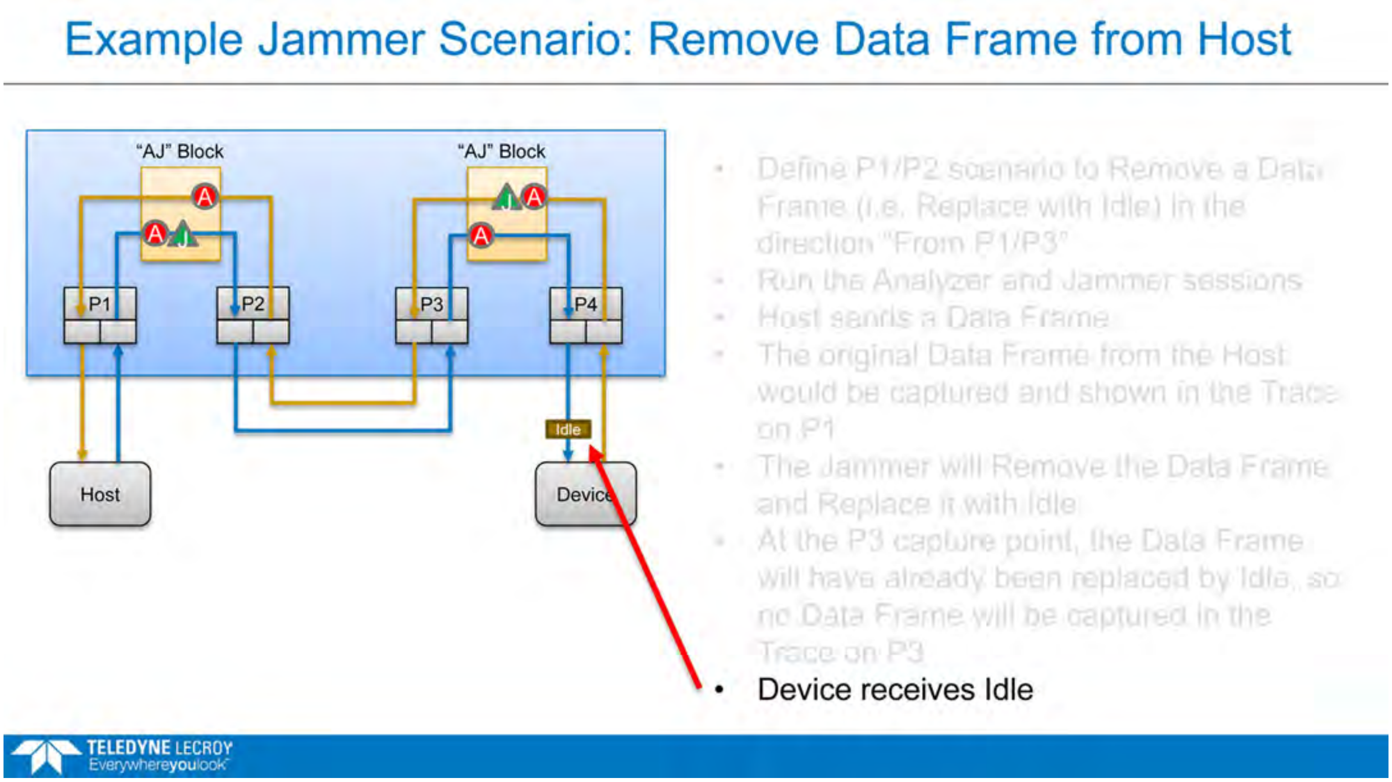
TELEDYNE LECROY
Everywhereyoulook

Example Jammer Scenario: Remove Data Frame from Host



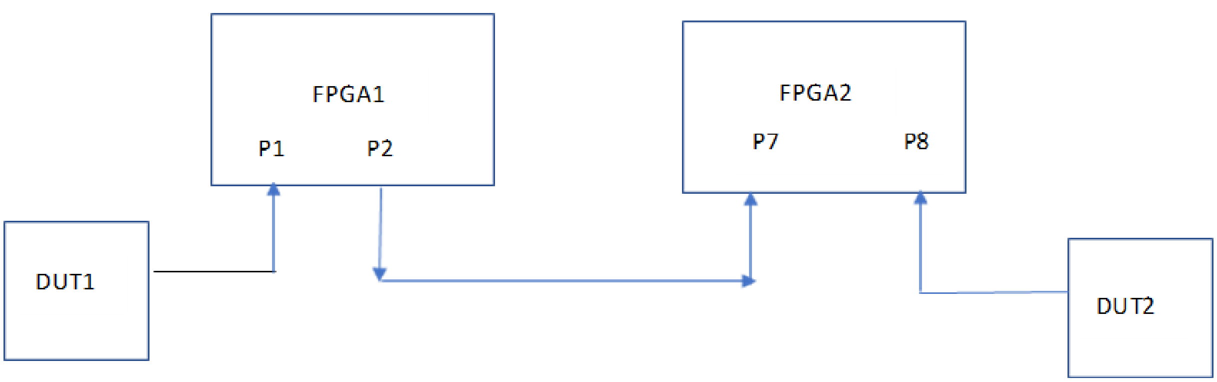
- Define P1/P2 scenario to Remove a Data Frame (i.e. Replace with Idle) in the direction "From P1/P3"
- Run the Analyzer and Jammer sessions
- Host sends a Data Frame
- The original Data Frame from the Host would be captured and shown in the Trace on P1
- The Jammer will Remove the Data Frame and Replace it with Idle
- At the P3 capture point, the Data Frame will have already been replaced by Idle, so no Data Frame will be captured in the Trace on P3
- Device receives Idle

TELEDYNE LECROY
Everywhereyoulook



AJA on the SierraNet M648 SFP Ports

AJA port configuration on the M648 SFP ports requires a special cabling solution, where the output of the Jammer will be looped back to the APT ports on the other hemisphere, as follows:



In the above figure, you can see that both P8 and P2 are receiving the same traffic as FPGA2 is just APT, essentially passing a duplicate copy of the traffic it sees to P2. To avoid showing the same traffic on multiple ports, P8 is filtered out by default, so that only the Jammed traffic is seen.

Appendix D

Supported Protocol Decoders

The Net Protocol Suite supports the following list of Protocols **and** Specifications:

Table D.1: Supported Protocols and Specifications (Sheet 1 of 4)

Protocol	Specification Name
AL	FC-AL-2 Rev 7.0
ARP	RFC 826
Auto Negotiation	IEEE 802.3 2018
AV	FC-AV ANSI+INCITS+356-2002+(R2007)
AVB	IEEE 802.1BA
AVTP	IEEE 1722-2011
BGP	RFC 4271
CN Tag	IEEE 802.1Qau-2010
ELS	FC-LS-5
Ethernet	IEEE 802.3 2018
Ethernet Training Sequence	IEEE 802.3 2018
FC	FC-FS-6
FC AE 1553	FC-AEP Rev 1.3
FC AE ASM	ISO/IEC JTC 1 N8556
FC Training Sequence	FC-FS-6
FC64 Marker	FC-FS-6
FCIP	RFC 3821
FCoE	FC-BB-5
FCP IU	FCP-4
FICON	FC-SB-3
FIP	FC-BB-5
GARP	IEEE 802.1Q-2005
IEEE 1588v2 PTP	IEEE1588-2018
GS	FC-GS-8
ICMP	RFC 792

Table D.1: Supported Protocols and Specifications (Sheet 2 of 4)

Protocol	Specification Name
IFCP	RFC 4172
IGMP	RFC 3376
IP v4	RFC 791
IP v6	RFC 2460
iSCSI	RFC 3720
iSER	RFC 7145
iSER over iWARP	draft-ko-iwarp-iser-v1.0
iSER over RoCE/RoCE v2	InfiniBandTM Architecture Specification Volume 1 Release 1.2.1
ISL	IEEE 802.1Q
ISNS	RFC 4171
iWARP	RFC 5040
iWARP	RFC 5041
LDP	RFC 5036
Link Aggregation	IEEE 802.3 2018
LLC	IEEE 802.2-1998
LLDP	IEEE 802.1AB-2005
LLDP	IEEE 802.1Qaz-2011
MAD	InfiniBandTM Architecture Specification Volume 1 Release 1.2.1
MPA	RFC 5044
MPCP	IEEE 802.1D-2004
MPLS	RFC 3031
MSTP	IEEE 802.1Q-2005
NBDS1	RFC 1002
NBDS2	RFC 1002
NBNS	RFC 1001,1002
NVGRE, GRE	RFC 2784
NVMe	NVM Express 1.4
NVMe	NVM Express 1.4 ECN
NVMe	NVMe – TP 4003b IO Determinism
NVMe	NVMe – TP 4016 Rebuild Assist
NVMe	NVMe – TP 4018a NVM Sets and Read Recovery Level
NVMe	NVMe – TP 4024 Traffic Based Keep Alive
NVMe	NVMe – TP 4030 Verify Command
NVMe	NVMe – TP 4032 PMR Write Elasticity Status
NVMe	NVMe – TP 4033 Enhanced Command Retry

Table D.1: Supported Protocols and Specifications (Sheet 3 of 4)

Protocol	Specification Name
NVMe	NVMe – TP 4004a ANA Base Protocol
NVMe	NVMe – TP 4004b ANA Base Protocol
NVMe	NVMe – TP 4005b Namespace Write Protect
NVMe	NVMe – TP 4005c Namespace Write Protect
NVMe	NVMe – TP 4007a Persistent Event Log
NVMe	NVMe – TP 4014 Sanitize Enhancements
NVMe	NVMe – TP 4025 IO Performance and Endurance Hints
NVMe	NVMe – TP 4027 UUIDs for VS Information
NVMe	NVMe – TP 4028a Path and Transport Error Enhancements
NVMe	NVMe – TP 4031a Shared Stream Write
NVMe	NVMe – TP 4039a Administrative Controller
NVMe	NVMe – TP 4039 Administrative Controller
NVMe	NVMe – TP 4042 Further Persistent Event Log Events
NVMe	NVMe – TP 4028a Path and Transport Error Enhancements
NVMe	NVMe – TP 4051 CMB Extensions
NVMe MI	NVM – Express-Management-Interface-1.1-Ratified NVMe – MI – TP 6010 Command Initiated Auto Pause 2019.06.24 – Ratified
NVMe over TCP	NVMe – TP 8000 TCP Transport
NVMe over Fabrics	NVMe – TP 8002 Resource Enumeration and State Change Announcements
NVMe over Fabrics	NVMe – TP 8005 Fabric SQ Flow Control
NVMe v2	NVMe – TP 8010 NVMe-oF Centralized Discovery Controller
FC-NVMe	FC – NVMe 1.19
FC-NVMe-2	T11 – 2019-00044-v000 Rev 1.04
NVMe	NVMe-over-Fabrics-1.1-2019.10.22-Ratified
NVMe over iWarp	NVMe over Fabrics 1.0a
NVMe over RoCE/RoCEv2	NVMe over Fabrics 1.0a
NVMe v2	NVM – Express-Base-Specification-2_0
NVMe v2	NVM – Express-Key-Value-Command-Set
NVMe v2	NVM – Express-NVM-Command-Set
NVMe v2	NVM – Express-Zoned-Namespace-Command-Set
OSPF	RFC 2328
Pause	IEEE 802.3 2018
RARP	RFC 903

Table D.1: Supported Protocols and Specifications (Sheet 4 of 4)

Protocol	Specification Name
RoCE	InfiniBandTM Architecture Specification Volume 1 Release 1.2.1
RoCE v2	InfiniBandTM Architecture Specification Volume 1 Release 1.2.1
SCSI-ADC	ADC-4
SCSI-MMC	MMC-6
SCSI-OSD	OSD-2
SCSI-SBC	SBC-4
SCSI-SMC	SMC-3
SCSI-SPC	SPC-5
SCSI-SSC	SSC-5
SMB 1	MS-CIFS
SMB 1	MS-SMB
SMB 2 , SMB 3	MS-SMB2
SMB Direct	MS-SMBD
SMB over iWARP	MS-SMBD
SMB over RoCE/RoCE v2	MS-SMBD
SMB over TCP/UDP	MS-SMBD
SNAP	IEEE 802-2001[1]
STP	IEEE 802.1D-2004
SW	FC-SW-5
TCP	RFC 793
Trill	RBridges: Base Protocol Specification
UDP	RFC 768
VI	FC-VI ANSI+INCITS+357-2002+(R2007)
VLAN	IEEE 802.1Q
VN tag	IEEE 802.1Qbh
VXLAN	RFC 7348

Appendix E

Logical Fields

The Net Protocol Suite supports the following list of Logical Fields:

TABLE E.1: Logical Fields (Sheet 1 of 3)

Logical Field name	Description
Analyzer speed	Traffic speed on the Port. This specifies the bit rate of the item (1G, 2G, 4G, 8G, 10G, 16G, 25G, 32G, 40G, 50G, 100G).
Brief	The transport function names listed in an exchange
Command Status	The status of the packet if the packet is a command, such as reject or complete. For example, specifies SCSI command status (Good, Check condition, …).
Count	The number of repeated order items. This specifies the number of instances for items with a repeated count (AN, Training, Ordered Sets).
Current State	Specifies the analyzer sequencer state number at the time the item was captured.
Data Length	The length of the data in the frame, if it is a data frame, such as FCP Data frames. This specifies the length of the data payload in byte For frame items.
Duration Time	The amount of time it takes to receive all of the data of the item. Time is specified in nanoseconds.
Ethernet Frame	Value if this field is “Ethernet” for Ethernet frames and is Null for other frames.
Ethernet Tag	The Tag name of the frame such as VXLAN. It shows string of Ethernet tags (if any), otherwise is null. Ethernet tags can be “ISL”, “VXLAN”, “GRE”, “NVGRE”.
EVPD	The “EVPD” field value in an inquiry SCSI command frame. This is “EVPD=True”, if the EVPD in SCSI Inquiry bit is 1; otherwise, it is null.
Exchange Status	The exchange status for each command. This specifies the exchange status in general. The exchange status can be one of the following values: 0x2: Success; 0x0x1: Fail; 0x0: Incomplete.
FC Frame	Link protocol name such as FC. It is “FC” for FC frames; otherwise, it is null.

