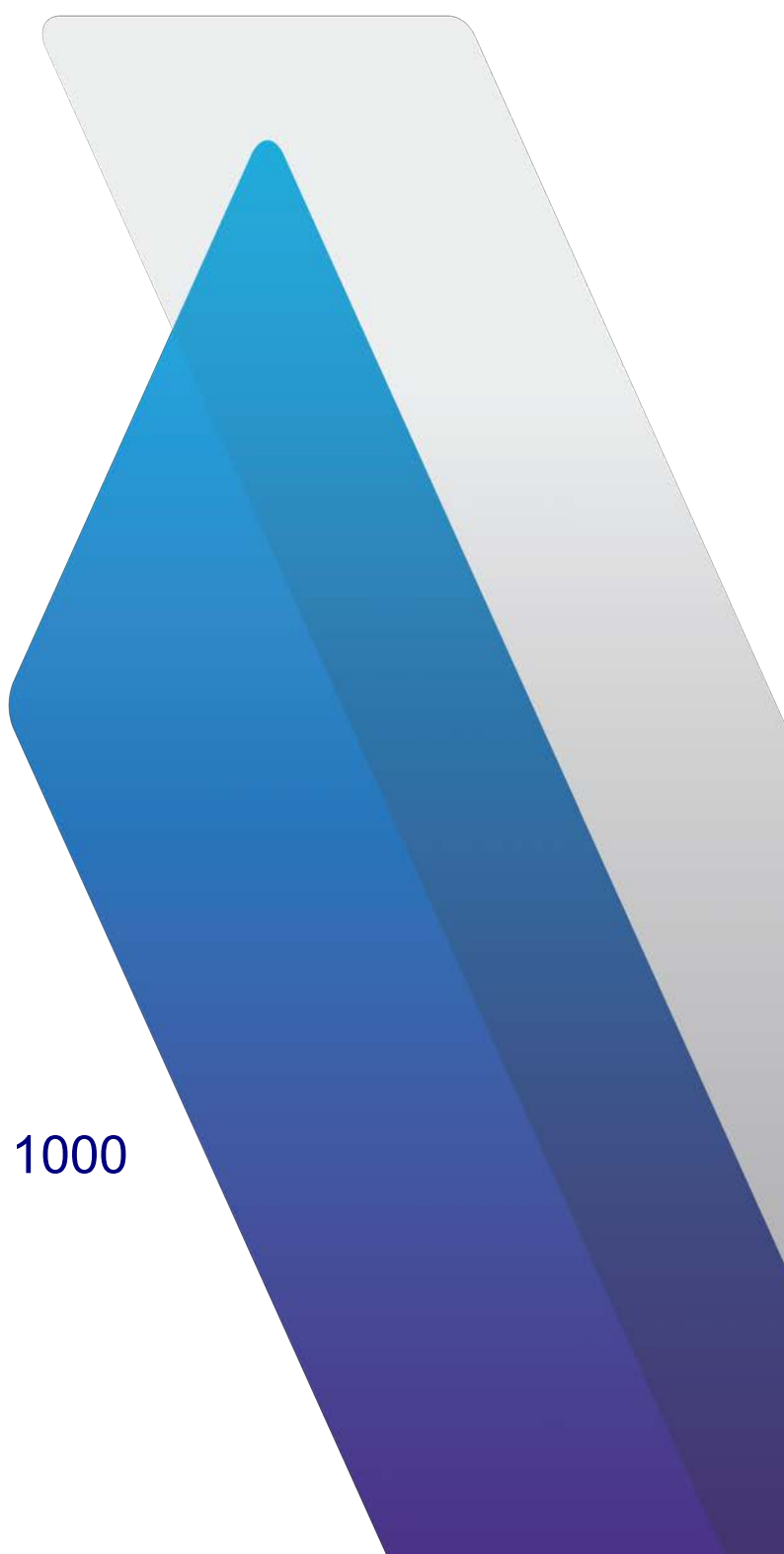




OneAdvisor 800/OneAdvisor 1000
400G Module

Users Guide
R013



OneAdvisor 800/OneAdvisor 1000 400G Module User Guide

R013



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

Notice

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

Copyright/Trademarks

© Copyright 2023 VIAVI Solutions Inc. All rights reserved. No part of this guide may be reproduced or transmitted, electronically or otherwise, without written permission of the publisher. VIAVI Solutions and the VIAVI logo are trademarks of VIAVI Solutions Inc. (“VIAVI”).

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by VIAVI is under license.

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

Copyright release

Reproduction and distribution of this guide is authorized for US Government purposes only.

Terms and conditions

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

Open Source Disclaimer - IMPORTANT READ CAREFULLY

The MSAM, CSAM, T-BERD / MTS 5800 family of instruments, OneAdvisor 800, OneAdvisor 1000, OneAdvisor 1000 400G Module, OneAdvisor 800 400G Module, MAP-2100, and SC 4800/4800P include third party software licensed under the terms of separate open source software licenses. By using this software you agree to comply with the terms and conditions of the applicable open source software licenses. Software originated by VIAVI is not subject to third party licenses. Terms of the VIAVI Software License different from applicable third party licenses are offered by VIAVI alone.



About this User Guide

This prefix explains how to use this User Guide and includes the following topics:

- [“Purpose and scope” on page vi](#)
- [“Assumptions” on page vi](#)
- [“Terminology” on page vi](#)
- [“Related Information” on page vi](#)
- [“Conventions” on page vii](#)
- [“Safety and compliance information” on page ix](#)
- [“Technical assistance” on page ix](#)

Purpose and scope

This manual is intended to help you use the capabilities of the OneAdvisor 800/OneAdvisor 1000 400G Module.

This manual includes task-based instructions that describe how to configure, use, and troubleshoot the test capabilities available on your instrument assuming it is configured and optioned to support the capabilities.

Assumptions

This manual is intended for novice, intermediate, and experienced users who want to use their instrument effectively and efficiently. We are assuming that you have basic computer experience and are familiar with basic telecommunication concepts, terminology, and safety.

Terminology

The following terms are used throughout this manual, and appear on the user interface when performing testing. Some terms are also used to label the available ports (connectors) on instrument connector panels.

Terms used to represent different test instrument platforms, hardware components, line rates, transceivers, and adapters are defined in the Terminology section of the *T-BERD/MTS/SC Getting Started Guide*.

- **100GE** — 100 Gigabit Ethernet.
- **400GE** — 400 Gigabit Ethernet.
- **RS-FEC** — Reed Solomon Forward Error Correction.
- **VIAMI Ethernet test set** — A test set marketed by VIAVI and designed to transmit an Acterna Test Packet (ATP) payload with a time stamp that is used to calculate a variety of test results. The 400G Module can be configured to transmit and analyze ATP payloads, and can be used in end-to-end and loopback configurations during testing.

Related Information

This manual is application-oriented and contains information about using these instruments to test service carried on each of the listed networks. It includes an overview of testing features, instructions for using the instruments to generate and transmit traffic over a circuit, and detailed test result descriptions. This manual also provides contact information for VIAVI's Technical Assistance Center (TAC).

Conventions

This manual uses conventions and symbols, as described in the following tables.

Table 1 Text formatting and other typographical conventions

Item(s)	Example(s)
Buttons, keys, or switches that you press or flip on a physical device.	Press the On button. – Press the Enter key. – Flip the Power switch to the on position.
Buttons, links, menus, menu options, tabs, or fields on a PC-based or Web-based user interface that you click, select, or type information into.	Click Start – Click File > Properties . – Click the Properties tab. – Type the name of the probe in the Probe Name field.
Directory names, file names, and code and output messages that appear in a command line interface or in some graphical user interfaces (GUIs).	<code>\$NANGT_DATA_DIR/results</code> (directory) – <code>test_products/users/defaultUser.xml</code> (file name) – <code>All results okay.</code> (output message)
Text you must type exactly as shown into a command line interface, text file, or a GUI text field.	– Restart the applications on the server using the following command: <code>\$BASEDIR/startup/npiu_init restart</code> Type: <code>a:\set.exe</code> in the dialog box.
References to guides, books, and other publications appear in <i>this typeface</i> .	Refer to <i>Newton's Telecom Dictionary</i> .
Command line option separators.	<code>platform [a b e]</code>
Optional arguments (text variables in code).	<code>login [platform name]</code>
Required arguments (text variables in code).	<code><password></code>

Table 2 Symbol conventions




	This symbol indicates a note that includes important supplemental information or tips related to the main text.
	This symbol represents a general hazard. It may be associated with either a DANGER, WARNING, CAUTION, or ALERT message. See Table 3 for more information.
	This symbol represents an alert. It indicates that there is an action that must be performed in order to protect equipment and data or to avoid software damage and service interruption.

Table 2 Symbol conventions (Continued)






	This symbol represents hazardous voltages. It may be associated with either a DANGER, WARNING, CAUTION, or ALERT message. See Table 3 for more information.
	This symbol represents a risk of explosion. It may be associated with either a DANGER, WARNING, CAUTION or ALERT message. See Table 3 for more information.
	This symbol represents a risk of a hot surface. It may be associated with either a DANGER, WARNING, CAUTION, or ALERT message. See Table 3 for more information.
	This symbol represents a risk associated with fiber optic lasers. It may be associated with either a DANGER, WARNING, CAUTION or ALERT message. See Table 3 for more information.
	This symbol, located on the equipment, battery, or the packaging indicates that the equipment or battery must not be disposed of in a land-fill site or as municipal waste, and should be disposed of according to your national regulations.

Table 3 Safety definitions

Term	Definition
DANGER	Indicates a potentially hazardous situation that, if not avoided, <i>will</i> result in death or serious injury. It may be associated with either a general hazard, high voltage, or other symbol. See Table 2 for more information.
WARNING	Indicates a potentially hazardous situation that, if not avoided, <i>could</i> result in death or serious injury. It may be associated with either a general hazard, high voltage, or other symbol. See Table 2 for more information.
CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in minor or moderate injury and/or damage to equipment. It may be associated with either a general hazard, high voltage, or risk of explosion symbol. See Table 2 for more information. When applied to software actions, indicates a situation that, if not avoided, could result in loss of data or a disruption of software operation.
ALERT	Indicates that there is an action that must be performed in order to protect equipment and data or to avoid software damage and service interruption.

Safety and compliance information

Safety and compliance information for the instrument are provided in printed form and ship with your instrument.

Technical assistance

If you require technical assistance, call 1-844-GO-VIAVI. For the latest TAC information, go to <https://support.viavisolutions.com>.



Table of Contents

About this User Guide	v
Purpose and scope	vi
Assumptions	vi
Terminology	vi
Related Information	vi
Conventions	vii
Safety and compliance information	ix
Technical assistance	ix
Chapter 1 Overview	1
400G Module overview	2
Exploring the modules	2
OneAdvisor 800	2
TM400GB-QQ	2
TM400GB-QO	3
OneAdvisor 1000	3
Module Installation	4
Connecting the module on the OneAdvisor 800	4
Connecting the module to the OneAdvisor 1000	6
Chapter 2 Basic Testing	9
Preparing to test	10
Using an external high accuracy timing reference signal	10
Step 1: Selecting a test application	10
Launching a test from the Quick Launch screen	10
Launching a test using the Test Menu	11
Step 2: Configuring a test	12
Step 3: Connecting the instrument to the circuit	12
Step 4: Starting the test	12
Step 5: Viewing test results	13
Setting the result group and category	13
Additional test result information	14
Timed Test	14

Chapter 3	Dual Port Applications	15
About dual port applications	16	
Dual applications	16	
Dual 400G	17	
Chapter 4	Ethernet Testing	19
About Ethernet testing	20	
Features and capabilities	20	
Understanding the graphical user interface	21	
Frame settings	21	
Adjusting the frequency of transmitted optical signals	21	
Enabling automatic traffic transmission	22	
Prerequisites for traffic transmission	22	
Issues to consider	22	
Enabling the feature	23	
Layer 2 testing	23	
Specifying interface settings	23	
Specifying Ethernet frame settings	24	
Things to consider	24	
Specifying the settings	24	
Configuring VLAN tagged traffic	27	
Configuring Q-in-Q traffic	27	
Configuring stacked VLAN traffic	28	
Specifying Ethernet Filter settings	28	
Filtering traffic using Q-in-Q criteria	30	
Filtering traffic using stacked VLAN criteria	31	
Filtering traffic using payload criteria	32	
Specifying traffic load settings	33	
Transmitting a constant load	33	
Transmitting a bursty load	34	
Transmitting a ramped load	36	
Transmitting and analyzing layer 2 traffic	37	
LBM (Y.1731)	38	
Layer 3 testing	38	
Specifying L3 interface settings	38	
Specifying the data mode and link initialization settings	38	
Specifying transmitted IPv4 packet settings	39	
Specifying IPv4 filter settings	40	
Specifying transmitted IPv6 packet settings	41	
Specifying IPv6 filter settings	43	
IPv6 Ping testing	44	
Specifying IP settings for Ping testing	45	
Transmitting ping request packets	46	
Transmitting and analyzing IP traffic	47	
Multiple Streams testing	48	
Streams Pipe soft key	48	
Using the action buttons	48	
Understanding the LED panel	48	
Streams pipe: multiple streams	49	

Understanding Multiple Streams test results	49	
Viewing results for a specific stream	50	
Viewing cumulative link results	50	
Viewing graphical results for all streams	50	
Enabling multiple streams	50	
Specifying the load type for all streams	51	
Specifying the load unit on a stream with burst	52	
Specifying the load unit for multiple streams	53	
Specifying common traffic characteristics for multiple streams	53	
Specifying layer 2 stream settings	54	
Transmitting multiple streams	55	
Capturing packets for analysis	56	
What is captured?	56	
Test Traffic	56	
Control plane traffic	57	
How is the capture buffer filled?	57	
Why use frame slicing?	57	
Understanding the Capture toolbar	57	
Specifying filter settings	58	
Capturing packets	59	
Saving or exporting captured packets	60	
Analyzing the packets using Wireshark®	62	
Ethernet Service Disruption	63	
Measuring Peak IFG	65	
LLDP	66	
Loopback testing	67	
Inserting errors	67	
Inserting alarms	68	
Measuring round trip delay or packet jitter	68	
Chapter 5 RS-FEC Testing		71
About RS-FEC testing	72	
Features and capabilities	72	
RS-FEC test applications	73	
Correctable RS-FEC errors	73	
Specifying RS-FEC settings	73	
Specifying layer 2 settings	74	
Transmitting traffic	74	
Chapter 6 Loopback Testing		77
About loopback testing	78	
Logical loopback terminology	78	
Local unit	78	
loopback unit	78	
Terminate mode	78	
loopback mode	78	

Key logical loopback concepts	78
Address swapping	79
Filter criteria on the loopback unit	79
VLAN and Q-in-Q traffic	79
Loop types	79
Understanding the graphical user interface	79
Loopback action buttons	79
Loopback messages	80
Specifying a unit identifier	80
Using LLB to loop received traffic back to the local unit	80
Using Loop Up to initiate a loopback from the local unit	81
Layer 1 (physical) loopback	82

Chapter 7 OTN Testing

85

About OTN testing	86
Features and capabilities	86
LED panel	86
Understanding OTN test results	86
OTN test applications	87
OTN Overhead Transparency	87
Running the OTN Check work flow	87
Specifying the Tx clock source	90
Measuring optical power	91
Inserting errors and alarms	91
Inserting errors	92
Inserting alarms	92
Alarm suppression	93
Observing and manipulating overhead bytes	93
Scrambling the signal	94
FEC testing	95
Specifying SM, PM, and TCM trace identifiers	96
Specifying FTFL identifiers	98
Specifying GCC BERT Channels	99
ODU RTD	100
Specifying the transmitted and expected payload type	100
Specifying the Multiplex Structure Identifier	102
BER testing	102
Measuring service disruption time	103

Chapter 8 Fibre Channel Testing

107

About Fibre Channel Testing	108
Features and capabilities	108
Understanding the graphical user interface	108
Configuring Fibre Channel tests	109
Specifying interface settings	109
Specifying Fibre Channel frame settings	113
Specifying Fibre Channel filter settings	114
Specifying traffic load settings	115

Transmitting and analyzing layer 2 traffic	115
Logical loopback testing	116
Measuring service disruption time with Peak IFG	116
Inserting errors	117
Measuring round trip delay	117
64G Fiber Channel RS-FEC Testing	118
Chapter 9 Optics AOC/DAC Testing and Parameters	119
Optics Self-Test	120
Running the Optics Self-Test	120
Generating Reports	121
Cable Test for AOC/DAC/AEC	122
Application Code Switching	124
CMIS Host Media apps	125
Switching an application code	125
ZR/ZR+ Tunable support	126
Coherent ZR statistics	126
Tunable settings	127
Fine Tuning	127
Output Power	128
Coherent Results	128
i ² C Peek/Poke	128
Expert Mode	129
Application Code setting	129
Host Transmit settings	129
Module Rx Output settings	129
CMIS pluggable optic reset	130
Chapter 10 Automated Testing Using Workflows	131
Launching an automated test	132
Automated Test Availability	133
Automated RFC 2544 tests	134
Features and capabilities	134
About loopbacks	135
QuickCheck	135
Understanding the QuickCheck stages	136
Test at configured Max Bandwidth	136
Layer 2 Quick Test	137
Throughput test	137
VIAVI zeroing-in method	137
Throughput test results	138
Pass/fail threshold	138
Latency (RTD) test	139
About the latency test	139
Pass/fail threshold	139
Packet Jitter test	139
About the Packet Jitter test	139
Packet Jitter test results	140
Pass/fail threshold	140

Frame Loss test	140
About the frame loss test	140
Frame Loss test results	140
Back to Back Frames test (Burst test)	140
About the Back to Back Frames test	141
Back to Back test results	141
Optimizing the test time	141
Importing and exporting RFC config files	142
Initiating the Enhanced RFC2544 Test	142
Configuring the Enhanced RFC 2544 tests	143
Specifying the external test settings	143
Setting Connection parameters	144
Configuration methods	144
Test selection	146
Running Enhanced RFC 2544 tests	148
About the Y.1564 SAMComplete test	153
Initiating the SAMComplete test	154
Configuring SAMComplete test settings	155
Choosing SAMComplete tests	160
Running SAMComplete tests	160
5G NR Discovery	164
Automated VLAN tests	165
Saving automated test report data	166

Chapter 11 Test Results

169

About test results	170
Summary Status results	170
Ethernet results	171
LEDs	171
SLA/KPI	174
Interface results	174
L2 Link Stats results	176
L2 Link Counts results	178
L2 Filter Stats results	179
L2 Filter Counts results	180
L3 Link Stats results	180
L3 Link Counts results	181
L3/IP Config Status results	182
BERT Stats results	182
PCS Stats	183
Ethernet Per Lane results	184
Error Stats results	185
RS-FEC results	186
RS-FEC Per Lane results	186
RS-FEC Error Distribution Results	187
Graphical results	187
Histogram results	187
Event Log results	188
Time test results	188

Temperature 189

Glossary **191**

Overview

This chapter provides a description of the 400G modules for the OneAdvisor 800 and OneAdvisor 1000. Topics covered in this chapter include:

Topics discussed in this chapter include the following:

- [“400G Module overview” on page 2](#)
- [“Exploring the modules” on page 2](#)
- [“Module Installation” on page 4](#)

400G Module overview

The VIAVI 400G modules provide line-rate and protocol coverage to address service activation, troubleshooting, and maintenance for 400G circuits on the OneAdvisor 800 and OneAdvisor 1000. The 400G module is available in three variants:

- TM400GB-QO — 400G Module for OneAdvisor 800 with one QSFP-DD port and one OSFP port.
- TM400GB-QQ — 400G Module for OneAdvisor 800 with two QSFP-DD ports.
- TM400GA — 400G Module for OneAdvisor 1000. The OneAdvisor 1000 can support up to two concurrent 400G Modules, including battery and SCPI operation.

Exploring the modules

The following sections describe the 400G modules.

OneAdvisor 800

The following sections describe the TM400GB-QO and TM400GB QQ modules.

TM400GB-QQ

Figure 2 shows the OneAdvisor 800 400G Module TM400GB-QQ.

Figure 1 OneAdvisor 800 400G Module TM400GB-QO



1	QSFP-DD	Port capable of up to QSFP56-DD support. Also hardware capable of supporting non-DD optics such as QSFP56, QSFP28, and QSFP+.
2	SFP-DD	Port capable of up to SFP56-DD support. Can also support non-DD SFP optics.
3	EXT CLK REF	SMA connector for external clock input.
4	1PPS	SMA connector for external 1PPS generator.
5	CLK OUT	SMA connector capable of providing a derivative of the clock as an output.

6	GNSS ANTENNA	SMA connector for external GNSS antenna.
7	SFP-DD	Port capable of up to SFP56-DD support. Can also support non-DD SFP optics.
8	QSFP-DD	Port capable of up to QSFP56-DD support. Also hardware capable of supporting non-DD optics such as QSFP56, QSFP28, and QSFP+.

TM400GB-QO

Figure 2 shows the OneAdvisor 800 400G Module TM400GB-QO.

Figure 2 OneAdvisor 800 400G Module TM400GB-QO

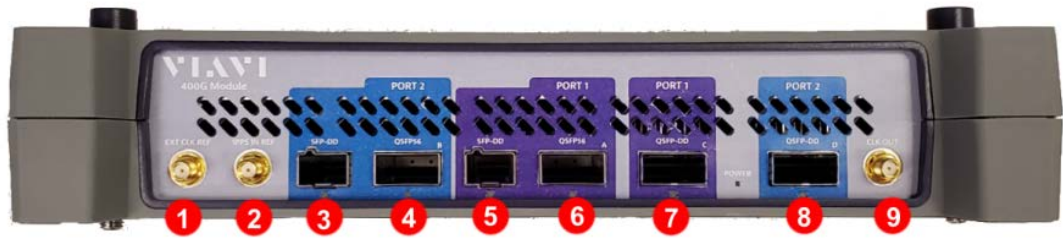


1	QSFP-DD	Port capable of up to QSFP56-DD support. Also hardware capable of supporting non-DD optics such as QSFP56, QSFP28, and QSFP+.
2	SFP-DD	Port capable of up to SFP56-DD support. Can also support non-DD SFP optics.
3	EXT CLK REF	SMA connector for external clock input.
4	1PPS	SMA connector for external 1PPS generator.
5	CLK OUT	SMA connector capable of providing a derivative of the clock as an output.
6	GNSS ANTENNA	SMA connector for external GNSS antenna.
7	SFP-DD	Port capable of up to SFP56-DD support. Can also support non-DD SFP optics.
8	OSFP	OSFP port. VIAMI provides an OSFP to QSFP adapter, allowing the port to be used for QSFP devices up to 200GigE.

OneAdvisor 1000

Figure 3 shows the OneAdvisor 1000 400G Module.

Figure 3 OneAdvisor 1000 400G Module TM400GA



1	EXT CLK REF	SMA connector for external clock input.
2	1PPS	SMA connector for external 1PPS generator.
3	SFP-DD	Port capable of up to SFP56-DD (Double Density) support. Can also support non-DD SFP optics.
4	QSFP56	Port capable if up to QSFP56 support. Also hardware capable of supporting QSDP28 and QSFP+.
5	SFP-DD	Port capable of up to SFP56-DD support. Can also support non-DD SFP optics.
6	QSFP56	Port capable of up to QSFP56 support. Also hardware capable of supporting QSFP28 and QSFP+.
7	QSFP-DD	Port capable of up to QSFP56-DD support. Also hardware capable of supporting non-DD optics such as QSFP56, QSFP28, and QSFP+.
8	QSFP-DD	Port capable of up to QSFP56-DD support. Also hardware capable of supporting non-DD optics such as QSFP56, QSFP28, and QSFP+.
9	CLK OUT	SMA connector capable of providing a derivative of the clock as an output.

Module Installation

The following sections describe how to install the 400G Module to the base.

Connecting the module on the OneAdvisor 800

The following procedure describes how to connect the module to the OneAdvisor 800 base.

To connect the module to the OneAdvisor 800

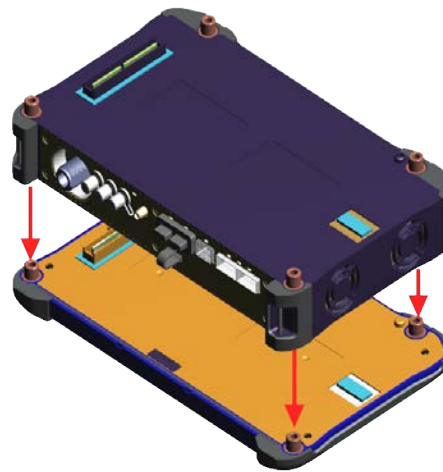


NOTE

If using the 400G module in combination with a Fiber Module Carrier (FMC), install the FMC onto the screen, then the 400G Module, followed by the OneAdvisor 800 base.

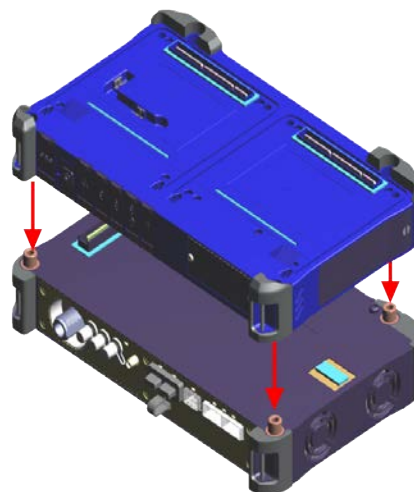
- 1 Power down the OneAdvisor 800 and disconnect from AC power.
- 2 Place the unit so that you have access to the back and remove the termination cover by removing the screws that hold it in place.
- 3 Set the module onto the screen, ensuring the mating connectors between the two pieces are aligned, as shown in [Figure 4](#).

Figure 4 Module to screen



- 4 Insert the hex key in the brass fittings on the rear of the module and tighten the internal captive fasteners to secure the module to the display.
- 5 Place the OneAdvisor 800 base onto the module, ensuring the mating connectors are aligned, as shown in [Figure 5](#).

Figure 5 OneAdvisor 800 base to module



- 6 Using the hex key, tighten the captive fasteners on the rear of the base that secure it to the module.
- 7 Re-attach the back termination cover or CAA/OTDR modules.

Connecting the module to the OneAdvisor 1000

The following procedure describes how to connect the module to the OneAdvisor 1000 base.

To connect the module to the OneAdvisor 1000

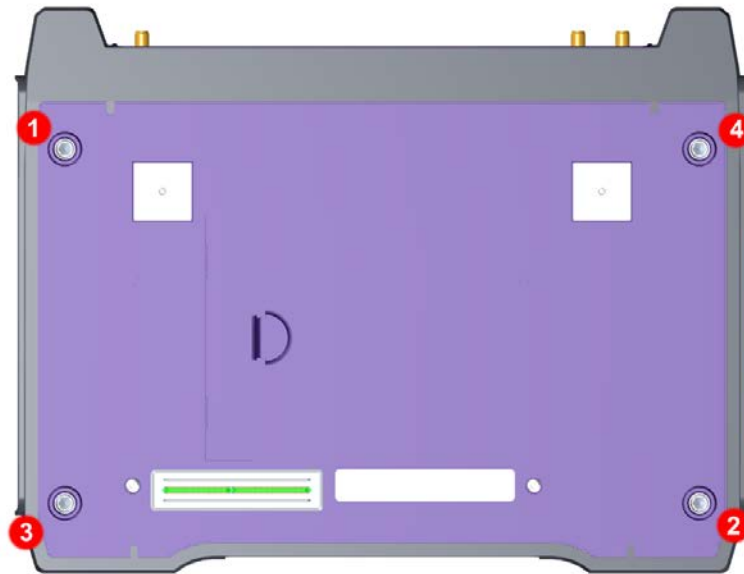
- 1 Verify that the power is OFF on your OneAdvisor 1000 and the power adapter is unplugged.
- 2 Using a flat blade screwdriver, loosen each of the 4 slotted bolts on the back of the OneAdvisor 1000.
- 3 Remove the blank termination cover from the base unit, and then remove the hex key from the groove on the inside panel of the blank termination cover.
- 4 The OneAdvisor 1000 base and module have rectangular mating connectors. These connectors *must* be aligned carefully before connecting the module to the OneAdvisor 1000.
 - a To align the connectors properly, place the base unit with the screen side down on your work surface. The mating connector on the back panel should be facing you, at the top of the unit.
 - b Position the module over the base unit, with the module's mating connector directly over the mating connector on the OneAdvisor 1000.
 - c Verify that the holes on each corner of the module are aligned precisely with the holes on each corner of the OneAdvisor 1000.
 - d Slowly lower the module until it is just over the holes on the OneAdvisor 1000, and then gently but firmly press the center of the module to attach it to the OneAdvisor 1000.
- 5 Starting at the upper right corner, do the following:
 - a Using the hex key, tighten screws 1 through 4 (in the sequence illustrated in figure) until you feel a slight resistance.
 - b After all four screws are tightened, using the hex key, tighten each screw at least one additional quarter turn in the sequence illustrated in [Figure 6](#).
- 6 Re-attach the blank termination cover.



NOTE:

The input power ratings for the TM400GA module are 11-27 VDC, 16 A Max. Power is supplied by the OneAdvisor 1000 base unit.

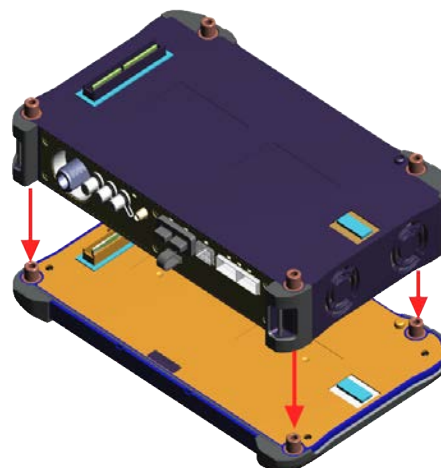
Figure 6 Sequence for securing and tightening the screws



To attach a Fiber Module carrier or Solution module

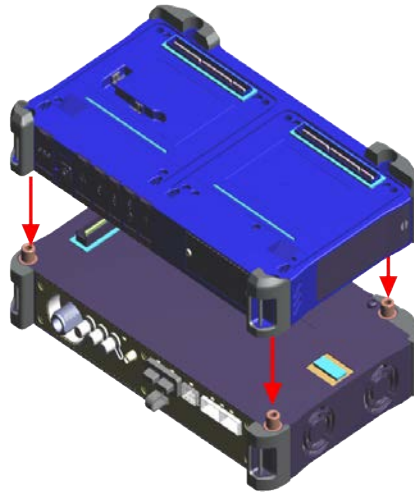
- 1 Power down the OneAdvisor 800 and disconnect from AC power.
- 2 Place the unit so that you have access to the back and remove the termination cover by removing the screws that hold it in place.
- 3 Set the module onto the screen, ensuring the mating connectors between the two pieces are aligned, as shown in [Figure 7](#).

Figure 7 Module to screen



- 4 Insert the hex key in the brass fittings on the rear of the module and tighten the internal captive fasteners to secure the module to the display.
- 5 Place the OneAdvisor 800 base onto the module, ensuring the mating connectors are aligned, as shown in [Figure 8](#).

Figure 8 OneAdvisor 800 base to module



- 6 Using the hex key, tighten the captive fasteners on the rear of the base that secure it to the module.
- 7 Re-attach the back termination cover or CAA/OTDR modules.

Basic Testing

This chapter provides information on basic testing services.

Topics discussed in this chapter include the following:

- [“Preparing to test” on page 10](#)
- [“Step 1: Selecting a test application” on page 10](#)
- [“Step 2: Configuring a test” on page 12](#)
- [“Step 3: Connecting the instrument to the circuit” on page 12](#)
- [“Step 4: Starting the test” on page 12](#)
- [“Step 5: Viewing test results” on page 13](#)
- [“Timed Test” on page 14](#)

Preparing to test

Before testing, VIAVI recommends:

- Reviewing the *Getting Started Guide* that shipped with your instrument; in particular, the instructions for connecting your test instrument to the circuit.
- Verifying that you have the correct cables, connectors, transceivers, and adapters required to connect to the circuit. Your *Getting Started Guide* provides important considerations when testing over optical circuits, verifying that optics support specific line rates.
- Determining whether you need to synchronize near and far end instruments to a high accuracy timing reference before beginning the test.
- Determining whether an external clocking reference, such as a BITS, SETS, or 10MHz, is required for precise measurements and analysis.

Using an external high accuracy timing reference signal

Some test applications documented within this manual require an external, high accuracy timing reference.

It is important to understand the connections required to input the reference and analyzed signals. The 400G Module is equipped with an external clock SMA connector.

Instructions for connecting a GNSS receiver are provided in the *Getting Started Guide* that shipped with your instrument.

Step 1: Selecting a test application

There are two methods available for selecting a test application. The first method uses the Quick Launch screen, which lists pinned (saved) and recently run tests. The second method uses the Test Menu, which lists *every available test* for the currently installed options and configuration of your instrument.






For a detailed explanation of the Quick Launch screen and Test Menu, refer to the Basic Testing chapter of the *Getting Started Guide* that shipped with your instrument.

Launching a test from the Quick Launch screen

The Quick Launch screen is used to launch tests that you use frequently. The last four selected tests are also automatically listed on the screen. When running tests, the icons

in appear to the left of each pinned test representing the application or technology that is supported. [Table 1](#) lists the icons used to represent key applications.

Table 1 Quick Launch Icons

Application	Icon	Application	Icon
Ethernet Quick Check		Y.1564 SAMComplete	
Ethernet Traffic		RFC 2544	
Optics Self-Test			

To launch a test from the Quick Launch screen

- 1 If the Quick Launch screen did not appear by default when you turned on your instrument, on the Main screen, click **Select Test**.
The Quick Launch screen appears.
The All Tests and Hide Tests buttons are used to display or hide the Test Menu to the left of the screen; the Customize button is used to maintain and customize the list of tests that appear on the screen.
- 2 If the test you want to launch appears on the screen, select the test; otherwise, customize the screen to add the test, then select the test on the Quick Launch screen.
- 3 Wait for the test to launch and appear on the Main screen, then proceed to [“Step 2: Configuring a test” on page 8](#).

The test is launched.

Launching a test using the Test Menu

Tests are grouped and listed on the Test Menu by technology, signal, payload, and test mode.

To select a test using the Test Menu

- 1 On the Main screen, click **Select Test**.
The Quick Launch screen appears.
 - If the Test Menu appears to the left of the screen, proceed to [step 2](#).
 - If the Test Menu does not appear, select the All Tests button (located at the bottom left of the Quick Launch screen). The Test Menu will appear.
- 2 Using the Test Menu, select the technology, signal, payload, and test mode for your test.
The instrument displays a message asking you to wait while it loads the test.

- 3 Wait for the Main screen to appear, and then proceed to [“Step 2: Configuring a test” on page 8](#).

The test is selected.

Step 2: Configuring a test

Before you configure a test, be certain to complete the information that you want to include when you generate reports of your test results. For details, refer to the Getting Started Guide that shipped with your instrument.

Configuring a test involves displaying the setup screens, specifying test settings, and optionally saving the test setup. Key settings are also available on the Main screen and on the Quick Config tabs. Changing key settings while running a test (for example, changing the pattern transmitted) triggers an automatic restart of the test.

To display the setup screens

- 1 Using the Test Menu or Quick Launch screen, select a test application (see [“Step 1: Selecting a test application” on page 10](#)).
- 2 Select the **Setup** soft key.
A setup screen with a series of tabs appears. The tabs displayed vary based on the test application you selected.
- 3 To navigate to a different setup screen, select the corresponding tab at the top of the screen. For example, to display the Traffic setup screen, select the Traffic tab.

Step 3: Connecting the instrument to the circuit

When connecting the unit to optical circuits, bear in mind that applied optical power must not exceed the power level supported by each optical connector on your instrument.

Step 4: Starting the test

After you configure a test, connect the unit to the circuit and turn the laser ON, you are ready to start your test.

- You must actively **Start Traffic** (using the action button).
- If you would like your unit to transmit traffic automatically, you can enable the automatic traffic generation feature.
- When a test is configured to establish a connection to a remote unit, the connection process queries the remote unit for its software version. If the software version level on the remote and local unit are different, a notice will be displayed encouraging you to update the older unit to avoid incompatibility issues and achieve optimal performance.

After you start a test, use the buttons at the bottom of the screen to perform actions such as turning the laser on and off, starting and stopping traffic, starting and stopping a local loopback, and inserting errors, alarms, or defects. [Table 2](#) lists some common Action buttons.

Table 2 Action buttons

Button	Action
Laser On/Off ¹	Turns the laser on or off when testing optical rates.
Insert Error	Inserts an error into the transmitted traffic.
Insert Alarm/Defect	Inserts an alarm or defect into the transmitted traffic.
Start Traffic/Stop Traffic	Starts or stops transmission of traffic over the circuit.