TABLE E.1: Logical Fields (Sheet 2 of 3)

Logical Field name	Description
FEC Status	The FEC status of the frame. This is “BASE-R FEC” for FEC 2112, and “Reed-Solomon FEC” for Reed Solomon FEC; otherwise, it is null.
FICON Non-Zero status flags	FICON status flag values. ◆ This is a string that shows the name of flags that are on (value is 1) the status flag of the FICON frame; otherwise, it is null. This field is applicable only for FICON frames. ◆ Status flags are “FFC”, “CI”, “CR”, “LRI”, and “RV”.
Fragment Offset	Displays the “offset” field value in the IP header. The IP “Fragment Offset” field is expressed in bytes.
Jammer Port Name	Jammer Port Name. This field is applicable to the AJA port configuration. It is “Before Jam” for frames that were captured before the jamming action; it is “After Jam” for frames that were captured after jamming.
Lane No	The Lane number of the item. It specifies the physical lane number for link training items at 40/50/100G.
Latency	The time between the first frame of the exchange and the last frame of the exchange. ◆ This value is valid for first frame of an exchange; it is not applicable for other frames of the exchange. ◆ The latency time of an exchange is expressed in nanoseconds.
Link Function Name	Link Function name. This is a string that includes a decoded abstract of item and shows Protocol and/or Frame type.
Link Service	Basic link ABTS type & Link ACK. ◆ This is applicable for FC Basic link service and the Link control frame. ◆ It specifies a string that shows the Basic Link Service/Link control frame plus its type. For example, “Basic Link Service-ABTS”.
Marker	Bookmark name of the item. This is an editable field shows marker name (if any) for an item.
Markers Count	The “Markers count” value for each frame.
Packet Length	The actual length of the packet. ◆ The frame length is expressed in bytes. ◆ If the item is not a frame, it is 0.
Pending Commands	The number of commands waiting to complete the exchange. This specifies the number of pending exchanges. It is an application of the first and last frame of each exchange. For other frames of the exchange, it is null (0).
Port	The port label of the analyzer (the physical port number).

TABLE E.1: Logical Fields (Sheet 3 of 3)

Logical Field name	Description
Preset Status	The preset status in training sequence frames. This is a decoded string for an Ethernet training sequence preset response. The decoded value is “Updated” or “Not Updated”.
Protocol Type	Ethernet or Fibre channel. This is “Ethernet” for Ethernet items and “FC” for FC items.
Response Time	Time between the command and response in an exchange. ◆ This specifies the response time of an exchange in nanoseconds. ◆ It is applicable for first frame of each exchange.; it is null (0) for other frames of the exchange.
Run Date	The Date the trace was captured. It specifies Date/Time that an item was captured.
Start Time	Time stamp of the item. It specifies start time.
Start/Stop	It is applicable only for SCSI Start/Sop Unit command and is a string decoded value for Start/Stop bit. If this bit is 1, decoded value is “START”, otherwise is “STOP”
TCP bits	TCP special bit values such as ACK, RST. ◆ This is a decoded string value for the following TCP frame bits: RESET, NS, SYNC, FINISH, CWR, ECE, URGENT, ACK, and PUSH. ◆ If any of above bits is 1, decoded string contains [name], for example if SYNC and ACK are 1, the decoded value is [SYN], [ACK].
TCP Payload Length	TCP Payload length of the packet if the frame is TCP. The TCP frame payload length is expressed in bytes.
Throughput	The total number of transferred bytes of an exchange divided by the duration of the exchange. In MB/s.
Time Delta	Delta time between current item and previous row. This specifies the start time difference between each item and the previous item.
Training sequence explanation	Explanation for training sequence frames. This is a decoded string for training sequence items.
Transport function name	The transport function name of the packet, if any. This is a string, including a decoded abstract of the item, depending on frame type; it contains decoded string of major field in the frame.

Appendix F

SierraNet Cabling Guide

When using the SierraNet platforms in your link or fabric under test, consideration of interconnect options is needed for maintaining signal integrity and link budget characteristics for the given speed(s) and limitations of the DUT(s).

The SierraNet platforms ship with a variety of cables to facilitate out of the box interoperability and ease of use. Furthermore, the SierraNet is tested for use with various other DAC and Optical interconnect solutions. As new interconnect solutions are available and tested with these platforms, this document will be updated accordingly.

A list of the interconnects and their application is provided here.

Ethernet DAC assemblies tested for use with SierraNet M328/T328/M328Q:

TABLE F.1: Ethernet DAC Assemblies Tested for Use with SierraNet M328/T328/M328Q (Sheet 1 of 3)

Cable Assembly	Manufacturer	Part Number (Gauge)	Description	Supported Rates	Comments
	Amphenol ICC	NDAQGF-T211 (30 AWG) (TDY OEM version of NDAQGF-0001)	1M QSFP to 4xSFP Copper Splitter Cable Assembly	1x10/25GbE, 2x10/25GbE, 4x10/25GbE, 1x50GbE (2x25G), 100GbE (4x25GbE), 100GbE (2x50GbE),	This assembly supports connection of the SierraNet M/T 328 platforms to a QSFP port on a device/link under test. This cable may be used to examine 1x, 2x, or 4x of a specific speed (i.e., 25GbE x1 lane, 2 lanes, etc.) and it may be used to examine aggregated lanes, (i.e., 2x25GbE for 50GbE, 4x25GbE for 100GbE) in the noted SierraNet platforms where a direct QSFP connection is unavailable

TABLE F.1: Ethernet DAC Assemblies Tested for Use with SierraNet M328/T328/M328Q (Sheet 2 of 3)

Cable Assembly	Manufacturer	Part Number (Gauge)	Description	Supported Rates	Comments
DAC Assemblies Tested for use with SierraNet M328/T328					
	Amphenol ICC	NDAQGJ-0003 (26 AWG)	3M QSFP to 4xSFP Copper Splitter Cable Assembly	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE, 1x50GbE (2x25G), 100GbE (4x25GbE), 100GbE (2x50GbE), 200GbE (4x50GbE)	Recommended for use in one leg only of a connection to the SierraNet
	Amphenol ICC	NDCCGF-0001 (30 AWG)	1M SFP to SFP Copper Cable	1x10/25/50GbE	
	Amphenol ICC	NDCCGF-0003 (30 AWG)	2M SFP to SFP Copper Cable	1x10/25/50GbE	

TABLE F.1: Ethernet DAC Assemblies Tested for Use with SierraNet M328/T328/M328Q (Sheet 3 of 3)

Cable Assembly	Manufacturer	Part Number (Gauge)	Description	Supported Rates	Comments
DAC Assemblies Tested for use with SierraNet M328Q					
	Amphenol ICC	NDAAFF0001 (30 AWG)	1M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	
	Amphenol ICC	NDAAFF0002 (30 AWG)	2M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	
	Amphenol ICC	NDAAFF0003 (30 AWG)	3M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	Recommended for use in one leg only of a connection to the SierraNet

TABLE F.2: DAC Assemblies Supplied and Tested with SierraNet M648 (Sheet 1 of 2)

DAC Assembly	Manufacturer	Part Number (Gauge)	Description	Supported Rates	Comments
	Amphenol ICC	NDAQGF-T211 (30 AWG) (TDY OEM version of NDAQGF-0001)	1M QSFP to 4xSFP Copper Splitter Cable Assembly	1x10/25/50GbE, 2x10/25/50GbE, 4x10/25GbE, 1x50GbE (2x25G), 100GbE (2x50G, 100GbE (4x25GbE), 200GbE (4x50GbE)	This assembly supports connection of the SierraNet M/T 328 platforms to a QSFP port on a device/link under test. This cable may be used to examine 1x, 2x, or 4x of a specific speed (i.e., 25GbE x1 lane, 2 lanes, etc.) and it may be used to examine aggregated lanes, (i.e., 2x25GbE for 50GbE, 4x25GbE for 100GbE) in the noted SierraNet platforms where a direct QSFP connection is unavailable
	Amphenol ICC	NDCCGF-0001 (30 AWG)	1M SFP to SFP Copper Cable	1x10/25/50GbE	
	NE Electronics	CA-PA-.5SFP56 (28AWG)	0.5M SFP to SFP Copper Cable	1x10/25/50GbE 1/16/32/64GFC	
	NE Electronics	CA-PA-1.8SFP (30AWG)	1.5M QSFP to 8xSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	4x lane limitation due to SierraNet M648 physical and logical connection capabilities.

TABLE F.2: DAC Assemblies Supplied and Tested with SierraNet M648 (Sheet 2 of 2)

DAC Assembly	Manufacturer	Part Number (Gauge)	Description	Supported Rates	Comments
DAC Assemblies Tested for use with SierraNet M648					
	Amphenol ICC	NDAQGJ-0003 (26 AWG)	3M QSFP to 4xSFP Copper Splitter Cable Assembly	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	Recommended for use in one leg only of a connection to the SierraNet
	Amphenol ICC	NDCCGF-0001 (30 AWG)	1M SFP to SFP Copper Cable	1x10/25/50GbE	
	Amphenol ICC	NDCCGF-0003 (30 AWG)	2M SFP to SFP Copper Cable	1x10/25/50GbE	
	Amphenol ICC	NDAAFF0001 (30 AWG)	1M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	
	Amphenol ICC	NDAAFF0002 (30 AWG)	2M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	
	Amphenol ICC	NDAAFF0003 (30 AWG)	3M QSFP to QSFP Copper Cable	1x10/25/50GbE 2x10/25/50GbE 4x10/25/50GbE 100GbE (4x25GbE) 100GbE (2x50GbE) 200GbE (4x50GbE)	Recommended for use in one leg only of a connection to the SierraNet

A list of the Optical Transceivers **tested for use** with the SierraNet Platforms and their application is provided here.

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 1 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
SierraNet T/M328 Fibre Channel Optics					
	Finisar	FTLF8524P2BNL	SFP+	Tri-Rate 2/4/8GFC	Multi-Mode 850nm
	Finisar/ Qlogic/ HP	FTLF8528P2BCV -QL -1H	SFP+	Tri-Rate 2/4/8GFC	Multi-Mode 850nm
	Finisar/ Emulex	FTLF8528P2BNV -EM	SFP+	Tri-Rate 2/4/8GFC	Multi-Mode 850nm
	Finisar	FTLF8528P3BCV	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar	FTLF8528P3BNV	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar/ Qlogic/ HP	FTLF8529P3BCV -QL -1H	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar	FTLF8532P4BCV	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Finisar	FTLF1432P3BCV	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm
	Cisco	DS-SFP16G-SW 10-2666-01	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Cisco	DS-SFP32G-SW 10-3206-01	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Cisco	DS-SFP-FC32G-LW 10-3207-01	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm, AKA: SFP28-32GLR-31 CISCO-INNOLIGHT PN: TR-PB13L-NCI, CISCO-FINISAR PN: FTLF1432P3BCV-C2 CISCO-FINISAR PN: FTLF1432P3BCV-C3
	Brocade	57-1000333-01	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Brocade	57-1000332-01	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 2 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
	Brocade	57-1000117-01	SFP	8GFC	Multi-Mode 850nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 3 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
SierraNet T/M328 Ethernet Optics					
	Finisar	FTLF8536P4BCV	SFP28	25GbE 10GbE	Multi-Mode 850nm
	Brocade	57-0000075-01	SFP+	10GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-703SDZ	SFP+	10GbE	Multi-Mode 850nm
SierraNet M328Q Fibre Channel Optics					
	Finisar	FTLC9555SEPM	QSFP28	128GFC 4x28Gb/s OTN	Multi-Mode 850nm
	Finisar	FTLC9551SEPM	QSFP28	128GFC 4x28Gb/s OTN	Multi-Mode 850nm
SierraNet M328Q: Ethernet Optics					
	Finisar	FTLC9555SEPM	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Finisar	FTLC9551SEPM	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Finisar	FTL410QE1C	QSFP+	40G SR4 4x10GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-79E4Z-D	QSFP+	40G SR4 4x10GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-89CDDZ	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Cisco	10-3142-01	QSFP+	100GBASE-SR4 4x25GbE	Om4 Mmf
	NVIDIA Mellanox	MMA1B00-C100D	QSFP28	100GBASE-SR4 40G SR4	Multi-Mode 850nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 4 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
SierraNet M648 Fibre Channel Optics					
	Broadcom/ Avago	AFBR-57H5MZ	SFP56	Tri-Rate 16/32/64GFC	Multi-Mode 850nm
	Brocade	57-1000333-01	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Brocade	57-1000332-01	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm
	Brocade	57-1000495-01	SFP+	Tri-Rate 16/32/64GFC	Multi-Mode 850nm
	Cisco	DS-SFP32G-SW 10-3206-01	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Cisco	DS-SFP-FC32G-LW 10-3207-01	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm, AKA: SFP28-32GLR-31 CISCO-INNOLIGHT PN:TR-PB13L-NCI, CISCO-FINISAR PN:FTLF1432P3BCV-C2 CISCO-FINISAR PN:FTLF1432P3BCV-C3
	Cisco	DS-SFP-FC64G-SW	SFP+	Tri-Rate 16/32/64GFC	Multi-Mode 850nm
	Finisar	FTLF8528P3BCV	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar	FTLF8528P3BNV	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar/ Qlogic/ HP	FTLF8529P3BCV -QL -1H	SFP+	Tri-Rate 4/8/16GFC	Multi-Mode 850nm
	Finisar / Qlogic / Emulex	FTLF8532P4BCV -QL -EM	SFP28	Tri-Rate 8/16/32GFC	Multi-Mode 850nm
	Finisar/ Qlogic/ Emulex	FTLF1432P3BCV -QL -EM	SFP28	Tri-Rate 8/16/32GFC	Single-Mode 1310nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 5 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
	Finisar	FTLC9555SEPM	QSFP28	128GFC 4x28Gb/s OTN	Multi-Mode 850nm
	Finisar	FTLC9551SEPM	QSFP28	128GFC 4x28Gb/s OTN	Multi-Mode 850nm
	Finisar	FTLF8564D1BCW	SFP56	Tri-Rate 16/32/64GFC	Multi-Mode 850nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 6 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
SierraNet M648 Ethernet Optics					
	Broadcom/ Avago	AFBR-79EQDZ	QSFP+	40G SR4 4x10GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-79E4Z	QSFP+	40G SR4 4x10GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-89CDDZ	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Broadcom/ Avago	AFBR-703SDZ	SFP+	10GbE	Multi-Mode 850nm
	Broadcom/ Avago /Intel	AFBR-703SDZ-IN2	SFP+	10GbE	Multi-Mode 850nm
	Brocade	57-0000075-01	SFP+	10GbE	Multi-Mode 850nm
	Cisco	10-2415-02	SFP	10GbE	Multi-Mode 850nm
	Cisco	10-3142-01	QSFP+	100GBASE-SR4 4x25GbE	Om4 Mmf
	Finisar	FTLX8571D3BCL	SFP+	10GbE	Multi-Mode 850nm
	Finisar	FTLF8536P4BCL	SFP+	25GbE	Multi-Mode 850nm
	Finisar	FTLF8536P4BCV	SFP28	25GbE 10GbE	Multi-Mode 850nm
	Finisar	FTLC9555SEPM	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Finisar	FTL410QE1C	QSFP+	40G SR4 4x10GbE	Multi-Mode 850nm
	Finisar	FTLC9551SEPM	QSFP28	100GBASE-SR4 4x25GbE	Multi-Mode 850nm
	Finisar/Intel	FTLX8571D3BCV- IT	SFP+	10GbE	Multi-Mode 850nm
	NVIDIA Mellanox	MMA1B00-C100D	QSFP28	100GBASE-SR4 40G SR4	Multi-Mode 850nm

TABLE F.3: Optical Transceivers Tested for use with SierraNet Platforms (Sheet 7 of 7)

Transceiver	Manufacturer	Part Number	Description	Supported Rates	Comments
	NVIDIA Mellanox	MMA1T00-VS	QSFP56	200GbE	Multi-Mode 850nm
	Qlogic	FTLX8571D3BCL-QL	SFP+	10GbE	Multi-Mode 850nm

Appendix G

Setting NVMe QP Port for Proper Decoding

G.1 Introduction

When decoding RoCEv2 packets either TCP RDMA or RoCE RDMA (for our subject matter), there are some decoding steps that might be necessary if a captured trace does not seem to decode correctly. When working with RoCE RDMA traces, there are two major ways that the analyzer “learns” of the information that it needs to know to decode the packets so that they are readable to the analyzer/user. The information that makes it readable to the analyzer is the NVMe QP ports. These NVMe QP ports with RoCEv2 can be read in a “natural” way during connection of the Initiator and Target that the analyzer uses to learn about the QP ports so it can decode the NVMe packets and then there are manual ways to enter these QP ports that might be necessary after connections have already taken place. When working with TCP RDMA traces, the only thing that must be present is the “NVMe/TCP ports” that usually already exist in the decoder which we will discuss further below. However, starting with release 4.40 we have made the steps for NVMe decoding much easier to ensure your trace can be decoded as an NVMe type trace or have the analyzer ready in advance to “Record” traces as NVMe traces without having to know anything about what your NVMe QP ports are. We will discuss the ease added for the release with version 4.40 decoding first and then cover the steps that must be done pre-4.40 for NVMe decoding.

G.1.1 Setting NVMe Decoding Starting with Release 4.40

Due to the complexities of ensuring every time a customer wanted to decode an NVMe trace or wanted to make sure the decoding was setup correctly no matter if the RoCE_V2-MAD packets had been captured (which was the only way we could load the decoding tables before), NVMe decoding can now be activated prior to starting a “Recording” by going to the **Setup** → **Preferences** → **SW Settings** → **Decoding Assignment** Page.

Under this page (Figure G.1), there is a setting for “QP Protocol:” with a drop down for NVMe. After this is set, all traces taken by new Recordings or old traces that are loaded are all properly decoded as NVMe traces. This takes care of all the NVMe QP port settings and thus the customer does not have to remember any frame Destination QP port hex settings, which makes it much easier.

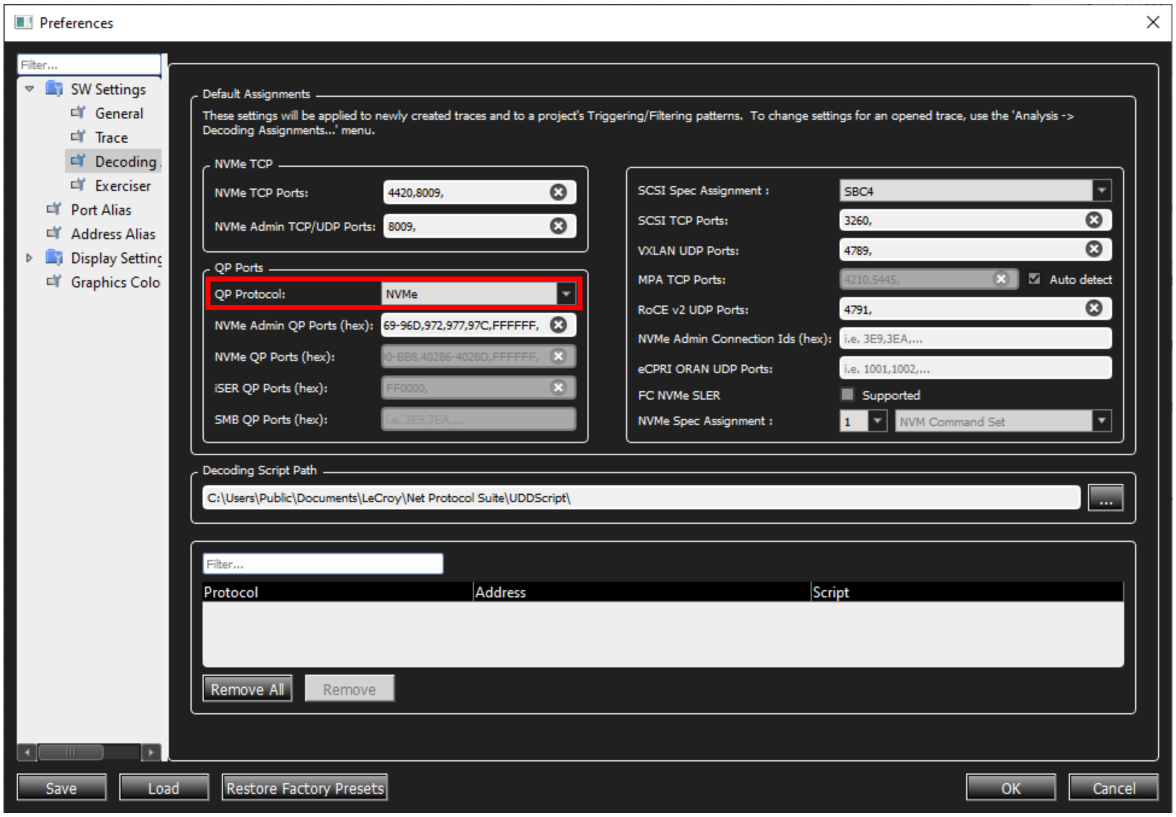


Figure G.1: Decoding Preferences

If you have already executed a “Record” and you have a RoCE Trace that you want to be decoded as an NVMe trace (and you have not already performed the steps above to set the analyzer in NVMe mode):

1. Go to the “Analysis” tab and select **Decoding Assignments**. A list will be displayed as shown in Figure G.2.
2. You must only choose NVMe within the QP Port Protocol field (highlighted below) and select the “Apply Changes to Preference” tab.

   This brings up a final message stating that the Quick View traces will be saved.
3. Select **Yes**. The Trace (and all subsequent RoCE Traces) will be decoded as NVMe Trace.

This is all that is needed to get your analyzer decoding NVMe, either prior to Recording or after Recording, starting with Release 4.40.

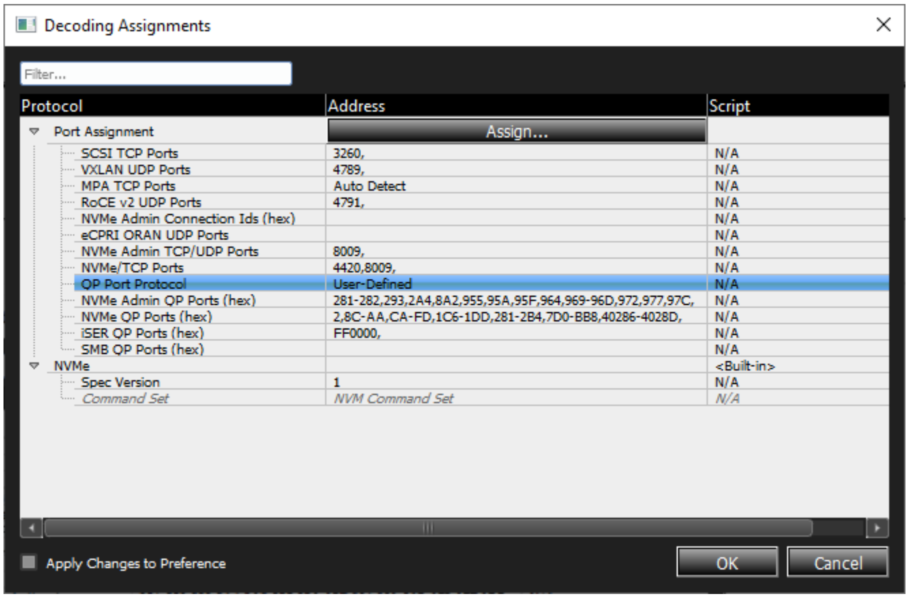


Figure G.2: Decoding Assignments List

G.1.2 Capturing a Decoded Trace Using RoCE RDMA – Pre-4.40 Releases

If the recording is started before the connection is made to the Target, this is when certain packets are exchanged that automatically load the decoding table. This makes it much easier, since all decoding is already being done as shown in Figure G.3, below.