1. You can optionally configure optical Ethernet applications to automatically transmit traffic after you turn the laser ON.

Step 5: Viewing test results

Test results appear in the Results Windows of the Main screen.

Setting the result group and category

To set the result group and category

- 1 Using the Test menu or Quick launch screen, select a test application see [“Step 1: Selecting a test application” on page 10](#)), and then configure your test (see [“Step 2: Configuring a test” on page 8](#)).
- 2 Select the **Results** soft key to return to the Main screen.
- 3 Connect your module to the circuit.
- 4 Select the **Laser** button.
- 5 Select the **Start Traffic** button to start generating and analyzing traffic. Results appear in the Results Windows.
- 6 *Optional.* Insert errors or anomalies into the traffic stream, or use the Action buttons to perform other actions. Only buttons that are applicable to the test you selected appear.
- 7 Use the Group and Category buttons to specify the type of results you want to observe. [Figure 9](#) illustrates buttons for a standard layer 2 Ethernet application.

Figure 9 Result Group and Category buttons



Results for the category you selected appear in the result window.

- 8 *Optional.* To observe results for a different group or category in another result window, press the buttons at the top of the window to specify the group and category.

For descriptions of each result, refer to [Chapter 11 “Test Results”](#).



TIP:

If you want to provide a screen shot of key test results, on the Main screen, click the camera icon at the top of the screen. A screen shot will be captured and stored as a PNG file in the `/bert/images` folder. You can include the screen shot when you create reports.

Additional test result information

For descriptions of each result, refer to [Chapter 11 “Test Results”](#).

Timed Test

Timed Test capabilities provide the possibility to automatically schedule the duration of a test. Test reports can be automatically generated upon completion. The following modes are available:

- **Timed Test with Traffic Control** — This mode controls the exact duration of a test from a few seconds to multiple days. The Traffic Control element ensures that when the test starts, no traffic transmission occurs from the unit as traffic starts one second into the test. When the test duration elapses, traffic transmission stops one second before the end of the test when results are frozen. The main goal of this selection is that when testing to a loopback device and when no control plane traffic originates from within the network, it is possible to compare the number of transmitted and received frames and to likely get a matching count.
- **Delayed-Start Timed Test with Traffic Control** — Delayed-Started Timed Test with Traffic Control operates the same as Timed Test with Traffic Control, except that it is possible to schedule when the test starts by providing a date and time.
- **Timed Test** — Strictly controls the amount of time over which statistics are collected. This mode does not schedule or control any of the traffic transmission capabilities.
- **Delayed-Start Timed Test** — Delayed Start Timed Test is identical to Timed Time except that it is possible to schedule when the test starts by providing a date and time

Dual Port Applications

This chapter provides information on dual port applications.

Topics discussed in this chapter include the following:

- [“About dual port applications” on page 16](#)
- [“Dual 400G” on page 17](#)

About dual port applications

The dual port application functionality provides the capability to run two independent tests concurrently. It is therefore possible to control each test individually for just about all parameters such as test start, stop, restart. This extends to workflows as well such as Optics Self-Test, RFC 2544, and Y.1564.

The test module faceplate identifies the ports for test applications; they are port 1 identified via a purple area and port 2 identified via a blue area. A port can include an SFP and QSFP or OSFP physical port; which one is used depends on the rate and pluggable optics to be used. See [“Exploring the modules” on page 2](#) for more information on the physical module faceplate.

Dual applications



NOTE

Dual applications in this context refers to software license CADUALAPPS; this provides dial concurrent and independent functions.

Dual application support is currently available for the following applications:

- 10/100/1000
- 1GigE Optical
- 10GigE LAN
- 25GigE
- 40GigE
- 50GigE
- 100GigE
- 100GigE KP4
- 200GigE
- Layer 1 loopback (available on OneAdvisor 800 TM 400GB modules)

On the OneAdvisor 800 TM400GB-QO, an OSFP to QSFP adapter is available to connect QSFP devices into Port 1 (OSFP). You can combine any two applications from this list to concurrently and independently run two test applications. For any other test application, it is possible to run a single test application per module. If two test applications are running concurrently, one of these applications must be closed in order to run an application not in the dual application list above.

Dual 400G



NOTE

Dual 400G refers to software license CADUAL400G. This functionality is strictly available on OneAdvisor 800 with modules TM400GB-QO or TM400GB-QQ.



NOTE

The CADUAL400G license enables both the testing of two 400GigE ports and of 400GigE and any other singular Ethernet rate concurrently. For the other singular Ethernet rate, the rate license must be present; examples include CA100GE or CA10GELAN



NOTE

To run dual 400G on battery, it is required to add a PEM to the OneAdvisor 800.

Dual 400G provides functionality for 2 concurrent 400GE ports via the Dual 400GE launch point, and adds the capability of running 400 GigE together with singular other Ethernet rates from 10/100/1000 to 200 GigE. For Dual 400 GigE on TM400GB-QO, this requires the use of one QSFP-DD and one OSFP. For Dual 400 GigE on TM400GB-QQ, this requires the use of two QSFP-DD pluggable modules. For Dual 400 GigE with Other Rate, 400 GigE is on port 2 and any other Ethernet singular rate is on port 1. Launching the test on port 1 is done in a separate step and does not affect the 400 GigE test on port 2. The control of each test is individual including test start, stop, restart and workflows such as RFC 2544 and Y.1564.

Each test has its own individual tab. For Dual 400 GigE, closing one of the two tabs will result in closing both tabs when in dual 400GE.

In the dual 400 GigE app, some RS-FEC statistics are not available on the Rx. This includes HI SER and uncorrectable BER. As well, Correctable RS-FEC BER Threshold alarm is not available.

To use multiple streams or capture or LLDP at 400 GigE, the 400 GigE Single Port launch point is required.

Ethernet Testing

This section provides information on testing Ethernet services.

- [“About Ethernet testing” on page 20](#)
- [“Adjusting the frequency of transmitted optical signals” on page 21](#)
- [“Enabling automatic traffic transmission” on page 22](#)
- [“Layer 2 testing” on page 23](#)
- [“Layer 3 testing” on page 38](#)
- [“Multiple Streams testing” on page 48](#)
- [“Capturing packets for analysis” on page 56](#)
- [“Measuring Peak IFG” on page 65](#)
- [“Loopback testing” on page 67](#)
- [“Inserting errors” on page 67](#)
- [“Inserting alarms” on page 68](#)
- [“Measuring round trip delay or packet jitter” on page 68](#)

About Ethernet testing

If your instrument is configured and optioned to do so, you can use it to provision Ethernet, verify end-to-end connectivity, and analyze link performance by simulating different traffic conditions.

Features and capabilities

Features and capabilities include the following when testing an Ethernet service. Several results are provided at the physical, PCS, RS-FEC, and MAC layers:

- 400 Gigabit Ethernet with RS(544,514) FEC — Measure pre-FEC and post-FEC performance using Ethernet/MAC layer traffic. Several results are provided at the physical, PCS, RS-FEC, and MAC layers.
- 4 x 100 Gigabit Ethernet with RS(544,514) FEC — One application for 4 or fewer ports on a single pluggable optics device such as QSFP-DD. This is a layer 2 feature with per port level control. The laser and traffic controls are available for each individual port or as joint actions
- 200 Gigabit Ethernet with RS(544,514) FEC — Measure pre-FEC and post-FEC performance using Ethernet/MAC layer traffic.
- 100 Gigabit Ethernet KP4 with RS(528,514) FEC — Support for both 100GAUI-4 (NRZ) and 100GAUI-2 (PAM4). Measure pre-FEC and post-FEC performance using the Ethernet/MAC layer traffic.
- 100 Gigabit Ethernet with no FEC or with RS(528,514) FEC — Measure pre-FEC and post-FEC performance using Ethernet/MAC layer traffic.
- 50 Gigabit Ethernet with RS(544,514) FEC — Measure pre-FEC and post-FEC performance using Ethernet/MAC layer traffic.
- 40 Gigabit Ethernet with no FEC — Measure Ethernet/MAC layer traffic.
- 25 Gigabit Ethernet with or without RS(528,514) — Measure pre-FEC and post FEC performance using Ethernet/MAC layer traffic.
- 10 Gigabit Ethernet LAN — Measure Ethernet/MAC layer traffic.
- 1 Gigabit Ethernet Optical — Measure Ethernet/MAC layer traffic. Supports auto-negotiation.
- 10/100/1000 Base-T electrical Ethernet using the CSFP-1G-CU pluggable — Measure Ethernet/MAC layer traffic. Supports auto-negotiation.
- RS-FEC — The instrument can transmit correctable or uncorrectable RS-FEC errors, and then measure post-FEC performance on the Ethernet/MAC layer using frame loss ratio measurements. The measurements are provided in a dedicated RS-FEC statistics result category.
- BER testing — You can verify circuit performance by sending BERT patterns over switched (layer 2) and unswitched (layer 1) networks.
- Layer 3 testing — Tests using IPv4.
- Layer 3 testing — Ping tests using IPv6.
- Class of Service testing — You can verify circuit performance using the Acterna payload pattern to obtain throughput, latency, real-time frame loss, and packet jitter results.

- VLAN and Q-in-Q testing — You can configure, transmit, and analyze traffic carrying SVLAN and CVLAN tags per IEEE 802.1ad to verify that your network can support and prioritize traffic for multiple customers without conflicts. Support of up to four levels of VLAN tags is provided.

For details, see “[Configuring Q-in-Q traffic](#)” on page 27.

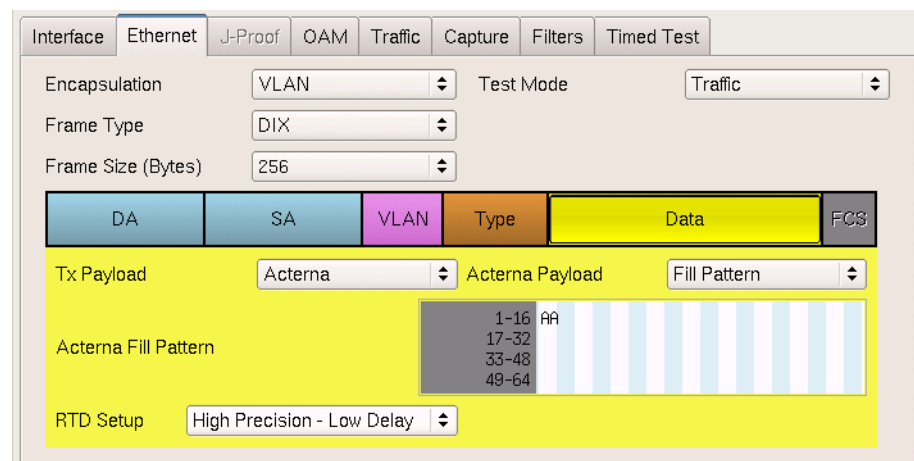
Understanding the graphical user interface

When you configure your module for testing, graphical displays of Ethernet frames are provided on the setup tabs for the application you selected. You can specify frame characteristics for transmitted and filtered traffic by selecting the corresponding field on the graphic, and then entering the value for transmitted or filtered traffic. Colored fields can be edited; fields in gray can not be modified.

Frame settings

Figure 10 illustrates the frame settings for a layer 2 traffic test, with the Data field selected.

Figure 10 Frame Settings



Adjusting the frequency of transmitted optical signals

You can adjust the frequency of transmitted optical signals in increments of 1 PPM or higher.

To adjust the frequency

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Connect the module to the circuit.

- 3 Select the **Laser** button.
- 4 Select the Laser action bar, and then do one of the following:
 - To increase the frequency by 1 PPM, press Freq Offset +1.
 - To decrease the frequency by 1 PPM, press Freq Offset -1.
 - You increase or decrease the frequency up to 150 PPM.
- 5 On the transmitting unit, observe the values for the following results in the Interface result group, Signal category:
 - Tx Freq Max Deviation (ppm)
 - Tx Frequency Deviation (ppm)
- 6 On the receiving unit, verify that the values for the following results match the transmitted frequency values.
 - Rx Freq Max Deviation (ppm)
 - Rx Frequency Deviation (ppm)

The frequency was adjusted.

Enabling automatic traffic transmission

You can optionally set up Ethernet test applications to generate and transmit traffic automatically whenever you turn the laser on.

Prerequisites for traffic transmission

If you enable automatic traffic generated, traffic is transmitted after the following occurs:

- You turn the laser ON (using the Laser ON action button).
- A signal is acquired.
- Synchronization is acquired.
- A link is established.

As always, you can turn traffic off at any time using the **Stop Traffic** action button.

Issues to consider

Consider the following issues and behavior before enabling automatic traffic generation:

- **Changing setups while tests are running.** Your unit is designed to handle traffic transmission appropriately when you change key setups while a test is running. In some instances, if you change key setups while running a test, traffic stops temporarily (as a result of the changed setup), and then starts again. In other instances, changing a setup stops traffic entirely until you actively start it again.

This is still the case when automatic traffic generation is enabled. If you change a setup that causes the unit to stop transmitting traffic entirely, you must actively start it again by pressing the **Start Traffic** action button.

- **loopback testing.** Ensure that your unit is not placed in loopback mode by verifying that the LLB action button is gray. If you intend to issue a command to loop up another unit, make certain automatic traffic generation is not enabled on the far end unit. If it is not disabled, the far end unit will not respond to the loop up command.

Enabling the feature

To enable automatic traffic generation

- 1 Using the Test menu, launch the test application for the optical interface you are about to test.
- 2 Select the Setup soft key, and then do the following:
 - a Select the Interface tab.
 - b Select the Physical Layer sub-tab.
 - c Set **Auto-start traffic when laser turned on** to **Yes**.

Traffic will be transmitted after you turn the laser on and the criteria listed in [“Prerequisites for traffic transmission” on page 22](#) is satisfied.

Layer 2 testing

Using the instrument, you can transmit, monitor, and analyze layer 2 Ethernet traffic. Step-by-step instructions are provided in this section for the following:

- [“Specifying interface settings” on page 23](#)
- [“Specifying Ethernet frame settings” on page 24](#)
- [“Specifying traffic load settings” on page 33](#)
- [“Transmitting and analyzing layer 2 traffic” on page 37](#)



NOTE:

If during the course of testing you change the frame length (or settings that impact the calculated frame length) while the unit is already transmitting traffic, the unit resets your test results, but some residual frames of the old length may be counted because they are already in the traffic stream.

Specifying interface settings

Before you transmit traffic, you can specify interface settings which specify the source of the reference Signal Clock”

- **Internal** - where synchronization with incoming signal is not necessary (default).
- **Recovered** - from timing signals embedded in incoming signal (Sync-E).
- **External** - stable reference signal input into connectors on the interface panel.

Specifying Ethernet frame settings

Before you transmit traffic, you can specify the frame characteristics of the traffic, such as encapsulation (VLAN, Q-in-Q, up to four stacked VLAN), and payload (Acterna test frames or BERT patterns).

Things to consider

Consider the following before specifying the settings:

- Changing BERT patterns or payload type. In order for a BERT analysis to be reliable, the test configuration must not change for the entire duration of the test. Changing any part of the configuration, including the pattern or source of the frames being analyzed (including changes in loopback) may result in momentary BERT bit errors and a pattern sync loss detected by the receiver after the traffic resumes.

If you do experience bit errors and sync losses after changing the test configuration (including initiating loop up) and starting traffic, press the Restart soft key to clear the initial burst of errors. If you no longer make configuration changes, you can stop and start traffic without experiencing extraneous bit errors or sync losses. If you continue to see BERT bit errors after performing a test restart, this indicates a problem with the circuit under test.

Specifying the settings

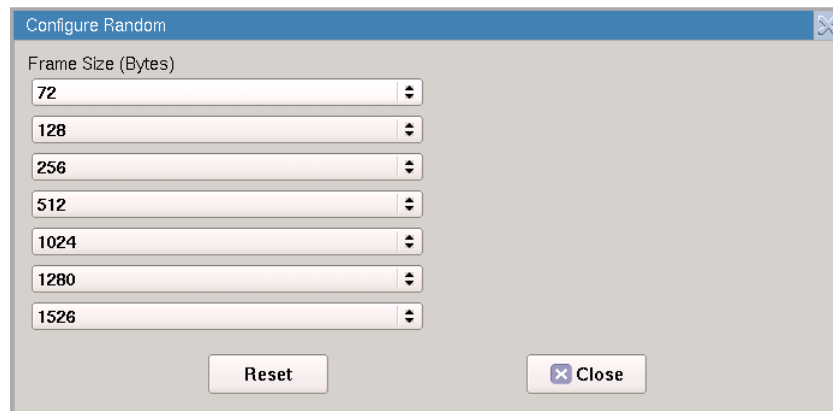
To specify Ethernet frame settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Ethernet** tab.
- 3 In **Encapsulation**, select one of the following:
 - **None**. If you do not want to encapsulate transmitted frames, select **None**.
 - **VLAN**. If you want to transmit VLAN tagged frames, select **VLAN**, and then refer to [“Configuring VLAN tagged traffic” on page 27](#).
 - **Q-in-Q**. If you want to transmit VLAN stacked (Q-in-Q) frames, select **Q-in-Q**, and then refer to [“Configuring Q-in-Q traffic” on page 27](#).
 - **Stacked VLAN**. If you want to transmit stacked VLAN frames, select **Stacked VLAN**, and then refer to [“Configuring stacked VLAN traffic” on page 28](#). Up to four levels of VLAN tags are provided.

- 4 In Test Mode, specify the category of testing being done:
 - **Traffic.** Standard mode that transmits unicast frames that satisfy the receiving unit's filter criteria.
- 5 In Frame Type, specify the type of frame you are transmitting, for example DIX or 802.3.
- 6 If you selected a layer 2 application, in **Frame Size (Bytes)**, select one of the IEEE recommended frame lengths, Random, EMIX or enter a specific Jumbo or User Defined frame length. Frame sizes up to 16,000 bytes can be used.
- 7 If you selected **VLAN, Q-in-Q, or Stacked VLAN** encapsulation, all IEEE recommended frame lengths will be increased in size by 4 bytes for each VLAN tag selected.

If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

Figure 11 Configure Random Frame Size



- If you are configuring layer 2 traffic, use the graphical display of a frame to specify the following:

Frame Label	Setting	Value
DA	Destination Type	Select the type corresponding to the Destination Address that will be inserted in the transmit frames: <ul style="list-style-type: none"> – Unicast. If you select Unicast, the least significant bit of the leftmost byte in the MAC address is forced to 0. – Multicast. If you select Multicast, the least significant bit of the leftmost byte in the MAC address is forced to 1. – Broadcast If you select Broadcast, the MAC address is automatically FFFFFFFF.
	Destination MAC	If you specified Unicast or Multicast as the destination type, enter the destination address using a 6 byte hexadecimal format.
	Loop Type	Select one of the following: <ul style="list-style-type: none"> – Unicast. The unit will issue a unicast message and loop-up the device with the Destination MAC address that you specified. – Broadcast. The unit will issue a broadcast hello message, and will then send a unicast loop-ip to the first device on the circuit that responds to the hello.
SA	Source Type	Select Factory Default or User Defined .
	User MAC	If you specified User Defined, enter the unicast source MAC address using a 6 byte hexadecimal format.
	Auto Increment MAC	If you would like the unit to automatically increment the MAC address carried in each frame by one, select Yes .
	# MACs in Sequence	If you indicated that you would like the unit to increment the MAC addresses, specify the number of MACs in the sequence. The addresses will be assigned in succession, and will repeat after the number specified for the sequence is complete.
	Disable OoS Results	If you indicated that you would like the unit to increment the mac addresses, any results from out of sequence result (lost frames) will show "N/A" in the results display.
Type	EtherType	If Tx Payload is Acterna, specify the desired Ethertype value form 0x0600-0xFFFF. Received ATP frames must have the same ethernet type to be recognized as Acterna Test Packets.

Frame Label	Setting	Value
Data	TX Payload	<p>Select from-</p> <ul style="list-style-type: none"> – Acterna. To transmit frames that contain a sequence number and time stamp so that lost frames, round trip delay, and jitter can be calculated, select Acterna. – Acterna Fill Pattern- these may be filled with any hexadecimal bytes, up to a total of 64 bytes. For 10GE, the fill pattern is 1 byte. – BERT. To transmit frames with payloads filled with the BERT pattern you specify, select BERT, and then select a pattern. – The pseudo-random patterns continue from one frame into the next. The fixed patterns, if available, restart each frame, such that the frame will always start with the beginning of the pattern.

- 8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The frame settings for transmitted traffic are specified.

Configuring VLAN tagged traffic

To configure VLAN tagged traffic

- 1 After selecting VLAN as your encapsulation, on the graphic of the frame, select **VLAN**
- 2 Enter the VLAN ID transmitted in the VLAN ID field in a decimal format ranging from 0 to 4095.
- 3 In User Priority, select the priority (0 to 7) from the drop-down menu.
- 4 If you are configuring traffic for a layer 2 application, return to [“Specifying Ethernet frame settings”](#).

VLAN settings are specified.

Configuring Q-in-Q traffic

To configure Q-in-Q traffic

- 1 After selecting **Q-in-Q** as your encapsulation, on the graphic of the frame, select SVLAN, and then specify the SVLAN ID, SVLAN User Priority, DEI Bit, and SVLAN TPID for the service provider.
- 2 Select CVLAN, and then specify the VLAN ID and User Priority for the customer’s traffic.
- 3 Return to [“Specifying Ethernet frame settings”](#) for details on specifying the remaining settings.

Q-in-Q settings are specified.

Configuring stacked VLAN traffic

To configure Stacked VLAN traffic

- 1 After selecting **Stacked VLAN** as your encapsulation, on the graphic of the frame, select VLAN Stack, and then specify the stack depth (number of VLANs).
- 2 For each VLAN, specify the SVLAN ID, SVLAN User Priority, DEI Bit, and SVLAN TPID for the service provider. You can now specify a User Defined TPID if you choose to.
- 3 Select CVLAN, and then specify the VLAN ID and User Priority for the customer's traffic.
- 4 Return to ["Specifying Ethernet frame settings"](#) for details on specifying the remaining settings.

Stacked VLAN settings are specified.

Specifying Ethernet Filter settings

Before transmitting traffic, you can specify settings that indicate the expected received payload and determine which frames or packets will pass through the filter and be counted in the test result categories for filtered traffic. For example, you can set up the filter to observe results for all traffic sent to a specific destination address. The filter settings may also impact other results.



NOTE

During Layer 2 BER testing, incoming frames must pass the filter to be analyzed from a BERT pattern. Local loopback is also only performed on frames that pass the filter. Use the filter to analyze BERT frames when non-test frames are present, such as spanning tree frames.

To specify Ethernet filter settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Filters** tab. By default, a summary of all applicable filter settings appears (Ethernet, IP, and TCP/UDP).
- 3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.
- 4 To specify layer 2 filter settings, in the panel on the left side of the tab, select Ethernet, then do the following:
 - a If you want to filter traffic based on the type of encapsulation used, specify the following values:

Setting	Value
Encapsulation	<p>Select one of the following:</p> <ul style="list-style-type: none"> – None. The instrument will only analyze analyze only unencapsulated traffic. – VLAN. The instrument will analyze only VLAN encapsulated traffic for the parameters you specify. – Q-in-Q. The instrument will analyze only Q-in-Q encapsulated traffic for the parameters you specify. – Stacked VLAN. The instrument will analyze only stacked VLAN encapsulated traffic for the parameters you specify. – Don't Care. The instrument will analyze traffic satisfying all other filter criteria regardless of encapsulation.
VLAN	If you specified VLAN as the encapsulation type, on the graphic display of the frame, select VLAN and then specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified VLAN as the encapsulation type and you want to filter for traffic with a specific user priority, specify the priority or select Don't Care .

b In the Frame Type, specify one of the following:

Frame Type	Description
DIX	To analyze DIX frames only, select DIX.
EtherType	If you specified DIX as the frame type, specify the EtherType by selecting the Type field on the graphic of the frame. If you do not specify the EtherType, the module will filter the traffic for DIX frames with the currently specified EtherType value.
802.3	To analyze 802.3 frames only, select 802.3.
Data Length (bytes)	If you specified 802.3 as the frame type, specify the data length by selecting the Length field on the graphic of the frame. If you do not specify the length, the module will filter the traffic for 802.3 frames with the currently specified length.
Don't Care	<p>If you want to analyze both DIX and 802.3 VLAN or Q-in-Q encapsulated traffic, select Don't Care.</p> <p>You must specify a frame type if you are filtering encapsulated traffic.</p>

Filtering traffic using Q-in-Q criteria

If your instrument is configured to transmit Q-in-Q encapsulated traffic, you can filter received traffic using Q-in-Q criteria.

To filter traffic using Q-in-Q criteria

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the layer 2 or layer 3 test application for the interface you are testing.
- 2 Select the Setup soft key, and then select the Ethernet tab. Verify that Q-in-Q is specified as the encapsulation.
- 3 Select the Filters tab. In the panel on the left side of the tab, select Ethernet, then specify the following:
 - a On the graphic of the frame, select **SVLAN** and specify the following:

Setting	Value
SVLAN ID	Specify the SVLAN ID carried in the filtered traffic.
SVLAN User Priority	If you want to filter traffic for a specific user priority, specify the priority; otherwise select Don't Care .
SVLAN DEI Bit	If you want to filter traffic for a specific DEI Bit, specify the bit value; otherwise select Don't Care .
SVLAN TPID (hex)	Specify the TPID carried in the filtered traffic. If you are transmitting traffic with a user defined TPID, your instrument will automatically use the TPID that you specified in the User SVLAN TPID (hex) field. NOTE: If you want to filter on a user-defined TPID, you must also enter that TPID on the RX Payload/TPID setup page.

- b On the graphic of the frame, select CVLAN and specify the following:

Setting	Value
Specify VLAN ID	If you specified Q-in-Q as the encapsulation type, and you want to filter traffic for a specific CVLAN, select Yes ; otherwise, select Don't Care .
VLAN ID	If you specified Q-in-Q as the encapsulation type and indicated you want to filter traffic for a particular CVLAN, specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified Q-in-Q as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the User Priority carried in the filtered traffic.

- 4 If you want to analyze/detect frames carrying User Defined SVLAN TPID as Q-in-Q traffic, you have to specify the expected User Defined TPID value(s) on the Filters->Rx->TPID page. The TPID values on this page are used to recognize Q-in-Q traffic with User Defined TPID. If you want to analyze/detect Q-in-Q traffic carrying the same TPID that you specified for transmitted traffic, check the box for Use Tx User SVLAN TPID.

- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The Q-in-Q filter settings are specified.

Filtering traffic using stacked VLAN criteria

If your instrument is configured to transmit stacked VLAN encapsulated traffic, you can filter received traffic using stacked VLAN criteria.

To filter traffic using stacked VLAN criteria

- 1 If you haven't already done so, use the Test Menu to select the layer 2 test application for the interface you are testing.
- 2 Select **Setup**, and then select the **Ethernet** tab. Verify that Stacked VLAN is specified as the encapsulation.
- 3 Select the **Filters** tab. In the panel on the left side of the tab, select **Ethernet**, then specify the following:
 - a On the graphic of the frame, select **SVLAN**, and then specify the following:

Setting	Value
SVLAN ID	Specify the SVLAN ID carried in the filtered traffic.
SVLAN User Priority	If you want to filter traffic for a specific user priority, specify the priority; otherwise, select Don't Care .
SVLAN DEI Bit	If you want to filter traffic for a specific DEI Bit, specify the bit value; otherwise, select Don't Care .
SVLAN TPID (hex)	Specify the TPID carried in the filtered traffic. If you are transmitting traffic with a user defined TPID, your instrument will automatically use the TPID that you specified in the User SVLAN TPID (hex) field.

- b On the graphic of the frame, select **CVLAN**, and then specify the following:

Setting	Value
Specify VLAN ID	If you specified stacked VLAN as the encapsulation type, and you want to filter traffic for a specific CVLAN, select Yes ; otherwise, select Don't Care .
VLAN ID	If you specified stacked VLAN as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified stacked VLAN as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the User Priority carried in the filtered traffic.

- 4 If you want to analyze/detect frames carrying User Defined SVLAN TPID as Stacked VLAN traffic, you have to specify the expected User Defined TPID value(s) on the Filters->Rx->TPID page. The TPID values on this page are used to recognize Stacked VLAN traffic with User Defined TPID. If you want to analyze/detect Stacked VLAN traffic carrying the same TPID that you specified for transmitted traffic, check the box for Use Tx User SVLAN TPID.
- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The stacked VLAN filter settings are specified.

Filtering traffic using payload criteria

You can filter traffic using payload criteria, or you can turn payload analysis off entirely.

To specify payload filter settings

- 1 In the panel on the left side of the tab, select **Rx Payload**, then specify the following:

Setting	Value
Payload Analysis	Specify one of the following: <ul style="list-style-type: none"> – Off. If you want the module to monitor and analyze live Ethernet traffic by suppressing lost frames (LF) or BERT errors in their associated result counts and as triggers for LEDs during payload analysis, select Off. – On. If you want to analyze traffic carrying a particular BERT pattern, select On.
Use Tx BERT settings	Specify one of the following: <ul style="list-style-type: none"> – If you want the module to monitor and analyze traffic carrying a different BERT pattern than the one specified for transmitted traffic, clear the box. – If you want to analyze traffic carrying the same BERT pattern carried in transmitted traffic, check the box.
Rx Payload (Payload Analysis On, and Use Tx BERT settings un-checked)	Specify Acterna or BERT .
Rx BERT Pattern Payload Analysis On, and Use Tx BERT settings un-checked)	If you unchecked Use Tx BERT settings, specify the BERT pattern carried in the filtered traffic.

Payload filter criteria is specified.

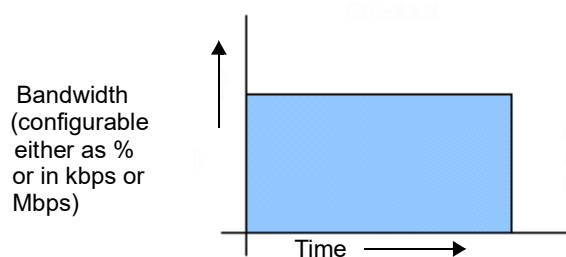
Specifying traffic load settings

Before transmitting traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty or Ramp). The settings vary depending on the type of load. When configuring a load, you can specify the bandwidth of the transmitted traffic in 0.001% increments.

Transmitting a constant load

With a **constant** load, the module transmits frames continuously with a fixed bandwidth utilization. You can specify the load as a percent or a bit rate. See [Figure 12](#).

Figure 12 Constant traffic



When you setup a constant traffic load, if you are running a standard Ethernet application, you can specify the bandwidth as a percentage of the line rate (%BW) or at a specific bit rate. The bit rate can be specified in Gbps.

To configure the module to transmit a constant load of traffic

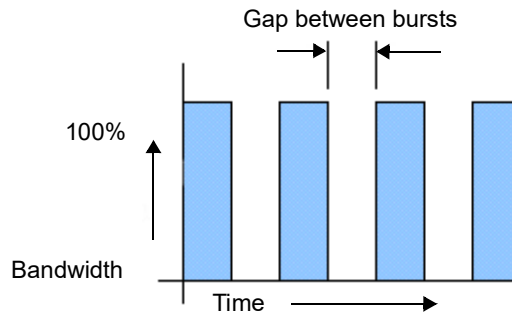
- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Traffic tab.
- 3 In Load Type, select **Constant**.
- 4 In Load Unit:
 - a select one of the following:
 - **Percent**. If you select Percent, in **Load %**, enter the duty cycle as a percentage.
 - **Bit Rate**. If you select Bit Rate, in **Load (Mbps)** or **Load (kbps)** enter the bit rate in Mbps or kbps.
 - **Frames Per Second**.
 - b Select the **Allow flooding** check box to transmit a true 100% load in those circuits that you are certain can handle the signal.
- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The module is configured to transmit a constant rate of traffic.

Transmitting a bursty load

With a **bursty** load, the module transmits frames at 100% bandwidth for a specific time interval, followed by no frame transmissions during the specified gap interval. See [Figure 13](#).

Figure 13 Bursty traffic



When you configure bursty traffic, if you are running a standard Ethernet application, you can specify the burst load as a percentage of the duty cycle, or by specifying the burst and gap intervals in units of time, bytes and Information Rate (IR). If you specify the burst load as a percentage of the duty cycle, and then specify the number of frames per burst, the module automatically calculates the burst gap.

To configure the module to transmit bursts of traffic

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Traffic tab.
- 3 In Load Type, select **Burst**.
- 4 In Load Unit, select one of the following:
 - **Bytes and Information Rate**. Proceed to [step 5](#).
 - **Burst Time and Information Rate**. Proceed to [step 5](#).
 - **Gap Time and Information Rate**. Proceed to [step 5](#).
 - **Bytes and Gap Time**. Proceed to [step 5](#).
 - **Burst Time and Gap Time**. Proceed to [step 5](#).
 - **Frames and Duty Cycle**. Proceed to [step 6](#).

- 5 If you selected any of the combinations of Time, Rates and Byte, the following parameters may need to be set:



NOTE:

Values may be automatically normalized (rounded to nearest appropriate values) from values entered.

- a **Information Rate.** Enter the average throughput rate in Mbps up to the maximum rate of the interface (layer 2 only).
 - b **Burst KBytes.** Enter the number of Kbytes of data desired to be transmitted in each burst of traffic.
 - c **Burst Time.** Enter the amount of time that each burst of traffic should be transmitted (will round to the nearest frame transmit time).
 - d **Time Unit.** Select unit for time entry - sec, msec, usec or nsec.
 - e **Gap/Idle Time.** Enter the amount of time between each burst. The valid range for this setting adjusts depending on the Burst Time that is entered, to ensure that the duty cycle is at least 1% in 0.001% intervals (will round to the nearest 0.001%).

The following parameters may be displayed as a result of the above selections:
 - f **Bit Rate (calculated).** Bits/Time Unit from Burst average throughput rate (will round down to the nearest frame size).
 - g **Actual KBytes (calculated).** Actual value of bytes/burst. Values above the line rate can not be entered.
- 6 If you selected Frames and Duty Cycle as the load unit, set the following:
- a **Duty Cycle (%).** Enter the percentage of the line rate (the duty cycle) during which traffic will be transmitted in the burst, from 0.001 - 100%.
 - b **Frames/Burst Time.** Select a predefined value, or User-Defined, for the number of frames that are to be included in each burst.
 - c **User Burst Size.** If User-Defined is specified for Frames/Burst, define the User Burst size, 1- 65535 frames.
- 7 Specify the burst type for the traffic:
- **Fixed.** Sends a fixed number of bursts and then stops. If you select Fixed, enter the number of bursts.
 - **Continuous.** Sends bursts continuously.
- 8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

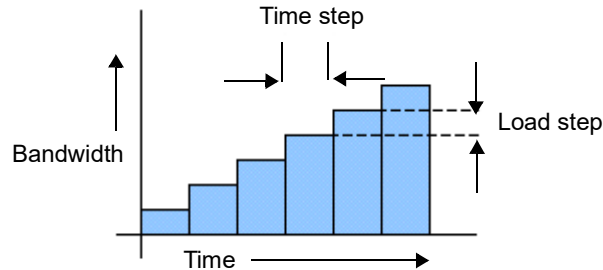
The module is configured to transmit bursts of traffic.

Transmitting a ramped load

With a **ramped** load, the module automatically increases the load by a percentage of bandwidth (specified as the load step) at a particular time interval (specified as the time

step). The process is repeated, allowing you to easily verify the maximum throughput of a link. See [Figure 14](#).

Figure 14 Ramped traffic



You can also specify criteria to tell the module to stop ramping if an error (or errors) occurs in a load step.

To configure the module to transmit a ramped load of traffic

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Traffic tab.
- 3 In Load Type, select **Ramp**, and then specify the following settings:
 - a **Time Step (sec)**. Enter the time step in seconds.
 - b **Load Step**. Enter the load step as a percentage of the total bandwidth.
- 4 *Optional*. If you want to stop the ramp from incrementing when certain errors occur, under Stop Load Increments, specify the following:
 - **Errored Frames**. If you want to stop incrementing the load if FCS errored frames are detected, select **Yes**, and then enter the number of errored frames that must be detected to stop the ramp.
 - **Dropped Frames**. If you want to stop incrementing the load if dropped frames are detected, select **Yes**, and then enter the number of dropped frames that must be detected to stop the ramp.



NOTE:

Acterna frames carry a sequence number which the unit uses to determine whether frames were dropped; therefore, you must configure your unit to transmit an Acterna payload, turn payload analysis on, and loop the far-end device back to the traffic originating unit.

- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The module is configured to transmit ramped traffic.