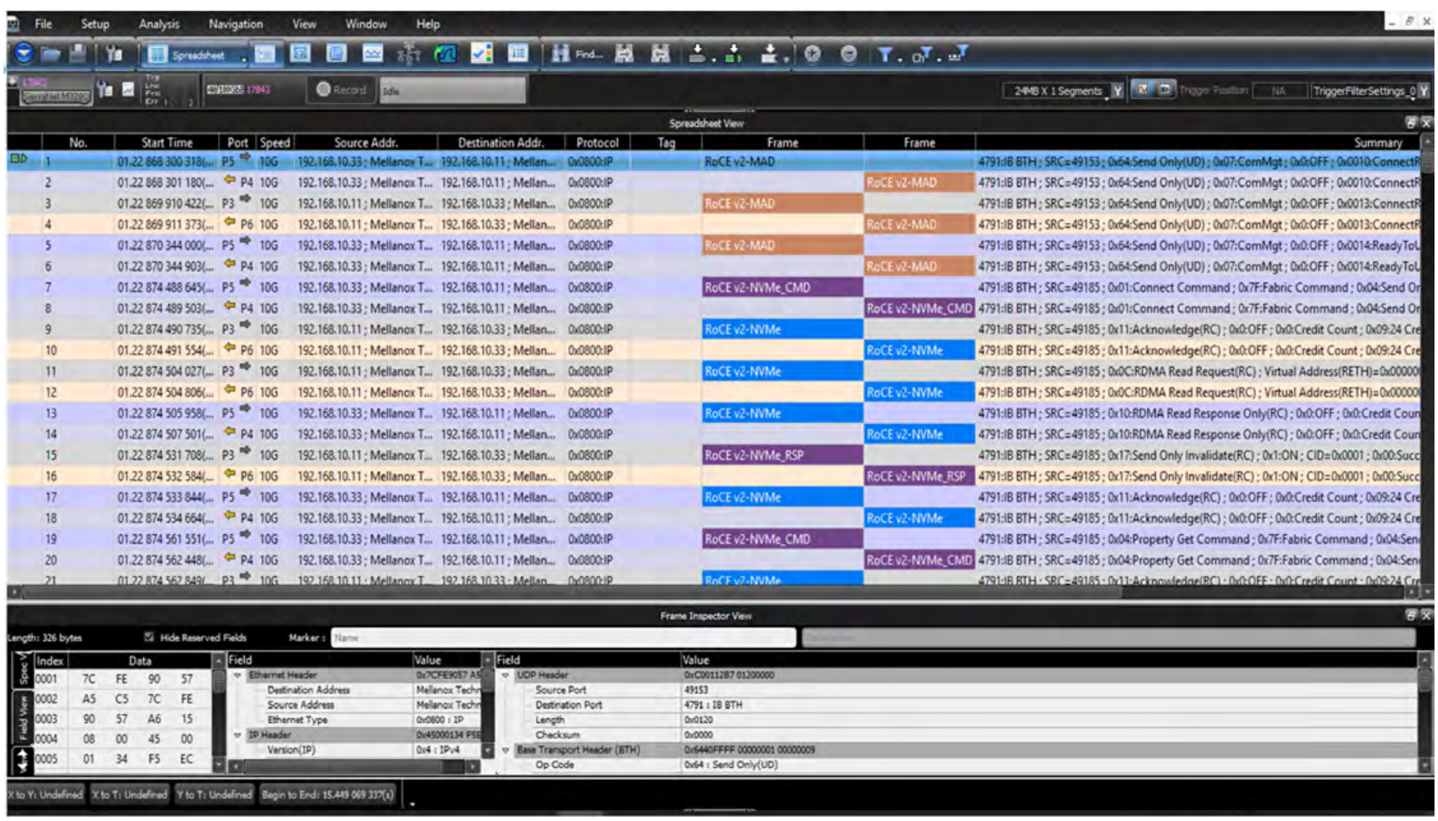


Figure G.3: Decoding Table

As you can see, the NVMe packets have been translated and correctly identified. This is because the decoding table has been prepopulated with the “NVMe/QP ports” that are necessary for all the packets to be translated. The decoding table shown in Figure G.4 contains the “NVMe QP ports” in the table after it has been automatically populated. The decoding table will be discussed further in the following sections.

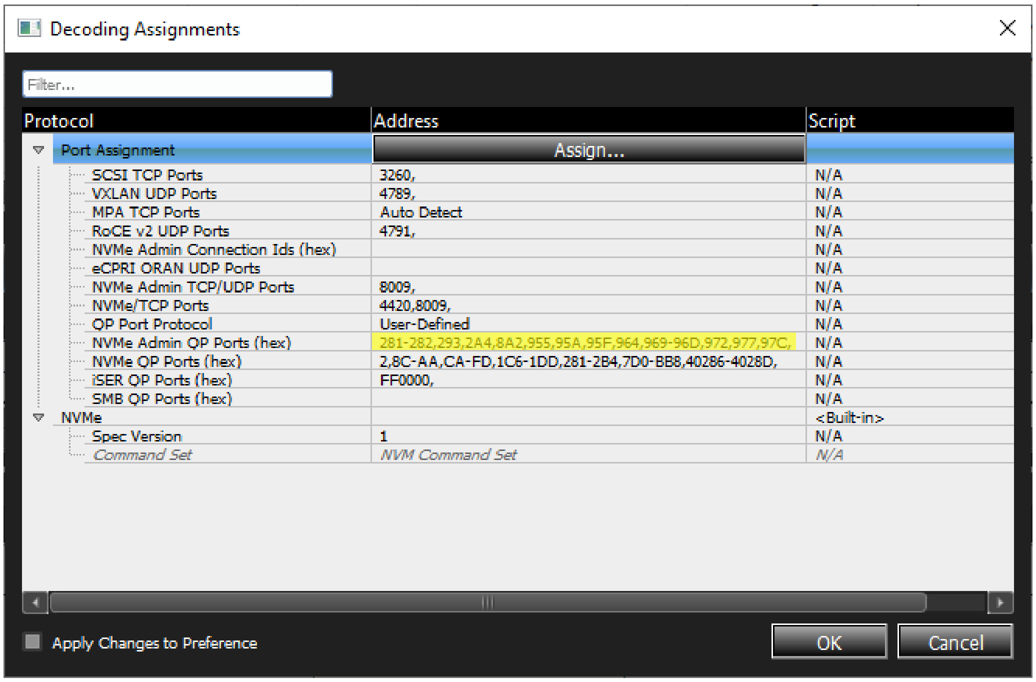


Figure G.4: Decoding Table with NVMe QP Ports

G.1.3 Capturing a Non-Decoded trace using RoCE RDMA – Pre-4.40 releases

If you have just recorded a Trace that looks like the table in Figure G.5 and when the RDMA is set to RoCE, there are steps you can take to allow this trace to show in a decoded state. Since this trace was taken after the connection sequence between Initiator and Target (missing the automatic NVMe port setup packets), the decoding must be fixed manually if packet decoding is desired.

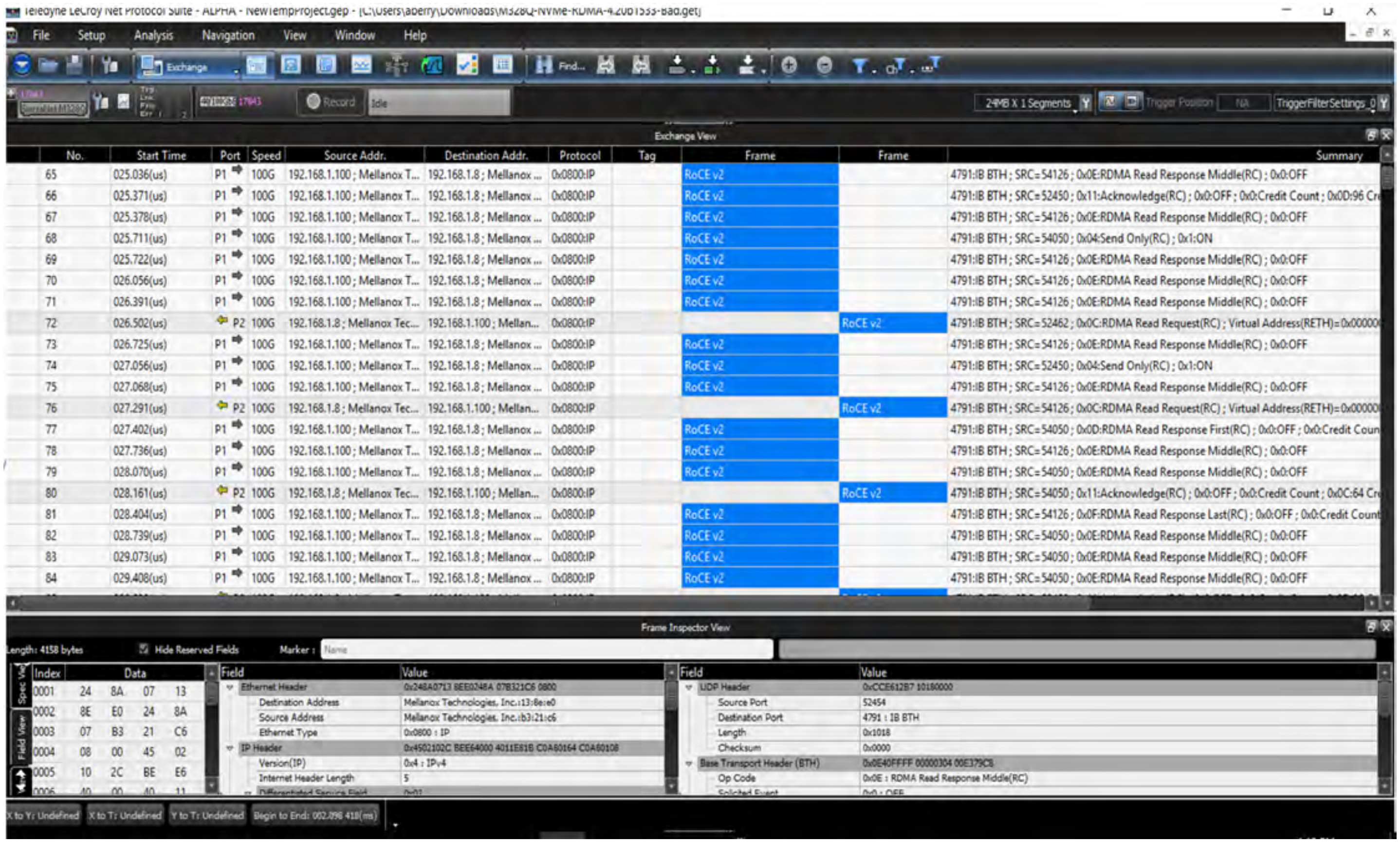


Figure G.5: Example Recorded Trace

To manually change the decoding:

1. Go to the Analysis tab and click **Decoding Assignments**. Before any “NVMe QP ports (hex)” have been learned or added, the table could look something like the example in Figure G.6.

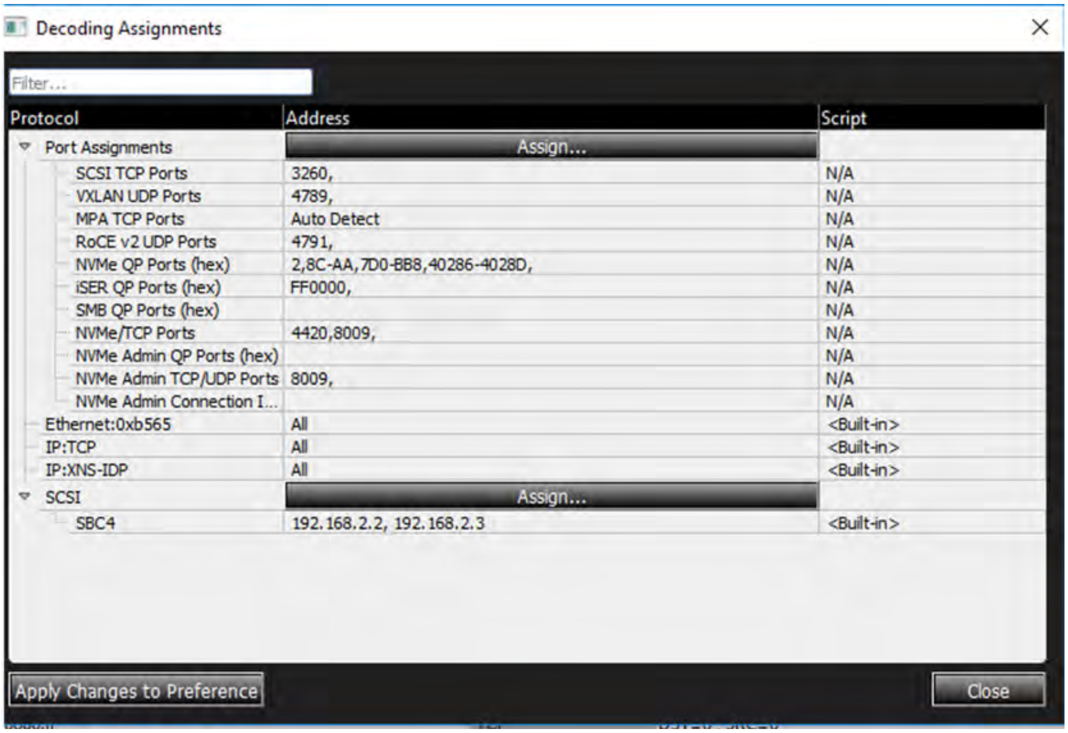


Figure G.6: Decoding Assignments Table

2. To get each packet to decode correctly, inspect (open and use the Frame Inspector View) each packet for the “Destination QP” field under the “Base Transport Header” main field as shown Figure G.7.

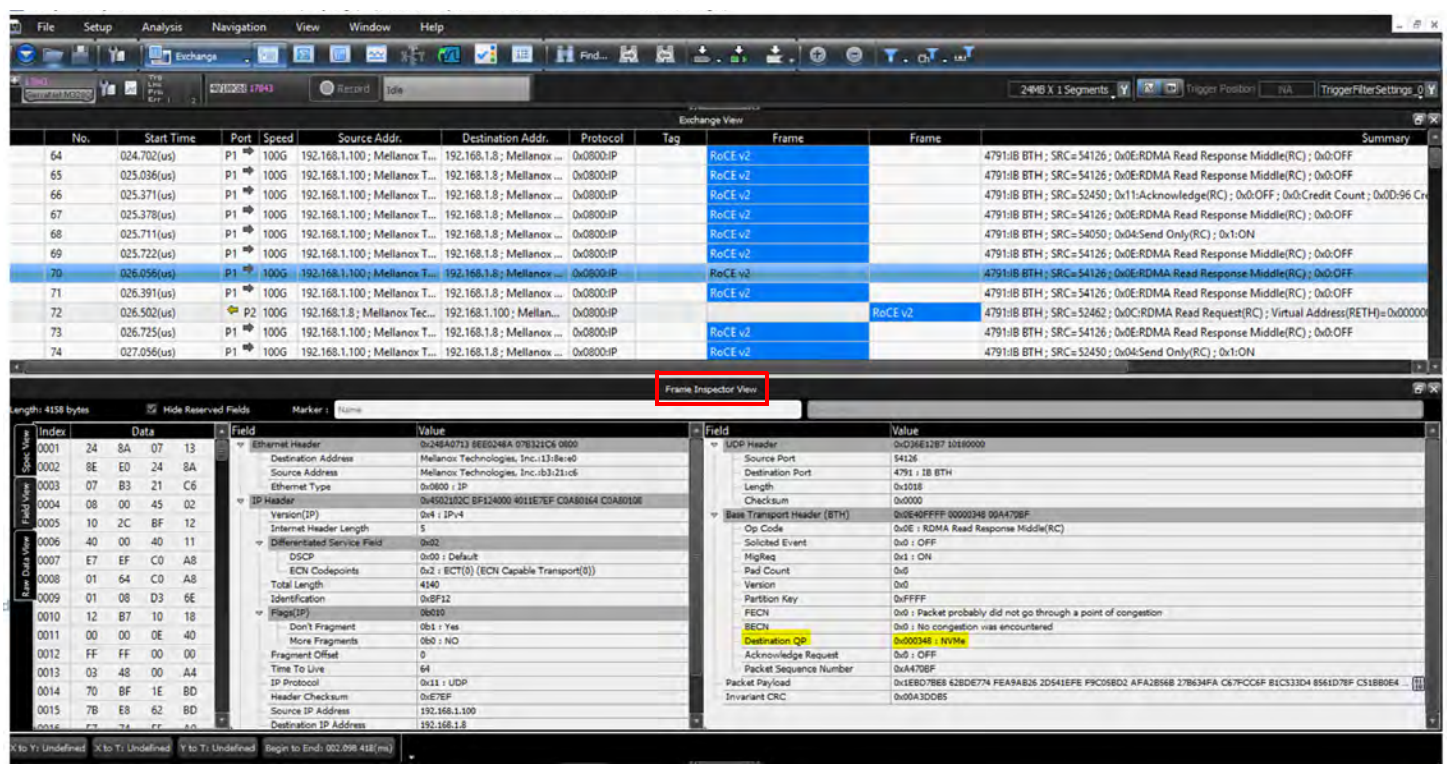


Figure G.7: Frame Inspector View

3. Make a note of the number, and return to the “Decoding Assignments” window, which is under the “Analysis” tab.
4. Add the Hex 348 to the line “NVMe QP Ports (hex)” field as shown in Figure G.8.

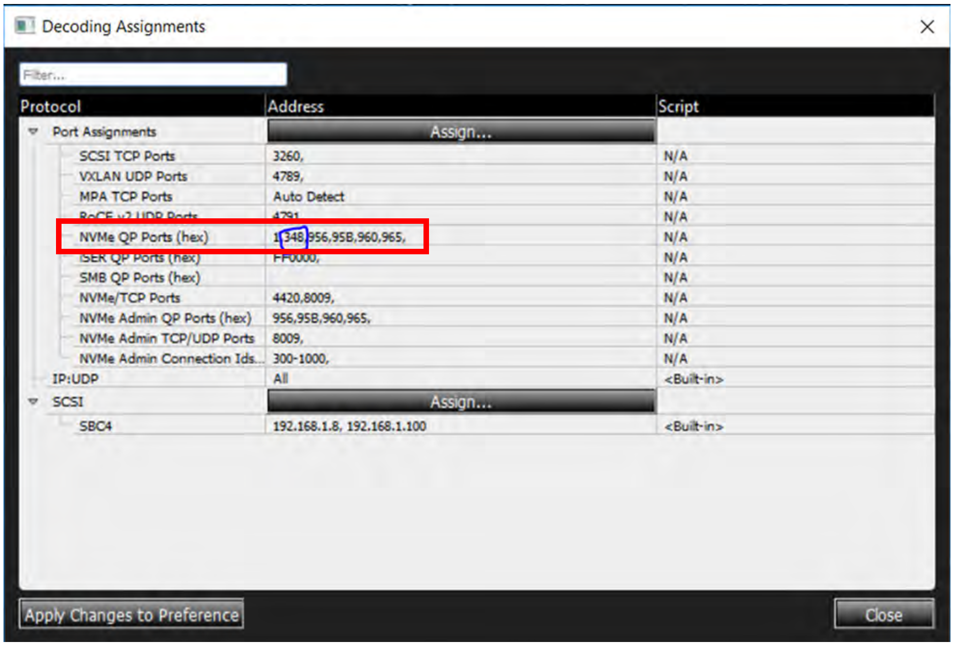


Figure G.8: Decoding Assignments Window

5. Press the **Apply Changes to Preference** button on the Decoder, then click **Close**. The analyzer adds your changes the Trace. An example of the new Trace with changes is shown in Figure G.9.

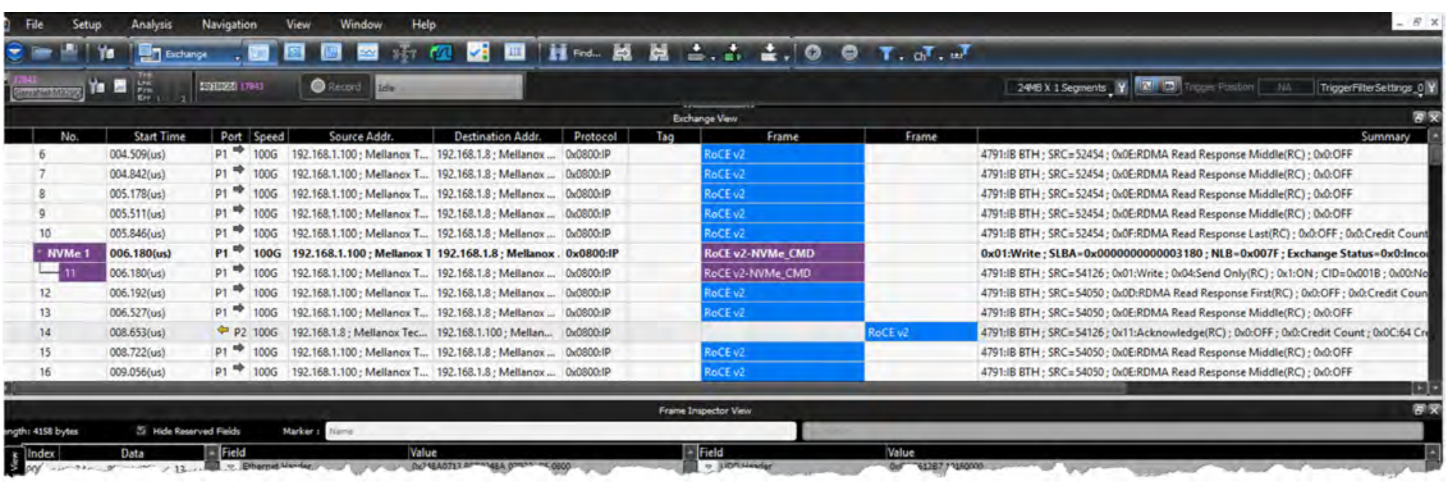


Figure G.9: Example of New Trace with Changes

- Note that it only decoded a few of the packets with that particular NVMe QP port. However, there will be some grouping of the NVMe QP ports so that you can add a large group of NVMe QP ports at one time.
- For example, this one has a NVMe Destination QP port of hex 348, but another packet has a Destination QP port of hex 304. Therefore, it is usually better to

translate many packets at once by adding a large sequence of “NVMe Destination QP ports”.

- As shown in Figure G.10, 2FF-2000 was added to accommodate a large group of NVMe QP ports so that a larger number of packets will be translated in this trace.

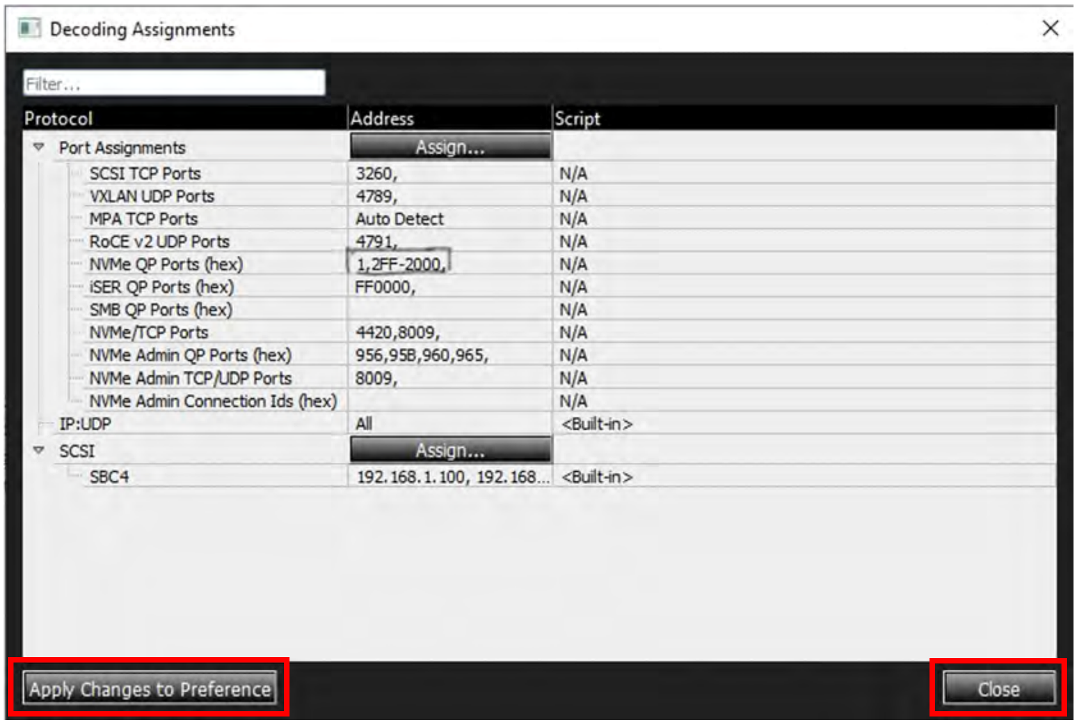


Figure G.10: Large Sequence of NVMe Destination QP Ports Added

6. Click **Apply Changes to Preference** on the Decoder, then click **Close**. The analyzer adds the changes to the Trace.
   - See Figure G.11 for an example of a new Trace with changes.