Transmitting and analyzing layer 2 traffic

Before you transmit layer 2 traffic, you must specify:

- Interface settings (see [“Specifying interface settings” on page 23](#)).
- Frame characteristics for the transmitted traffic (see [“Specifying Ethernet frame settings” on page 24](#)).
- Traffic load settings (see [“Specifying traffic load settings” on page 33](#)).

After you specify the layer 2 settings, you are ready to transmit and analyze the layer 2 traffic.



NOTE: Layer 2 BERT testing

Layer 2 BERT patterns carried in a BERT payload are not compatible with BERT patterns carried in an ATP payload. When testing using two instruments, be certain to configure both using the same payload type and BERT pattern.

To transmit and analyze layer 2 traffic

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see [“Specifying interface settings” on page 23](#)).
- 3 Select the **Ethernet** tab to specify settings that define the frame characteristics of the transmitted traffic (see [“Specifying Ethernet frame settings” on page 24](#)).
- 4 Select the **Ethernet Filter** tab to specify settings that filter the received traffic based on specified frame characteristics (see [“Specifying Ethernet frame settings” on page 24](#)).
- 5 Select the **Traffic** tab to specify the type of load the unit will transmit (see [“Specifying traffic load settings” on page 33](#)).
- 6 Press **Results** to return to the Main screen.
- 7 Connect the module to the circuit.
- 8 If you are testing an optical interface, select the **Laser** button.
- 9 Select **Start Traffic** to transmit traffic over the circuit.
- 10 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 11 At a minimum, observe the summary, link statistics and counts, filter statistics and counts, error statistics, and layer 2 BERT statistics results.

You have analyzed layer 2 traffic.

LBM (Y.1731)

Traffic can be generated up to the line rate using **Test Mode LBM** on the **Ethernet** tab; this is available in the Layer 2 multiple streams application. In this mode, the application generates LBM frames that contain ATP as payload for analysis. A third-party device, typically a router, is expected to loop this traffic back toward the traffic generating test unit as LBR frames; the LBR frame ATP payload can then be analyzed. This is available at Ethernet line rates except 400GigE and 4x100GigE.

Layer 3 testing

Using the instrument, you can transmit, monitor, and analyze layer 3 IPv4 or IPv6 traffic. Step-by-step instructions are provided in this section for the following:

Specifying L3 interface settings

You can specify interface settings before you transmit traffic. Specification of the interface settings is similar for Layer 2,3, and 4 applications. An explanation of these settings can be found at [“Specifying interface settings” on page 23](#).

Specifying the data mode and link initialization settings

Before transmitting Layer 3 traffic, you must provide the appropriate link initialization settings.

To specify the data mode and initialization settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Ethernet** tab.
- 3 In Encapsulation, select one of the following:
 - **None**. If you do not want to encapsulate transmitted traffic, select **None**.
 - **VLAN**. If you want to transmit VLAN tagged frames, select VLAN, and then refer to [“Configuring VLAN tagged traffic” on page 27](#).
 - **Q-in-Q**. If you want to transmit VLAN stacked (Q-in-Q) frames, select **Q-in-Q**, and then refer to [“Configuring Q-in-Q traffic” on page 27](#).
 - **Stacked VLAN**. If you want to transmit stacked VLAN frames, select **Stacked VLAN**, and then refer to [“Configuring stacked VLAN traffic” on page 28](#). Up to four levels of VLAN tags are provided.
- 4 If you want the unit to issue an ARP request to determine the destination MAC address of the instrument's link partner, in ARP mode, select **Enabled**; otherwise, select **Disabled**, and then be certain to manually specify the destination MAC address, (see [“Specifying Ethernet frame settings” on page 24](#)).

If you enabled ARP, and you only want to respond to ARP requests from devices on the same VLAN specified for transmitted traffic, select **Match VLAN ID(s)**.

NOTE: If you need your unit to respond to ARP requests from other devices (for example, a second test instrument on the circuit), be certain to enable ARP.

- 5 In Frame Type, specify **DIX** or **802.3**.
- 6 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.
 - **Frame Size.** If you select Frame Size, select a pre-defined size, or select User Defined or Jumbo, and then specify the size. The calculated packet length (in bytes) appears to the right of the field.
 - **Packet Length.** . If you select Packet Length, select a pre-defined length, or select User Defined or Jumbo and then specify the length. The calculated frame size (in bytes) appears to the right of the field.
- 7 If you want to specify a source address for the traffic, select **SA**, and then specify the following:
 - **Source MAC Address.** Select Factory Default or User Defined.
 - **User MAC Address.** If you specified User Defined, enter the source MAC address using a 6 byte hexadecimal format.
- 8 Select the **Filter** tab, and then specify the Ethernet filter settings for the destination type, source type, and encapsulation.

Specifying transmitted IPv4 packet settings

Before you transmit layer 3 IPv4 traffic, you can specify the IP characteristics of the traffic, such as the IP address, the type of payload, and the type of service.

To specify transmitted IPv4 packet settings

- 1 If you have not already done so, use the Test Menu or Quick Launch screen to select the layer 3 test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **IP** tab.
- 3 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.
 - **Frame Size.** If you select Frame Size, you must specify the size on the Ethernet tab, then return to the IP tab to specify the remaining settings.
 - **Packet Length.** If you select Packet Length, select a pre-defined length, or select User Defined or Jumbo and then specify the length. The calculated frame size (in bytes) appears to the right of the field.
- 4 On the illustration of the IP packet, select the **TOS/DSCP** field, and then do the following to indicate how the packet should be prioritized during the transmission:
 - In Type, select **TOS** or **DSCP**.
 - Specify the TOS or DSCP value. DSCP values are shown as code points with their decimal values in () following. For example: EF(46).

- 5 Select the **TTL** field, and then specify maximum number of hops to travel before the packet is dropped.
- 6 Select the **Source/Destination Address** field, and then specify the Source IP Type, Source IP, Default Gateway, Subnet Mask and Destination IP.
- 7 Select the Data field, and then do the following:
 - If you want to transmit packets with a time stamp and sequence number, select **Acterna**.



NOTE:

You must select an Acterna payload to measure round trip delay and count lost packets.

- If you want to populate the payload by repeating a specific pattern of bytes, select **Fill Byte**, type the byte value using a 1 byte hexadecimal format.
- 8 If you need to specify the other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The transmitted IPv4 packet settings are specified.

Specifying IPv4 filter settings

Before transmitting layer 3 IPv4 traffic, you can optionally specify settings that indicate the expected received payload and determine which packets will pass through the receive filter and be counted in the test result categories for filtered IP traffic. The settings may also impact other results.

To specify received IPv4 packet settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the IPv4 test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Filters** tab.
- 3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.
- 4 Specify the Ethernet filter settings (see [“Specifying Ethernet Filter settings” on page 28](#)).
- 5 To specify layer 3 filter settings, in the panel on the left side of the tab, select **IP**.
- 6 Set the IP Filter to **Enable**., then do the following:
 - a If you are running an application in Monitor mode, in **IP Version**, select IPv4.
 - b In **Address Filter**, select one of the following:
 - Single Direction**. To pass through the filter, traffic must satisfy the source and destination address criteria you specified for the filter to be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

Either Direction. The filter will not care which direction the traffic is coming from; therefore, the source address carried in the filtered traffic can be the source address of the near-end unit or port, or the source address of the far end unit or port. Traffic from either source will be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

- c On the illustration of the IP packet, select the **TOS/DSCP**, **Protocol**, **Source IP**, or **Destination IP** field, and then enter the filter criteria. This is the criteria that must be carried in the analyzed (filtered) traffic. For descriptions of each of these settings, see [“Specifying transmitted IPv4 packet settings” on page 39](#).
- 7 If you want the module to monitor and analyze live Ethernet traffic, in the panel on the left side of the tab, select **Rx Payload**, then turn Payload Analysis Off. The instrument will suppress lost frames (LF) in their associated result counts and as triggers for LEDs.
- 8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings for IPv4 packets are specified.

Specifying transmitted IPv6 packet settings

Before you transmit layer 3 IPv6 traffic, you can specify the IP characteristics of the traffic, such as the source type and default gateway.

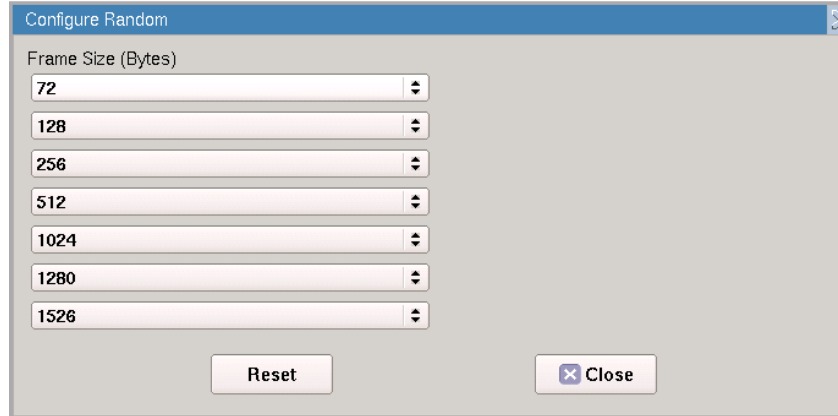
To specify transmitted IPv6 packet settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the IPv6 test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **IP** tab.
- 3 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.
 - **Frame Size.** If you select Frame Size, you must specify the size on the Ethernet tab, then return to the IP tab to specify the remaining settings.
 - **Packet Length.** If you select Packet Length, select a pre-defined length, or select User Defined, Jumbo, or Random and then specify the length. The calculated frame size (in bytes) appears to the right of the field.

If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that

controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

Figure 15 Configure Random Frame Size



- 4 On the illustration of the IP packet, select the **Traffic Class** field, and then specify a number representing the traffic class using a hexadecimal format ranging from 0x0 to 0xFF.
- 5 Select the **Flow Label** field. If you are certain the routers on the circuit support flow labels for traffic prioritization, specify the flow label using a hexadecimal format ranging from 0x0 to 0xFFFF; otherwise, use the default (0x0).
- 6 Select the **Next Header** field, then specify the code representing the type of data carried in the next header in the packet using a hexadecimal format ranging from 0x0 to 0xFF.
- 7 Select the **Hop Limit** field, then specify the time after which a packet can be deleted by any device on a circuit as a number of hops. The default Hop Limit setting is 64 hops.
- 8 Select the **Source Address** field, then select one of the following:
 - **Stateful.** Select Stateful if you want to obtain the required global, default gateway, and DNS server addresses from a DHCPv6 server.
 - **Stateless.** Select Stateless if you know that routers on the network allow stateless configuration. When you use Stateless configuration, the instrument generates a tentative link-local address, and then performs Duplicate Address Detection to verify that the address isn't already used. If DAD is successful, the instrument then obtains a subnet prefix from the router to build the required global address.
 - **Manual.** Select Manual if you want to specify the source link-local address, global address, subnet prefix length, and default gateway.
- 9 Select the **Destination Address** field, and then specify the destination address for the traffic.
- 10 Select the Data field, and then select do the following:
 - If you want to transmit packets with a time stamp and sequence number, select **Acterna**.

Indicate whether you want the payload to carry a BERT pattern, or a Fill-Byte pattern, then specify the pattern.

- If you want to populate the payload by repeating a specific pattern of bytes, select **Fill Byte**, type the byte value using a 1 byte hexadecimal format, and then specify the **Protocol**.

- 11 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The transmitted IPv6 packet settings are specified.

Specifying IPv6 filter settings

Before transmitting layer 3 IPv6 traffic, you can optionally specify settings that indicate the expected received payload and determine which packets will pass through the receive filter and be counted in the test result categories for filtered IPv6 traffic. The settings may also impact other results.

To specify received IPv6 packet settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the IPv6 test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Filters** tab.
- 3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.
- 4 Specify the Ethernet filter settings (see [“Specifying Ethernet Filter settings” on page 28](#)).
- 5 To specify layer 3 filter settings, in the panel on the left side of the tab, select **IP**.
- 6 Set the IP Filter to **Enable**, then do the following:
 - a If you are running an application in Monitor mode, in **IP Version**, select IPv6.
 - b In **Address Filter**, select one of the following:
 - **Single Direction**. To pass through the filter, traffic must satisfy the source and destination address criteria you specified for the filter to be reflected in the L3 Filter Counts and L3 Filter Stats result categories.
 - **Either Direction**. The filter will not care which direction the traffic is coming from; therefore, the source address carried in the filtered traffic can be the source address of the near-end unit or port, or the source address of the far end unit or port. Traffic from either source will be reflected in the L3 Filter Counts and L3 Filter Stats result categories.
 - c On the illustration of the IP packet, select the **Traffic Class**, **Next Header**, **Source Address**, or **Destination Address** field, and then enter the filter criteria. This is the criteria that must be carried in the analyzed (filtered) traffic. For descriptions of each of these settings, see [“Specifying transmitted IPv6 packet settings” on page 41](#).

- 7 If you want the module to monitor and analyze live Ethernet traffic, in the panel on the left side of the tab, select **Rx Payload**, then turn Payload Analysis Off. The instrument will suppress lost frames (LF) in their associated result counts and as triggers for LEDs.
- 8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings for IPv6 packets are specified.

IPv6 Ping testing

IPv6 ping is available in the IPv6 test application.

Using the instrument, you can verify connectivity with another layer 3 or IP device by sending ping request packets to the device. If responsive, the device responds to the ping request with a ping reply or with another message indicating the reason no ping reply was sent.

Ping testing tells you if the destination device is reachable, how long it took the ping to travel to the destination device and back, and if ping packets were dropped or lost along the way.

Before you transmit ping request packets, you must specify:

- Interface settings (see [“Specifying interface settings” on page 23](#))
- Ethernet Frame settings (see [“Specifying Ethernet frame settings” on page 24](#))



NOTE

Jumbo packets are only supported for DIX traffic (the 802.3 specification does not support jumbo packets).

Jumbo frames are also not supported when the instrument is configured to transmit fast ping packets.

- IP Settings (see [“Specifying IP settings for Ping testing” on page 45](#))

After you specify the ping settings, you are ready to transmit ping request packets.



NOTE


When transmitting ping packets with the with ping Response Time set to Throttled, your instrument automatically inserts a delay. The delay is reflected in the corresponding test results within the Ping and Delay categories.

Specifying IP settings for Ping testing

Before you transmit ping request packets, you can specify settings indicating the source of the IP address (static or assigned by a DHCP server), the destination type (IP address or host name), and attributes of the ping request packets (type, size, type of service, and time to live).

The following procedure describes how to specify IP settings.

To specify IP settings

- 1 Select the **Setup** soft key, select the **Ethernet** tab, and then specify the Ethernet frame settings (see [“Specifying Ethernet frame settings” on page 24.](#)) Ensure the data mode is set (IPoE or PPPoE)
 - 2 Select the **IP** tab.
 - 3 In Source Type, select one of the following:
 - **Manual:** To manually assign an IP address as the source address for the traffic, select **Static IP**, and then type the address, subnet mask, and default gateway in the corresponding fields.
 - **Stateful:** Stateful autoconfiguration requires a DHCPv6 service.
 - **Stateless:** Allows the client device to self-configure its IPv6 address and routing based on router advertisements.
 - 4 In DNS Type, select manual or auto.
 - 5 In Destination Type, select IP Address or Host Name, and then type the destination IP address or the host name for the ping.
 - 6 Specify the following settings:
 - a In Ping Type, indicate whether you want to transmit a **Single** ping packet, **Multiple** ping packets, a **Continuous** stream of ping packets, or a **Fast** stream of ping packets. If you specify Multiple, enter the number of packets to transmit.
-  **NOTE**
The rate at which the instruments sends pings depends on the Ping Response Time Setting. Throttled introduces a delay after receiving a response.
- b In Packet Size (Bytes), enter the size of the ping request packet or packets.
 - c Make selections for the Traffic Class, Flow Label, and Hop Limit fields.
 - 7 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The IP settings for ping testing are specified.

Transmitting ping request packets

After specify the interface, frame, and IP settings, you can transmit ping request packets to verify connectivity.

To transmit ping packets

- 1 Use the Test Menu to select the layer 3 Ping test application for the interface you are testing.

- 2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see [“Specifying interface settings” on page 23](#)).
- 3 Select the **Ethernet Frame** tab to specify settings that define the frame characteristics of the transmitted traffic, and then select the **IP** tab to specify settings that characterize the ping packets (see [“Specifying IP settings for Ping testing” on page 45](#)).
- 4 Press **Results** to return to the Main screen.
- 5 Connect the module to the circuit.
- 6 If you are testing an optical interface, select the **Laser** button.
- 7 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 8 On the Main screen, select the **Ping** button to transmit the packet or packets.
- 9 At a minimum, observe the ping and IP configuration status test results.

You have transmitted ping request packets

Transmitting and analyzing IP traffic

Before you transmit layer 3 IP traffic, you must specify:

- Interface settings (see [“Specifying interface settings” on page 23](#)).
- IP characteristics of the transmitted traffic (see [“Specifying transmitted IPv4 packet settings” on page 39](#)).
- Traffic load settings (see [“Specifying traffic load settings” on page 33](#)).

After you configure the layer 3 IP settings, and you either manually specify the destination device’s MAC address or the unit determines the address using ARP, you are ready to transmit traffic over the link.

To transmit and analyze IP traffic

- 1 Use the Test Menu to select the layer 3 IP traffic terminate test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see [“Specifying interface settings” on page 23](#)).
- 3 Specify settings that define the Ethernet frame and the IP packet characteristics of the transmitted traffic (see [“Specifying transmitted IPv4 packet settings” on page 39](#)).
- 4 Select the **Setup** soft key, and then select the **Ethernet filter** tab to specify the Ethernet filter settings (see [“Specifying Ethernet Filter settings” on page 28](#)).
- 5 Select the **Traffic** tab to specify the type of load the unit will transmit (see [“Specifying traffic load settings” on page 33](#)).
- 6 Press **Results** to return to the Main screen.

- 7 Connect the module to the circuit.
- 8 Select the **Laser** button.
- 9 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.
- 10 Verify that the green Signal Present, Sync Acquired, Link Active, and IP Packet Detect LEDs are illuminated.
- 11 At a minimum, observe the summary, layer 2 and 3 link counts and statistics, layer 2 and 3 filter counts and statistics, layer 3 configuration status, and error statistics.

You have analyzed IP traffic.

Multiple Streams testing



NOTE

At this time, Multiple Streams testing applies to Layer 2 and Layer 3 IPv4 at all Ethernet rates. Up to 16 streams are available.

Multiple Streams testing uniquely characterizes each stream of traffic, allowing for the verification that the network handles VLAN tagged traffic properly by assigning a high priority to one stream and a lower priority to a second stream.

When running Multiple Stream applications, unique destination MAC and IP addresses can be assigned to each stream. Alternatively, the same addresses can be used for all streams.

Streams Pipe soft key

Press the **Streams Pipe** soft key to observe summarized test results and information for each individual stream. A variety of views are provided:

- **Overview** — This view provides key source and destination addresses and the bandwidth received and transmitted for each stream.
- **Addressing** — This view shows the source and destination IP addresses carried in each transmitted stream. The default gateway and subnet mask for each stream are also provided.
- **Traffic Loads** — This view provides more detailed information for the traffic carried in each stream, such as the currently received frame size, the received bandwidth, the transmitted traffic load type (constant or ramped), the transmitted bandwidth, and a count of transmitted Acterna frames.
- **VLAN/VPLS** — These views show key encapsulation data for each stream. For example, if you are analyzing layer 2 Q-in-Q streams, the SVLAN ID and priority for received and transmitted streams appears.

Using the action buttons

The buttons on the Main screen are used to perform actions for all enabled streams. For example, if stream 1, stream 2, and stream 3 are enabled, pressing the **Start Traffic** button transmits traffic for all three streams simultaneously.

Understanding the LED panel

When a Multiple Streams application is selected, the module provides LEDs in the panel for each *enabled traffic streams*. Figure shows the Multiple Stream LEDs.

Figure 16 Multiple Streams LEDs



Streams pipe: multiple streams

When running multiple streams applications, use the Streams Pipe softkey to specify the load unit, as described in “[Enabling multiple steams](#)” on page 50, and to access the Load Distribution dialog box.

Figure shows the Streams Pipe display for layer 4 traffic streams.

Figure 17 Streams Pipe Display: layer 4 stream



Traffic can be started and stopped from the pipe display. Specify the load and Throughput units, and press the **Configure Streams** button to enable specific streams and specify the traffic load carried in each stream.



NOTE

When observing the pipe, the Frame Length or Packet Size displayed represents the maximum length or size received for each individual stream.

Understanding Multiple Streams test results

When running Multiple Streams applications, the following results can be observed:

- Cumulative test results for the entire link
- Detailed test results for a particular stream
- Graphical results for all analyzed streams

Viewing results for a specific stream

Detailed test results for a particular stream can be viewed on the result display by specifying the stream number as the result group, then selecting the category with the results you want to observe.

Viewing cumulative link results

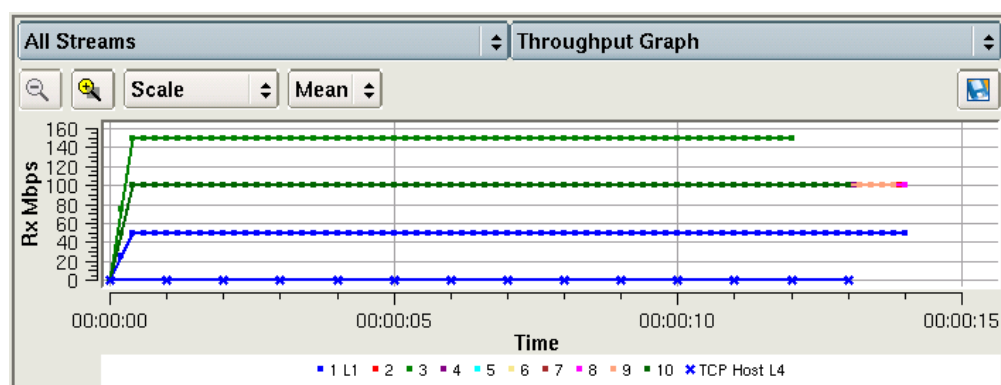
Cumulative link results for all transmitted streams can be observed by selecting the **Link** group, then selecting the corresponding **Stats**, **Counts**, **Error Stats**, or **AutoNeg Status** category.

Viewing graphical results for all streams

Throughput, latency (RTD), packet jitter, and frame loss results can be observed graphically by selecting the All Streams group, and then the category with the results you want to observe. When observing graphical results, it's helpful to view the entire result window by selecting **View > Result Windows > Full Size**.

Figure shows the Throughput Graph for multiple traffic streams.

Figure 18 Throughput Graph: Multiple Streams application



A color coded legend appears under the graph, indicating which color is used to present results for each of the analyzed streams, in [Figure 18](#), the green lines provide results for Stream 3, the blue lines provide results for Stream 1, and the bright pink line provides results for Stream 8.

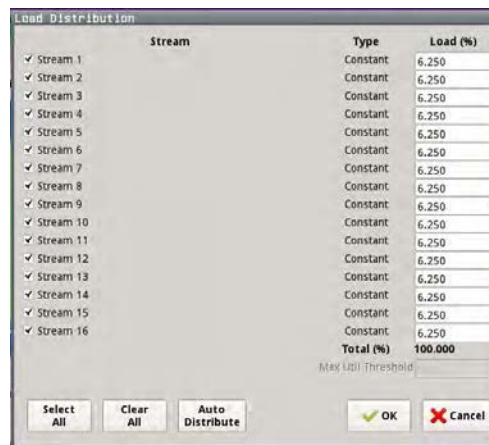
Enabling multiple steams

Perform the following procedure to enable streams on the Load Distribution dialog box when a Multiple Streams application is selected.

To enable multiple streams

- 1 Select the **Streams Pipe** soft key.
- 2 Select **Configure Streams**.
- 3 The Load Distribution screen appears, as shown in Figure.

Figure 19 Load Distribution screen



- 4 Select the streams to transmit.
Streams are enabled. If you have already specified the load type for each stream, the load can be specified.



NOTE

The **Auto Distribute** button is disabled if one or more traffic streams is configured to transmit a ramped load of traffic.

Specifying the load type for all streams

If you selected a Multiple Streams application, you can transmit a constant load or a ramped load of traffic in any stream.



NOTE:

A single stream may be defined as having a a burst load. See [“Specifying the load unit on a stream with burst” on page 52.](#)

To specify the load type for all streams

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the Multiple Streams test application for the interface you are testing.

- 2 Select the **Setup** soft key.
- 3 By default, the module transmits a constant load of traffic for each enabled stream. If this is acceptable, proceed to [step 4](#). If you want to transmit a *ramped* load of traffic for a particular stream or streams, do the following:
 - a Select the tab corresponding to the stream.
 - b Select the Traffic sub-tab.
 - c In Load Type, select **Ramp**, and then specify the time step (in seconds) and the load step (in Mbps, as a percentage of the line rate or in frames per second). For details, see [“Transmitting a ramped load” on page 130](#).
NOTE: When configuring a ramped load of traffic for a stream, the triggers used to stop the ramp *are not available*.
 - d Repeat [step a](#) through [step c](#) for each ramped stream of traffic, and then proceed to [step 4](#).
- 4 Select the **Streams Pipe** soft key, and then select **Configure Streams**.
The Load Distribution screen appears.
- 5 Do one of the following:
 - If you are transmitting a constant load of traffic for every enabled stream, and you want to distribute the load evenly across the streams, select **Auto Distribute**. The module automatically calculates the load for each stream.
 - If you are transmitting one or more ramped streams of traffic, or a combination of constant and ramped loads, enter the load for each enabled stream.
- 6 Select **OK** to store the loads and return to the Streams Pipe dialog box.
- 7 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

The traffic load is specified.

Specifying the load unit on a stream with burst

If a burst signal is necessary in a multiple streams signal, any stream may be defined to carry that bursty signal. Only one stream may be defined as carrying a bursty signal.

Defining a stream as having a Burst load type automatically changes any other stream defined as Burst to the Constant Load Type. It also restricts all enabled streams to be configurable based on Layer 2 bit rate (Eth. IR (Mbps)).

To configure the load unit on a stream with burst load type

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the Multiple Streams test application for the interface you are testing.
- 2 Select the **Setup** soft key.

- 3 Select the **All Streams** tab. Verify that a burst Stream has been specified in the Stream Selection portion of the window. If not specified, select the desired stream from the **Burst Stream** drop-down list.
- 4 Select the tab of the individual stream specified as being the Burst Stream.
- 5 On the Traffic tab, select a **Load Unit**, then do the following:
 - If you selected **Burst Time** and **Information Rate**, enter the Burst Time, then enter the units for the Burst Time.
 - If you selected **Bytes** and **Information Rate**, enter the Burst Kbytes. The actual Kbytes will be recalculated and appear in the window with the Information Rate (based on the value you entered when you configured the individual stream).
 - If you selected **Gap Time** and **Information rate**, enter the Gap Time (period that burst is not being transmitted). The Burst Rate will appear based on the Gap Time specified.

Specifying the load unit for multiple streams

If you selected a Multiple Streams application, the traffic load for each stream transmitted (except when configured for burst) can be specified in Mbps, or as a percentage of the line rate. If a stream is to be configured with a Burst load type (only one stream may be defined to have a Burst load type), see [“Specifying the load unit on a stream with burst” on page 52](#) for instructions on selecting the load unit on the stream carrying the burst signal.

To specify the load unit

- 1 If you haven’t already done so, use the Test Menu or Quick Launch screen to select the Multiple Streams test application for the interface you are testing.
- 2 Select the **Setup** soft key.
- 3 In the Stream Selection section, verify that the Burst Stream is set to None and then under Load Unit, select one of the following:
 - Bit Rate
 - Percent
- 4 Select the Allow flooding checkbox to transmit true 100% load in those circuits that can certainly handle the signal.
- 5 If you selected Bit Rate, the Throughput Bit rate definition source must also be specified. Select either **L(ayer)1 (Mbps)** or **L(ayer)2 (Eth IR (Mbps))**.

The load unit is specified. You can specify the traffic load for each stream (see [“Specifying the load type for all streams” on page 51](#)).

Specifying common traffic characteristics for multiple streams

If you selected a Multiple Streams application, common characteristics shared by all streams are specified on the All Streams tab.

To specify traffic characteristics shared by every enabled stream

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the Multiple Streams test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **All Streams** tab. Depending upon the application being used, it may be desired to set one of the following:



NOTE:

Although the SP source and destination MAC addresses, and the customer's source MAC address are assigned to every enabled stream, you can specify a unique customer destination MAC address for each individual stream. See ["Specifying layer 2 stream settings" on page 54](#).

- **Layer 2 streams:** To specify a single address, in Source MAC Mode, select **Single**, and then indicate whether you want to use the factory default address, or specify your own.
To specify an address for each stream, in Source MAC Mode, select **Per Stream**, and then specify the addresses on the tabs corresponding to each enabled stream.
- 3 To specify the parameters located in the Stream Selection section of the window, follow the procedures for ["Specifying the load type for all streams" on page 51](#), ["Specifying the load unit on a stream with burst" on page 52](#) or ["Specifying the load unit for multiple streams" on page 53](#).
 - 4 To specify additional settings for each individual stream, see ["Specifying layer 2 stream settings" on page 54](#).
 - 5 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

Common traffic characteristics are specified.

Specifying layer 2 stream settings

You can specify the frame type, frame size, and encapsulation settings for each individual stream when configuring standard Multiple Streams applications, you can optionally copy the settings to every stream.

To specify layer 2 stream settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the Multiple Streams, Triple Play, or TCP Wirespeed test application for the interface you are testing .

- 2 Select the **Setup** soft key, and then select the tab corresponding the stream or type of stream you are configuring.
- 3 Select the **Ethernet** sub-tab, and then specify the frame type, length type, and optional encapsulation settings. For details, refer to:
 - [“Specifying Ethernet frame settings” on page 109.](#)
 - [“Configuring VLAN tagged traffic” on page 116.](#)
 - [“Configuring Q-in-Q traffic” on page 117.](#)
- 4 Do one of the following:
 - Select the tab corresponding to the next stream or the next type of stream you want to characterize, then repeat [step 3](#).
 - *Optional.* If you want to use the same settings for all enabled streams, select **Copy Setups to other Streams**.
Traffic load settings are not copied. Load settings must be configured for each individual stream.
- 5 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

Layer 2 traffic characteristics are specified.

Transmitting multiple streams

Before transmitting multiple traffic streams, you must:

- Specify the required interface settings.
- Specify the load unit for the transmitted traffic (Bit Rate or Percent). This setting indicates whether you want to specify the load for each stream as bit rate or as a percent of the line rate. For details, see [“Enabling multiple steams” on page 50.](#)
- Enable the streams you want to transmit (see [“Enabling multiple steams” on page 50.](#))
- Specify common traffic characteristics for all enabled streams. For example, if you intend to use the factory default source MAC address, and a static IP address as the source addresses for every enabled stream, these are specified on the All Streams tab. For details, see [“Specifying common traffic characteristics for multiple streams” on page 53.](#)
- Specify unique traffic characteristics for each enabled stream or type of stream. For example, you can verify that a network handles VLAN tagged traffic properly by assigning a high priority to one stream, and a lower priority to a second stream.
- Specify the load for each enabled stream, or let the module automatically distribute the load evenly between enabled streams. For example, if you specify the load unit as a percent, selecting **Auto Distribute** distributes a 25% traffic load to each stream. For details, see [“Specifying the load type for all streams” on page 51.](#)

To transmit multiple streams

- 1 Select the **Setup** soft key, and then select the Interface tab to specify the settings required to initialize the link (see [“Specifying interface settings” on page 106](#)).
- 2 Configure the test. For details, refer to:
 - [“Enabling multiple steams” on page 50](#).
 - [“Specifying the load type for all streams” on page 51](#).
 - [“Specifying common traffic characteristics for multiple streams” on page 53](#).
- 3 Select **Results** to return to the Main screen.
- 4 Select **Start Traffic** to transmit the streams over the circuit.

Multiple streams are transmitted. For an overview of the test results presented when transmitting multiple streams, see [“Understanding Multiple Streams test results” on page 49](#).

Capturing packets for analysis

If your instrument is configured and optioned to do so, you can use it to capture transmitted and received packets, save it on the instrument or to an external USB key, and then either send the packets to another technician for analysis, or analyze it yourself using the Wireshark® protocol analyzer.



NOTE

The term “packets” is used interchangeably with “frames” throughout the following section, and represents any of the layer 2 or layer 3 datagrams.

You can capture packets when running any of the Ethernet applications.

What is captured?

All received traffic (test traffic, control plane traffic, and live traffic) that satisfies the user-specified criteria on the Filter setup tab can be captured for all supported interfaces.

Only control plane traffic for transmitted traffic is captured. The scope (extent) of the control plane traffic captured depends on:

- The bandwidth remaining after received traffic captured
- The bandwidth of the transmitted control plane traffic.

Test Traffic

Test traffic is the traffic generated and transmitted by your test instrument carrying an ATP or BERT payload. Test traffic can be captured when it is transmitted, looped back and then captured when it is received, or it can be captured when received from a transmitting instrument on the far end.

You can capture received test traffic for all supported interfaces.

Control plane traffic

Control plane traffic is traffic used to establish a connection with another network element or instrument, request information from the element, or to verify connectivity with the element. Examples of control plane traffic include ARP packets, Ping packets, and software application layer datagrams, such as HTTP, TCP/UDP, or FTP control packets.

You can capture transmitted and received control traffic from all supported interfaces.

How is the capture buffer filled?

You can control how your instrument handles the packets when the buffer becomes full. The instrument can stop capturing packets entirely, or it can wrap (overwrite) the oldest packets in the buffer with new captured packets in 1 MB increments.

After capturing packets to the buffer, you can save them to a PCAP (packet capture) file, which can optionally be compressed using gzip for efficient storage.

Why use frame slicing?

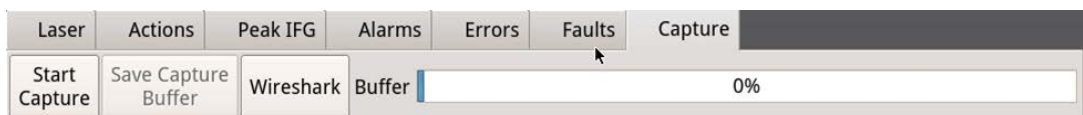
When you configure your instrument to capture packets, you can tell the instrument to capture only the first 64, 128, or 256 bytes of each packet. This allows you to analyze the most important data carried in the packet headers (at the beginning of the packets), and to capture and store more packets in the buffer.

Understanding the Capture toolbar

The buttons on the Capture toolbar start and stop the capture process, save the packets in the capture buffer to the internal USB drive or external drive, or launch Wireshark®.

Figure 20 shows the Capture toolbar.

Figure 20 Capture toolbar



The **%Buffer Full** gauge shows the percentage of the available buffer capacity that is used.

When you capture traffic at a high bandwidth or specify a small buffer size, if you configure the capture to wrap (overwrite) the oldest packets in the buffer with new captured packets in 1 MB increments, the buffer gauge may appear to move erratically.

If you do not wrap the packets the capture process may stop very soon after it is started as the buffer reaches capacity quickly. This is expected behavior.

Specifying filter settings

If you specify filter settings when configuring the application, the settings determine which traffic is captured to the buffer.

Transmitted control plane frames are always captured to the buffer.

To specify filter settings before capturing frames

- 1 If you have not already done so, use the **Test Menu** or **Quick Launch** screen to select the test application for the interface you are testing.
- 2 Select the **Setup** soft key, then select the **Filters tab**.
By default, a summary of all currently configured filter settings appear (Ethernet and IP)
- 3 If you want to clear the filters to specify new settings for the capture process, select **Clear All Filters**.
- 4 If you launched a layer 2 application, the panel of the left of the tab displays the **Summary** and **Ethernet** selections. If you launched a layer 3 application, the panel displays the **Summary**, **Basic**, **Ethernet**, and **IP** selections.

Either:

- a For a layer 2 application, select Ethernet, then specify the settings that capture the received traffic that you want to analyze, as described in [“Specifying Ethernet Filter settings” on page 28](#).
- b For a layer 3 application specifying basic filter information, select **Basic**, then specify the **Traffic Type** and **Address Type** carried in the received traffic you want to capture.
- c For a layer 3 application specifying detailed filter information, select **Basic** then set the **Filter Mode** to Detailed.

Use the Ethernet and IP selections in the pane on the left to display the filter settings for your particular test, then specify the settings that capture the received traffic that you want to analyze. See [“Specifying Ethernet Filter settings” on page 28](#), [“Specifying IPv4 filter settings” on page 40](#), or [“Specifying IPv6 filter settings” on page 43](#).

The filter settings are specified for the capture.