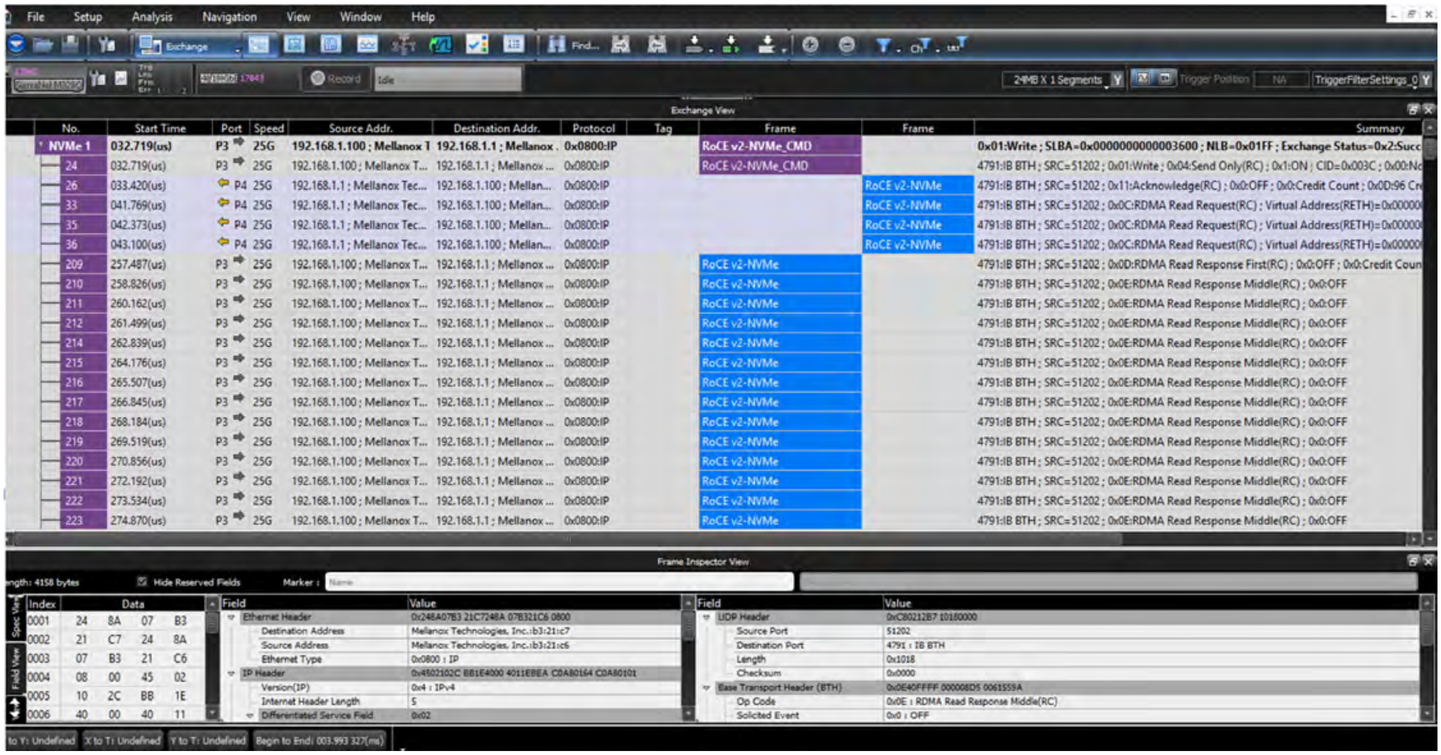


Figure G.11: Example of New Trace with Changes

- Note that most, if not all, of the RoCEv2 packets have been translated to NVMe and the analyzer shows the proper decoding.

G.1.4 Capturing a Decoded trace using TCP RDMA – Pre-4.40 releases

When using TCP with RoCEv2 the decoding is far less complex since most of the decoding depends on the “NVMe/TCP Ports” (see Figure G.12), which are usually a standard equal to 4420 used by most when connecting to the Target.

So, when the NVMe with a Source or Destination port of 4420 is seen under the TCP header, the decoding happens automatically.

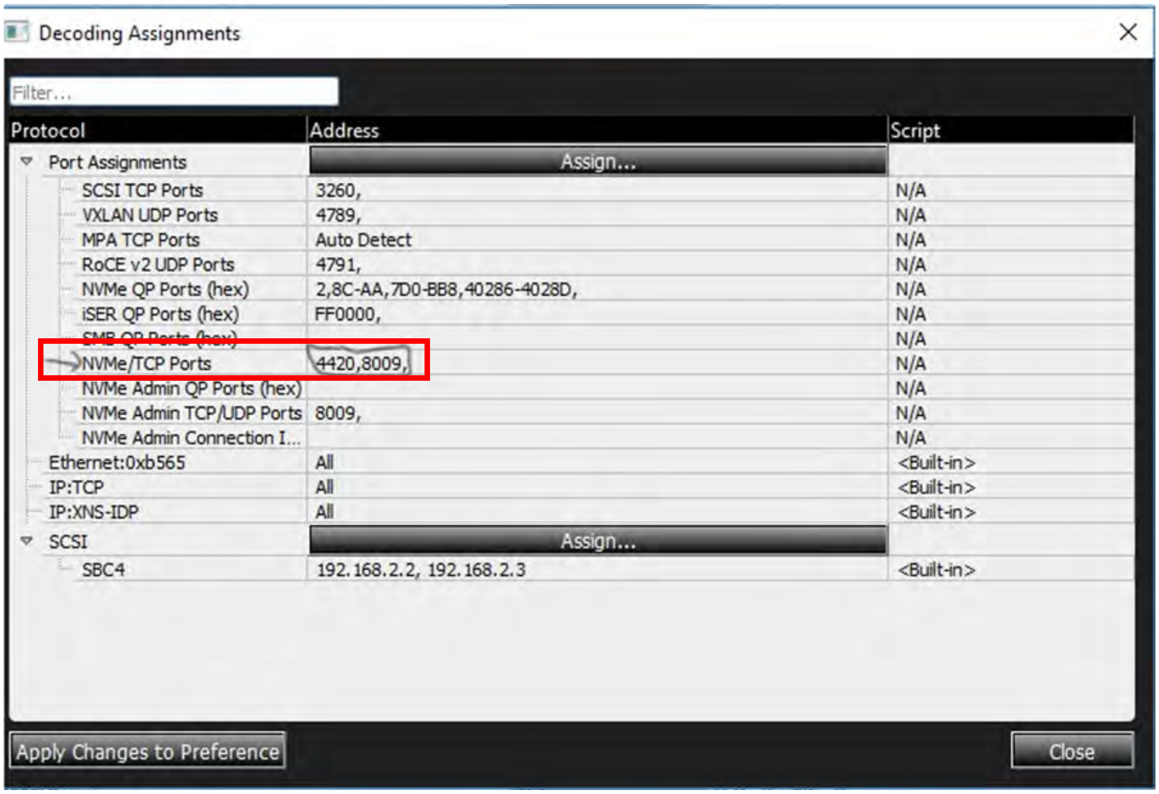


Figure G.12: Table Showing NVMe/TCP Ports

Figure G.13 shows a RoCEv2 TCP Trace that has Destination and Source ports of 4420 and thus all ports are being decoded correctly.

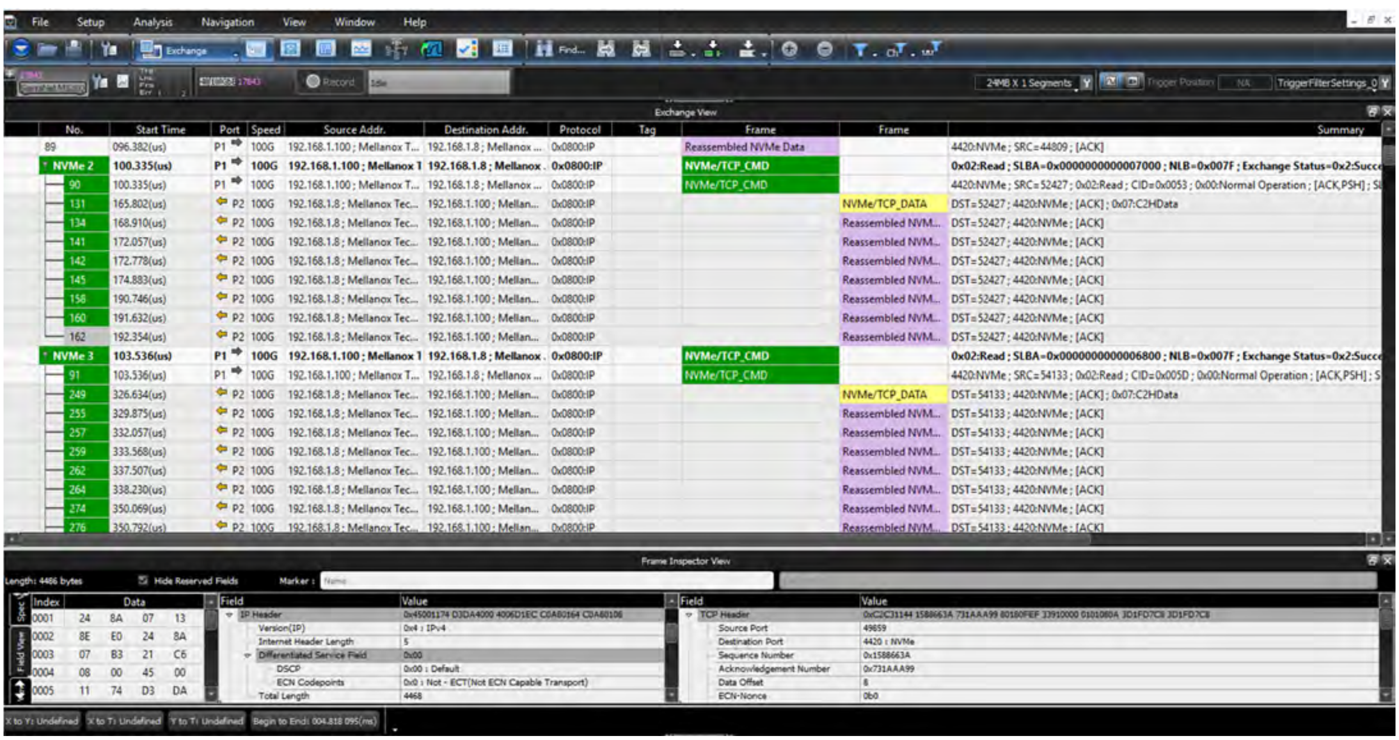


Figure G.13: Example Trace with Destination and Source Ports of 4420

G.1.5 Getting Out of NVMe Decoding Mode

There are several ways you can get out of the NVMe decoding mode, some are accidental and some are intentional.

- The accidental ways usually happen when there is a downgrade or the decoding information is manually overwritten the for some reason.

  In Pre-4.40 versions, changing or removing the HEX numbers in the decoder (the **Analysis → Decoding Assignments** page) will not allow the NVMe decoding that is taking place in the analyzer, thus removing NVMe decoding either accidentally or intentionally.

  When downgrading to an older release, the release may not support the newer 4.40 settings or may erase all decoding settings altogether for any release.

- The intentional ways to get out of NVMe mode is to unset the NVMe setting for 4.40 under the **Setup → Preferences → SW Settings → Decoding Assignment** window to another setting, such as “User-Defined”, “iSER” or “SMB”.

  Before the 4.40 release, only the NVMe QP ports must be removed from the “**Analysis → Decoding Assignments**” window (the decoder), which are important to each Trace. The NVMe decoding will not take place properly anymore.

Appendix H

Windows Server 2016 / 2019 Installation

If you are using **Windows Server** 2016/2019, the Teledyne LeCroy Net Protocol Suite Software needs to be added to the firewall exceptions to ensure that the application can find the Analyzers over your Ethernet network.

To add the Net Protocol Suite Software application to the firewall exceptions perform the following steps.

1. Open the Control Panel (Figure H.1).

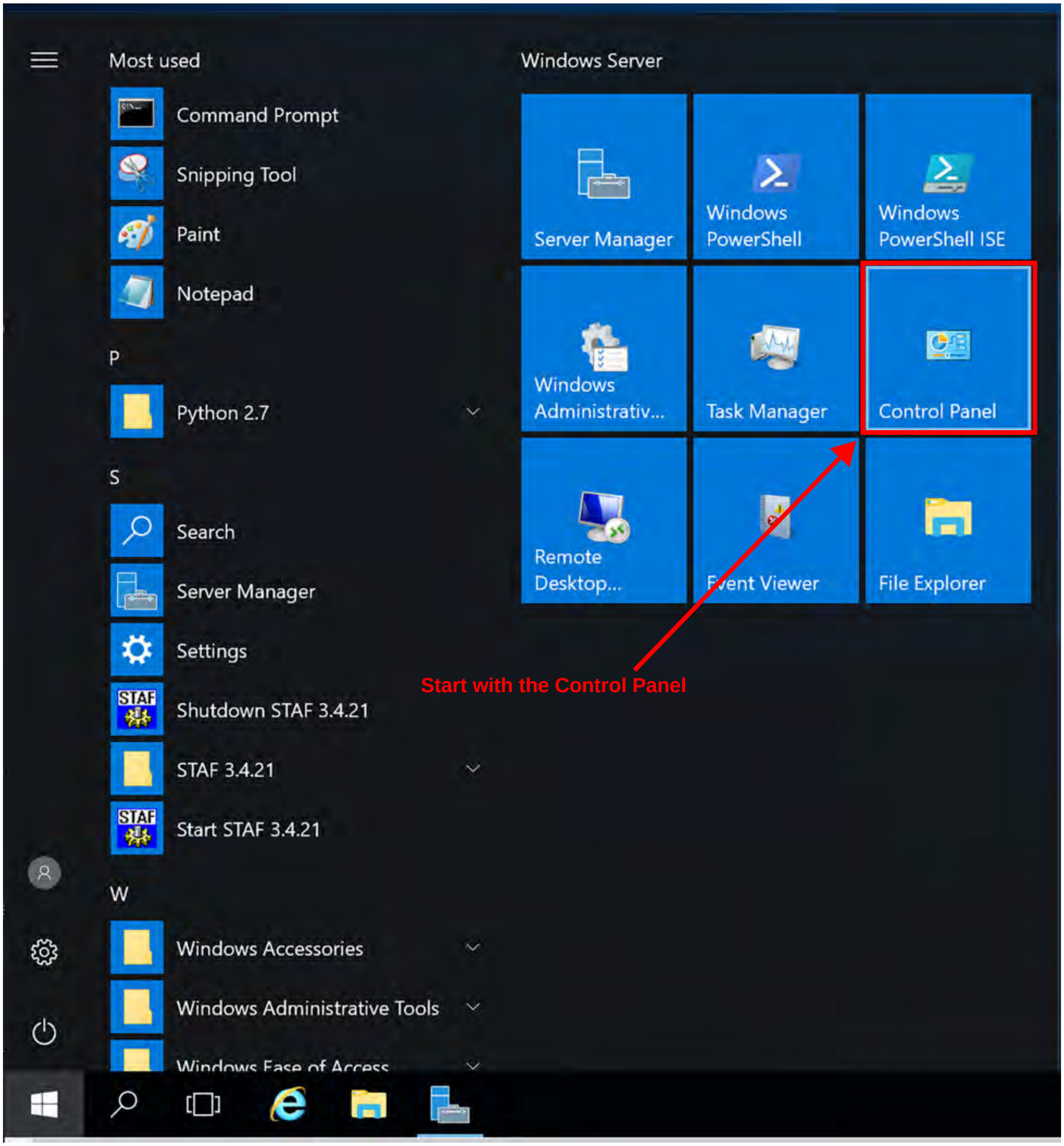


Figure H.1: **Windows Server** 2016/2019, Start Menu

2. From the Control Panel, select **Systems and Security** (Figure H.2).

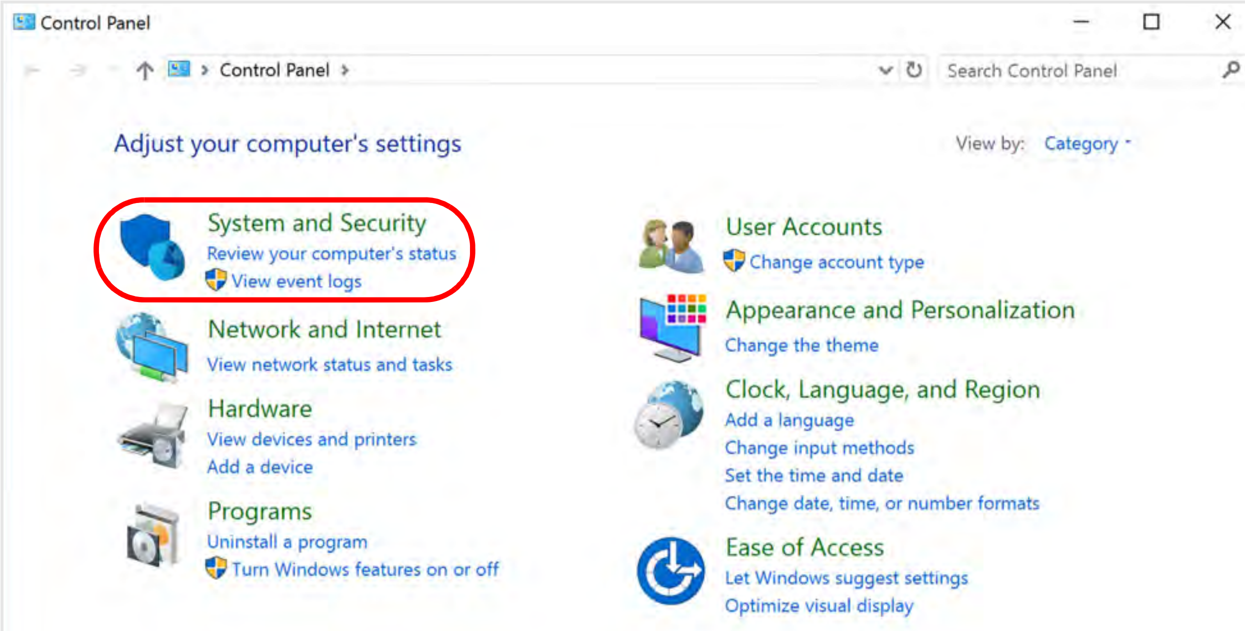


Figure H.2: Control Panel

3. From *System and Security*, select **Allow an App through Windows Firewall** Figure H.3). The Allowed apps dialog window appears (Figure H.3).

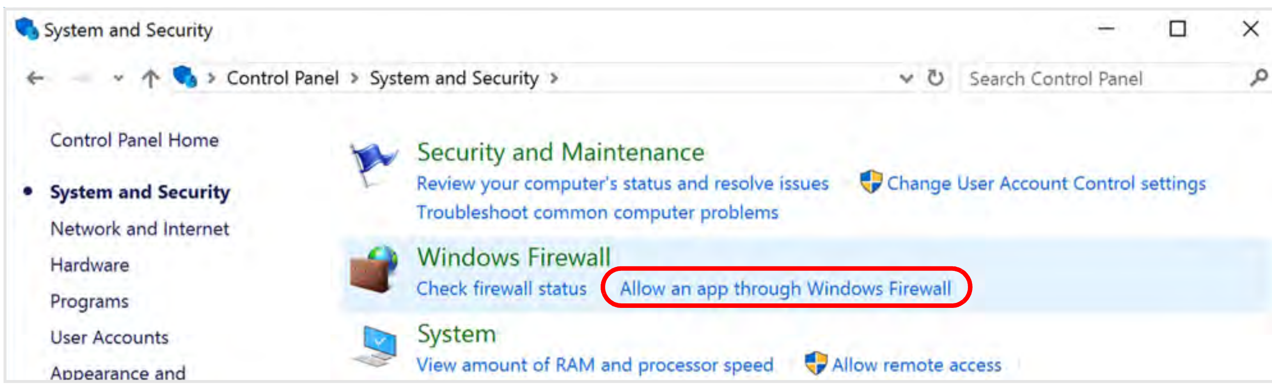


Figure H.3: Allow an App Through Windows Firewall

4. Click **Change settings**, then click **Allow another app...** (Figure H.4). The User Account Control pop-up box appears.

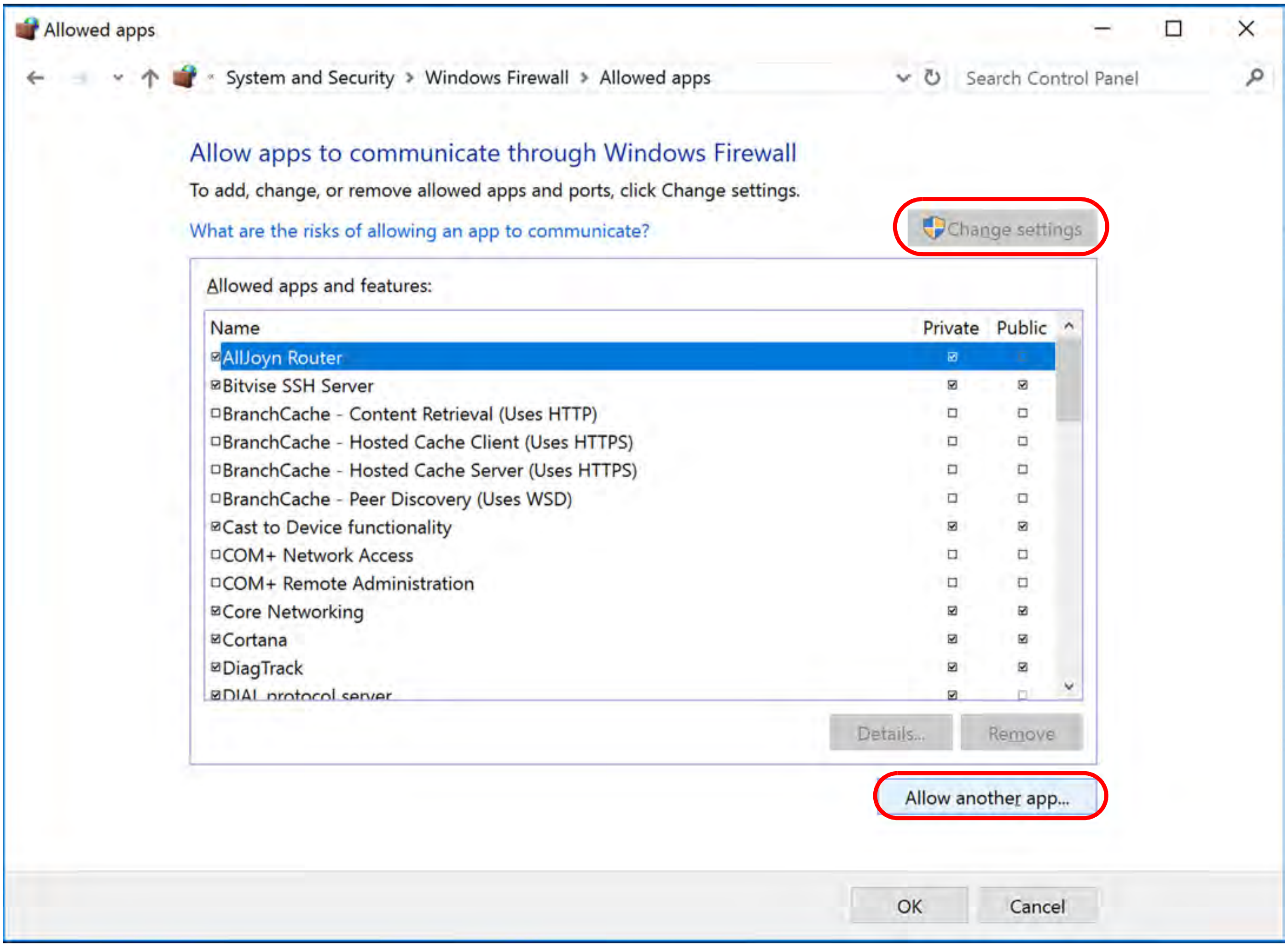


Figure H.4: Change Settings, Allow Another App

5. Select **Yes** (Figure H.5). The *Add an app* dialog box appears (Figure H.6).

NOTE: This may be optional if you have already allowed **Microsoft Windows** to make changes to your computer.

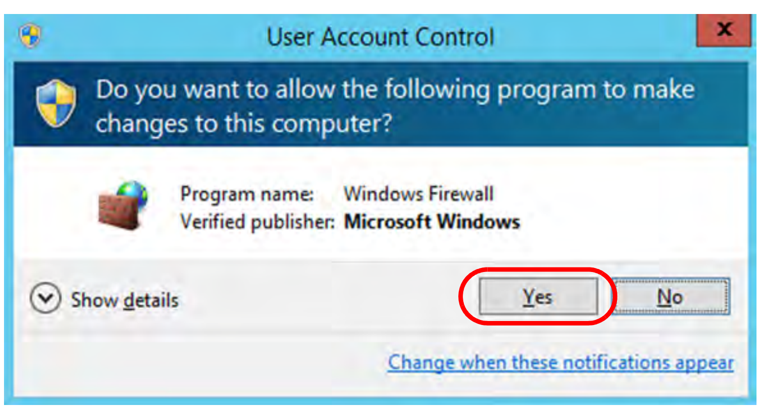


Figure H.5: **Windows Server** 2016/2019: User Account Control

6. Click **Browse** button, then navigate to the location of the installation directory for the Net Protocol Suite you are installing.