Capturing packets

Capturing packets involves launching and configuring an Ethernet application, specifying the capture settings, and specifying the filter settings. If you are capturing received traffic only, you can start the capture process immediately.



NOTE

Configuring the capture for a large buffer (for example, 256 MB) with small packets (for example, 46 byte ping packets), it will take a long time to fill the buffer. Configuring the capture for a small buffer with large packets will take less time.

To capture packets on the instrument

- 1 Launch an Ethernet application.
- 2 Select the **Setup** soft key, then do one of the following:
 - Specify the settings required to filter received traffic for the type you want to capture and analyze.
 - Clear all of the filters to capture all received traffic. See [“Specifying filter settings” on page 58](#) for more information.
- 3 Select the **Capture** setup tab, then configure the following settings:

Setting	Description
Capture Buffer Size (MB)	Specify a capture buffer size in a 1 MB increments.
Capture frame slicing	Select to capture the first 64, 128, or 256 bytes of each frame (and ignore the rest of the frame; otherwise, select None to capture the entire frame.
When capture buffer is filled	If you want to overwrite the oldest packets with new packets when the buffer becomes full, select Wrap Capture; otherwise, select Stop Capture.

- 4 Select the **Results** soft key to return to the **Main** screen.
- 5 If you are capturing transmitted or looped traffic, select **Start Traffic**.
- 6 Select the **Capture** toolbar, then do the following:
 - a Select **Start Capture**. A message appears in the message bar indicating that the capture has started. The **Action** key states Capture Started.
 - b If you want to capture packets that show how the traffic is impacted by various events, use the buttons on the **Actions**, **Errors**, and **Fault Signaling** tool bars to insert the events into the transmitted traffic stream.
- 7 If you want to manually stop capturing packets, select the **Capture Started** action key.

Packets are captured and stored temporarily in the capture buffer. A count of the number of packets processed is provided in the **Ethernet** result group in the **Capture** category.

Capturing packets based on a trigger

When troubleshooting problems that occur intermittently or inconsistently, the trigger feature allows capture to begin based on a given event. For this scenario, the filters are used as trigger.

To trigger with Filters or FCS Errors

- 1 Press the **Setup** soft key.
- 2 Set **Use Filters as** to Trigger.
- 3 Specify a post-trigger size. This is the amount of data, in MB, to capture after the trigger event occurs.
- 4 Either:
 - Select **Trigger On Filters** to use settings from the Filters tab as a trigger and continue to Step 5.
 - Select **FCS Error** to trigger on the first FCS error received and skip to Step 8.
- 5 Select the **Filters** tab, then in the panel on the left side, select **Summary**.
- 6 Select the **Clear all Filters** button to clear any current filter settings.
- 7 Select the filter properties that match the traffic criteria you want to include in the capture.
- 8 Select the **Results** soft key to return to the Main screen.
- 9 Select the **Capture** toolbar, then select **Start Capture**. A message appears in the message bar indicating that the capture has started and the action key states Capture Started.

The capture begins when the trigger even occurs, which is when the data matches the Filter criteria or FCS Error. Captured packets are stored temporarily in the capture buffer until saved to a file. A count of the number of packets processed and packets captured is provided in the **Ethernet** result group in the **Capture** category.



NOTE

When capturing packets based on a trigger, the capture buffer saves in wraparound mode, in which the oldest packets are overwritten with new packets when the buffer becomes full, until the trigger condition is met.

Saving or exporting captured packets

After capturing packets, you can save the packets in the buffer to the internal disk, or export it to an external USB drive. You can save the entire buffer, or you can indicate that you want to save part of the buffer. You can also optionally turn on zip compression.

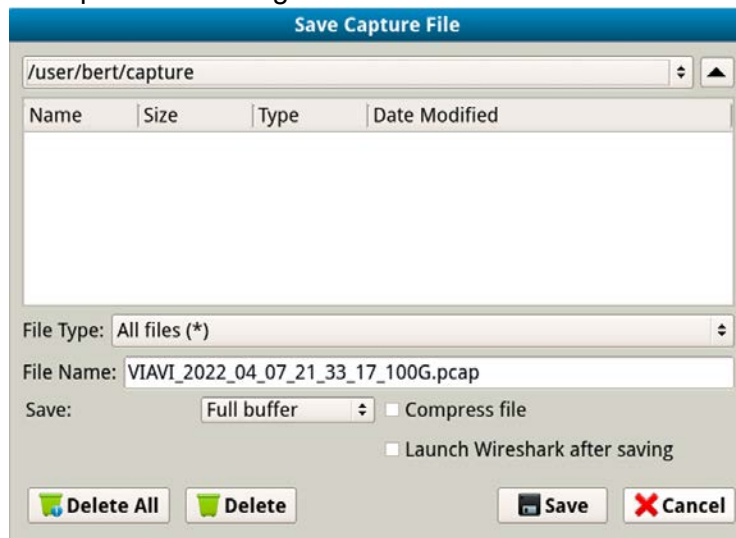
You can also optionally import a pcap file from an external USB drive to analyze it on your unit.

To save the packets in the capture buffer

- 1 Capture the packets, as described in “Capturing packets” on page 59 and “Capturing packets based on a trigger” on page 60.
- 2 Select **Save Capture Buffer**.

The Save Capture File dialog box appears, as shown in Figure 21.

Figure 21 Save Capture File dialog box



- 3 At the top of the dialog box, select one of the following:

To	Select
Save the captured packets to the internal USB drive	/user/bert/capture
Save the captured packets to an external USB drive	/user/bert/usbflash

- 4 Configure the following:

Setting	Description
File Type	To see all files stored in the location specified in Step 3, select All Files . Otherwise, select PCAP files to view only the captured files.
File Name	To specify a filename instead of accepting the default, type the name using the popup keypad. You do not have to specify the .pcap file extension, as the instrument will do so automatically.

Setting	Description
Save	Select one of the following: To save all of the packets in the buffer, select Full Buffer . To save only some packets in the buffer, select Partial Buffer .
From	If you indicated that you only want to save part of the buffer by selecting Partial Buffer, specify one of the following: Start of buffer End of buffer
Amount	If you indicated that you only want to save part of the buffer by selecting Partial Buffer, specify one of the following: The number of MB to save The percentage of the buffer to save
Compress File	By default, the instrument does not compress the file. Select this setting to save the packets in a compressed format (.gz).
Launch Wireshark after saving	Select this setting to launch Wireshark® immediately after saving the packets.

5 Select the **Save** button at the bottom of the dialog box.

A box appears above the Main screen showing the percentage of the buffer that has been saved. When the buffer is saved, the box closes. If you indicated that you wanted Wireshark® to launch immediately after saving the buffer, the Wireshark® application appears.

The packets in the capture buffer are saved or exported.



ALERT

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Analyzing the packets using Wireshark®

After saving the packets in the capture buffer to a PCAP file, you can analyze the packets in detail on the instrument using the Wireshark® protocol analyzer.

Files exceeding 16 MB should not be analyzed on the instrument. Large files should be exported for analysis on another device. If you attempt to analyze a file with more than 50,000 packets, the instrument will alert you that the file should be exported for analysis.

files exceeding 16 MB should not be analyzed on the instrument.



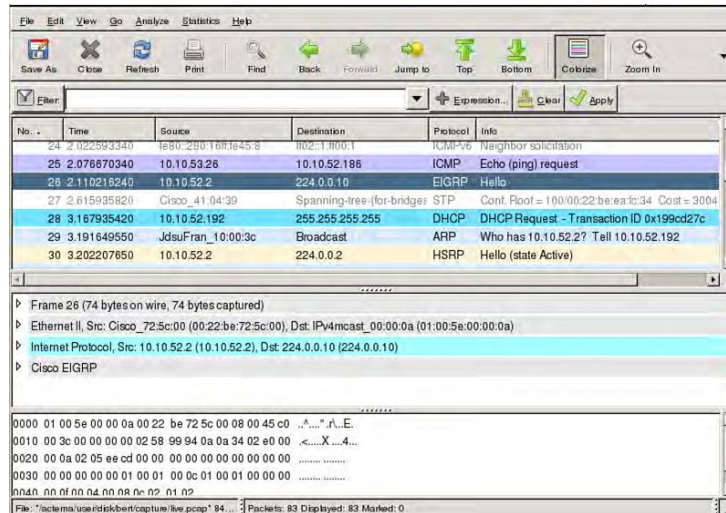
IMPORTANT: Wireshark® Support

VIAMI distributes Wireshark® under the GNU General Public License, version 2. It is not a VIAMI product. For technical support, go to the product website at www.wireshark.org.

To analyze captured packets

- 1 On the Capture toolbar, select the Wireshark action key. The Open Capture File dialog box appears.
- 2 Navigate to and select the file you want to analyze.
The Wireshark® splash screen appears, then a small dialog box appears while the application loads the packets in the file you selected.
- 3 After the packets are loaded, a screen similar to the one shown in figure appears.

Figure 22 Sample Wireshark® screen



- 4 Use the controls at the top of the screen to locate and evaluate the packets. For technical support and product documentation, go to www.wireshark.org.

You are analyzing captured packets.

Ethernet Service Disruption

You can use the instrument to measure the Ethernet Service disruption time resulting from a switch in service to a protect line. Ethernet Service disruption provides a more complete version of service disruption time measurement when compared to Peak IFG.

To measure Ethernet Service disruption

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.

- 2 Select the **Setup** soft key. A series of setup tabs appears.
- 3 Select the **Service Disruption** tab.
- 4 Under Event Settings, do the following:
 - a Select **Enable Service Disruption**.
 - b *Optional*. To edit the displayed Separation Time, tap the field and then type the new time in milliseconds (ms), or select **Default** to restore the time to its default value (300.0 ms). This is the duration during which each trigger of a specific type will be counted as a single disruption event.
 - c *Optional*. To edit the displayed Threshold Time, tap the field, and then type the new time in milliseconds (ms), or select **Default** to restore the time to its default value (50.0 ms). Disruption measurements that exceed this duration will be interpreted as failed.
- 5 Under Event Triggers, do one of the following:
 - To measure disruption time for each of the triggers listed, select **Set ALL**.
 - To measure disruption time for a specific trigger or group of triggers, select **Clear ALL**, and then select each of the triggers for measurements.



NOTE

The default settings are optimal for most testing.

- 6 If additional settings need to be modified to reflect the network configuration, select the appropriate tab, and then modify the settings as required.
- 7 To return to the Main screen, select the **Results** soft key.
- 8 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 9 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 10 To force the switch to a protect line, use one of the following methods:
 - Interrupt the signal. Physically interrupt the signal by pulling the signal from the add-drop multiplexer (ADM).
 - Insert errors. Use another unit in through mode to insert errors until the network switches to the backup lines.

The network switches to a protect line, the instrument detects that service has been disrupted, and then the module begins to measure the disruption time in milliseconds until the condition returns to normal.
- 11 To observe the service disruption results, set one of the result windows to display the Service Disruption Log, and set another window to display the Service Disruption Log Stats.

Service disruption is measured for each of the triggers you selected. [Table 3](#) describes the results.

Table 3 Service Disruption test results

Category	Description
SD Summary	The SD - Summary category provides the service disruption number, the start time, and the duration for the disruption.
SD Details	The SD - Details category displays a log providing the time a disruption event (such as a Bit/TSE error) occurred, and its duration in milliseconds. The instrument alerts you when the log becomes full and prompts you to clear it.
SD Statistics	The SD - Statistics category displays the longest, shortest, last (most recent), and average disruptions logged during the course of your test. It also provides a total count of disruptions.

Measuring Peak IFG

You can use two instruments or ports in an end-to-end configuration, or one port to a loopback point to measure the Peak InterFrame Gap (IFG). This measurement determines the service disruption time typically resulting from a link switchover on a network.



NOTE

VIAVI recommends sending traffic at constant line rate (100%) for the most accurate measurement.

By default (as per Ethernet standards), a port typically stops transmitting traffic when a fault or alarm is detected on the receive path. For Peak IFG, it is recommended you decouple Tx and Rx on the test port, such that the transmitter will ignore the state of the receiver; the default setting is Couple.

The Peak IFG function measures the longest IFG during a test. Before measuring a service disruption event, it is recommended that you click the Reset Peak IFG Result button on the Peak IFG panel at the bottom of the main screen. This is also where the Tx and Rx couple/decouple settings are found.



NOTE

Decoupling Tx and Rx is only applicable to the Peak IFG function. For any other measurements or analysis, set to Couple (default). This meets the standard Ethernet requirements.

To measure Peak IFG

- 1 Using the Test Menu, select the layer 2 or layer 3 traffic terminate test application at the Ethernet rate to use.
 - If using 1 port to a loopback, this is done on that single port.
 - If using 2 ports, both should run the same application; one will transmit traffic while the other will measure the Peak IFG time.
- 2 Connect to the network under test. Blinking LEDs on the connector panels indicate which connectors to use for your test.
- 3 Set the Traffic Rate on the transmitter port from the **Setup > Traffic** tab. It is recommended to set
 - **Load Unit** to percent
 - **Load%** to 100%
 - **Allow flooding** enabled.
- 4 On the transmitting port, ensure the **Setup > Laser** button is set to enabled
- 5 On the receiving port which can be the same or different as the transmitting port depending on the set up, verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 6 On the transmitting port, Start traffic under the **Actions** tab.



NOTE

You can eliminate this step by selecting 'Auto-start traffic when laser turned on under **Results > Interface > Physical Layer**.

- 7 On the receiving port that will measure the Peak IFG:
 - a Go to **Results**.
 - b In the **Peak IFG** tab at the bottom of the screen, set **Tx and Rx** to decouple.
- 8 Click the **Reset Peak IFG Result** button to clear the PEAK IFG time.
- 9 Set a result pane to **Ethernet > L2 Link Stats** and scroll to the bottom to see the Peak IFG value. This should be a fairly small value.
- 10 Initiate the protection switching mechanism in the network under test
- 11 Observe the **Peak InterFrame Gap** result in **Ethernet > L2 Link Stats**
- 12 Repeat steps 8 to 11 for each additional measurement required.
Peak IFG time as been measured.

LLDP

LLDP supports the advertisement of LLDP information (transmit) and reports/decodes incoming LLDP information (receive).

To use LLDP

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key. A series of setup tabs appears.
- 3 Select the **LLDP** tab.
- 4 Configure the Tx Configuration parameters, then tap the **Results** button.
- 5 On the **Results** screen, turn on the laser.
- 6 Tap the Actions tab, then tap **Start LLDP**.

Once LLDP has started, results can be viewed on the **Ethernet > LLDP tab**.

Loopback testing

Loopback testing allows you to transmit traffic from one VIAVI Ethernet test set, and then loop the traffic back through a second unit on the far end of a circuit. For details, refer to [Chapter 6 “Loopback Testing”](#).

Inserting errors

Action buttons on the Main screen allow you to insert errors and pause frames into the traffic stream. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

To insert errors

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 When inserting errors, select one of the following error types:
 - RS-FEC Corr. CW
 - RS-FEC Uncorr. CW
- 3 Specify the Insertion Style (**Single**, **Burst**, **Rate**, or **Continuous**).
 - If you specified Burst, specify the number of errors in the burst.
 - If you specified Rate, select a rate.
 - Select **OK**.
- 4 Press the **Error Insert** button.
- 5 At a minimum, observe the summary, layer 2 link counts and statistics, error statistics, and event log.

If you are inserting errors at a particular rate, the associated button turns yellow. To stop insertion, press the corresponding button again. Error insertion stops, and the associated button turns gray.

Inserting alarms

You can insert multiple types of alarms simultaneously.

To insert alarms or faults

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 3 Select the **Laser** button.
- 4 Select an alarm type.
- 5 For alarms that apply to multi-lane applications, specify the number of the lane in which the alarm is to be inserted or select **All**.
- 6 Press the **Alarm Insert** button.
The module inserts an alarm or defect, and the button turns yellow.

To stop insertion (Multiple alarms)

- Press the **Alarm Insert** button again.

Alarm insertion stops, and the button turns gray.

Test results associated with the alarm appear in the Status result category.

Measuring round trip delay or packet jitter

You can measure round trip delay or packet jitter by transmitting an Acterna payload. The Acterna payload carries frames with timestamps, enabling the instrument to calculate the delay and jitter. To measure round trip delay, you must use a loopback configuration.

You can measure packet jitter (the difference in one-way-delay as experienced by a series of packets) using either a loopback or an end-to-end configuration. When measuring packet jitter, your unit must receive three or more Acterna frames or packets before measurement begins.

To measure round trip delay or packet jitter

- 1 Use the Test Menu to do one of the following:
 - Select the layer 2 or layer 3 traffic terminate test application for the interface you are testing.

- 2 Select the **Setup** soft key, and then do the following:
 - With a layer 2 traffic application, select the Ethernet setup tab.
 - Select the DATA field to specify that transmitted frames will carry an Acterna payload.
- 3 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.
- 4 Connect the module to the circuit.
- 5 If you are testing an optical interface, select the **Laser** button.
- 6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 7 At a minimum, observe the delay and jitter test results in the Ethernet L2 Link Stats.

Round trip delay and packet jitter are measured.

RS-FEC Testing

This section provides information on RS-FEC testing.

Topics include the following:

- [“About RS-FEC testing” on page 72](#)
- [“Specifying RS-FEC settings” on page 73](#)
- [“Specifying layer 2 settings” on page 74](#)
- [“Transmitting traffic” on page 74](#)

About RS-FEC testing

The RS-FEC layer uses a 64 bit / 66 bit to 256 bit / 257 bit Physical Coding Sublayer (PCS) transcoder. Figure 23 shows an RS(544,514) FEC Block.

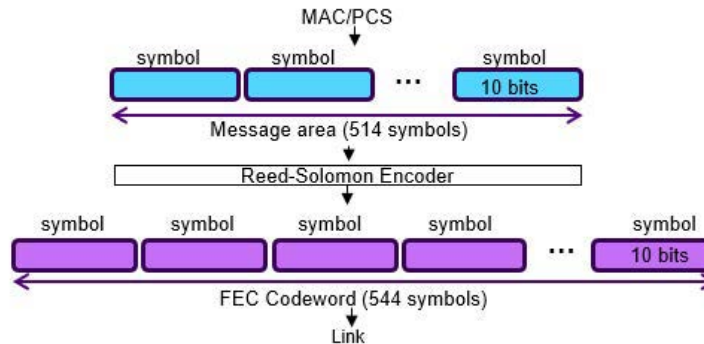


Figure 23 RS(544,514) FEC Block

Features and capabilities

You can perform RS-FEC testing by using your instrument to:

- Troubleshoot pluggable optics errors and verify the stability of a connected QSFP-DD (400GE) pluggable optics transceiver.
- Troubleshoot pluggable optics errors and verify the stability of a connected QSFP56 (200GE) pluggable optics transceiver.
- Troubleshoot pluggable optics errors and verify the stability of a connected QSFP28 (100GE) pluggable optics transceiver.
- Troubleshoot pluggable optics errors and verify the stability of a connected SFP56 (50GE) pluggable optics transceiver
- Troubleshoot pluggable optics errors and verify the stability of a connected SFP (25GE) pluggable optics transceiver.
- Monitor the RS-FEC layer of received traffic for errors (for example, correctable bit errors and uncorrectable symbol errors).
- Insert uncorrectable FEC errors into transmitted signals, and then observe alarm LEDs and counts, ratios and seconds of received uncorrectable FEC errors.
- Monitor and insert RS-FEC alarms and errors while performing Layer 2 tests to verify connectivity to the network and determine the latency (delay) between the instrument and the destination network element under alarm and error conditions.
- RS(544,514) FEC is used at 50GE, 100GE, 200GE and 400GE. At 100GE and 25GE, either no FEC is used, or RS(528,514). 10GE and 40GE do not use RS-FEC.

RS-FEC test applications

With RS(544,514) FEC, VIAVI instruments have a user settable correctable RS-FEC BER Threshold with an associated alarm which defaults to 2.4×10^{-4} as per the IEEE recommendation in clause 12. RS-FEC is available in Ethernet Testing and with Optics Self-Test.

Correctable RS-FEC errors

Correctable RS-FEC errors are expected when running 200GE or 400GE RS-FEC applications; therefore, they are not reported as errors in the event log, histogram, or error statistics result category. However, correctable errors are reported within the RS-FEC Stats categories. If the rate of correctable RS-FEC errors received exceeds the level deemed acceptable per IEEE 802.3 standards, a high symbol error rate (HI SER) alarm is declared and reported as an error. Uncorrectable errors are a severe condition tracked in the event log.



NOTE

100GigE interfaces come with one of three physical layer implementations:

- No FEC: This is used with interfaces such as LR4, CLR4, and IEEE ER4
- RS(528,514) FEC, also called KR4: This is used with interfaces such as SR4, PSM4, CWDM4
- RS(544,514) FEC, also called KP4: This is used with single lambda interfaces such as DR, FR1, LR1

For 100GigE with RS(544,514), QSFP28 optics are typically implemented with a built-in DSP which can provide the FEC function. It is possible to disable the RS(544,514) FEC from the DSP. To run with the FEC from the DSP, use 100GE no FEC.

To run FEC from the test unit, the media FEC from the DSP needs to be disabled. The instrument attempts to automatically disable this media FEC when using 100GigE with RS(544,514). As not all optics vendors use the same methods to disable media FEC, it is recommended to use the 100GigE FR QSFP28 devices sold by VIAVI. See the *Recommended Optics List* on the unit under **Help > Recommended...**

Specifying RS-FEC settings

When configuring your test instrument for RS-FEC testing, you can optionally indicate how the instrument should handle detected errors (fix and report, report only, or ignore). You can also optionally indicate that your test instrument should not declare HI SER Alarms.

To specify RS-FEC settings

- 1 Using the Test Menu or Quick Launch screen, select the Ethernet test application at a rate which uses:
 - RS(544,514) FEC (400GE, 200GE, 100GE, 50GE)
 - RS(528,514) FEC (100GE, 25GE)
 - No FEC (100GE, 40GE, 125GE, 10GE LAN)
- 2 Select the **Setup** soft key, and then select the **RS-FEC** tab.
- 3 In **Incoming FEC**, select one of the following:
 - Find and fix errors (the default)
 - Find but don't fix
 - Ignore
- 4 Set **Disable HI SER Alarm** to **Off** (the default), or **On**. When Off, the test instrument will declare HI SER Alarms when they are detected; when On, the test instrument will ignore HI SER Alarms.
- 5 Configure the remaining parameters as appropriate.

You have specified the RS-FEC settings.

Specifying layer 2 settings

Before you perform RS-FEC testing, be certain you are comfortable configuring and running basic layer 2 tests. You must first initialize the Ethernet link and specify the appropriate layer 2 settings (for example, the frame type and frame encapsulation settings). For details, refer to [Chapter 4 “Ethernet Testing”](#) on [page 19](#).

Transmitting traffic

After you verify and, if necessary, modify the default RS-FEC settings and specify the required settings, you are ready to transmit RS-FEC traffic.

To transmit RS-FEC traffic

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select an Ethernet test application that uses RS-FEC.
- 2 Select the **Setup** soft key, and then select the **Interface** tab.
- 3 Specify the RS-FEC settings (see [“Specifying RS-FEC settings”](#) on [page 73](#))
- 4 Press **Results** to return to the Main screen.
- 5 Select the **Laser** action button by pressing **Start Traffic** to transmit traffic over the circuit.
- 6 Verify that the green Signal Present, Sync Acquired, Link Active, and Marker Lock LEDs are illuminated.

- 7 Observe the RS-FEC results. At a minimum, observe the test results in the following categories:
 - Summary
 - RS-FEC Stats

RS-FEC traffic has been transmitted. For descriptions of RS-FEC test results, see [“RS-FEC results” on page 186](#). Inserting RS-FEC alarms and errors

You can insert (and analyze received traffic for) HI-SER or Loss of Alignment Marker Payload Sequence (LOAMPS) alarms, correctable FEC errors, and uncorrectable FEC errors.

Correctable RS-FEC errors are expected when running RS-FEC applications; therefore, they are not reported as errors in the Event Log, Histogram, or Error Stats result category. A count and the rate of correctable errors are reported within the RS-FEC Stats result category.

To insert RS-FEC alarms or errors

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select an Ethernet test application that uses RS-FEC.
- 2 Configure the test (see [“Specifying RS-FEC settings” on page 73](#) and [“Specifying layer 2 settings” on page 74](#)).
- 3 Transmit RS-FEC traffic (see [“Transmitting traffic” on page 74](#)).
- 4 Verify that the green Signal Present, Sync Acquired, Link Active, and Marker Lock LEDs are illuminated.
- 5 On the Actions Panel, do one of the following:
 - Alarm insertion: If you intend to insert an alarm, select the **Alarms** tab, then select **HI SER, LOAMPS, or a potentially degraded alarm**.
 - Error insertion: If you intend to insert an error, select the **Errors** tab, then
 - Select FEC-Uncorrectable (the default error), or FEC-correctable.
 - Specify the Insertion Style (**Single** or **Continuous**).
- 6 Press the **Alarm Insert** or **Error Insert** button.
- 7 At a minimum, observe the Summary, RS-FEC Stats, Error Stats, and Event Log.

Alarm or error insertion starts.

If you are inserting errors continuously, the associated button turns yellow. To stop insertion, press the corresponding button again. Error insertion stops, and the associated button turns gray.

Loopback Testing

This section provides information on looping back Ethernet traffic.

Topics discussed in this chapter include the following:

- [“About loopback testing” on page 78](#)
- [“Specifying a unit identifier” on page 80](#)
- [“Using LLB to loop received traffic back to the local unit” on page 80](#)
- [“Using Loop Up to initiate a loopback from the local unit” on page 81](#)
- [“Layer 1 \(physical\) loopback” on page 82](#)

About loopback testing

You can transmit Ethernet and IP traffic from one instrument, and then loop the traffic through a second instrument back to the sending instrument. By transmitting and then looping traffic back, you are essentially emulating a longer circuit on the network.

Before looping back traffic, it is important to understand the terminology and concepts in the following sections.

Logical loopback terminology

The following terms are used to explain loopback testing in this chapter.

Local unit

Used in this chapter to refer to the traffic-originating unit (which is always placed in *Terminate* mode).

loopback unit

Used in this chapter to refer to the unit that loops received traffic back to the traffic-originating (local) unit.

Terminate mode

Mode used for loopback applications when both the local unit and the loopback unit are capable of *generating traffic*. Also used by local unit to generate traffic that will be looped back by another unit.

loopback mode

Loopback tests are performed with both the local traffic transmitting unit and the loopback unit in *Terminate* mode.

The loopback unit must be placed in *LoopBack (LLB)* mode.

You can initiate the loopback from your local unit using the **Loop Up** action button or you can actively loop traffic back from the loopback unit using the **LLB** action button.

Key logical loopback concepts

The following concepts apply when configuring loopback applications.

Address swapping

On the loopback unit, received frames are looped through to the transmitter after the destination and source MAC addresses and IP are swapped.

Filter criteria on the loopback unit

Only Unicast frames that pass the filter criteria specified on the loopback unit are looped back to the local unit.

If the Ethernet filter settings are all Don't Care and/or the IP filter, traffic carrying *any payload* will pass through the filter for analysis.

VLAN and Q-in-Q traffic

The loopback unit uses the same IDs and priorities assigned to the received traffic, and loops the traffic back on the same virtual LAN using the same priority.

Loop types

When configuring the local traffic-generating unit, you can specify that you want to issue a Unicast loop-up command, or a Broadcast loop-up command.

If you are running an Ethernet application, Unicast commands are used to loop up a specific test instrument on the far end; Broadcast commands are used to loop up the first instrument on the circuit that responds.

Understanding the graphical user interface

When running loopback tests, the user interface looks much like it does for standard end-to-end or multiple streams tests.

Loopback action buttons

Three action buttons are used for the purpose of initiating or ending loopback tests, and placing a unit into loopback mode.

Loop Up

Press **Loop Up** when you want to initiate the loopup of another unit on the circuit from your unit. In this scenario, you are initiating the loopup from the *local unit*.

Loop Down

Press **Loop Down** when you want to end the loopup of another unit on the circuit. In this scenario, you are ending the loopup from the *local unit*.

LLB

Press **LLB** to loop received traffic back through to a unit's transmitter, or to stop looping traffic back through to the transmitter. In this scenario, you are initiating or ending the loopup from the *loopback unit* itself.

Loopback messages

During loopback testing, if you initiate or end the loopback from the local unit using the **Loop Up** and **Loop Down** actions, messages are sent to each loopback partner indicating the status of the loopback. These messages appear in the Message Bar provided on the Main screen of the user interface.

When you configure your unit for a loopback test, you can specify a "Unit Identifier" which will be provided in each loop up or loop down frame sent from the unit.

Specifying a unit identifier

You can specify an identifier to be carried in all loop up and loop down frames originating from your unit. This allows a technician on the far end to determine where the loop commands came from.

To specify a unit identifier

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the application for the interface you are testing.
- 2 Select the Setup soft key, and then select the Interface tab, and then Network Visibility.
- 3 Select the Unit Identifier setting, and then type the identifier using up to 25 characters.

The identifier is specified.

Using LLB to loop received traffic back to the local unit

You can loop received traffic through to a unit's transmitter and back to the local (traffic-originating) unit by selecting the LLB action button provided on the loopback unit.

To loop received traffic back using LLB

- 1 If you haven't already done so, on both units, launch the layer 2 application for the circuit you are testing (see "[Step 1: Selecting a test application](#)" on page 6).

- 2 On the local unit, specify the link initialization settings.
 - If you are looping back traffic on an Ethernet circuit, see [“Specifying interface settings” on page 23](#).
- 3 On the local unit, specify the settings for transmitted traffic.
For a single stream of layer 2 traffic, refer to [“Layer 2 testing” on page 23](#)
- 4 On the loopback unit, do the following:
 - a Verify that the applicable filter settings are either disabled, set to **Don’t Care**, or that they match the settings for the traffic transmitted from the local unit.
 - b On the Main screen, select the Actions tab, and then select **LLB**.
- 5 On the local unit, select the Actions tab, and then select one of the following:
 - **Start Traffic** (if you configured a constant or bursty load).
 - When the loopback unit receives the traffic, it does the following:
 - Determines which frames satisfy its filter criteria. Only traffic that satisfies the criteria will be looped back to the near end unit.
 - Swaps the destination and source addresses for every frame it receives.
 - Transmits the traffic back to the local unit.

Traffic is looped back to the local unit.

Using Loop Up to initiate a loopback from the local unit

You can select the Loop Up button on the local (traffic generating) unit to loop up another unit on the circuit. After sending the Loop Up frame, a confirmation message from the loopback unit appears in the message bar of the Main screen of your local unit informing you that the loopback is successful.

Before sending the Loop Up frame, your unit must be configured as follows:

- If you are looping back layer 2 Ethernet traffic, the near end unit automatically detects the MAC address for the next unit on the circuit; therefore, you do not need to configure the destination MAC address. It will be populated automatically for you.
If you want to loop up a specific device, you can specify that you are using a Unicast loop type, and then specify the destination MAC address for the device you are looping up.
- You can optionally specify unit identifiers for each unit (for example, “SamsUnit” and “JoesUnit”). When the units send confirmation messages to each other indicating the status of the loopback, the messages will identify each unit using the identifier. For details, see [“Using LLB to loop received traffic back to the local unit” on page 80](#).

To initiate a loopback from the local unit

- 1 If you haven’t already done so, launch the layer 2 application for the circuit you are testing.

- 2 On the local unit, specify the link initialization settings (see “[Specifying interface settings](#)” on page 23).
- 3 On the local unit, specify the settings for transmitted traffic. See “[Layer 2 testing](#)” on page 23 for more information.
- 4 On the far end unit, do the following:
 - a Ensure that automatic traffic generation is not enabled. If it is not disabled, the unit will not respond to the loop up command.
 - b If you are looping back multiple streams of TCP/UDP traffic, specify a listen port for each enabled stream that matches the destination port in the corresponding stream received from the near end unit.
- 5 On the near end unit, select the Action tab, and then select **Loop Up** to put the far end unit in loopback mode. A confirmation message appears in the message bar of the near end unit indicating that the loopback was successful.
- 6 On the near end unit, select one of the following:
 - **Start Traffic** (if you configured a constant or bursty load).
 - **Start Ramp** (if you configured a ramped traffic load).
 - When the far end unit receives the traffic, it does the following:
 - Determines which frames or packets satisfy its filter criteria. Only traffic that satisfies the criteria will be looped back to the near end unit.
 - **Start Ramp** (if you configured a ramped traffic load).

Traffic is transmitted and looped through the unit on the far end (if it passes the far end unit’s filter criteria).

To loop down the far end unit

- 1 On the near end unit, select the Action tab, and then select **Stop Traffic** or **Stop Ramp**.
- 2 On the near end unit, select **Loop Down**.

The far end unit is looped down, and a confirmation message appears in the message bar of the near end unit indicating that the loop down was successful.

Layer 1 (physical) loopback



NOTE

Layer 1 Loopbacks apply to the OneAdvisor 800 on QSFP/QSFP-DD port 2. Such loopback functionality can be used standalone to perform a loopback or used within the Cable Test application for AOC/DAC/AEC testing.

Layer 1 Loopbacks provide a bit-by-bit physical loopback with the following settings:

- Rate selection:
 - 425 Gbps (8x53G)
 - 212.5 Gbps (4x53G)
 - 206.25 Gbps (8x25G)
 - 106.25 Gbps (2x53G)
 - 106.25 Gbps (4x26G)
 - 103.125 Gbps (4x25G)
 - 41.25 Gbps (4x10G)
- Number of Media Lane selection
- Number of Host Lane selection
- Host Lane Modulation indication (NRZ or PAM4)
- Selection of Host Lane for Clock Recovery purposes

OTN Testing

This chapter provides step-by-step instructions for performing OTN tests.

Topics discussed in this chapter include the following:

- [“About OTN testing” on page 86](#)
- [“OTN Overhead Transparency” on page 87](#)
- [“Running the OTN Check work flow” on page 87](#)
- [“Specifying the Tx clock source” on page 90](#)
- [“Measuring optical power” on page 91](#)
- [“Inserting errors and alarms” on page 91](#)
- [“Observing and manipulating overhead bytes” on page 93](#)
- [“Scrambling the signal” on page 94](#)
- [“FEC testing” on page 95](#)
- [“Specifying SM, PM, and TCM trace identifiers” on page 96](#)
- [“Specifying FTFL identifiers” on page 98](#)
- [“Specifying GCC BERT Channels” on page 99](#)
- [“ODU RTD” on page 100](#)
- [“Specifying the transmitted and expected payload type” on page 100](#)
- [“Specifying the Multiplex Structure Identifier” on page 102](#)
- [“BER testing” on page 102](#)
- [“Measuring service disruption time” on page 103](#)

About OTN testing

If your instrument is configured and optioned to do so, you can use it to analyze the performance of OTN networks by performing FEC tests, BER tests, and inserting errors and alarms to verify that network performance conforms to G.709 standards.

When you configure the instrument for OTN testing, a number of the test parameters vary depending on the line rate you select.

Features and capabilities

The following features are supported:

- OTN Check work flow —You can run a work flow to check the OTN link before service activation.
- FEC testing—You can use the module to verify that network elements on an OTN network are configured to handle errors properly.
- BERT patterns—You can transmit and detect BERT patterns for each rate available.
- Error/anomaly and alarm/defect insertion—You can insert a variety of errors, anomalies, alarms, and defects into traffic, such as FAS and logic errors.
- Section Monitoring (SM), Path Monitoring (PM), and TCM identifiers—You can specify outgoing and expected identifiers, and indicate whether or not you want the module to show a trace identifier mismatch (TIM) whenever the expected and received identifiers do not match.
- Payload types—You can specify transmitted and expected payload types, and indicate whether the module should show test results associated with payload type mismatches in the OPU result category.
- Service disruption measurements—You can measure service disruption time resulting from signal loss or a variety of errors, anomalies, alarms, or defects. For details, see [“Measuring service disruption time” on page 103](#).
- Static skew injection- Bit-level static skew injection and alarm threshold setting for excessive skew is possible in all 40G/100G applications.

LED panel

When you configure your unit to transmit a bulk BERT payload, Summary and OTN LEDs appear on the Main screen.

Understanding OTN test results

When you configure your unit to transmit or monitor a bulk BERT payload over an OTN circuit, test result associated with the interface, FEC, framing, OTU/ODU/OPU, FTFL, TCM1 through TCM6, and the payload are provided in the OTN result group. For details, refer to [“OTN results” on page 274](#).

OTN test applications

Table 4 lists each of the OTN test applications.

Table 4 OTN test applications

Signal	Rate	Payload	Test Mode
OTU4	111.8	Bulk BERT	Terminate
		100GigE	Terminate
OTU2e	11.1	Bulk BERT	Terminate
		10GigE	Terminate
OTU1e	11.05	Bulk BERT	Terminate
		10GigE	Terminate
OTU2	10.7	Bulk BERT	Terminate

OTN Overhead Transparency

This feature provides the capability of testing overhead channels to ensure data does not get corrupted in a network. It offers the following functions:

- selection of overhead fields where a stress pattern is applied and tested to a loopback point before being verified for transmission errors
- test functionality over the GCC bytes
- the possibility of using a free running pattern or a pattern aligned to the multi-frame sequence of OTN frames, more specifically reset when MFAS=0. The main application is when encryption keys are transferred using the OTN overhead with the purpose of encrypting OTN payload. In such a case, aligning the test pattern to the MFAS sequence is important, especially when testing through a multi-vendor network.

Running the OTN Check work flow

If your instrument is configured to support OTU n signals, you can run the OTN check work flow to support the turn up of an OTN link or service.

The OTN Check work flow includes three key tests:

- **Payload BERT.** The classic turn up test, based on PRBS payload, with a programmable test duration.
- **Round Trip Delay.** The test uses G.709 standards-based techniques to qualify latency (round trip delay) with OTN.

- **Overhead Transparency.** A unique test developed by VIAVI, used to evaluate a GCC channel for transparency and to verify management connections between nodes.

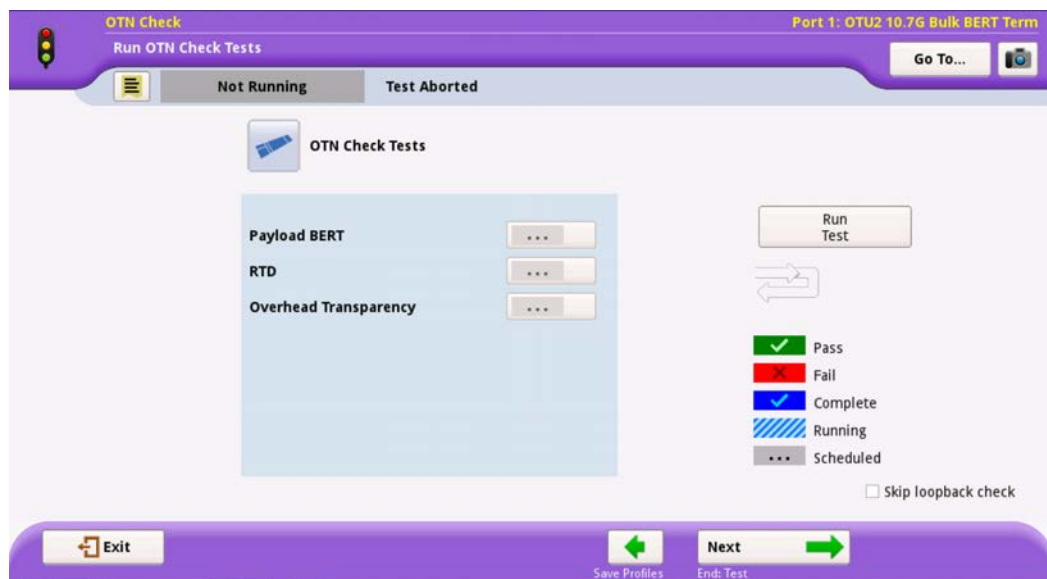
The GCC (General Communication Channel) typically carries node-to-node management information:

- GCC0 at the OTU-level (i.e. line level)
- GCC1 and GCC2 are at the ODU level
- transmission of the GCC pattern per byte (byte 1, 2 and both)

OTN check requires a hard loopback at the far-end of the OTN circuit, typically accomplished using a looped back fiber on an OTN client port. A hard loopback may also be set up on an equipment line card that supports loopback or using another VIAVI test instrument at the far end of the circuit that is running an OTN Monitor/Thru application. By default, your instrument will indicate whether or not a loopback has been detected; you can optionally disable loopback detection.

To run the OTN Check

- 1 Using the Test Menu or Quick Launch screen, select an OTN application with a Bulk BERT payload, then select **OTN Check**.
- 2 Configure the test.
 - a Specify the **Payload BERT** settings.
 - Set the **Test duration**. The test duration can be auto-calculated based on test objectives: set the time directly or use Bit Error Rate theory to derive the test time.
 - Use the check box to specify whether to show the overall pass/fail result.
 - Enter the **BER Threshold**.
 - Specify the **BERT pattern**.
 - Set the **Confidence Level**. This is the statistical probability that the actual measured BER is below the user-specified BER threshold.
 - b Specify **Round Trip Delay** settings.
 - Select the channels to include in the test.
 - For each channel, indicate whether a pass/fail status should be provided, then specify the **Threshold** for declaring that the channel failed.
 - c Specify the **OH (Overhead) Transparency** settings.
 - Specify which **GCC channel** to test.
 - Select whether to include a pass/fail indication.
 - Enter the **GCC BER Threshold**.
 - d Select the BERT pattern as **free running** or reset with each **MFAS=0**; the latter case is primarily used for encryption key transparency testing.
 - e If you want to run the test without waiting for the instrument to detect a hard loopback on the far end, select **Skip loopback check**.



3 Click Run Test.

- The button turns yellow, and the label changes to *Stop Test*.
- The instrument checks for a hard loopback at the far end of the circuit (indicated with green arrows under the *Stop Test* button).
 - If the instrument detects a hard loopback, the arrows remain green, and the *Loopback Detected* status appears.
 - If the instrument does not detect a hard loopback, the arrows change to gray, and the tests do not proceed.
- The test status bars keep you informed of the progress and the success or failure of each test. A key of status indicators is available on the screen for easy reference.

4 After the test finishes, do one of the following:

- To create a report of the results of the test that just completed, select the **Go** arrow on the “Create Report” line. Go to [step 5](#).
- To repeat the test that just ran, select the **Go** arrow on the “Repeat Test” line.
- To reconfigure the test and then run it again, select the **Go** arrow on the “Change Configuration and Rerun Test” line.
- To view detailed results of the performance achieved during the test, select the **Go** arrow on the “View Detailed Results” line.

The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

On the last page of the results select the right-pointing green arrow. Go to [step 5](#).

- 5 Enter report information, including:
 - Customer Name
 - Technician ID
 - Test Location
 - Work Order
 - Comments/Notes
 - Logo (must be saved in the `/disk/bert/images` directory)
- 6 Select **Create Report** (the green arrow).

Do the following:

 - a Select the format in which the report is to be saved by selecting the radio button in Format pane.
 - b Specify the filename of the report. To review the filenames of other, currently saved reports on the unit, select the Select button.
 - c You may view saved reports by selecting the **View Report** button.
 - d To show a copy of the current report after saving it, check the **View report after creation** check box. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.
 - e To include the message log with the report, select the **Include Message log** check box.
 - f When ready to save the report, select the **Create Report** button. After it has been saved (and viewed), select the right-pointing green arrow.
- 7 The post-report/results window appears. Select the **Exit** soft key to return to the OTN Check test window.
- 8 To exit the test application, select the **Exit** button.

Do one of the following:

 - To exit to the base application, retaining all setups from the OTN test, select the **Exit to Results** button.
 - To return to the previous window, select **Cancel**.
 - To restore the OTN Test configuration to the values that were set before you started the OTN Check application, select the box **Restore Setups on Exit**. To completely exit the application, select **Exit**.

The OTN Check is finished.

Specifying the Tx clock source

You specify the Tx clock (timing) source on the Interface setup screen.

To set the Tx clock source

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key, select the **Interface** tab, and then select the **Signal** tab. Select the arrows to the right of the Clock Source field, and then select one of the following:
 - **Internal.** Select Internal to derive timing from the instrument's clock, and then specify any required frequency offset in PPM.
 - **Recovered.** Select Recovered to recover timing from the received signal.
 - **External.** Select External - Bits/Sets timing to derive timing from one of the following signals, in the following order: BITS, SETS, 2.048 MHz, or a 10 MHz clock.
- 3 Select the **Results** soft key to return to the Main screen, or select another tab to specify additional test settings.

The Tx clock source is specified.

Measuring optical power

You can use the instrument to measure the optical power of a received signal.

To measure optical power

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 3 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 4 Verify the following LEDs:
 - If your module is in TestPad mode, verify that the Signal Present, Frame Sync, and Pattern Sync LEDs are green.
 - If your module is in ANT mode, verify that the LOS, LOF, and LSS LEDs are *not* red.
- 5 Display the Interface result group, and then observe the Optical Rx Level (dBm) test result.

Optical power is measured.

Inserting errors and alarms

You can insert multiple types of errors and alarms simultaneously into the traffic stream.

Inserting errors

To insert errors

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 3 Select the **Laser** button.
- 4 Display the Alarms/Errors action bar, then select an error or anomaly type (for example, correctable or uncorrectable FEC word errors, bit errors, FAS, or MFAS errors, or SM, PM, or TCM errors).
- 5 Do the following:
 - For OTN that uses multiple lanes (like **OTU4**, **OTL FAS**, **OTL MFAS**, **OTL LLM**, **Code**, **Alignment Marker**, or **BIP-8**) or STL (**FAS** or **LLM**) lane errors, select the lane into which the error is to be inserted.
 - If you selected a FAS or MFAS Word (non-OTL), specify the number of errors you want to insert, and then select **OK**.
 - If you selected any other type of error, specify the insert type (**Single**, **Burst** or **Rate**).
 - If you specified **Rate** or **Burst**, select one of the available rates or burst counts.
- 6 Press the **Error Insert** button.
Error insertion starts, and the associated button turns yellow.

Test results associated with the error or anomaly appear in the Summary Status result category, and in the categories provided for each type of error or anomaly. For example, test results associated with bit error insertion are provided in the Payload BERT category; results associated with FEC testing are provided in the OTN FEC category. Refer to [“OTN results” on page 274](#) for descriptions of each OTN test result.

To stop insertion

- Press the **Error Insert** button again.

Error or anomaly insertion stops, and the associated button turns grey.

Inserting alarms

To insert alarms

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.

- 2 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 3 Select the **Laser** button.
- 4 Select an alarm type.
- 5 For alarms that apply to multi-lane applications, specify the number of the lane in which the alarm is to be inserted or select **All**.
- 6 Press the **Alarm Insert** button.
The module inserts an alarm, and the button turns yellow.

Test results associated with the alarm or defect appear in the Status result category.

To stop insertion

- Press the **Alarm Insert** button again.

Alarm or defect insertion stops, and the button turns grey.

Alarm suppression

This functionality is available via a selection under Setup > Interface > Signal. This functionality allows for the ignoring of low error rates for errors related to FAS, MFAS, LLM, and Correctable FEC errors. The particular usage is for when optical interfaces in a network are using PAM4 electrical buses for rates such as OTU4. In such cases, low level bit errors can naturally appear, creating a need to ignore them for a successful test. With this level of suppression, major errors and alarms will still be reported.

Observing and manipulating overhead bytes

The following procedure describes how to observe the value of OTN overhead bytes, and manipulate the values for key bytes.

To observe and manipulate OTN overhead bytes

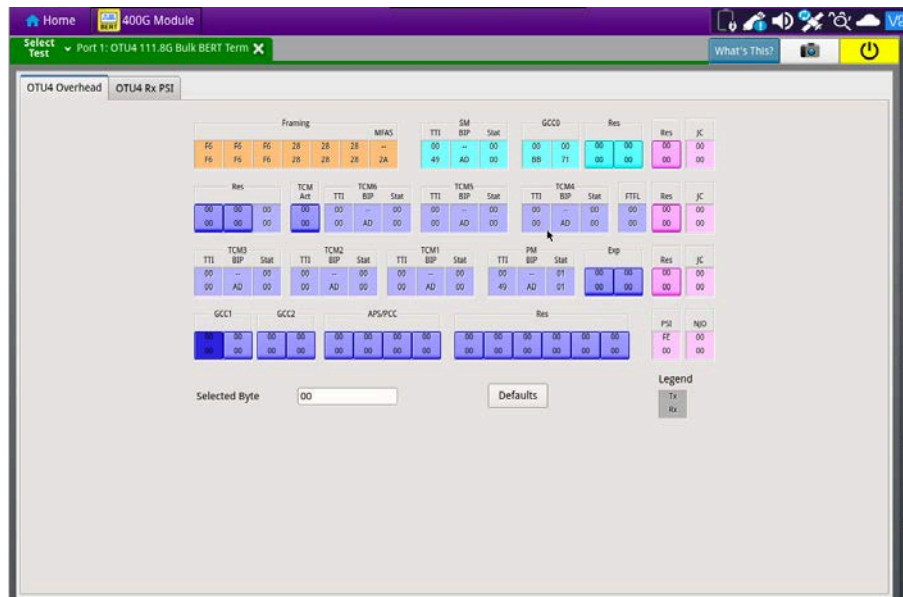
- 1 Using the Test Menu or Quick Launch screen, select the test application for the signal, rate, and payload you are testing.
- 2 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 3 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 4 Select the **Laser** button.

- 5 Press the **OTN Overhead** soft key.



The OTN Overhead screen appears, as shown in Figure 24.

Figure 24 OTN Overhead screen



The Overhead tabs allow you to manipulate bytes. The values at the top of each byte on the Overhead tabs indicate the transmitted value; the values at the bottom of each byte indicate the received value.

The Rx PSI tabs allow you to observe the Payload Structure Identifier (PSI) bytes carried in received traffic. These byte can not be changed.

- 6 *Optional.* Bytes with values in black on the Overhead tab(s) can be manipulated; bytes with values in grey can not. If you want to manipulate a byte value, do the following:
 - a Select the byte on the graphical display.
 - b In the **Selected Byte** field, type the new value, then press OK.You can restore the values to their defaults at any time using the **Defaults** button.

The bytes are displayed and can be manipulated.

Scrambling the signal

You can scramble the signal at the line rate for the interface you are testing.

To scramble the signal

- 1 Using the Test Menu or Quick Launch screen, select the test application for the signal, rate, and payload you are testing.
- 2 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 3 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 4 Select the **Laser** button.
- 5 Select the **Setup** soft key. A series of setup tabs appears.
- 6 Select the **Interface** tab, and then do the following:
 - a If more than one sub-tab is available, select the **Signal** sub-tab.
 - b If you want to descramble the received signal, in Rx - Descramble, select the **Descramble** setting.
 - c If you want to scramble the transmitted signal, in Tx - Scramble, select the **Scramble** setting.

The signals are scrambled and descrambled as specified.

FEC testing

Using the instrument, you can verify that network elements on an OTN network are configured to handle errors properly. FEC (forward error correction) testing involves:

- Stressing network elements by transmitting the maximum number of errors (to ensure that they are corrected as expected).
- Verifying that alarms are triggered as expected on network elements when errors exceeding the maximum are transmitted.

When you configure your unit for FEC testing, you can control how FEC is handled for outgoing and incoming traffic.

To verify the FEC capabilities of your network elements

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key. A series of setup tabs appears.
- 3 On the Interface tab, specify the transmit clock settings if the defaults are not acceptable (see [“Specifying the Tx clock source” on page 90](#)).
- 4 Select the **OTN** tab, and then select **FEC** from the pane on the left of the tab.
- 5 In Outgoing FEC, if you want your unit to include valid FEC bytes in outgoing traffic, select **Turn On**. If you select **Turn Off (send zeros)**, zeros are transmitted in place of the FEC bytes.

- 6 If you are determining how a network element handles correctable FEC errors, in Incoming FEC, select the following:

To:	Select this:
Identify any correctable FEC errors that unexpectedly have not been corrected by the network element, but warrant additional attention with a yellow Summary pane.	Find and fix errors
Identify any correctable FEC errors that unexpectedly have not been corrected by the network element, and indicate that a problem requiring correction has occurred with a red Summary pane.	Find, but don't fix errors
Ignore all FEC errors. FEC results will not be available.	Ignore

- 7 Select the **Results** soft key to return to the Main screen.
- 8 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 9 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 10 Select the **Laser** button.
- 11 Insert FEC errors (see ["Inserting errors and alarms" on page 91](#)), and then observe the behavior of the Summary pane as described in [step 6](#).

Test results associated with FEC testing appear in the Status and FEC result categories. For descriptions of each of the results, refer to ["FEC test results" on page 280](#).

Specifying SM, PM, and TCM trace identifiers

You can specify the SM, PM, and TCM source and destination trace identifiers for transmitted traffic, and you can also specify the identifiers that you expect in received traffic. After specifying the identifiers, you can indicate whether your unit should show a Trace Identifier Mismatch (TIM) when expected and received identifiers do not match.

To specify the SM, PM, and TCM trace identifiers

- Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- Select the **Setup** soft key.

- 3 To define the trace identifiers for OTU, select the **OTUn** tab or for ODU trace identifiers, select **ODUn** tab and then select one of the following from the pane on the left side of the tab:
 - **SM Traces**, if you want to edit the expected or outgoing (transmitted) SM trace identifier.
 - **PM Traces**, if you want to edit the expected or outgoing (transmitted) PM trace identifier.
 - **TCM1 - TCM6**, if you want to edit the expected or outgoing (transmitted TCM) trace identifiers.

Settings appear for the traces.

- 4 Do one of the following:
 - If you are specifying SM or PM identifiers, skip this step and proceed to proceed to [step 5](#).
 - If you are specifying TCM trace identifiers, in Incoming (Rx) TCM, specify **Analyze** to analyze received signals for TCM trace identifiers, or **Don't Care** if you do not want to analyze the signals.
- 5 For the Expected Traces, do the following:
 - If you want to manually specify the identifiers, select the SAPI or DAPI field, type the corresponding identifier, and then select **OK**.
 - Use the **= Rx button** if you want the expected SAPI and DAPI to be the same as the received SAPI and DAPI, or use the **= Tx button** if you want the expected SAPI and DAPI to be the same as the transmitted SAPI and DAPI. The currently received SAPI and DAPI are displayed in the **Incoming (Rx) Traces SM** area at the top of the tab.
 - *Optional.* If you want the unit to display a SM-TIM, PM-TIM, or TIM alarm if the expected and incoming trace values do not match, select **on SAPI mismatch, on DAPI mismatch, or on SAPI or DAPI mismatch**; otherwise, select **No**.



NOTE:

You can reset the expected trace and outgoing trace identifiers at any time using the **Default** buttons.

- 6 Do one of the following:
 - If you are specifying SM or PM identifiers, specify the Outgoing (Tx) Trace identifiers.
 - If you are specifying TCM trace identifiers, and you want to transmit identifiers, in Outgoing (Tx) TCM, specify **Enable**, and then specify the identifiers.
 - If you are specifying TCM trace identifiers, and you do not want to transmit TCM identifiers, in Outgoing (Tx) TCM, specify **Don't Care**.
- 7 Select the **Results** soft key to return to the Main screen.
- 8 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 9 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.

- 10 Select the **Laser** button.
- 11 Loop up the far-end of the network.
- 12 Verify the Signal Present, Frame Sync, and Pattern Sync LEDs are green.
- 13 To view the trace identifier results, select the OTN result group, and then select the OTU, ODU, or TCM result categories. If mismatches occurs, the results also appear in the Summary Status result category.

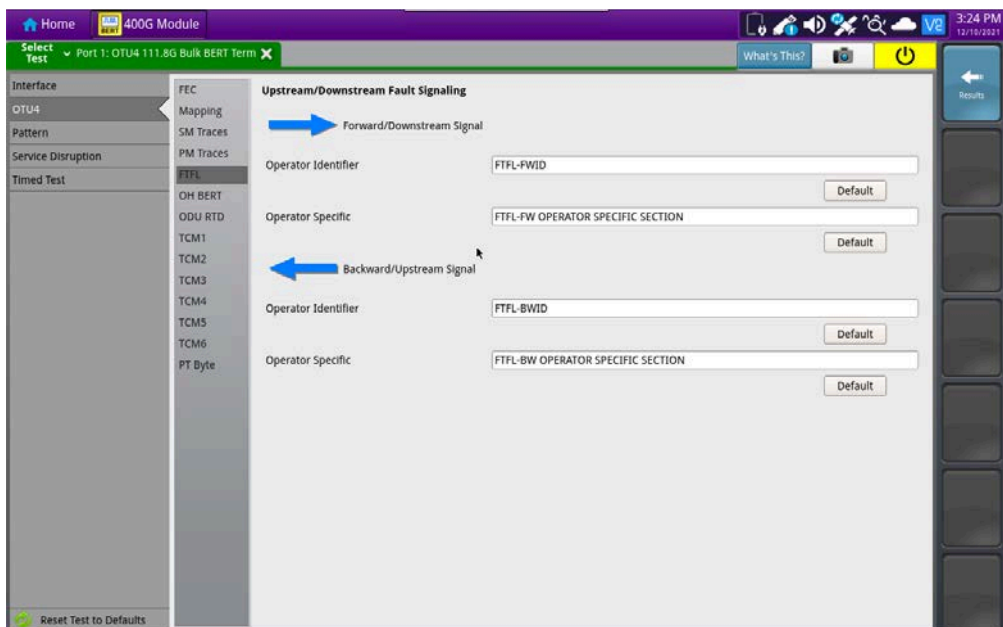
The SM, PM, or TCM trace identifiers are specified.

Specifying FTFI identifiers

You can specify the FTFI (fault type fault location) identifiers for Forward/Downstream and Backward/Upstream signals using up to nine characters, or 118 characters for operator specific identifiers.

To specify the FTFI identifiers

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key. A series of setup tabs appears.
- 3 Select the **OTN** tab, and then select FTFI from the pane on the left side of the tab. Settings appear for the identifiers.



- 4 For the Forward/Downstream and Backward/Upstream signals, select each identifier field, type the corresponding identifier, and then select **OK**.



NOTE:

You can reset the identifiers at any time using the **Default** buttons.

- 5 Select the **Results** soft key to return to the Main screen.
- 6 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 7 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 8 Select the **Laser** button.
- 9 Loop up the far-end of the network.
- 10 Verify the following LEDs:
 - If your module is in TestPad mode, verify that the Signal Present, Frame Sync, and Pattern Sync LEDs are green.
 - If your module is in ANT mode, verify that the LOS, LOF, and LSS LEDs *are not* red.
- 11 To view the FTFL identifier results, select the OTN result group, and then select the FTFL result category.

The FTFL identifiers are specified.

Specifying GCC BERT Channels

You can specify a GCC channel in both the OTU signal and ODU client.

To specify the GCC channel

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key.
- 3 Select the **OTUn** or **ODUn** tab (depending upon the application)
- 4 Select **GCC BERT** from the column on the left side of the screen.
- 5 Specify the GCC channel to be used.
- 6 Select the **Results** soft key to return to the Main screen.

The GCC channel is set.

ODU RTD

Path delay between two Path Connection Monitoring End Points (P-CMEP) by activating a DMp signal can be measured. Round Trip Delay (RTD) can also be measured on TCM channels.

Activating ODU RTD measurements

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key.
- 3 Select the **OTUn** tab.
- 4 Select all the channels on which RTD is to be measured by placing a check mark in their box.
- 5 Select the **Results** soft key.
- 6 To initiate RTD measurements, select the **RTD Measurement** action button.

ODU RTD measurements have been activated.

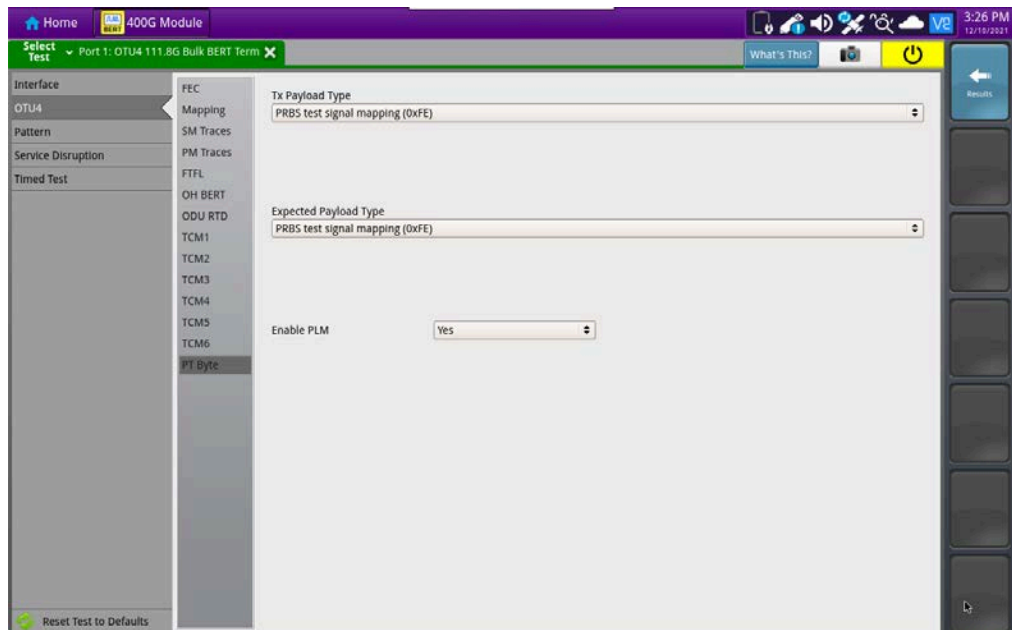
Specifying the transmitted and expected payload type

You can specify the payload type for transmitted traffic, and an expected payload type for received traffic.

To specify the payload type

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key.
- 3 Select the **OTN**, **OTUn**, or the **ODUn** tab (depending upon the application and the SFP or XFP installed) and then select **PT Byte** from the pane on the left side of the tab.

Settings appear for the payload type.



NOTE: In the background channels, the unit transmits valid OTN frame structure and correct SM/PM BIPs, with the payload type byte set to 'FD' (Null test signal mapping) and the client data is all zeros.

- 4 In Tx Payload Type, specify the payload type for transmitted traffic.
- 5 In Expected Payload type, specify the payload expected in received traffic.
- 6 If you want the unit to show test results associated with a mismatched received and expected payload type, in Show Payload Type mismatch, select **Yes**; otherwise, select **No**.
- 7 Select the **Results** soft key to return to the Main screen.
- 8 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 9 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 10 Select the **Laser** button.
- 11 Loop up the far-end of the network.
- 12 Verify the following LEDs:
 - If your module is in TestPad mode, verify that the Signal Present, Frame Sync, and Pattern Sync LEDs are green.
 - If your module is in ANT mode, verify that the LOS, LOF, and LSS LEDs are *not* red.

- 13 To view results associated with mismatched payloads, select the OTN result group, and then select the OPU result category. If a mismatch occurs, the results also appear in the Summary group.

The payload types are specified.

Specifying the Multiplex Structure Identifier

The Multiplex Structure Identifier (MSI) is used to encode the ODU multiplex structure and is located in the mapping-specific area of the PSI signal. The MSI is made of PSI Bytes. When multiplexing ODU1 in ODU2, only Bytes 2 to 5 have a meaning; Bytes 6 to 17 are set to 0, as they are intended for multiplexing applications with ODU3.

The MSI settings on the instrument affect the overhead settings only, not the payload mapping for the Tributary Slots.

To specify the MSI

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing.
- 2 Select the **Setup** soft key.
- 3 Select the **OTN**, **OTUn**, or the **ODUn** tab (depending upon the application and the SFP or XFP installed) and then select **MSI TX** from the pane on the left side of the tab.
- 4 Select the **ODU Type** for each Tributary.
- 5 If you would like the TX MSI and the RX MSI to match, select = **RX MSI**.

The MSI is specified.

BER testing

The following procedure illustrates a typical scenario for setting up the instrument to terminate an OTN signal for BER testing.

To perform an OTN BER test

- 1 Using the Test Menu or Quick Launch screen, select the test application for the signal, rate, and payload you are testing.

- 2 Select the **Setup** soft key, and then select the Pattern tab.

Interface	Rx=Tx	Yes
OTU4	Tx BERT Pattern	2^31-1
Pattern	Rx BERT Pattern	2^31-1
Service Disruption		
Timed Test		

- a Select whether the received BERT pattern should be the same as the transmitted pattern (Rx<=Tx).
- b Select the pattern mode (ANSI or ITU), if applicable to the application selected.
- c Select a BERT Tx pattern (for example, 2²³-1).
- d Select a BERT RX pattern (if Rx<=Tx was set to **NO**).



NOTE:

You can automatically detect and transmit the correct BERT pattern for the circuit by pressing the Auto button on the Main screen after you specify your interface settings. See [“Detecting the received BER pattern” on page 85](#).

- 3 Select the **Results** soft key to return to the Main screen.
- 4 Connect a cable from the appropriate RX connector to the network’s TRANSMIT access connector.
- 5 Connect a cable from the appropriate TX connector to the network’s RECEIVE access connector.
- 6 Select the **Laser** button.
- 7 Loop back the far-end of the network.
- 8 Verify the following LEDs:
 - If your module is in TestPad mode, verify that the Signal Present, Frame Sync, and Pattern Sync OTN LEDs are green.
 - If your module is in ANT mode, verify that the LOS, LOF, and LSS OTN LEDs are *not* red.
- 9 Verify that All Results OK appears in the results display.
- 10 *Optional.* Insert five Bit / TSE errors (see [“Inserting errors and alarms” on page 91](#)), and then verify that the five errors were received in the BERT Payload result category.
- 11 Run the test for an appropriate length of time.

The BER test is finished.

Measuring service disruption time

You can use the instrument to measure the service disruption time resulting from a switch in service to a protect line.

To measure service disruption time

- 1 Using the Test Menu or Quick Launch screen, select the terminate test application for the signal, rate, and payload you are testing .
- 2 Select the **Setup** soft key. A series of setup tabs appears.
- 3 Select the Service Disruption tab.
- 4 Under Event Settings, do the following:
 - a Select **Enable Service Disruption**.
 - b *Optional*. To edit the displayed Separation Time, press the keypad icon, and then type the new time in milliseconds (ms), or select **Default** to restore the time to its default value (300.0 ms). This is the duration during which each trigger of a specific type will be counted as a single disruption event.
 - c *Optional*. To edit the displayed Threshold Time, press the keypad icon, and then type the new time in milliseconds (ms), or select **Default** to restore the time to its default value (50.0 ms). Disruption measurements that exceed this duration will be interpreted as failed.
- 5 Under Event Triggers, do one of the following:
 - To measure disruption time for each of the triggers listed, select **Set ALL**.
 - To measure disruption time for a specific trigger or group of triggers, select **Clear ALL**, and then select each of the triggers for measurements.
- 6 If additional settings need to be modified to reflect the network configuration, select the appropriate tab, and then modify the settings as required.
- 7 To return to the Main screen, select the **Results** soft key.
- 8 Connect a cable from the appropriate RX connector to the network's TRANSMIT access connector.
- 9 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.
- 10 To force the switch to a protect line, use one of the following methods:
 - Interrupt the signal. Physically interrupt the signal by pulling the signal from the add-drop multiplexer (ADM).
 - Insert errors. Use another unit in through mode to insert errors until the network switches to the backup lines.

The network switches to a protect line, the instrument detects that service has been disrupted, and then the module begins to measure the disruption time in milliseconds until the condition returns to normal.
- 11 To observe the service disruption results, set one of the result windows to display the Service Disruption Log, and set another window to display the Service Disruption Log Stats.

Service disruption is measured for each of the triggers you selected. [Table 5](#) describes the results.

Table 5 Service Disruption test results

Category	Description
SD Summary	The SD - Summary category provides the service disruption number, the start time, and the duration for the disruption.
SD Details	The SD - Details category displays a log providing the time a disruption event (such as a Bit/TSE error) occurred, and its duration in milliseconds. The instrument alerts you when the log becomes full and prompts you to clear it.
SD Statistics	The SD - Statistics category displays the longest, shortest, last (most recent), and average disruptions logged during the course of your test. It also provides a total count of disruptions.

Fibre Channel Testing

This chapter provides information on testing Fibre Channel services.

- [“About Fibre Channel Testing” on page 108](#)
- [“Features and capabilities” on page 108](#)
- [“Configuring Fibre Channel tests” on page 109](#)
- [“Transmitting and analyzing layer 2 traffic” on page 115](#)
- [“Logical loopback testing” on page 116](#)
- [“Measuring service disruption time with Peak IFG” on page 116](#)
- [“Inserting errors” on page 117](#)
- [“Measuring round trip delay” on page 117](#)
- [“64G Fiber Channel RS-FEC Testing” on page 118](#)

About Fibre Channel Testing

If your instrument is configured and optioned to do so, you can use it to provision Fibre Channel services, verify end-to-end connectivity, and analyze link performance by simulating different traffic conditions. Use cases include Fibre Channel testing through transport equipment, internworking with a fabric, and testing pluggable optics.

Features and capabilities

Features and capabilities include the following when testing Fibre Channel services:

- 64 Gigabit —You can run Layer 2 traffic tests over 64Gb Fibre Channel circuits in **Terminate** mode using an SFP28 optic module. RS-FEC (544, 514) is supported for 64 Gigabit testing.
- Fibre Channel login and flow control —The instrument supports Exchange of Link Parameters through distance extension equipment when turning up a circuit, allowing the user to login to another module at the far end. Before logging into another module, the number of buffer credits to verify that flow control is functioning properly can be specified.
- Frame verification —You can verify that the size and format of Fibre Channel frames conform to ANSI X3T11 requirements, ensuring that network elements can support reliable communications.
- Class of Service testing — The user can verify circuit and network performance by using Acterna Test Protocol payload in order to verify throughput, latency, frame loss.
- Explicit Fabric/N-Port login; fabric topology—Use the instrument to login to an N_Port, and then verify that it can establish an operating environment with a fabric and communicate with other destination N Ports by indicating that the service under test uses a fabric topology. When testing on a fabric topology, specify the source *and* destination N Port and Node names for the login process.
- Explicit Fabric/N-Port login; point-to-point topology—Use the instrument to login to an N_Port, and then verify that it can communicate with other destination N Ports by indicating that the network under test uses a point-to-point topology. When testing on a point-to-point topology, specify a source N Port and Node name, and a destination and source ID for the login process.
- TTS Connectivity — The user can verify connectivity using Transmitter Training Sequence (TTS) and Link Speed Negotiation (LSN).
- Pluggable Optics Testing — Test pluggable optics at the specified Fiber Channel rate. Includes traffic generation and optics parameter setting.

Understanding the graphical user interface

When configuring the instrument for testing, graphical displays of Fibre Channel frames are provided on the setup tabs. Specify frame characteristics for transmitted and filtered traffic by selecting the corresponding field on the graphic, and then entering the value

for transmitted or filtered traffic. Colored and white fields can be edited; fields in gray can not be modified.

Figure 25 illustrates the Frame Details for a layer 2 traffic test.

Figure 25 Frame Details

Frame Channel Details	
SOF	
R_CTL	D_ID
CS_CTL	S_ID
Data Type	F_CTL
SEQ_ID	DF_CTL
	SEQ_CNT
OX_ID	RX_ID
Parameter	
Data	
CRC	
EOF	

For details on specifying frame characteristics, see [“Specifying Fibre Channel frame settings” on page 113](#) and [“Specifying Fibre Channel filter settings” on page 114](#).

Configuring Fibre Channel tests

The instrument can transmit, monitor, and analyze Fibre Channel traffic. Step-by-step instructions are provided in this section for the following:

- [“Specifying interface settings” on page 109](#)
- [“Specifying Fibre Channel frame settings” on page 113](#)
- [“Specifying Fibre Channel filter settings” on page 114](#)
- [“Specifying traffic load settings” on page 115](#)

Specifying interface settings

Before transmitting layer 2 traffic, specify the interface settings:

- Turn flow control on or off, and specify the login method (Implicit, Explicit E-Port, or Explicit Fabric/N-Port) and the number of transmit or receive buffer to buffer credits to communicate to the module’s link partner during the login process. When flow control is turned on, the module:
 - Generates an R_RDY message for each frame received.
 - Provides a count of received R_RDY messages.
- If using login, specify a unit identifier to identify all traffic originating from the module. It uses its default source ID when doing E-Port login and its user-specified port name when logging into a fabric.

To specify interface settings prior to configuring Fiber Channel

- 1 Use the Test Menu or Quick Launch screen to select the layer 2 terminate test application for the required interface.
- 2 Select the **Setup** soft key interface, and then the Physical Layer sub-tab to specify flow control, TTS, and login parameters, as described in [Table 6](#).