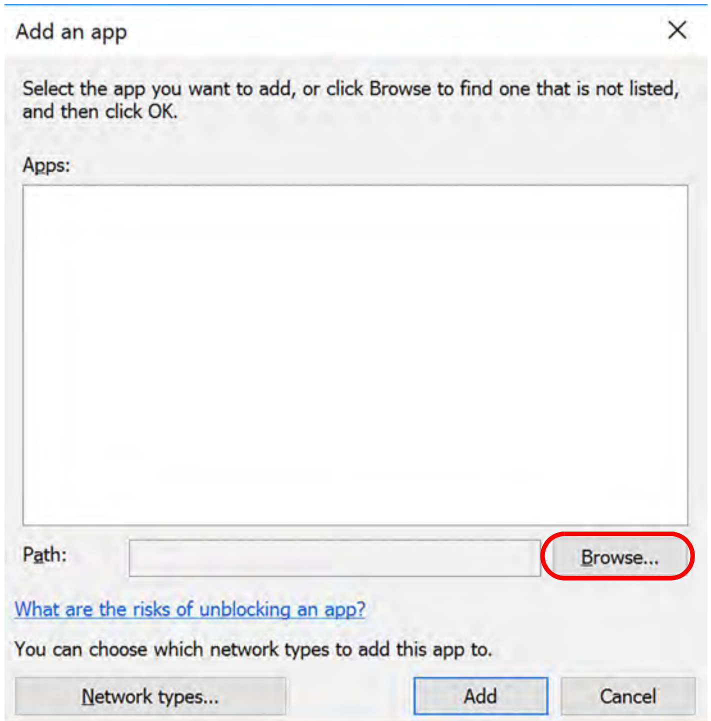


Figure H.6: Add an App

In the Browse window The Teledyne LeCroy Net Protocol Suite is typically installed on your machine in the C:\Program Files\LeCroy\Net Protocol Suite directory. See Figure H.7.

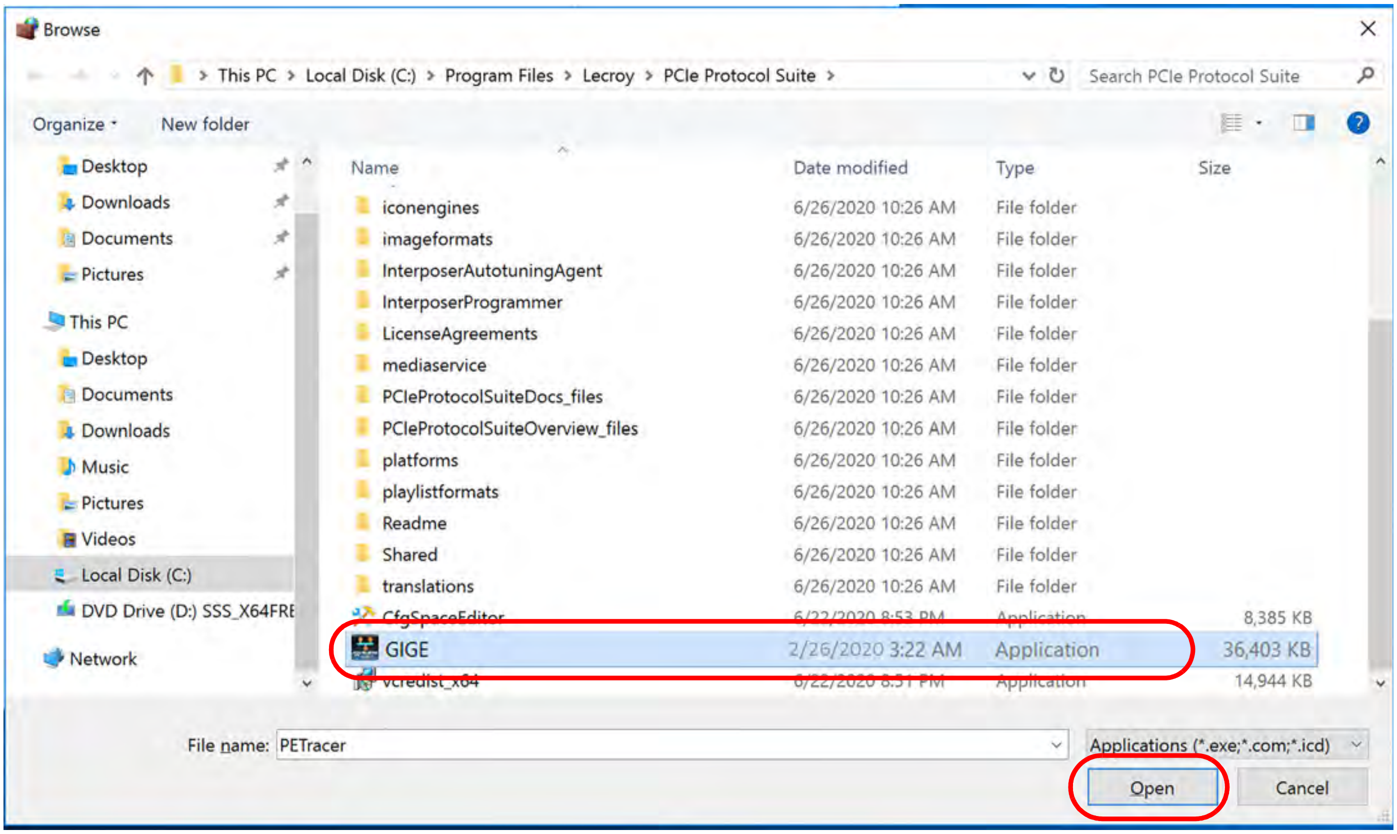


Figure H.7: **Windows Server** 2016/2019: Browse to Find Application, Net Protocol Suite Application

7. Do one of the following:
   - Select the **Net Protocol Suite** executable file (GIGE with the **.exe** extension) and click **Open**.
   - Select the specific Teledyne LeCroy Net Protocol Suite you want to add, then click **ADD**.

   This adds the Teledyne LeCroy Net Protocol Suite software to the Apps allowed through the Firewall (Figure H.8).

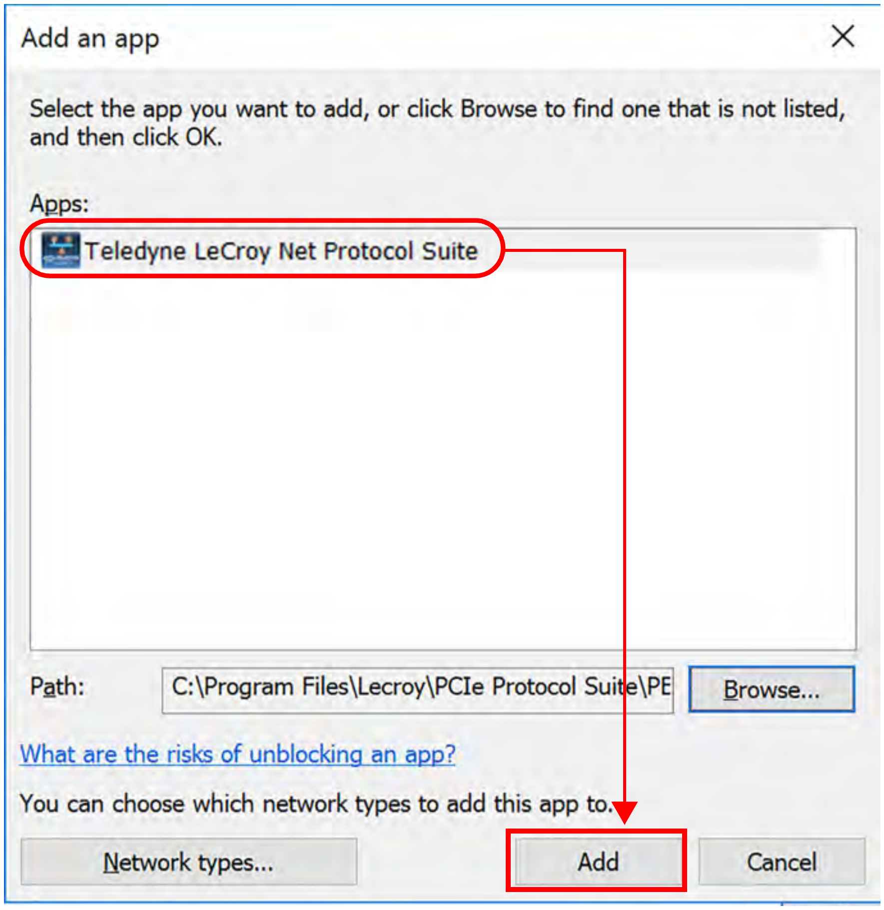


Figure H.8: **Windows Server** 2016/2019 – Add an Application to the Firewall Exceptions

After the Application has been added, you can see it in the *Allow apps to communicate through Windows Firewall* screen. See Figure H.9.

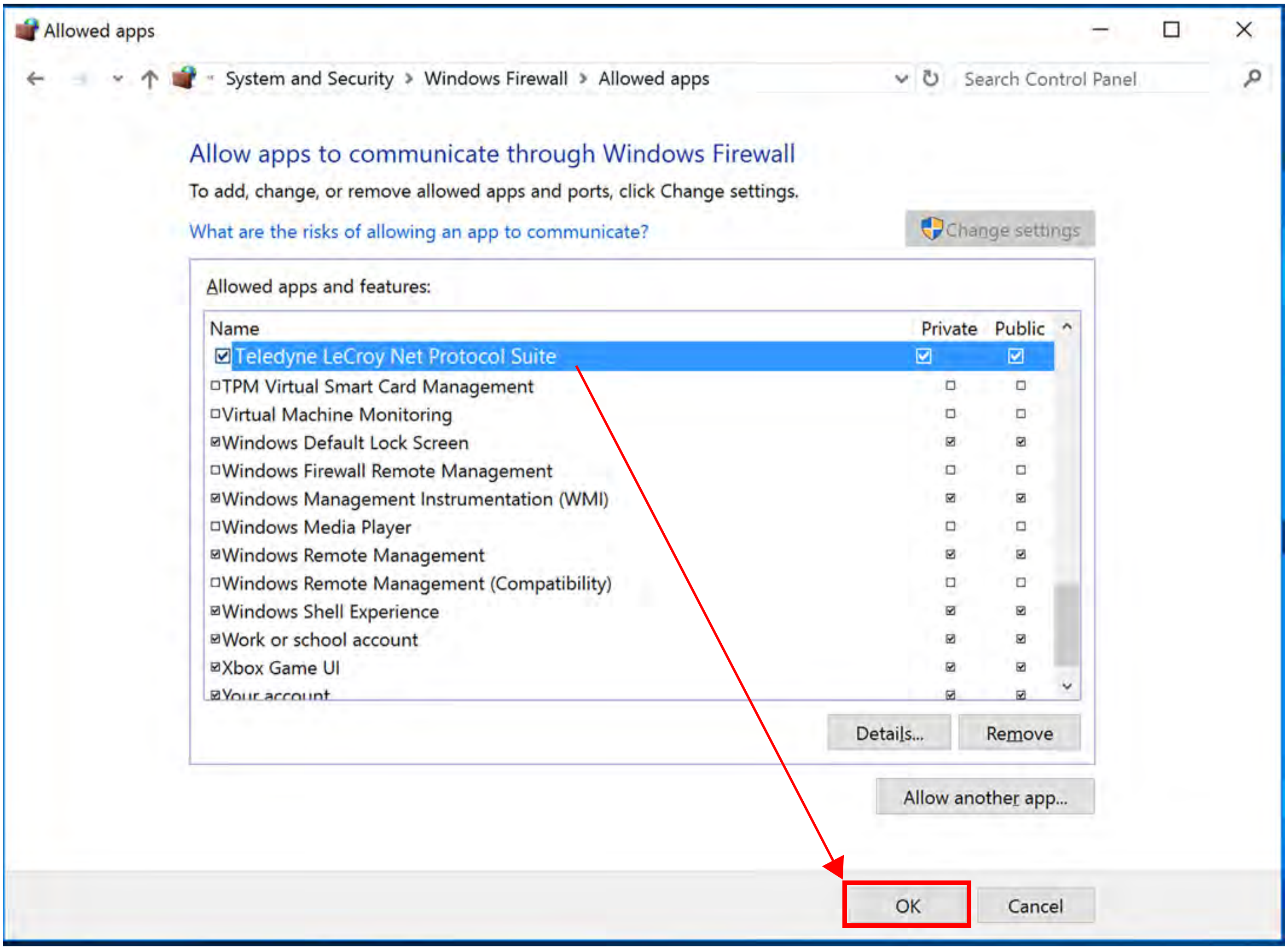


Figure H.9: **Windows Server** 2016/2019 – Add Teledyne LeCroy Net Protocol Suite to Allowed Applications

8. Click **OK** to finish updating the Firewall.