Table 6 Fibre Channel Physical Layer settings

Setting	Values	Implicit	Explicit (E-Port)	Explicit (Fabric/N-Port)	
				Point-to-Point Topology	Fabric Topology
FlowControl	<ul style="list-style-type: none"> – Select On if you want the instrument to operate as a credit-based transmitter. – Select Off to generate frames without flow control. <p>NOTE: You must turn flow control ON to specify Login settings.</p>	X	X	X	X
Login (FlowControl is On)	<ul style="list-style-type: none"> – To verify that both devices use flow control and no login is required, select Implicit, and then specify the Tx Buffer to Buffer credits. – To discover another instrument or device's settings, select Explicit (E-Port), and then specify the Rx Buffer to Buffer credits. – To login to an N-Port on a circuit using a Point-to-Point or Fabric topology, select Explicit (Fabric/N-Port), and then specify the Rx Buffer to Buffer Credits. 	X	X	X	X

Table 6 Fibre Channel Physical Layer settings (Continued)

Setting	Values	Implicit	Explicit (E-Port)	Explicit (Fabric/N-Port)	
				Point-to-Point Topology	Fabric Topology
TTS	When setting to Enable, this enables Transmitter Training Sequence and Link Speed Negotiation. When setting to Disable in 64GFC, assumes PAM4 electrical for 64GFC. An automatic retry is associated with TTS Enable.	X	X	X	X
Link Initialization	Enables the instrument to run the Link Initialization Protocol which FC requires to set up a link. Disable for R&D functions such as transmit only. Forces Flow Control to off.	X	X	X	X
Tx Buffer to Buffer Credits (Near-end B-B)	If you specified an Implicit login, select this field, and then type the number of buffer credits the far end device can support. This number should match the receive buffer size for the far end device.	X	N/A	N/A	N/A
Rx Buffer to Buffer Credits (Far-end B-B)	If you specified an Explicit (E-Port) or Explicit (Fabric/N-Port) login, select this field, and then type the number of buffer credits the instrument will advertise that it can support during the ELP login exchange with the far end device.	N/A	X	X	X

Table 6 Fibre Channel Physical Layer settings (Continued)

Setting	Values	Implicit	Explicit (E-Port)	Explicit (Fabric/N-Port)	
				Point-to-Point Topology	Fabric Topology
Topology	<ul style="list-style-type: none"> – To login to an N Port, and then verify that it can communicate with other destination N Ports, select Point-to-Point. – To login to an N_Port, and then verify that it can establish an operating environment with a fabric and communicate with other destination N Ports, select Fabric. 	N/A	N/A	X	X
Source N Port Name	Specify the source port name carried in the login request.	N/A	N/A	X	X
Source Node Name	Specify the source node name carried in the login request.	N/A	N/A	X	X
Destination N Port Name	Specify the destination port name carried in the login request.	N/A	N/A	N/A	X
Destination Node Name	Specify the destination node name carried in the login request.	N/A	N/A	N/A	X
Destination ID	Specify the destination ID carried in the login request.	N/A	N/A	X	N/A
Source ID	Specify the source ID carried in the login request.	N/A	N/A	X	N/A



NOTE:

When testing flow control on a Fibre Channel circuit, specify the *same number of buffer credits* for both the near-end and far-end instruments. If you specify a different number of credits, or if you specify a very low number, you may not achieve desired bandwidth utilization.

- 3 *Optional.* If you want to transmit an ID for all loop up and loop down frames originating from the module, select the Unit Identifier field, and then type the ID. The default ID is VIAVI 6000.
- 4 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The interface settings are specified. Verify the login status and observe test results associated with the login process by displaying the Fibre Channel Login Status result category (see [“Login Status results” on page 541](#)).

Specifying Fibre Channel frame settings

Before transmitting layer 2 traffic, specify the frame characteristics of the traffic, such as the frame length, and the type of payload carried in the frames. Optionally specify the destination, source, sequence, originator exchange, and responder IDs for transmitted frames.



NOTE:

If the frame length is changed when the unit is already transmitting traffic, the unit resets the test results, but some residual frames of the old length may be counted if they are already in the traffic stream.

To specify Fibre Channel settings

- 1 Select the **Setup** soft key, and then select the **Fibre Channel** tab.
- 2 In Tx Payload, select **Acterna** to transmit frames that contain a sequence number and time stamp so that lost frames and round trip delay can be calculated.



NOTE

Select an Acterna payload to measure round trip delay and count lost packets. For details, see [“Measuring round trip delay” on page 117](#)

- 3 In Frame Length, select one of the listed frame lengths, or select User Defined, and then enter a specific frame length in the USER Frame Length field.
- 4 Under Frame Channel Details, specify the following settings for the transmitted frames:

Settings	Values
D_ID	Type the destination ID of the port the frames will be transmitted to using a 3 byte format.
S_ID	Type the source ID for the port transmitting the frames using a 3 byte format.
SEQ_ID	Type the sequence ID for the frames using a 1 byte hexadecimal format.

Settings	Values
OX_ID	Type the originator exchange ID for the frames using a 2 byte hexadecimal format.
RX_ID	Type the responder ID for the frames using a 2 byte hexadecimal format.

- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The frame settings are specified.

Specifying Fibre Channel filter settings

Before transmitting layer 2 traffic, specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.

For example, the incoming frames must pass the filter to be analyzed for a BERT pattern. Local loopback is also only performed on frames that pass the filter.

To specify Fibre Channel filter settings

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the layer 2 terminate test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the **Fibre Channel Filter** tab.
- 3 If you want to filter received traffic for a specific destination or source ID, or using routing control, data type, or sequence control criteria, under Frame Channel Details, select the corresponding field, enable the filter, by selecting **Yes**, and then specify the filter value:

Settings	Values
R_CTL	Enter the routing control for filtered frames.
D_ID	Enter the destination ID for filtered frames.
S_ID	Enter the source ID for filtered frames.
Data Type	Enter the data type for filtered frames.
SEQ_CNT	Enter the sequence ID for filtered frames.

- 4 If required, specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings are specified.

Specifying traffic load settings

Before transmitting layer 2 traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty, or Ramp). The settings vary depending on the type of load. When configuring a load, you can specify the bandwidth of the transmitted traffic in 1% increments.



NOTE:

If you are certain the elements can support true 100% traffic, select the Allow flooding check box when configuring the Constant load.

Transmitting and analyzing layer 2 traffic

Before transmitting layer 2 traffic, specify:

- Interface settings (see [“Specifying interface settings” on page 109](#)).
- Frame characteristics of the transmitted traffic (see [“Specifying Fibre Channel frame settings” on page 113](#)).
- Frame characteristics used to filter received traffic (see [“Specifying Fibre Channel filter settings” on page 114](#)).
- Traffic load settings (see [“Specifying traffic load settings” on page 115](#)).

After you specify the layer 2 settings, you are ready to transmit and analyze the layer 2 traffic.

To transmit and analyze layer 2 traffic

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the layer 2 terminate test application for the interface under test.
- 2 Select the **Setup** soft key, and then select the **Interface** tab to specify settings that control the Fibre Channel interface (see [“Specifying interface settings” on page 109](#)).
- 3 Select the **Fibre Channel** tab to specify settings that define the frame characteristics of the transmitted traffic (see [“Specifying Fibre Channel frame settings” on page 113](#)).
- 4 Select the **Fibre Channel Filter** tab to specify settings that filter the received traffic based on specified frame characteristics (see [“Specifying Fibre Channel filter settings” on page 114](#)).
- 5 Select the **Traffic** tab to specify the type of load the unit will transmit (see [“Specifying traffic load settings” on page 115](#)).



NOTE:

The Gap/Idle time parameter that rounds to 0.001% in Ethernet applications rounds to the nearest 1% in FibreChannel applications.

- 6 Press **Results** to return to the Main screen.
- 7 Connect the module to the circuit.
- 8 On the Main screen, select the **Laser** button.
- 9 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.
- 10 Verify that the green Signal Present, Sync Acquired, Link Active, and Frame Detect LEDs are illuminated.
- 11 At a minimum, observe the summary, layer 2 link statistics and counts, layer 2 filter statistics and counts, error statistics, and layer 2 BERT statistics.

You have analyzed layer 2 traffic.

Logical loopback testing

Loopback testing allows you to transmit traffic from one VIAVI test set, and then loop the traffic back through a second unit on the far end of a circuit.

Measuring service disruption time with Peak IFG

The user can measure the service disruption time resulting from a switch in service to a protect line using the Peak IFG function.

To measure service disruption time with Peak IFG

- 1 Use the Test Menu or Quick Launch screen to select the layer 2 terminate test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Traffic tab to configure a constant load of traffic (see [“Transmitting a constant load” on page 128](#)).
- 3 If you need to specify other settings for the test on the near-end unit, select the appropriate tab; otherwise, press **Results** to return to the Main screen.
- 4 Connect the unit to the circuit.
- 5 On the Main screen, select the **Laser** button.
- 6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 7 Do the following on the unit:
 - a Start traffic.
 - b Clear the Peak IFG time by selecting the Reset Peak IFG Result button.
- 8 Initiate the switch to the protect line.
- 9 Observe the Peak IFG result in the Fibre Channel L2 Link Stats category.

Peak IFG time is measured.

Inserting errors

Buttons on the Main screen allow you to insert errors into the traffic stream. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

To insert errors

- 1 Select one of the following error types.
 - FEC
 - CRC
 - Bit (BERT payload only)
- 2 Do the following:
 - Specify the insert type (**Single**, **Burst**, or **Rate**).
 - If you specified **Burst**, enter the quantity of errors in the burst, and then select **OK**.
 - If you specified **Rate**, select the rate.
- 3 Press the **Error Insert** button.

Error insertion starts, and the associated button turns yellow. To stop error insertion, press the button again. Error insertion stops, and the associated button turns gray.

Measuring round trip delay

When you perform loopback tests, you can measure round trip delay by transmitting an Acterna payload. Frames with an Acterna payload carry time stamps, enabling the instrument to calculate the delay.



NOTE:

If you perform an end-to-end Fibre Channel test, invalid delay results appear. You must use a loopback configuration when measuring round trip delay.

To measure round trip delay

- 1 Use the Test Menu or Quick Launch screen to select the layer 2 terminate test application for the interface you are testing.
- 2 Select the **Setup** soft key, and then select the Fibre Channel tab.
- 3 Under Tx Payload, select an **Acterna** payload. The Acterna payload transmits frames with a time stamp and sequence number. You must select an Acterna payload to measure round trip delay.

- 4 In Frame Length, select one of the listed frame lengths, or select User Defined, and then enter a specific frame length in the USER Frame Length field.
- 5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.
- 6 Connect the module to the circuit.
- 7 On the Main screen, select the **Laser** button.
- 8 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.
- 9 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 10 At a minimum, observe the delay test results in the Fibre Channel L2 Link Stats category.

Round trip delay is measured.

64G Fiber Channel RS-FEC Testing

Perform the following for 64G Fiber Channel RS-FEC testing.

To specify RS-FEC settings

- 1 Select the **Setup** soft key, and then select the **RS-FEC** tab.
- 2 In **Incoming FEC**, select one of the following:
 - Find and fix errors (the default)
 - Find but don't fix
 - Ignore
- 3 Set **Disable HI SER Alarm** to **Off** (the default), or **On**. When **Off**, the test instrument will declare HI SER Alarms when they are detected; when **On**, the test instrument will ignore HI SER Alarms.
- 4 The user can change the RS-FEC BER Threshold. This is a threshold above which an excessive correctable BER alarm gets generated. The default value is mentioned in the standards.

You have specified the RS-FEC settings.

To insert alarms

If you intend to insert an alarm, select the **Alarms** tab, then select **HI SER** or **LOAMPS** (the default alarm).

If you intend to insert an error, select the **Errors** tab, then select **FEC-Uncorrectable** (the default error), or **FEC-correctable**. Specify the **Insertion Style (Single or Continuous)**.

Optics AOC/DAC Testing and Parameters

This chapter provides information about Optics Testing.

Topics discussed in this chapter include the following:

- [“Optics Self-Test” on page 120](#)
- [“Cable Test for AOC/DAC/AEC” on page 122](#)
- [“Application Code Switching” on page 124](#)
- [“ZR/ZR+ Tunable support” on page 126](#)
- [“I²C Peek/Poke” on page 128](#)
- [“Expert Mode” on page 129](#)

Optics Self-Test

The Optics Self-Test is available at all base rates corresponding to Ethernet and OTN line rates. The purpose is to troubleshoot or sample test pluggable optics.

Running the Optics Self-Test

The following procedure describes how to run the Optics Self-Test.

To run the Optic Self-Test

- 1 Connect an optical cable between the interface input and output ports.
- 2 Use the Test Menu screen to select the **Optics Self-Test** application for the interface you are testing.
- 3 On the next screen you have three configuration options, each with a **Go** button:
 - Edit Previous Configuration
 - Load Configuration from a Profile
 - Start a New Configuration (reset to defaults)Select an option by clicking the **Go** button next to it.
- 4 On the next screen, specify the following:
 - **Test Duration.** If test duration is set to User Defined, you can define your value in minutes or seconds.
 - **BER Threshold.** For Ethernet rates with a FEC, there is a BER Threshold Type selection of Pre-FEC (default) or Post-FEC.
 - **Optic Temperature Threshold (C).** Determines the temperature above which a fail condition will be declared. The default is 75C.



NOTE:


The recommended test times are calculated using BER theory based on the following:

- confidence level (CL) set to 95%
- the user-defined BER threshold
- the duration depends on the line rate selected from the applications menu

- **Stop on Error.** If enabled, the test stops immediately upon discovery of an out-of-parameter result.

Once you have configured your test, you can create a saved profile by clicking the blue **Save Profiles** link. Afterwards you can load these profiles by pressing the **Go To** button and clicking **Configure** to return to the earlier test configuration screen where you can restart the tests.

With an Ethernet rate that uses RS-FEC, there is a configuration called 'BER Threshold Type' which can be set to pre-FEC or post-FEC.

- 5 On the next Report Info screen, either:
 - go to the Job Manager menu under System to use Job Manager.
 - Fill out all entries and press **Next**.
- 6 On the Run Test screen, start your test by clicking the test button. The results overview appears on the left pane.
- 7 *Optional.* To verify the specifics of the optic being tested, select the  symbol next to the graphic of the transceiver. A list of specifications (including the SN) similar to the following will appear.

Nominal Wavelength (nm)	0	Power Level Type	OMA
Vendor	ELPEUS TECHNOLOG	Rx Max Lambda Power (dBm)	-0.849169
Vendor PN	QSFP-LB	Tx Max Lambda Power (dBm)	Unavail
Vendor SN	P32331000026	Nominal Bit Rate (Mbits/sec)	—
Vendor Rev	00	Diagnostic Byte	0
Date Code	110407		
Lot Code			
Transceiver	00 00 00 00 00 00 00 00 59		

Select the **Back** button to return to the test.

- 8 Click **Next** to proceed to the Report screen.

Generating Reports

- 1 After the Optics Self-Test has concluded, select the **Next** arrow at the bottom of the screen.
The Report screen appears.
- 2 Select the report format in the **Format** pane.
- 3 To view the report without saving it, select the **View Report button**.
- 4 To save a report, do the following:
 - a Enter the filename of the report to be saved. File names of other saved reports are accessible via the **Select** button after the File Name box.
 - b Click the **Create Report button**. If the **View Report after Creation** check box was checked, the report appears. If not checked, a message appears confirming that the report was saved. Select **OK**.
 - c If checked, the **Include message log** box will add a message log to the report.
- 5 If **Job Manager** was activated, the generated report will be available in the report section of the Job Manager application. The reference information lists the Serial Number, Optics type and Vendor.
- 6 A summary Job Manager report can be generated to provide the summary of all the cable and optics tests performed.

Cable Test for AOC/DAC/AEC

The Cable Test workflow is available for the following Ethernet base rates:

- 10GigE LAN — For straight and breakout cables
- 25GigE — For straight and breakout cables
- 40GigE — For straight cables
- 100GigE — For straight and breakout cables
- 100GigE KP4 — For straight and breakout cables



NOTE

The 100GE KP4 application refers to the 106.25Gbps line rate. The OneAdvisor 800 supports both 100GAUI-4 (NRZ) and 100GAUI-2 (PAM4) electrical buses. This applies to the basic application and to the 100GigE KP4 Cable Test.

In the L1 loopback application on the OneAdvisor 800, the 106.25 Gbps rate supports both 100GAUI-4 (NRZ) and 100GAUI-2 (PAM4).

- 200GigE — For straight and breakout cables
- 400GigE — For straight cables



NOTE

400G-400G straight cables can be tested using a single TM400GB-QQ module. For this functionality, launch **400GigE Cable Test** on port 1. If software license CALPBK is present, it is possible to launch a layer 1 loopback on the 2nd port from within Cable Test.

Use this workflow to troubleshoot or sample test cables including Active Optical Cables (AOC), Direct Attach Cables (DAC), and Active Electrical Cables (AEC). This covers both straight cables with similar connectors at both endpoints, as shown in and breakout cables, as shown in [Figure 26](#).

Figure 26 Cable with similar connectors



In the case of breakout cables, as shown in [Figure 27](#), launch Cable Test at the Ethernet rate corresponding to the branch endpoints. For example, with a 4x100G QSFP28 to QSFP-DD cable, launch Cable Test from the 100GigE rate. For 4x100G QSFP56 to QSFP-DD cables, launch Cable Test from the 100GigE KP4 rate, which is

available on the OneAdvisor 800. The Cable Test workflow can be used on a single module together with the Layer 1 QSFP Loopback application.



NOTE

Layer 1 Loopback application is strictly available on the OneAdvisor 800 400G modules TM400GB-QO and TM400GB-QQ

Table 7 describes the cables.

Table 7 Cables

Cable Test Launchpoint	Cable Type	Form Factor	Loopback (CALPBK)
400GE	Straight	QSFPDD-QSFPDD	425G (8x53G)
200GE	Straight	QSFP-QSFP	212.5G (4x53G)
	Breakout (x2)	QSFP-QSFPDD	425G (8x53G)
100GE	Straight	QSFP-QSFP	103.125G (4x25G)
	Breakout (x4)	QSFP-QSFPDD	425G (8x53G)
100GE KP4	Straight	QSFP-QSFP	106.25G PAM4 (2x53G)
	Breakout (x4)	QSFP-QSFP-DD	425G (8x53G)
40GE	Straight	QSFP-QSFP	41.25G (4x10G)
25GE	Straight	SFP-SFP	Planned
	Breakout (x4)	SFP-QSFP	103.125G (4x25G)
10GE LAN	Straight	SFP-SFP	Planned
	Breakout (x4)	SFP-QSFP	41.25G (4x10G)

Figure 27 Breakout cable



Cable Test verifies multiple parameters in testing cables. The key parameter to help determine the pass/fail criteria is Bit Error Rate (BER) where a threshold is specified. Having a BER above the threshold causes a fail condition. Please note that for rates the do not use FEC (Forward Error Correction) like 10GigE LAN and 40GigE, this is

based on the payload BER; for rates that use FEC like 25GigE, 100GigE KP4, 200GigE, 400GigE, the recommendation is to use the Pre-FEC BER as the threshold. It is also possible to use the Post-FEC rate as threshold; the post-FEC rate result is expected to be zero. Cable Test defaults to a given BER threshold (10^{-5}) which meets the vast majority of requirements; however, this target threshold could vary for certain cables and manufacturers. It is hence best to verify whether the cable manufacturer specifies a BER threshold and if so, it should be set as the BER threshold in Cable Test. Other parameters are used as pass/fail criteria such as the max Optic Temperature and excessive skew.

Cable Test includes the following functions:

- The workflow itself to simplify cable testing
- On OneAdvisor 800, the integration and control of Layer 1 QSFP Loopback on the second port to test a cable using a single module
- For breakout cables and from cable test, the setting of the loopback clock recovery host lane based on the breakout branch selection
- The setting of test time including a recommended mode which calculates the test time based on the target Bit Error Rate
- A high temperature threshold
- An immediate stop on error function
- Pass/fail results against an adjustable bit error rate threshold
- Usage of FEC with pre-FEC and post-FEC results for Ethernet rates that use FEC
- For breakout cables, use of job manager to provide a single report for all branches into one
- A test report which captures the serial number of the cable tested, as well as the setup and results.
- The user can save and reuse configuration files
- Access to the pluggable device information including an expert mode to troubleshoot using advanced parameters such a pre-emphasis
- The reporting of additional parameters such an optical power, power consumption, current draw

Application Code Switching

This function is found under the **QSFP/OSFP Expert** tab. It provides the ability to switch the application code to a different value for CMIS QSFP/OSFP devices. This applies to optical pluggable devices that support multiple application codes. You can look up application codes in the **Results** panel under **Interface**.

CMIS Host Media apps

Application codes corresponding to a **Host App Name** of 400GAUI-8 C2M are those that can run at 400GigE. Other examples include 100GAUI-2 for 100GigE KP4/4x100GigE, 200GAUI-2 for 200GE, and CAUI-4 for 100GigE.

You can switch to other application codes that correspond to a valid Host App Name on the **QSFP/OSFP Expert** tab. For example, you can switch between ZR and ZR+ if the pluggable device supports both. As well, some CMIS optics can be switched between 400GE and 4x100GE mode using application codes.



NOTE

Switching application codes takes some time as the pluggable device goes through an elaborated CMIS state machine. An hourglass on the user interface typically indicates a transitory state.

Switching an application code

Switching CMIS application codes may require additional information from the vendor of the pluggable optics device in the form of a detailed data sheet. The following procedure describes how to switch application codes when multiples are provided by pluggable optics.

To switch application codes

- 1 Select the line rate application, ensuring the correct port (1 or 2) is selected.
[Table 8](#) lists OneAdvisor rate applications and matching host names.

Table 8 Rate applications and matching host names

Host App Name	OneAdvisor Line Rate application ^a
400GAUI-8	400 GigE
200GAUI-4	200 GigE
100GAUI-2 (Nx100GAUI-2)	4x100 GigE
100GAUI-2 (N=1)	100 GigE KP4 (PAM4 Host Lanes)
CAUI-4	100 GigE

a. License dependent

- 2 Connect a pluggable optic device to the physical port.



NOTE

Some CMIS devices take some time to run through the CMIS state when first connected.

- 3 In the Results panel, select the Interface and CMIS Host-Media apps.

A table appears displaying all app codes for the pluggable device, as show in [Figure 28](#). Only those app codes with a host app name matching the OneAdvisor Line Rate application can be selected.

Figure 28 App codes for pluggable device

App Code	Host Code (hex)	Host App Name	Host Lane Count	Host Path Count	Host Lane Assign. (hex)	Media Code (hex)	Media Code (hex)
1	11	400GAUI-8 C2M	8	1	01	3E	400ZR, DWDI
2	11	400GAUI-8 C2M	8	1	01	3F	400ZR, 1-Wa
3	0D	100GAUI-2 C2M	2	4	55	3E	400ZR, DWDI
4	11	400GAUI-8 C2M	8	1	01	C5	
5	11	400GAUI-8 C2M	8	1	01	C0	
6	0D	100GAUI-2 C2M	2	4	55	C0	
7	0D	100GAUI-2 C2M	2	4	55	C1	
8	11	400GAUI-8 C2M	8	1	01	CE	
9	0D	100GAUI-2 C2M	2	4	55	CE	
10	0D	100GAUI-2 C2M	2	4	55	CF	
11	0D	100GAUI-2 C2M	2	4	55	C2	
12	41	CAUI-4 C2M (Anx.83E) w/o FEC	4	2	11	C2	
13	0D	100GAUI-2 C2M	2	4	55	C4	
14	41	CAUI-4 C2M (Anx.83E) w/o FEC	4	2	11	C4	
	FF	End of List	0	0	00	00	

- Click **Setup > Connector > QSFP Expert/OSFP Expert**.
Allowable Host Names are displayed in the Allowable Host App Names section.
- Select an app code from the **App Code** pull down.
Selecting a new app code causes the pluggable device to go through the CMIS initialization sequence. Once complete, the device can be used with the new application code. It is then possible to perform actions such as enabling the laser and generating traffic.

ZR/ZR+ Tunable support

This functionality specifically applies when using QSFP-DD/OSFP ZR devices equipped with tunable lasers with register support for CMIS. The primary purpose is to set the transmit channel to a value corresponding to a C-Band frequency. Other parameters including grid spacing, fine tuning and output power can be set. The Tunable Device tab under Setup Connector is only visible when a tunable QSFP-DD/OSFP device is inserted when running a 400GigE application. Other applications that can control tunable lasers via CMIS include 100GigE, 100GigE KP4, 4x100GigE, and 200GigE.

NOTE

When using ZR/ZR+ modules with the need to operate on battery, it is recommended to equip a OneAdvisor 800 with one PEM (Power Expansion Module) which provides an additional battery for additional current capabilities. The OneAdvisor 1000 is always equipped with two batteries.

Coherent ZR statistics

This function reads the statistics specific to the ZR/ZR+ CMIS pluggable devices. It accesses Versatile Diagnostics Monitoring (VDM) registers via the descriptor method

to access statistics. This method of access is compatible with pluggable optics vendors that follow CMIS.

The statistics are found in the **Results** panel under **Interface > Coherent** when a ZR/ZR+ device is used. These include:

- Media Pre-FEC
- Chromatic Dispersion (pn/nm)
- Differential Group Delay (ps)
- Second Order Polarization Mode Dispersion (ps²)
- Polarization Dependent Loss (dB)
- Optical Signal to Noise Ratio (dB)

Tunable settings

This includes being able to select the Grid Spacing as supported by the ZR device. The supported spacing values are also advertised. Changing the Grid Spacing or the channel takes a number of seconds as the pluggable device needs to run through a state machine to apply such settings.

The 400G Module offers a Tuning Mode selection where the user can use one of the following parameters to set the transmit channel:

- Channel No. — As per CMIS. Channel 0 is the default central value of 193.1THz
- Frequency — Type a value in THz that will round off to the nearest available value
- Wavelength— Type a value in nanometers that will round off to the nearest available value

Progress indicators such as Tuning in Progress and Wavelength Unlock guide the user on the progress when values are changed. An hourglass indicator shows that changes are in progress.



NOTE

It takes several seconds for the parameters to change. An hourglass on the user interface typically indicates a transitory state. An hourglass on the user interface typically indicates a transitory state.

Fine Tuning

This is an optional setting to make small adjustments in GHz around the current channel selection.

Output Power

Type a value in dBm to set the optical transmit power. OneAdvisor supports high power pluggable devices that can reach up to 0 dBm; the key factor is the cooling of pluggable optics.



NOTE

Maximum Output Power is an absolute value that the pluggable module cannot always reach, as there are several dependencies for this parameter.

Coherent Results

These results only become available with ZR specific devices that explicitly report coherent results. These results include:

- Media Pre-FEC BER
- CD (Chromatic Dispersion) in ps/nm
- DGS (Digital Group Delay) in ps
- SOPMED (Second Order Polarization Mode Dispersion) in ps²
- PDL (Polarization Dependent Loss) in dB
- OSNR (Optical Signal to Noise Ratio) in dB

If the Ethernet > Coherent menu does not show any information, the CMIS pluggable optic does not provide these results.

I2C Peek/Poke

I²C Peek/Poke functionality allows you to read (peek) or write (poke) to SFP or QSFP/OSFP devices via an I2C interface. For CMIS devices, the CMIS process is used.

For Peek and Poke, the following can be entered as decimal numbers:

- Page Select
- Register Address



NOTE

Typically these values from SFP or CMIS documentation are in decimal. The device uses hexadecimal values.

For Poke, the poke value is also a hexadecimal value typically mapping to individual bits for each register

A peek or poke success result is available; 1 indicates success.

In addition, there is a full register dump file which gets updated with each application launch or when a pluggable device gets reseated. This file gets automatically generated in the bert/reports directory with the following name:

- For SFP devices: SFP_RegisterDump.txt
- For QSFP devices: QSFP_RegisterDump.txt
- For QSFP-DD devices: QSFPDD_RegisterDump.txt
- For OSFP devices: OSFP_RegisterDump.txt

Additionally, it is possible to generate these files via manual action under **Save Register Values in All Pages**. It is also possible to save the registers for a specific page via the user **Save** action.

Expert Mode

For QSFP/OSFP devices, expert mode provides pre-emphasis settings. Depending on the rate and device type, the following settings are available.

Application Code setting

For CMIS applications, you can change the Application Code on pluggable devices. The allowable applications are based on the host application used by the current OneAdvisor software application being run. Host application refers to the electrical bus format used by the current pluggable optics. You can view the list of available application codes using the **Interface > CMIS Host-Media Apps** result menu. Only those application codes that match allowable applications corresponding to the current host application used are permitted. This function provides the current data path state toward acceptance of an application code value.

Host Transmit settings

Host Transmit settings affect the electrical pulse shape on all lanes in the transmit direction from the 400G Module towards the pluggable module. The settings are:

- Default — The default values provided by the instrument.
- Advanced — Pre-cursor and post-cursor parameters affect electrical pulse shape at a rising edge (pre-cursor) or at a falling edge (post cursor.) There are no units for these parameters.

The **Swing** parameter is in millivolts.

Module Rx Output settings

The Module Rx Output settings affect the electrical pulse shape on all lanes in the transmit direction from the pluggable module toward the 400G Module. These correspond to CMIS registers in the pluggable device itself. The options are:

- Vendor Defaults — The default values from the pluggable device itself. If manually selecting vendor defaults from **Advanced**, the pluggable module will go through a reset sequence.

- Advanced — Includes a **Swing** parameter in millivolts.



NOTE

For **Vendor Defaults**, if the Vendor advertises that it does not support configuration of those settings, then the Vendor **Pre-Cursor**, **Post-cursor**, and **Swing** will be reported as “n/a”.

CMIS pluggable optic reset

It is possible to issue a reset command from Expert Mode to exercise the Module State Machine. This is used to reset a CMIS pluggable and make it run through its sequence, including going through low power mode.

Automated Testing Using Workflows

This section provides information on using the automated scripting programs that are available, depending on the how the unit is equipped and configured.

Topics discussed in this chapter include the following::

- [“Launching an automated test” on page 132](#)
- [“Automated RFC 2544 tests” on page 134](#)
- [“About the Y.1564 SAMComplete test” on page 153](#)
- [“Automated VLAN tests” on page 165](#)
- [“Saving automated test report data” on page 166](#)

Launching an automated test

There are two ways to launch automated test scripts from the Test Select application and the automated script in which it is to be run.

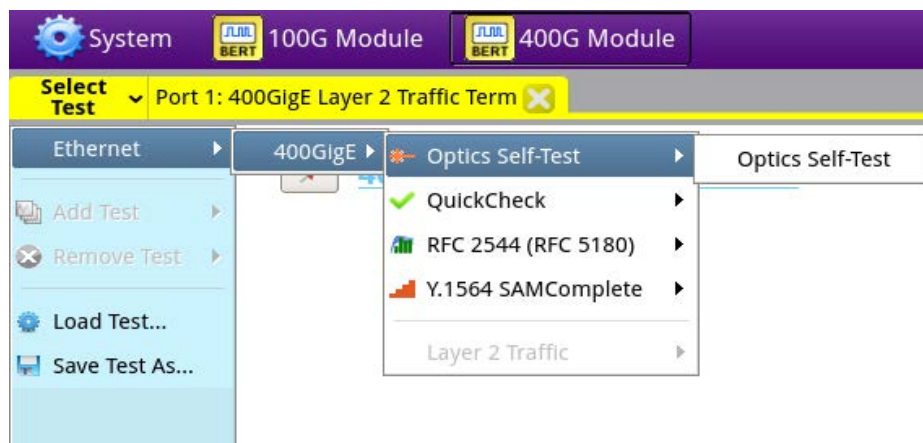
- Directly from the Select Test menu, for example by choosing Ethernet, then the line rate, then the automated test RFC 2544, and then the layer L2 Traffic.
- From within a base application, such as “400GigE>Layer 2 Traffic> Term”, specifying the automated test to be run by a soft key on the right side of the interface, or by a button inside the Toolkit which is opened by the Toolkit softkey. Note that all toolkit functions are also provided in the Tools menu (depending on your model, accessed from the menu bar along the top of the interface, or from the Tools icon in the lower-left corner.)

In most cases, the relevant configuration settings are available within the automated test, but if the base application configuration must be changed before running the automated test, use option 2 above to launch the base application, then make the necessary configuration changes, then launch the automated test. You may also use the ‘Load Test...’ menu choice to configure the base application from a Saved Test file before starting the automated test. For the 4x100GE application, you can select one of the up to four ports on the pluggable optics to run a test with RFC 2544.

To launch from the Select Test menu

- 1 From the Select Test application tree, select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed.

Figure 29 Select Test application tree



- 2 Select the automated script from the top levels of the tree, then the specific test desired. The automated script is launched.

To launch for later use

- 1 Select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed. (See [Figure 29](#) above).

- 2 Select the base application (from the lower part of the application tree) and then initiate the desired automated script using the on-screen soft key on the right side of the interface.

The automated script will be launched, ready to be configured.



NOTE:

The Quick Launch window displays previously run and/or saved configurations of applications. Automated scripts launched simultaneously with base applications are fully identified with the script.

To launch from a running application

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the appropriate application.
- 2 Connect the modules on the near-end and the far end to the circuit.
- 3 Select the **Laser** button to turn the laser on.
- 4 On both modules, verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.
- 5 On the Main screen, do one of the following:
 - If you are running the RFC 2544 test, press the **Enhanced RFC 2544 Test** soft key, and proceed to [“Configuring the Enhanced RFC 2544 tests” on page 143](#).
 - If you are running the automated multiple Ethernet service verification SAMComplete test, press the **SAMComplete** soft key, and proceed to [“About the Y.1564 SAMComplete test” on page 153](#).

The automated test is launched.

Automated Test Availability

Table 9 lists the available automated tests for each application.

Table 9 Automated Tests

Automated Test	Application
QuickCheck	Ethernet – Layer 2 Traffic
Enhanced RFC 2544 Test	Ethernet – Layer 2 Traffic
SAMComplete (Y.1564)	Ethernet – Layer 2 Traffic
VLAN	Ethernet – Layer 2 Traffic



ALERT: CORRUPTED RESULTS

Pressing Restart during a test could corrupt the results. To ensure accurate script results, wait for the script to complete before pressing Restart.

Automated RFC 2544 tests

You can use the instrument to run tests that automate the procedures recommended in RFC 2544 for layer 2 Ethernet. The tests prompt you to select key parameters for throughput, round trip delay, frame loss rate, and back to back frame tests, run the tests, and then automatically generates a report file of results for the tests and a log file detailing the progress of the script. The generated report file includes the test results in tabular and graphical formats. In the case of the 4 x 100GE application, you can select one of the four ports on the pluggable optics to run a test with RFC 2544.

The following topics are discussed in this section:

- [“Features and capabilities” on page 134](#)
- [“About loopbacks” on page 135](#)
- [“QuickCheck” on page 135](#)
- [“Throughput test” on page 137](#)
- [“Latency \(RTD\) test” on page 139](#)
- [“Packet Jitter test” on page 139](#)
- [“Frame Loss test” on page 140](#)
- [“Back to Back Frames test \(Burst test\)” on page 140](#)
- [“Optimizing the test time” on page 141](#)
- [“Importing and exporting RFC config files” on page 142](#)
- [“Configuring the Enhanced RFC 2544 tests” on page 143](#)
- [“Specifying the external test settings” on page 143](#)
- [“Setting Connection parameters” on page 144](#)
- [“Test selection” on page 146](#)
- [“Running Enhanced RFC 2544 tests” on page 148](#)

Features and capabilities

The instrument supports the following features when running the RFC 2544 tests:

- Support for Ethernet line rate
- QuickCheck—Before running the Enhanced RFC 2544 test, you can run the QuickCheck application to verify that the local and remote instruments are configured properly to bring up the link, establish the link, establish a loopback, and then verify that the link can support 100% traffic utilization. There is also an extended Layer 2 traffic test useful for quick turn-ups.

- Graphical output of key results. When running the tests, frame loss, throughput, and latency (round trip delay) results are displayed graphically in their own result categories.
- Status bar. A status bar is also provided that lets you know how far the test has progressed, and provides an estimate of the time remaining to run the test.
- Report output. You can save the test results to a user-named file in PDF, XML, or TXT format.
- Enhanced test. You can run the Enhanced RFC 2544 test to run a symmetrical test.
- Exporting and importing of configurations for the Enhanced RFC test.
- The Enhanced RFC tests supports round-trip delay (RTD).

About loopbacks

During the automated tests, the instrument checks for a loopback. It could be one of the following types:

Active loop — the destination has responded to a loop command.

Hard loop — the source and destination addresses are the same for both the returned frames and the outgoing frames.

Permanent loop — the source and destination addresses are switched in the returned frames.

QuickCheck

The QuickCheck application is used to verify that the local and remote instruments are configured properly to bring up the link, establish the link, establish a loopback, and then verify that the link can support 100% traffic utilization. QuickCheck can be launched stand-alone or used integrated into the RFC 2544 or SAMComplete scripts.

There are a number of ways in which the QuickCheck test may be initiated:

- launch QuickCheck directly from the Test menu
- relaunch Quick-Check from an underlying L2 traffic application via the Quick-Check button on the right side of the screen.
- the original simple verification that the local and remote instruments are configured properly to bring up the link accessed through the QuickCheck button in the tool kit.
- an extended Layer 2 Turnup test
- an automatic initiation of the full RFC 2544 test upon completion of the Quick-Check test link verification utilizing maximum throughput rates determined by the QuickCheck test

These options can be run in combination or separately.



NOTE:

After specifying settings for QuickCheck in the standalone QuickCheck test (from the Test menu), you may return to the main app if desired, but you should not change any settings or you must change them back before re-entering QuickCheck. Running the test with settings different than originally set may result in some unexpected errors or failures. To restore test defaults, select restore test to defaults or manually restore any settings that were changed.

Understanding the QuickCheck stages

At each of the three stages of the QuickCheck application, the instrument automatically performs certain actions. Some actions must occur before others can take place. For example, the local port must be up before a loopback can take place.

Local Port

If application for an optical circuit indicates that the local port is down, (indicated by a red **Not Connected** button), verify that the laser is ON on both near and far end instruments. If the application is for an electrical circuit, verify that frame sync and link LEDs are illuminated on both instruments.

Auto-negotiation

Auto-negotiation can not take place until the physical link is established. If at any time during this phase the link or frame synchronization is lost, the instrument will alert the user, and will then restart the application automatically. There is no auto-negotiation at rates above 1GigE.

Remote Loop (traffic test mode)

A remote loop up can not take place until the physical link is established.

Basic Load Test

The load test can not take place until a remote loop is established or detected. If a loop is in place, the near end instrument automatically transmits a full load of traffic (100% at the selected line rate) using the frame size that was specified for the application. The instrument then calculates the average layer 2 bandwidth utilization, and displays it as a percentage.

Test at configured Max Bandwidth

With this option selected, the RFC 2544 test will automatically be run upon completion of the QuickCheck test using the Max Bandwidth setting pre-configured on the Setup-All Tests tab.

Layer 2 Quick Test

The Layer 2 Quick Test extended test option operates in the symmetric, loopback mode. The test can be configured to set the length of time the test is to be run and to configure the CIR in the RFC 2544 settings with a percentage of the Throughput value detected. The default value will be 100% (i.e. CIR will be 100% of the QuickCheck Throughput).

Throughput test

The throughput test is used to determine the highest possible bandwidth at which no frames are lost.

VIAMI zeroing-in method

The VIAMI zeroing-in method functions as follows:

Attempting Phase

- The test starts transmitting traffic at the Maximum Bandwidth, then waits 3 seconds.
- The test does a restart, then waits 5 seconds.
- The test calculates the average layer 2 bandwidth utilized (L2 Avg. % Util).
- If the Bandwidth Accuracy is 1% and the L2 Avg. % Util is less than 99.98%, the throughput is the integer value of the measurement. Otherwise, throughput is 100%.
- If the Bandwidth Accuracy is .1% or .01%:
 - The test increases the load 3% over the L2 Avg. % Util measured above.
- If the Bandwidth Accuracy is .1% or .01%:
 - Start traffic at the rate calculated above
 - Wait 3 seconds
 - Do a test restart
 - Wait 5 seconds
 - Get the L2 Avg. % Util

For .1% accuracy, Throughput is calculated as:

- The (integer value of L2 Avg.) % Util * 10 divided by 10

For .01% accuracy, Throughput is calculated as:

- The (integer value of L2 Avg.) % Util * 100 divided by 100

Verifying Phase

The load is set to the calculated throughput value, and transmitted for the Throughput Duration time. If the frame loss tolerance is exceeded, instructions are provided for testing the link manually for intermittent problems, and the test is aborted.

Throughput test results

The following results are reported for every frame length selected.

Cfg Length (Mbps)

The bit rate for transmitted traffic (expressed in Mbps) at which no frames were lost for a particular frame length.

Measured Rate (Mbps)

The measured bit rate (expressed in Mbps) at which no frames were lost for a particular frame length.

Measured Rate (%)

The bit rate (expressed as a percentage of the line rate) at which no frames were lost for a particular frame length.

Measured Rate (frms/sec)

The peak frame rate (expressed in frames per second) at which no frames were lost for a particular frame length.

Pause Detected

These results are also reported when you run the Latency and Packet Jitter tests.

**NOTE:**

If QuickCheck is not performed, the report may show loop type achieved.

Pass/fail threshold

You can configure the test to optionally indicate whether the Throughput test passed or failed. To do so, you specify the bandwidth for the Throughput Pass Threshold. If the highest rate at which frames are not lost is equal to or exceeds the threshold, the test indicates that the test passed for each transmitted frame length. If it falls below the threshold, the test indicates that the test failed.

Latency (RTD) test

If the Latency test is a desired part of the test, the Throughput test must also be run.

About the latency test

The Latency test transmits traffic at a specified percentage of the bandwidth at which no frames were lost (as determined during the Throughput test) for each frame length you selected. The average delay is then measured after transmitting traffic for each frame length for the period of time that you specified as the Latency (RTD) Trial Duration. The test measures delay for each trial (specified as the Number of Latency (RTD) Trials), and each measurement is then added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average.

If the Throughput test reached the lowest bandwidth limit without ever successfully receiving all transmitted frames (in other words, it lost frames), the average delay will also be unavailable. Unavailable measurements are not included in the total trial average.

Pass/fail threshold

You can configure the test to optionally indicate whether the Latency test passed or failed. To do so, you specify the Latency (RTD) Pass Threshold. If the total trial average for measured average delay is equal to or less than the threshold, the test indicates that the test passed for each transmitted frame length. If it exceeds the threshold, the test indicates that the test failed.

Packet Jitter test

If you intend to run the Packet Jitter test as part of the test, you must also run the Throughput test.

About the Packet Jitter test

The Packet Jitter test transmits traffic at the maximum bandwidth at which no frames were lost (determined using the Throughput test) for each frame length you selected. The packet jitter is then measured after transmitting traffic for each frame length for the period of time that you specified as the Packet Jitter Trial Duration.

The test measures the average packet jitter and maximum packet jitter for each trial (specified as the Number of Packet Jitter Trials), and then each measurement is added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average measurement.

If the Throughput test reached the lowest bandwidth limit without ever successfully receiving all transmitted frames (in other words, it lost frames), the packet jitter measurements will also be unavailable. Unavailable average or maximum average measurements are not included in the total trial average.

Packet Jitter test results

Packet Jitter results are presented statistically.

Pass/fail threshold

You can configure the test to optionally indicate whether the Packet Jitter test passed or failed. To do so, you specify the Packet Jitter Pass Threshold. For each frame length you selected, the test compares the average packet jitter for the trial to the value that you specified as the threshold. If the average packet jitter is less than or equal to that specified for the threshold, the test indicates that the test passed. If it exceeds the threshold, the test indicates that the test failed.

Frame Loss test

The Frame Lost test measures bandwidth until no frames are lost.

About the frame loss test

For each frame length you select, beginning at the maximum test bandwidth you specified, the instrument transmits traffic for the amount of time you specified as the Frame Loss Trial Duration. If frames are lost during that time frame, the instrument reduces the transmitted bandwidth by the amount you specified as the Frame Loss Bandwidth Granularity, and then transmits the traffic at the reduced bandwidth.

The test decreases the transmitted bandwidth accordingly until either no frames are lost during the duration specified, or the transmitted bandwidth reaches the lowest bandwidth limit (specified as the Frame Loss Bandwidth Granularity).

If the instrument succeeds in transmitting frames without losing any at a particular bandwidth, it then reduces the bandwidth one more time (by the granularity amount). If no frames are lost, the test stops. If frames are lost, the instrument starts the entire process over again until two successive trials occur without losing frames.

Frame Loss test results

Frame Loss results are presented in a tabular format, illustrating the frame loss rate versus the percent of the bandwidth.

Back to Back Frames test (Burst test)

This test determines the maximum back to back burst size supported by the network under test. Upstream and downstream back to back (burst size) tests can now be run concurrently (rather than sequentially).

About the Back to Back Frames test

Using the frame length and other settings such as the frame type and encapsulation, the instrument calculates the burst size required to transmit back to back frames for the duration that you specify as the Back to Back Max Trial Time. It then transmits the burst of frames over the circuit. If the number of frames transmitted carrying an Acterna payload does not equal the number of received frames carrying an Acterna payload (indicating that frames were lost during the transmission), the instrument goes through the stages described for the Throughput test (see [“Throughput test” on page 137](#)) until no frames are lost, or until the number of frames per burst from the last successful burst exceeds the Back to Back Frames Granularity by a 1 frame burst.

The test counts the number of frames received for each trial (specified as the Number of Back to Back Frame Trials), and each count is added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average count. The test then uses this count to calculate the average amount of time a burst can be transmitted before a frame is dropped.

Back to Back test results

Back to Back test results are presented in a table.

Optimizing the test time

When you configure an Enhanced RFC test in symmetric mode, you can optimize the time it takes to run the test time by doing the following:

- Ensure that the duration time for the Throughput, Packet Jitter, and Latency (RTD) tests is the same.
- Ensure that the number of trials for the Latency (RTD) and Packet Jitter tests is “1” (one trial only).

If you configure the test in this manner, all three tests (Throughput, Latency, and Packet Jitter) will be run simultaneously. If the duration times vary, or if you indicate that you want to run more than one trial, each test will be executed in succession. As a result, the test will take longer to complete.

In addition to the duration time and number of trial settings, you can control the bandwidth transmitted during the course of the test.

- If you select Top Down, the test transmits traffic at the maximum bandwidth specified, and then *decreases* the bandwidth for each trial by the granularity you specify until you reach the minimum bandwidth specified.
- If you select Bottom Up, the test transmits traffic at the minimum bandwidth specified, and then *increases* the bandwidth for each trial by the granularity you specify until you reach the maximum bandwidth specified.

Importing and exporting RFC config files

The instrument allows importing and exporting of configuration files. This allows consistent testing configurations which yield more reliable test results. You will need a USB stick for transferring the files.

To export a RFC configuration

- 1 Verify that you have a USB stick inserted into the instrument.
- 2 After specifying the settings for your Enhanced RFC test, save the configuration.
- 3 Exit the test.
- 4 From the Tools menu, select **Export to USB**, and then **Saved Test Config**.
- 5 Locate the *.expert_rfc file or files you wish to export. Click on the file to select it (click again to clear it).
- 6 Do one of the following:
 - If exporting multiple files and you wish to zip them before exporting, click the **Zip selected files as** box and specify a file name for the resulting .tar file, and then click **Zip & Export**.
 - If exporting files without zipping or are exporting a single file, Click **Export**.

The files are copied to the USB stick.

To import a RFC configuration

- 1 Verify that you have a USB stick inserted into the instrument.
- 2 From the Tools menu, select **Import from USB**, and then **Saved Test Config**.
- 3 Locate the file or files you wish to import. Click on the file to select it (click again to clear it).
- 4 Do one of the following:
 - If importing a zipped file, click **Unzip & Import**.
 - If importing one or more files that are not compressed, click **Import Test**.

The files are copied to the instrument's file directory. The next time you launch the test, the imported configuration(s) appear in the configuration list.

Initiating the Enhanced RFC2544 Test

There are two ways to initiate the RFC2544 test using the on screen softkey.

- Select the base application and then initiate the RFC2544 test using the on screen soft key.
- Select the RFC2544 implementation for the technology and interface you want to use.

The first option will be necessary if you have “No Configurations” saved where you can load the parameters of the test to be run. Alternatively, if you are coming back to run of a saved configuration (or modify an existing profile), you can select the direct initiation of the automatic script, load the existing profile and start testing. For more information see [“Launching an automated test” on page 132](#).

Configuring the Enhanced RFC 2544 tests

Before running these tests, it’s important to understand which settings need to be specified externally (outside of the automated test screens), and how to navigate through the screens and menus presented when you run the tests.

Specifying the external test settings

The automated tests allow you to specify most required settings; however, certain settings need to be specified outside of the automated test screens (using the procedures listed in [Table 10](#)).

To specify the external test settings

Table 10 RFC 2544 Setup Tab Settings

Table 11

Layer/Setting	To specify, see....
Ethernet Layer 2	“Specifying Ethernet frame settings” on page 24
– Frame Type	
– Destination Type	
– Ether Type	
– Unit Identifier	“Specifying interface settings” on page 23

- 1 Select the **Setup** soft key, and then do the following:
 - If you are running the test with layer 2 Ethernet traffic, select the Ethernet tab to specify settings that define the frame characteristics of the transmitted traffic, such as an 802.3 frame type, or a VLAN ID and priority (see [“Specifying Ethernet frame settings” on page 24](#)).
- 2 Verify the following settings:
 - Payload analysis is ON for your current test application. You can not run the RFC 2544 test when the module is configured to analyze live traffic.
 - The module is not configured to run a timed test. You can not run the RFC 2544 test during a timed test.
- 3 Select the **Results** soft key to return to the Main screen.

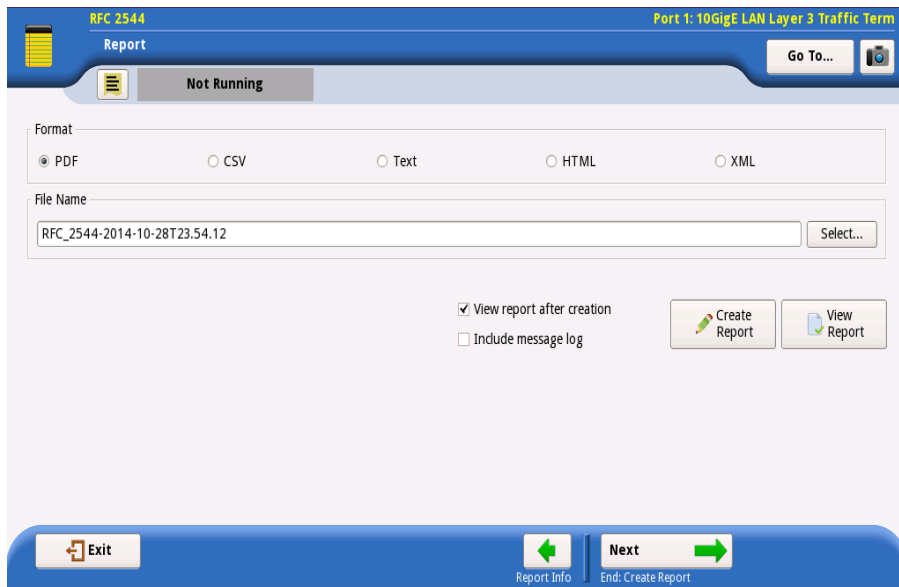
The external settings are specified.

Setting Connection parameters

Before running any of the RFC2544 automated tests, the connection parameters must be defined so the local and remote units can link.

Configuration methods

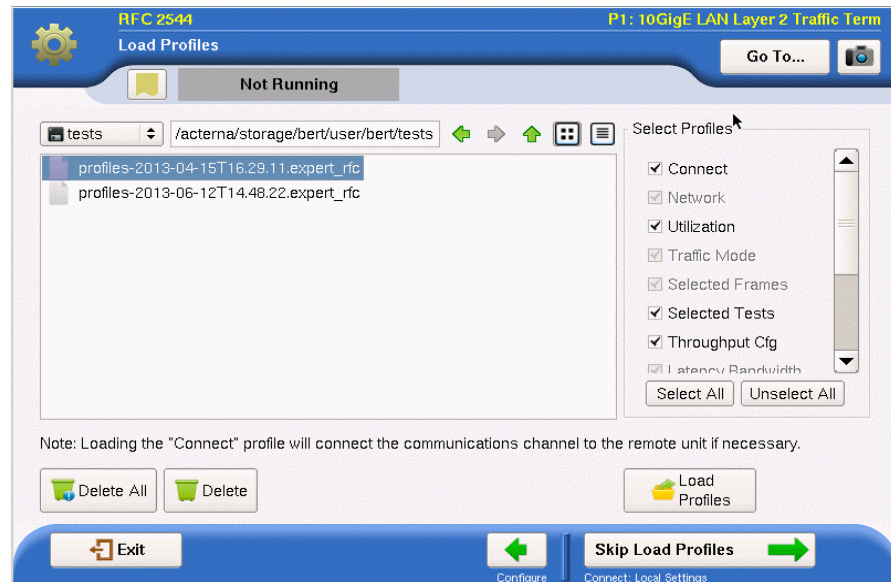
Upon initiation of the RFC2544 Automated configuration, the user is given the option of defining all parameters manually or restoring a configuration from a previously saved file. In either case any parameter may be modified prior to running the tests.



Retrieving configuration from previously saved file

- 1 To select a configuration currently saved on the unit, select the **Go** button (right green arrow) after “Load Configuration from Profile”. The interface shown in [Figure 30](#) will appear..

Figure 30 RFC 2544 Load Profiles screen



- 2 After selecting one of the files on the left side, the configured scripts that comprise the profile will be shown checked. To prevent any portion of the saved configuration from loading, clear any of the activated sections. Any portion of the test may be configured after the saved file is loaded.
- 3 Select the **Load Profile** button. The test will be configured as saved and if the connect data is detailed in the file, the unit will attempt to establish that connection.
- 4 If a desired configuration is not found, select the **Skip Load Profiles** button (right green arrow). Go to [step 2](#) of “[Manually configuring all parameters](#)” on [page 145](#).

Manually configuring all parameters

- 1 To manually configure the tests to be run, from the main menu, select the **Go** button (right green arrow) after Configure Test Settings Manually.
- 2 The first Connection parameters screen describes the Symmetry of the connection to be established.
 - a Select the Throughput.
 - **Symmetric** - same parameters for up and downstream connections
 - b Define the Measurement Direction as **Looped**.
Select **Next** (the green arrow).

- 3 For all symmetry schema, except loopback, the Connection parameters pertaining to the local and remote instrument must be defined. These parameters are Frame Type and encapsulation.

Optional settings **MAC Address Source** and **Number** are accessed via the **Advanced** button.

When all local settings have been specified, select **Next** (the green arrow).

Test selection

After all connection parameters have been defined, the user is able to select which tests are to be included in the automated sequence. In addition to the standard RFC 2544 tests: Throughput, Latency, Frame Loss, and Back to Back, additional tests are included for Packet Jitter, Burst and Extended Load.

Choosing tests to be included

- 1 Upon opting to select which tests to run, the test screen appears.
The Enhanced RFC tests include Throughput, Latency, Frame Loss, Back to Back, Buffer Credit and Buffer Credit Throughput.
- 2 Select the tests that are to be included in the Enhanced RFC 2544 automated test by checking the box in front of the tests desired. Note that some tests will be unavailable with certain connections or in combinations with other tests.
When all desired tests have been chosen, select **Next** (the green arrow).
- 3 Depending upon which test(s) have been selected there are a number of parameters that must be set to define the results.
 - a On the Utilization screen, the **Bandwidth Unit** and the **Max Bandwidth** can be selected.
To choose whether the bandwidth units used for the tests are chosen from **Layer 1** or **Layer 2**, make the selection in the Bandwidth Unit drop-down box. Then enter the **Max Bandwidth (in Mbps)** in the entry box (Upstream and/or Downstream for non-symmetric test).



NOTE:

The load value cannot be set to a value that cannot be measured on the other side due to an imbalanced line rate.

To further refine the Utilization configuration, select **Set advanced Utilization settings**. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

- b On the Frame Lengths screen, select the number of frame lengths to be tested by checking the appropriate number of boxes and then entering a value for each checked Upstream and/or Downstream Frame length to be tested.

Select **Next** (the green arrow).

- c On the Throughput Test screen, select whether the RFC 2544 Standard or JDSU Enhanced version of the test is to be used for the **Zeroing-in Process** and the level of **Measurement Accuracy**.

To further refine the Zeroing-in Process configuration, select **Set advanced Throughput Latency measurement settings** and then specify the **Latency Bandwidth** or **Configure Max Bandwidth per Frame Size**. Select **Back** to return to the previous screen.

- d On the Frame Loss Test screen, select the test procedure to be used.

RFC 2544. Transmits traffic at the maximum bandwidth, and then decreases the bandwidth for each trial by the granularity you specify. The test ends after two successive trials with no frames lost. This procedure also requires specification of **Bandwidth Granularity** in Mbps.

Top Down. Transmits traffic at the maximum bandwidth specified in the **Test Range** setting, and then decreases the bandwidth for each trial by the **Number of Steps** specified until the minimum bandwidth is reached for the specified Test Range.

Bottom Up. Transmits traffic at the minimum bandwidth specified in the **Test Range** setting, and then increases the bandwidth for each trial by the **Number of Steps** specified until the maximum bandwidth is reached for the specified Test Range.

To further refine the frame loss configuration, select **Set advanced Frame Loss measurement settings** and then choose whether to **Measure Latency** or **Measure Packet Jitter** by selecting their checkbox. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

- e For the Back to Back Test screen, define the **Max Duration** (Upstream and/or Downstream for non-symmetric test) of each test and **Burst Granularity** in kB.

To further refine the Back to Back test, select **Set advanced Back to Back settings** and then choose the **Ignore Pause Frames** checkbox. Select **Back** to return to previous screen.

- f For the Burst Test screen, select the Burst Test Type - either **Committed Burst Size, CBS Policing (MEF 34)** or **Burst Hunt** and the **CBS (in kB)** (Upstream and/or Downstream for non-symmetric test), **CBS Duration** and **Burst Sizes (kB)** (Upstream and/or Downstream for non-symmetric test) depending on which Burst test type is chosen.

- g For the Extended Load test screen, enter **Throughput Scaling (%)** and **Frame Length** values.

Select **Next** (the green arrow). **Next** (the green arrow).

When the individual tests have been configured, select **Next** (the green arrow).

- 4 The overall test control configuration items need to be set.

- a On the Test Duration screen, specify whether all tests are to have common durations or are individual tests to have their durations specified separately by selecting **Yes** or **No** radio button.

If Yes is chosen specify the **Durations** and the **Number of Trials**.

Select **Next** (the green arrow).

- b** On the Test Thresholds screen, specify whether **Pass/Fail** indications are to be shown for individual tests and what is the pass/fail **Threshold** value (Upstream and/or Downstream for non-symmetric test) for each test.

When the overall test control configuration items have been set, select **Next** (the green arrow).

- 5** The RFC 2544 test has been completely configured.

- a** If it is not desired to save this configuration profile, at this time, go to [step 6](#).
- b** To save the profile of this configuration, specify the filename under which it is to be saved by entering the desired filename in the **File Name** box. To discover the name of previously saved files click on **Select**.

To preserve the configuration so it won't be changed by future users, select the **Save as read-only** checkbox.

When all file attributes have been set, select the **Save Profiles** button. and then select **OK** to return to the previous screen.

Select **Next** (the green arrow).

- 6** The Run/Edit screen appears.

Do one of the following:

- To return to the beginning and modify the current configuration, select the **Go** arrow after “Change Configuration”. Go to [“Manually configuring all parameters” on page 145](#).
- To load a previously saved set of configuration parameters, select the **Go** arrow after “Load Configuration from a Profile”. Go to [“Retrieving configuration from previously saved file” on page 145](#).
- To run the test, as configured, select the **Go** arrow after “Run Tests”. The Run QuickCheck screen appears. Go to [“Running Enhanced RFC 2544 tests” on page 148](#)

Running Enhanced RFC 2544 tests

After configuration has been completed, the Enhanced RFC 2544 tests can be run.

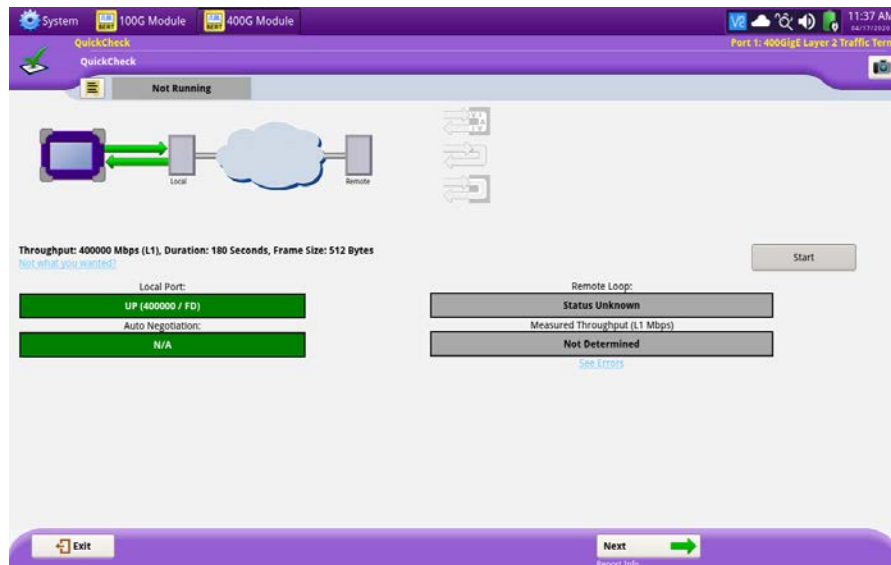
The first test to be run is the QuickCheck test. The QuickCheck application uses the configured parameters for the connection to either run a bi-directional test or establish a loopback to verify that the link can support 100% traffic utilization allowing the other tests to be run effectively.

The balance of the tests will run without any user intervention necessary after initiation.

Initiating QuickCheck test

- 1 The screen in [Figure 31](#) appears. Notes appear on the left side of the screen indicating the current settings to be used for the test. If different settings are desired for throughput and Frame parameters, click the **Not what you wanted?** link.

Figure 31 QuickCheck Screen



- a Select the **Test using configured RFC 2544 Max Bandwidth** or **Use the Measured Throughput measurement as the RFC2544 Max Bandwidth** check boxes and/ or enter a new frame size value via the pop-up keypad.
 - b When configured for layer 2 loopback test, you can select **VLAN Discovery**. This mode will transmit a burst of VLAN frames to automatically discover test instruments on the network.
 - c When configured for a loopback test, you can select **Maximum Frame Search**. When selected after a successful loop detection, bursts of various frame sizes will be transmitted in order to determine the largest frame size you network can support.
 - d Select **Back** to return to previous screen.
- 2 To initiate the QuickCheck test, press the **Start** button.
 - 3 Observe the network diagram. The following occurs:
 - a For both end running terminate application - The instrument indicates that it is waiting for a link, then connecting the link, and provides the status of the auto-negotiation capabilities.
 - b The instrument checks for a hardware loop. If a hardware loop is not found, we check for a permanent loop. If a permanent loop is not found, the instrument declares "No Loop Found"

- 4 The instrument moves on to transmit traffic over the link at 100% of the line rate to verify the link's ability to support a full load of traffic. If the test is successful, the button under Measured Throughput displays the expected throughput (Up and Down if appropriate).

Green graphics on the screen indicate that an action was successful, yellow indicates an action is currently taking place (for example, connecting the local port to the link), and red indicates that an action failed (for example, the remote loop failed).

When QuickCheck has reported acceptable results, select **Next** (the green arrow).

Initiating Enhanced RFC 2544

The RFC 2544 testing status screen keeps the user informed of the progress and the success or failure of the tests while they are running. A key of status indicators is available on the screen for easy reference.

- 1 To initiate the test sequence, select the **Run Test** button.

The time remaining displays in the top tab, and each test scheduled will be displayed with its current status.



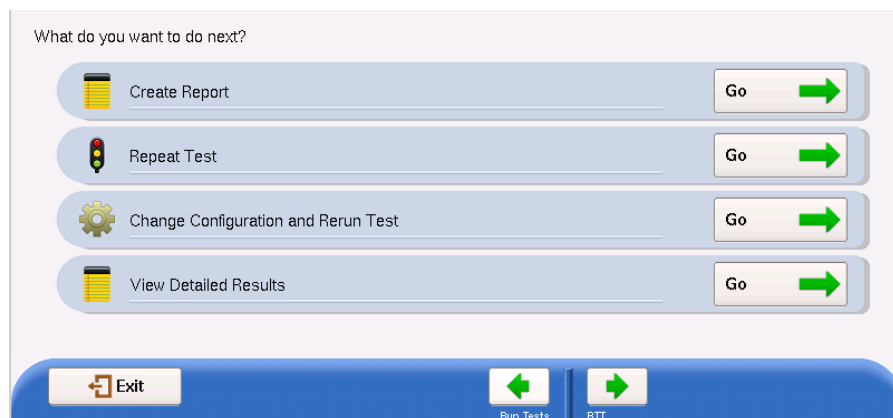
NOTE:

To switch between the test and the Setup panel on the user interface, click the **Go To** button at the top of the screen and then click the **Results** button in the dialog. This function is intended allow you to verify the settings. Note that the RFC2544 button is yellow to indicate it has been launched. You should not change the settings during a test, as you may get undesired results. To return to the test, click the RFC2544 button.

- 2 When the tests have completed, select the **Next** (the green arrow).

The Test Complete page appears.

Figure 32 Enhanced RFC 2544 or FC Post-test Window



Do one of the following:

- To create a report of the results of the test that just completed, select the **Go** arrow on the “Create Report” line. Go to [step 3](#).
- To repeat the test that just ran, select the **Go** arrow on the “Repeat Test” line. Go back to [“Running Enhanced RFC 2544 tests” on page 148](#).
- To reconfigure the test and then run it again, select the **Go** arrow on the “Change Configuration and Rerun Test” line. Go to [step 2](#) of [“Manually configuring all parameters” on page 145](#).
- To view detailed results of the performance achieved during the test, select the **Go** arrow on the “View Detailed Results” line.

The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

On the last page of the results select the right-pointing green arrow. Go to [step 3](#).

3 The report info screen will display.

This screen allows the user to enter information about the test environment which will be added to the report.

This information includes:

- Customer Name
- Technician ID
- Test Location
- Work Order
- Comments/Notes
- Custom Logo (from memory)



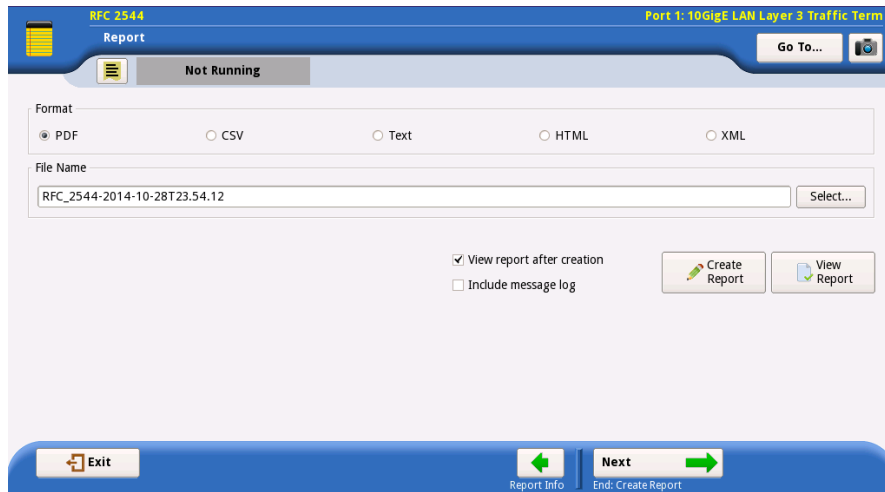
NOTE:

This screen is also associated with VIAVI’s Job Manager functionality, which enables you to run tests based on a documented test plan. You can also save multiple tests in one resulting report file.

4 After all the desired data is entered into the entry boxes, select **Next** (the green arrow).

5 The Report window appears.

Figure 33 RFC 2544 Report Window



Do the following:

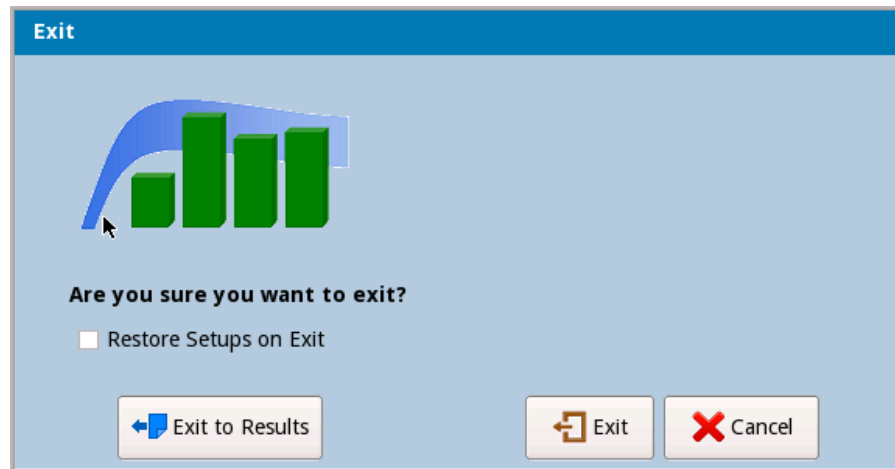
- a Select the format in which the report is to be saved by selecting the radio button in Format pane.
 - b Specify the filename of the report. To review the filenames of other, currently saved reports on the unit, select the Select button.
 - c You may view saved reports by selecting the **View Report** button.
 - d To show a copy of the current report after saving it, check the **View report after creation** checkbox. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.
 - e To include the message log with the report, select the Include Message log check box.
 - f When ready to save the report, select the **Create Report** button. After it has been saved (and viewed), select the right-pointing green arrow.
- 6 The post-report/results window appears.

All options available on this window are described in [step 2](#) with the exception of the “Exit RFC 2544 test”.

To exit the RFC 2544 test application, select the **Go** arrow after “Exit RFC 2544 test”.

7 The Exit window appears.

Figure 34 Enhanced RFC 2544 test exit page



Do one of the following:

- To exit to the base application, retaining all setups from the RFC2544 test, select the **Exit to Results** button.
- To restore the configuration setups to their default values when leaving the application, check the box **Restore Setups on Exit**. To completely exit the Enhanced RFC 2544 application, select **Exit**.
- To return to the previous window, select **Cancel**.

The Enhanced RFC 2544 test has been run.

About the Y.1564 SAMComplete test

This test is a multi-stream test based on ITU-T Y.1564 that performs a two-phase test. First, the test verifies whether each Ethernet service is properly configured. Second, multiple Ethernet service instances are verified simultaneously, each meeting its assigned Committed Information Rate (CIR). All services are transmitted at CIR and must pass all SLA parameters (FDV, FTD, RTD and Availability).

The following topics are discussed in this section:

- [“Initiating the SAMComplete test” on page 154](#)
- [“Configuring SAMComplete test settings” on page 155](#)
- [“Choosing SAMComplete tests” on page 160](#)
- [“Running SAMComplete tests” on page 160](#)

Initiating the SAMComplete test

SAMComplete functionality is standard on all units and all Ethernet line rates are supported. Although all applications do not include SAMComplete functionality, if your instrument is appropriately configured, you can use it to run the SAMComplete test.

There are two ways to initiate the SAMComplete test; both from the Select Test application tree.

- Select the base application and then initiate the SAMComplete test using the on-screen softkey.
- Select the SAMComplete implementation for the technology and interface you want to use.

The first option will be necessary if you have no configurations saved to load the parameters of the test to be run. Alternatively, if you are coming back to run a saved configuration (or modify an existing profile) you can select the direct initiation of SAM Complete, load the existing profile and start testing. For more information see [“Launching an automated test” on page 132](#).

To launch the SAMComplete test (from base application)

- 1 If you haven't already done so, use the Test Menu or Quick Launch screen to select the desired application for the circuit you are testing (see [“Launching an automated test” on page 132](#)), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.
- 2 Select the SAMComplete soft key on the right side of the interface.
- 3 Go to [“Configuring SAMComplete test settings” on page 155](#)

SAMComplete has been launched.

To Launch SAMComplete simultaneously with base application

- 1 From the Select Test application tree, select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed.
- 2 Select **Y.1564 SAMComplete** from the tree, then the specific test desired such as Layer 2 Traffic >Term.
- 3 Go to [“Configuring SAMComplete test settings” on page 155](#).

SAMComplete has been launched.



NOTE:

The Quick Launch window displays previously run and/or saved configurations of applications. Automated scripts launched simultaneously with base applications are fully identified with the script and base application. See *T-BERD/MTS/SC Getting Started Manual* for more information on the Quick Launch window.

Configuring SAMComplete test settings

From the configuration page, the settings can be configured manually, or if a profile has been previously configured and saved, the test settings can be loaded into SAMComplete.



NOTE:

QuickCheck is integrated into SAMComplete.

To configure test settings

To make changes to the existing settings, select the green arrow to the right of **Edit Previous Configuration**. Go to [step 2 on page 156](#).

To reset all settings to their default values and configure all options yourself, select the green arrow to the right of **Start a New Configuration**. Go to [step 2 on page 156](#).

To load configuration settings set from a previously saved file, select **Go To...** and proceed to **Load Profiles**.

- 1 The Profile selection window appears.

The filenames of the saved profiles will be listed on the left side of the window and all sections of the currently loaded profile will be listed on the right side of the screen.

Do the following:

- a Select a profile from the list whose configuration is to be loaded.



NOTE:

If you load a profile that was configured on another unit, and that profile specified including a logo in the test report, make sure that the .png, .jpg, or .jpeg is in the following folder on your unit:

`/disk/bert/images`

- b Check those sections, on the right side of the screen, that are to be loaded into the test. If no profile has yet been selected, the currently configured profile sections will be checked.

Any section not selected will not be configured into the test. Any parameter of the test (checked or not checked) may be reconfigured at a later point in the configuration process.

- c Select the **Load Profiles** button to load all checked sections into the test. After profile has successfully loaded select, **OK** and then select **Next** (the green arrow). Go to [“Choosing SAMComplete tests” on page 160](#).



TIPS:

1. Generally, selecting the **Next** button (right green arrow) on each page will advance to the next step you need to do, but if at any time, you need to return to the test configuration, skip to running tests, or review test results, select the **Go To...** button, and then select the step to which you need to return.
2. To save a view of the screen on the unit for future reference, use the camera icon to capture a screenshot.

- 2 The first Symmetry page appears.

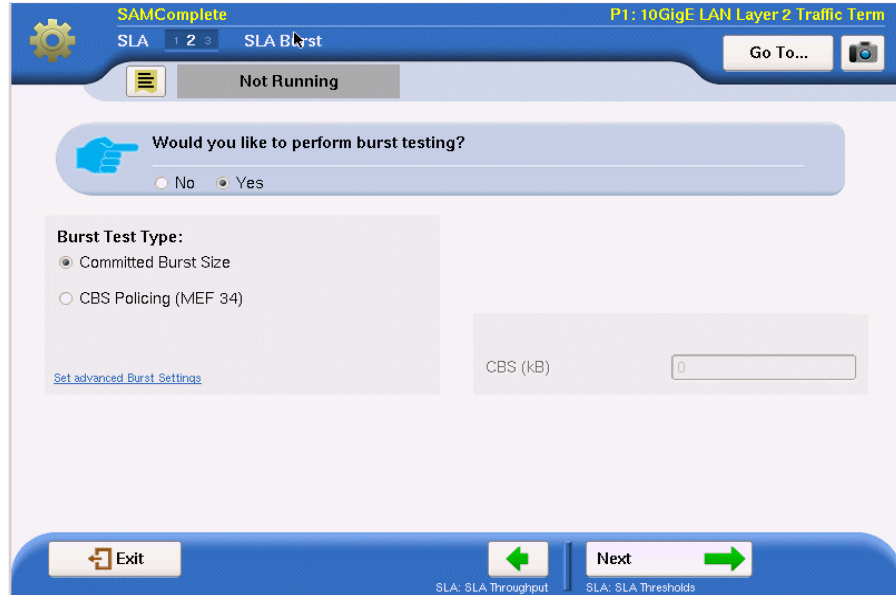
To configure a SAMComplete Test

- 1 Configure the Throughput type as **Symmetric**.
- 2 Configure the Measurements type as **Loop Back** and select **Next** (the green arrow).
- 3 The Local Network Settings page appears. Do the following:
 - a Select the **Service Name** for each of the services being configured. This specifies which service you are configuring.
 - b Select **Configure Triple Play**, if needed. The Triple Play properties screen appears. You can specify the properties for Voice, Data, HDTV and SDTV. Repeat for each of the services defined.
 - c Select the Layer for bit rate layer definition mode. When L2 is selected, the max value of the Load unit will remain in terms of L1. L2 utilization is affected by frame size and therefore a value may be selected that is greater than can actually be transmitted.
 - d Choose, from the drop-down list, which encapsulation is desired - **None**, **VLAN**, or **Q-in-Q**.
 - e For Layer 2 applications, select the frame size from the values in the drop-down box.
 - f To specify **Source** and **Destination MAC addresses**, **Loop Type** and **Auto-Incrementing Address** settings, select the **Advanced** link at the lower right side of the window.
 - g Select the **Next** (the green arrow).

- 4 The SLA Throughput page appears.
 - a Specify the SLA values. Depending upon the application selected, the SLA Threshold and Throughput can be specified for both the Local and Remote unit.
 - **CIR** – Committed Information Rate. The threshold used to indicate the maximum sustained throughput guaranteed by the SLA. If the CIR is 0, the CIR test is skipped. When multiple services are specified and the Enable Aggregate Mode checkbox is not selected, values entered into the **All** line are copied to each service.
 - **EIR** – Excess Information Rate. The threshold used to indicate the maximum sustained throughput allowed by the SLA by which a service can exceed the CIR. The throughput between CIR and EIR is not guaranteed. If the EIR is 0, the EIR test is skipped. When multiple services are specified and the Enable Aggregate Mode checkbox is not selected, values entered into the **All** line are copied to each service.
 - **Policing** – Selects that policing be applied to the test. All traffic greater than CIR + EIR is removed by the policier. (If the test shows frame loss, the test passes – it indicates the policier is doing its job. If there is no frame loss even with the overage percentage, the test fails.) When multiple services are specified, selecting the Policing checkbox on the All (or Total) line, selects Policing for all services.
 - **Max Load Display** - Calculated from the values of CIR and EIR and changes based upon policing selection, it is the maximum rate of traffic to be generated. (If policing is not selected, Max Load is CIR+EIR. If policing is selected, Max Load is CIR + 1.25xEIR, or when EIR is less than 20% of CIR, Max Load is 1.25xCIR + EIR).
 - **M** – Tolerance, or delta, in traffic rate which is allowed to be received above CIR+EIR before declaring a policing failure. For some applications, the desired **M** value is specified on the SLA Throughput page. For Multistream or Truespeed applications, **M** will be entered on a following page labeled “SLA Policing”. Specify the desired value for **M**.
 - b If it is desired to transmit the burst at a true 100% load, in those circuits that can handle the signal, select **Set Advanced Traffic Settings** and then check the **Allow True 100% traffic** checkbox. Select the left green arrow to return to SLA Throughput screen.
 - c Select the **Next** (the green arrow).

- The SLA Burst page appears.(If SLA Policing appears, see discussion of M above, in [step a](#)).

Figure 35 SAMComplete SLA Burst screen



Do the following:

- Specify whether burst testing will be performed by selecting the radio button next to **Yes** or **No**.
If **No** is selected, go to [step 6](#).
If **Yes** is selected, enter the CBS (in kB) where kB = 1000 bytes.
- Select whether to run the **Committed Burst Size** or the **CBS Policing** test by selecting the radio button next to either.
- To further refine the SLA Burst test, select the **Set Advanced Burst Setting** link.
 - If desired, select the **Ignore Pause frames** checkbox.
 - If CBS Policing was selected, specify the desired **+%** and **-%** tolerance to specify Pass values from expected.
 - Select the **BACK** button (left green arrow) to return to the SLA Burst screen.
- Select **Next** (the green arrow).

- 6 The SLA Performance page appears.
 - a Specify the desired Threshold values. Each service may have its own values.
 - **Frame Loss Ratio**– The maximum ratio allowed of frames lost to total frames.
 - **Frame Delay** – The maximum allowed average OWD delay/latency for all throughput values.
 - **Delay Variation** – The maximum allowed frame delay variation for all throughput values.
 - b Select **Next** (the green arrow).
- 7 The Test Controls page appears.
 - a Specify the Service Configuration and Service Performance settings.
 - **Number of steps below CIR** – The number of steps, in information rate, needed to reach the CIR.

The corresponding number of Step Values % CIR appear. The default values will be equal parts, based on the number of steps (for example, if 3 steps are used, each will be 25%). The values can be changed, if required.
 - **Step Duration** – The duration, in seconds, that traffic is generated for each step.
 - **Test Duration** – The duration, in minutes, that traffic is generated before the service performance test completes.
 - b To further refine the Test Controls select the **Advanced** button.

% CIR – These will be automatically populated with the equal part values calculated from the Number of Steps below CIR parameter but can be changed to any value between 0 and 100.
 - c Select the **right green arrow**.
- 8 The Save Profiles window appears.

Do one of the following:

 - a If no Profile is to be saved at this time, select the **right-facing green arrow** at the bottom of the window. Go to [step 9](#).
 - b If it is desired that the configuration be saved to memory (disk or USB), specify the filename. To save somewhere other than the default location, press the **Select** button after the filename to define the directory where it is to be stored.
 - c If it is desired that subsequent users be restricted from being able to modify this profile, check the box **Save as read-only**.
 - d To save the file to memory, select the **Save Profiles** button. Then select the **OK** button, then select the **right-facing green arrow**.
- 9 The Run/Edit window appears.

Do one of the following:

- To return to the beginning and modify the current configuration, select the **Go** arrow after “Change Configuration”. Go to [step 2 of “To configure test settings” on page 155](#).
- To load a previously saved set of configuration parameters, select the **Go** arrow after “Load Configuration from a Profile”. Go to [step 1 of “To configure test settings” on page 155](#).
- To run the test, as configured, select the **Go** arrow after “Select and Run Tests”. Go to [“Choosing SAMComplete tests” on page 160](#)

SAMComplete has been configured.

Choosing SAMComplete tests

After specifying test settings, you must choose whether to run one or both of the tests: Service Configuration or Service Performance.

To choose the tests

- 1 On the Select Y.1564 Tests page, select **Enable** if you wish to run the Service Configuration and/or Service Performance tests.
- 2 If you wish to **include the optional throughput measurement** in the test, check the box to enable the test, and then specify the **Max** throughput allowed.
- 3 Select **Next** (the green arrow).
The QuickCheck page appears. Go to [“Running SAMComplete tests” on page 160](#).

Running SAMComplete tests

After choosing the tests, you are ready to run the test.

To run tests

- 1 From the QuickCheck page, do one of the following:
 - When you configured for layer 2 loopback test, you can select **VLAN Discovery**. This mode will transmit a burst of VLAN frames to automatically discover test instruments on the network.
 - When configured for a loopback test, you can select **Maximum Frame Search**. When selected after a successful loop detection, bursts of various frame sizes will be transmitted in order to determine the largest frame size you network can support.
 - Select the **Start** button.

The QuickCheck test, using the source and destination data entered, verifies that the connections detailed in the test setup are functioning as needed for the proper operation of the test. As QuickCheck is completing its analysis of the circuit, graphics along the top of the page provide a visual indication of the circuit structure and its suitability for the selected test.

If a remote device is necessary, QuickCheck first checks to see if a connection to the remote device has been established. If it has not, a message is displayed indicating the connection must first be established.

For loopback tests, QuickCheck tests the Local port for proper operation and then checks for loopback in a remote device. If no remote active loop is detected, it then verifies whether a hard loop is in place.

After QuickCheck completes, select **Next** (the green arrow). Go to [step 2](#).

- To skip the QuickCheck test, select the **Skip QuickCheck** button at the bottom of the window.

2 The Run Y.1564 Tests page appears.

There is a display bar for each service under Service Configuration and also for each test verdict under Service Performance. These indicate the status of each test to be run. Please refer to the Test Status Key at the bottom of the page to interpret these display bars.

Do the following:

- a** If you would like the test to continue when a failure occurs, clear the **Stop on failure** box.

- b** Select the **Start** button.

The test begins.

As the tests are run, the status display bars will show the results of each test. In each case, you may view detailed results of that test by selecting the “magnifying glass” icon when it appears on the status bar.

While the tests are running, the status panel near the top of the screen displays a blue progress bar and indicates the estimated time remaining to complete the testing.

After the test finishes, the pass/fail results appear (green check mark or red X) on each of the tests. The status panel near the top of the screen displays an overall OK (PASS) or FAIL result

- c** Once the testing is completed, select **Next** (the green arrow).

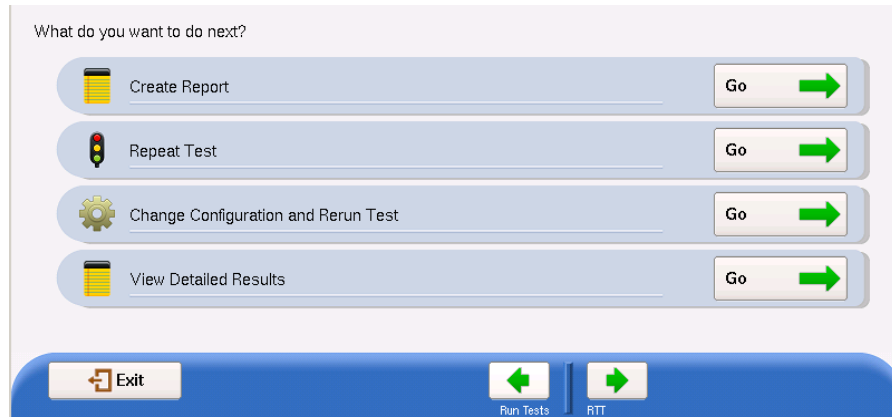


NOTE:

To switch between the test and the Setup panel on the user interface, click the **Go To** button at the top of the screen and then click the **Results** button in the dialog. This function is intended allow you to verify the settings. Note that the SAMComplete button is yellow to indicate it has been launched. You should not change the settings during a test, as you may get undesired results. To return to the test, click the SAMComplete button.

3 The Test Complete page appears.

Figure 36 SAMComplete Post-test Window



Do one of the following:

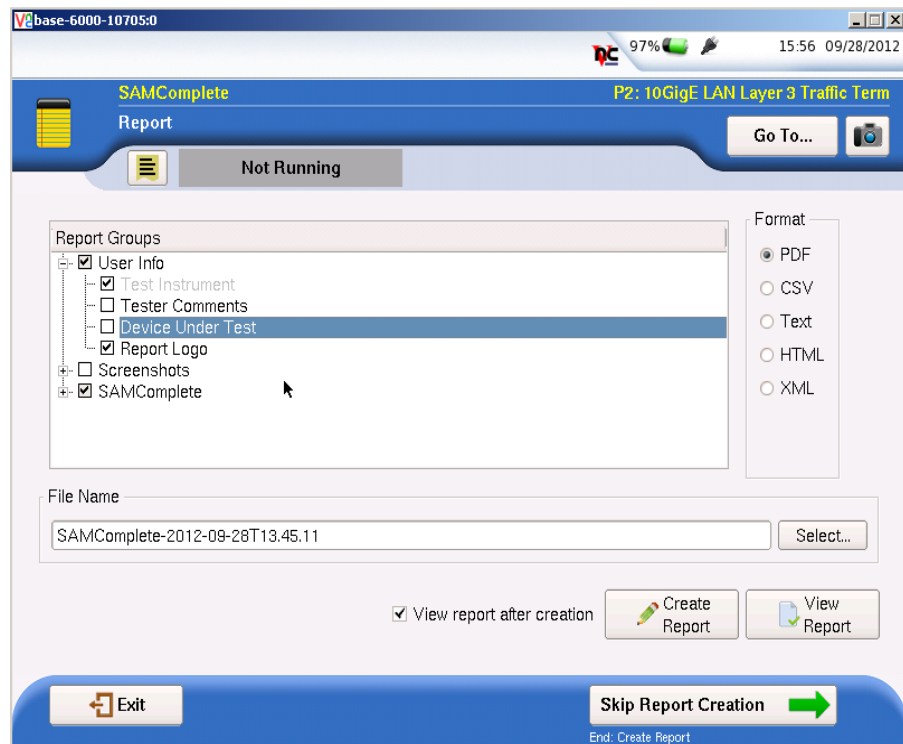
- To create a report of the results of the test that just completed, select the **Go** arrow on the “Create Report” line. Go to [step 4](#).
- To repeat the test that just ran, select the **Go** arrow on the “Repeat Test” line. Go back to [“Choosing SAMComplete tests” on page 160](#).
- To reconfigure the test and then run it again, select the **Go** arrow on the “Change Configuration and Rerun Test” line. Go to [step 2 of “Configuring SAMComplete test settings” on page 155](#).
- To view detailed results of the performance achieved during the test, select the **Go** arrow on the “View Detailed Results” line.

The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

On the last page of the results select the right-pointing green arrow. Go to [step 5](#).

4 The Report window appears.

Figure 37 SAMComplete Report Window



Do the following:

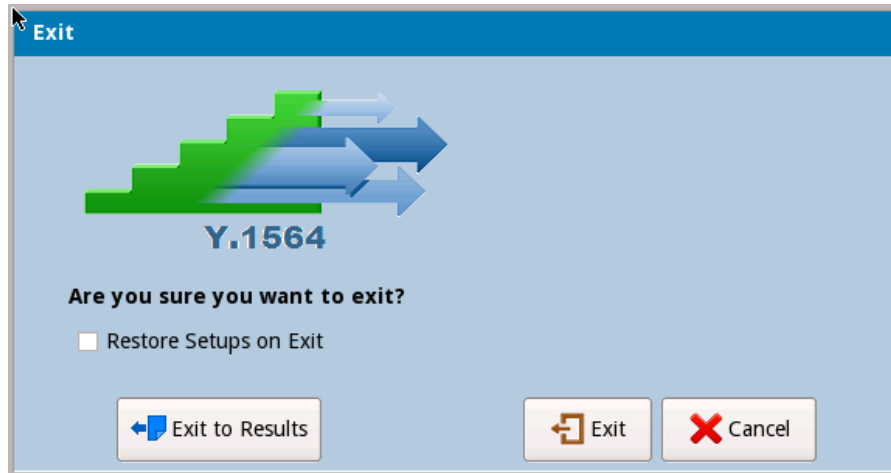
- a Select the items to be included in the report by putting a checkmark in front of the item. Entire groups may be selected or individual items within a group. To expand the group listing to see the individual items, select the “+” in front of the group name.
 - b Select the format in which the report is to be saved by selecting the radio button under Format.
 - c Specify the filename of the report.
 - d You may view saved reports by selecting the **View Report** button.
 - e To show a copy of the current report after saving it, check the “View report after creation” checkbox. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.
 - f When ready to save the report, select the Create Report button. After it has been saved (and viewed), select the right-pointing green arrow.
- 5 The post-report/results window appears.

All options available on this window are described in [step 3](#) with the exception of the “Exit Y.1564 test”.

To exit the SAMComplete application, select the **Go** arrow after “Exit Y.1564 test”.

6 The Exit window appears.

Figure 38 SAMComplete Exit page



Do one of the following:

- To exit to the base application, retaining all setups from the SamComplete test, select the **Exit to Results** button.
- To restore the configuration setups to their default values when leaving the application, check the box **Restore Setups on Exit**. To completely exit the SAMComplete application, select **Exit**.
- To return to the previous window, select **Cancel**.

The SAMComplete test has been run.

5G NR Discovery

You can use 5G NR Discovery to discover key information from a 5G NR device. To begin, select the **5g NR Discovery** option on the appropriate Ethernet interface for your 5G NR device. The supported interfaces are:

- 10 GigE LAN
- 25 GigE

Optionally, select to **Save capture file** for the discovery session, and then press the **Run Test** button. The **5G NR Discovery** test begins and performs the following:

- Initializes and checks the Ethernet link
- Collects and analyzes transmissions from the radio and reports key radio configuration information, including:
 - MAC Address(es)
 - VLAN ID(s)
 - IPv6 Address(es)
 - Network protocols in use

- Attempts communication with the radio on each discovered VLAN and IP address pair.

At the conclusion of the test an option to create a test report is available.

Automated VLAN tests

If your instrument is configured and optioned to do so, you can use it to run the automated VLAN test. This test is used to test a range of VLANs by transmitting and looping back frames for each VLAN in the range for a user-specified test period, and then comparing the number of frames transmitted to the number received. Pass criteria can be specified as No frames lost or Some frames received as meet your needs.

To test a range of VLANs

- 1 Establish a connection to the network using one of the Ethernet test interfaces. *Do not use the management RJ-45 connector provided on the base unit.*
- 2 If you haven't already done so, use the Test Menu or Quick Launch screen to select the Layer 2 Traffic Terminate application for the circuit you are testing (see [“Launching an automated test” on page 132](#)), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.
- 3 Specify the settings required to initialize the link (see [“Specifying interface settings” on page 23](#)), and to establish a connection to the network (see [“Layer 2 testing” on page 23](#)).
- 4 To Launch the VLAN scan, select the Toolkit softkey on the lower right of the Results screen. Then select the **VLAN Scan** button. The VLAN Scan Loading intermediate screen appears followed by the VLAN Scan window.
- 5 Enter the **Duration per ID(s)**. This specifies the length of time (in seconds) for which each VLAN ID will be searched.
- 6 Enter the **Number of ranges** (the number of ranges of VLAN ID's you want to be searched).
- 7 Enter **VLAN ID Min** (one for each Range). The minimum value in the range to be searched.
- 8 Enter **VLAN ID Max** (one for each Range). The maximum value in the range to be searched.
- 9 To specify the **Frame size**, **Bandwidth** or the **Pass Criteria**, select the **Advanced VLAN Scan Settings** link on the lower right corner. Select **Back** when complete to return to VLAN Scan window.
- 10 To run the test, select **Start Test**.
- 11 A progress bar, and the remaining time to test completion, will appear at the top of the screen. To cancel the test at any time press the **Abort Test** button.
- 12 When the test is complete, a dialog box appears asking if you would like to save a test report. For details, see [“Saving automated test report data” on page 166](#).

The VLAN test is complete. The report will provide the total number of VLANs tested, the total number of successes, and the total number of failures. It can also optionally include the test progress log that appeared as you were running the test.

Saving automated test report data

When each automated test is complete, a dialog box appears asking if you would like to save a test report. You can optionally append the progress log (the text that appeared while you were running the test) to the end of the report.

To save automated test report data

- 1 When the report dialog box appears, if you would like to append a progress log to the end of the report, select the option on the dialog box, then reply with **Yes** or **No**. If you select Yes, specify the following:
 - The customer's name.
 - Your name.
 - Work Order No.
 - The test location.
 - Any additional comments you might have concerning the test.Select the right-facing green arrow. The Report screen appears.
- 2 This screen allows two actions - Generating a report of the most current results or viewing a previously saved report. To generate a new report:
 - a Select the radio button for the format desired.
 - b Change the default file name, if desired, or click on the Select button to open the report file management screen to find existing file names. To overwrite an existing file, select it from the list and then click the Select button to return to the Report screen.
 - c To display the report on the screen after it is generated, check the View report after creation checkbox.
 - d To include the message log in the generated report, check the Include message log checkbox.
 - e Select the Create Report button.
- 3 To View previously saved report;
 - a Select the create Report Button. The View Report screen appears.
 - b from this screen you can see the list of currently saved reports in available locations. To view an existing report, select its filename then, click on View. the report will display on the screen.
 - c When finished with the report, select the Exit button to return to the Report screen.
- 4 When completed with the Reports, select the left-facing green button to re-specify your report or the Exit button.

The Exit screen appears.

- 5 To restore the setups to their previous settings, check the Restore Setups on Exit checkbox.
- 6 To return to the base application, select the Exit button.
- 7 To return to the Report screen, select the Cancel button.
- 8 Select **Close** to close the dialog box and return to the Main screen.

The report is saved.

Test Results

This section describes the categories and test results that are available when performing Ethernet tests.

Topics include the following:

- [“About test results” on page 170](#)
- [“Summary Status results” on page 170](#)
- [“Ethernet results” on page 171](#)
- [“RS-FEC results” on page 186](#)
- [“RS-FEC Per Lane results” on page 186](#)
- [“Histogram results” on page 187](#)
- [“Event Log results” on page 188](#)
- [“Time test results” on page 188](#)

About test results

After you connect the instrument to the circuit and press the START/STOP button, results for the configured test accumulate and appear in the Result Windows in the center of the screen. The result groups and categories available depend on their applicability to the test you configured.

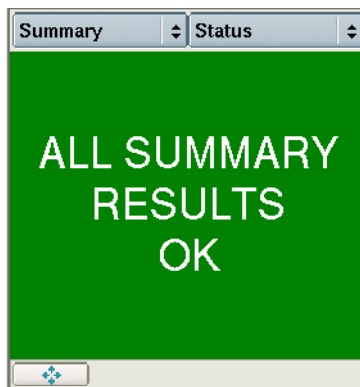
A number of enhancements have been made to the test result layout; for details, see [“Step 5: Viewing test results” on page 9](#).

The following sections describe the test results for each of the categories.

Summary Status results

When running most applications, the Summary Status category displays a large “ALL SUMMARY RESULTS OK” message on a green background if no errors or alarms have been detected (see [Figure 39](#)).

Figure 39 ALL SUMMARY RESULTS OK message



If errors or alarms have been detected, the background is red and the error results are displayed.

This allows the user to immediately view errored results without searching through each category. The errored results are listed by group and category. To see all results for the group/category, select the arrow key to the right of the group/category name. You can also collapse or expand the results by selecting the box to the left of the name.

If, for example, OoS (out of sequence) or Layer 3 Packets conditions occur, and *no other errors occurred*, the background is yellow, indicating you should research each condition displayed. In some instances, the conditions constitute errors; in other instances, the conditions are expected and should not be interpreted as errors.

Ethernet results

Test results such as link counts, statistics, error statistics, and BER results are available when performing Ethernet testing.



FCS Errored Acterna Test Packets:

If you are running a Layer 2 traffic application using an Acterna Test Packet (ATP) payload, received FCS errored Acterna frames will not impact link counts, link statistics, or error statistics.

Categories discussed in this section include the following:

- [“LEDs” on page 171](#)
- [“SLA/KPI” on page 174](#)
- [“Interface results” on page 174](#)
- [“L2 Link Stats results” on page 176](#)
- [“L2 Link Counts results” on page 178](#)
- [“L2 Filter Stats results” on page 179](#)
- [“L2 Filter Counts results” on page 180](#)
- [“L3 Link Stats results” on page 180](#)
- [“L3 Link Counts results” on page 181](#)
- [“BERT Stats results” on page 182](#)
- [“PCS Stats” on page 183](#)
- [“Ethernet Per Lane results” on page 184](#)
- [“Error Stats results” on page 185](#)
- [“RS-FEC results” on page 186](#)

LEDs

[Table 12](#) describes the LEDs provided during Ethernet testing. Only the LEDs that are applicable for your test appear in the LED panel.

If the instrument loses any of the LED events, the green Status LED extinguishes, and the red Alarm LED in the history column illuminates indicating an error condition has occurred.

Table 12 describes the LEDs.

Table 12 Ethernet LEDs

LED	Indicates
ATP Detect	Green – A frame with an Acterna payload has been detected. Yellow (History) – An Acterna payload was detected, and then not present for ≥ 1 second.
VLAN Frame Detect	Green – Valid frames with VLAN have been detected. Red – Frames with VLAN were detected, and then not present for ≥ 1 second.
Frame Detect	Green – Valid frames have been detected. Yellow – Frames were detected, and then not present for ≥ 1 second.
HI-BER	Red (Status) – High Bit Error Rate alarm is currently being detected Red (History) – High Bit Error Rate alarm was detected at some point since the last restart of the test.
Link Active	Green – Link is established with the instrument's link partner. Red – A link to the instrument's link partner has been lost since the last test restart.
Local Fault Detect	Red (Status) – Local faults are currently being detected. Red (History) – A local fault occurred since the last test restart.
Loss of Align.	Red (Status) – Loss of alignment has been detected. Red (History) – A loss of alignment occurred since the last test restart.
Marker Lock	Green – (Alignment) Marker Lock has been achieved across all lanes. Red – Alignment Marker Lock was lost on some lane since the last test restart.

Table 12 Ethernet LEDs (Continued)

LED	Indicates
Remote Fault Detect	<p>Red</p> <ul style="list-style-type: none"> – Remote faults are currently being detected. <p>Red</p> <ul style="list-style-type: none"> – A remote fault has occurred since the last test restart.
RS-FEC LOA	<p>Red</p> <ul style="list-style-type: none"> – Loss of Alignment (LOA) has occurred between lanes. <p>Red</p> <ul style="list-style-type: none"> – Loss of Alignment (LOA) has occurred between lanes at some point since the last restart of the test.
RS-FEC LOAMPS	<p>Red</p> <ul style="list-style-type: none"> – Loss of Alignment Marker Payload Sequence (LOAMPS) has occurred. <p>Red</p> <ul style="list-style-type: none"> – Loss of Alignment Marker Lock (LOAML) has occurred between lanes at some point since the last restart of the test.
RS-FEC HI SER	<p>Red</p> <ul style="list-style-type: none"> – RS-FEC Hi Symbol Error Rate has occurred. <p>Red</p> <ul style="list-style-type: none"> – Loss of Block Lock (LOBL) has occurred between lanes at some point since the last restart of the test.
Signal Present	<p>Green</p> <ul style="list-style-type: none"> – Light and bit transitions are detected <p>Red</p> <ul style="list-style-type: none"> – Light and bit transitions were lost at some point since the last restart of the test.
Summary	<p>Green</p> <ul style="list-style-type: none"> – N/A <p>Red</p> <ul style="list-style-type: none"> – An error has been recorded by the instrument, as shown in a red Summary Status window.
SVLAN Frame Detect	<p>Green</p> <ul style="list-style-type: none"> – SVLAN tagged Ethernet frames have been detected. <p>Red</p> <ul style="list-style-type: none"> – SVLAN tagged Ethernet frames were detected, and then not present for ≥ 1 second.
Sync Acquired	<p>Green</p> <ul style="list-style-type: none"> – Synchronization is established. <p>Red</p> <ul style="list-style-type: none"> – Synchronization has been lost since the last test restart.

Table 12 Ethernet LEDs (Continued)

LED	Indicates
VLAN Frame Detect	<p>Green</p> <ul style="list-style-type: none"> – Valid frames with VLAN have been detected. <p>Red</p> <ul style="list-style-type: none"> – Frames with VLAN were detected, and then not present for >= 1 second.

SLA/KPI

The Summary SLA/KPI results provide the results relevant to the Service Level Agreement (SLA) and Key Performance Indicators (KPI).

Interface results

Table 13 describes the Interface/Signal results.

Table 13 Interface/Signal results

Test Result	Description
Link Loss Seconds	Number of seconds during which the link was down (lost).
Local Fault Seconds	Displays the number of test seconds during which a local fault occurred, indicating that the unit could not detect a received signal.
Optical Rx Level (dBm)	Displays the receive level in dBm when testing optical interfaces using average power consumption (sum of all lanes).
Optical Rx Overload	Displays ON if the received optical power level is greater than the receiver shutdown specification.
Remote Fault Seconds	Displays the number of test seconds during which the instrument transmits a remote fault indication in response to the receipt of a remote fault indication from its link partner.
Rx Frequency (Hz)	Frequency of the clock recovered from the received signal, expressed in Hz.
Rx Freq Deviation (ppm)	Current received frequency deviation. Displayed in PPM.
Rx Freq Max Deviation (ppm)	Maximum received frequency deviation.
Signal Loss Seconds	Number of seconds during which a signal was not present.
Sync Loss Seconds	Number of seconds during which a synchronization was not present.
Tx Clock Source	Shows the source of the transmit timing standard
Tx Frequency (Hz)	Current transmitter clock frequency, expressed in Hz.
Tx Freq Deviation (ppm)	Current transmitted frequency deviation. Displayed in PPM.
Tx Freq Max Deviation (ppm)	Maximum transmitted frequency deviation.

Table 14 describes the Interface/Lambda results.

Table 14 Interface/Lambda Results

Test Result	Description
Freq Measurement Reference	The reference against which PPM offsets are measured.
Optical Rx Level (dBm)	Displays the receive level in dBm.
QSFP/OSFP Laser Bias Current (mA)	The total current applied to lasers across lanes.
QSFP/OSFP Laser Bias Current Lambda (mA)	Displays the individual current levels applied to each laser.
QSFP/OSFP Rx Level per Lambda (dbm)	Displays the individual power for each lane and total optical power received in all lanes.
QSFP/OSFP Tx Level per Lambda (dBm)	Displays the individual power for each lane and total optical power transmitted in all lanes.
QSFP/OSFP Per Lane Signal Present	Verifies the presence of an active signal in each lane. Designation of Not Ready indicates presence of device in unit in powered down condition.
QSFP/OSFP State	The start of the QSFP/OSFP pluggable optics
QSFP/OSFP Supply Voltage (V)	The reference against which PPM offsets are measured.

Table 15 describes the Interface/Pluggable results.

Table 15 Interface/Pluggable results

Test Result	Description
QSFP/OSFP Module State	Displays the QSFP/OSFP Module state.
QSFP/OSFP Laser Bias Current (mA)	Displays the QSFP/OSFP Laser Bias current.
QSFP/OSFP Supply Voltage (V)	Displays the QSFP/OSFP Supply voltage.
QSFP/OSFP Module Current (A)	Displays the QSFP/OSFP Module current.
QSFP/OSFP Module Power (W)	Displays the QSFP/OSFP Module power.

Table 16 describes the Interface/CMIS Host-Media Apps results

Table 16 Interface/CMIS Host-Media Apps results

Test Result	Description
Hex Code (hex)	Displays the hex code of the app.
Host App name	Displays the name of the app.
Media Code (hex)	Displays the code of the media app.

Table 16 Interface/CMIS Host-Media Apps results

Test Result	Description
Media App Name	Displays the name of the media app.

L2 Link Stats results

Table 17 describes the L2 Link Stats results such as the average frame rate, peak frame rate, and the maximum, minimum, and average round trip delay measurements. Only results that are applicable to the test appear in the category.

Table 17 L2 Link Stats results

Test Result	Description
ATP Total Util Cur%	Current utilization receiving Acterna frames.
ATP Frame Rate Cur	Current frame rate in fps receiving Acterna frames.
ATP RX Mbps, Cur L1	Current Acterna frame bandwidth measured at Layer 1.
ATP RX Mbps, Cur L2	Current Acterna frame bandwidth measured at Layer 2.
Current Util.%	The current bandwidth utilized by received Broadcast, Unicast, or Multi-cast traffic expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time.
Delay (μ s), Round Trip	An Acterna payload is required to measure round trip delay. If a unit is in loopback mode, or if the far end unit is not looped back, invalid results appear because the unit is not originating the traffic. Current – The current round trip delay calculated in microseconds. Maximum – The maximum round trip delay calculated in microseconds. Minimum – The minimum round trip delay calculated in microseconds.
Frame Rate	Current – The current rate of received frames taken over the prior second of test time. Average – The average rate is calculated over the time period elapsed since the last test restart. Minimum – The minimum rate is taken over a one second period. Peak – The maximum rate is taken over a one second period since frame detection. All rates are expressed in <i>frames per second</i> .

Table 17 L2 Link Stats results (Continued)

Test Result	Description
Frame Size	The average, maximum, and minimum size of frames received since frame detection.
Packet Jitter (μ s)	<p>Instantaneous</p> <ul style="list-style-type: none"> – The current Packet Jitter measured over the prior second of test time. <p>Average</p> <ul style="list-style-type: none"> – The smoothed average value of the packet delay variation since the last test restart (per RFC 1889), calculated in microseconds. <p>Max Average</p> <ul style="list-style-type: none"> – The maximum Packet Jitter, Avg (μs) measured since the last test restart, calculated in microseconds. <p>Peak</p> <ul style="list-style-type: none"> – The highest packet delay variation measured since the last test restart, calculated in microseconds.
Peak Interframe Gap (μ s)	The Peak IFG time (maximum inter-frame gap) when service switches to a protect line calculated in microseconds. For best results, specifically when measuring a service disruption, use Couple Mode (Tx and Rx).
Rx Mbps, Cur L1	The current bandwidth utilized by the received traffic expressed in L1 megabits per second, including the preamble, start of frame delimiter, and minimum inter-frame gap.
Rx Mbps L1, Average	The average L1 rate of received frames calculated since the last test restart.
Rx Mbps L1, Minimum	The minimum current L1 rate of received frames calculated since the last test restart.
Rx Mbps L1, Maximum	The maximum current L1 rate of received frames calculated since the last test restart.
Rx Mbps, Cur L2	The current data rate of received frames calculated over the prior second of test time. Data rate is the frame bandwidth, excluding the preamble, start of frame delimiter, and minimum inter-frame gap.
Rx Mbps L2, Average	The average data rate of received frames calculated since the last test restart
Rx Mbps L2, Minimum	The minimum current data rate of received frames calculated since the last test restart.
Rx Mbps L2, Maximum	The maximum current data rate of received frames calculated since the last test restart.
SVLANs	Displays the SVLAN ID, priority, and DEI of stacked VLANs.
SVLAN DEI	Displays the DEI of the last received tagged frame.
SVLAN ID	Displays the SVLAN ID of the last received tagged frame.
SVLAN PRI	Displays the SVLAN priority of the last received tagged frame.

Table 17 L2 Link Stats results (Continued)

Test Result	Description
Total Util %	<p>Average</p> <ul style="list-style-type: none"> – The average bandwidth utilized by the received traffic, expressed as a percentage of the line rate of available bandwidth calculated over the time period since the last test restart. <p>Current</p> <ul style="list-style-type: none"> – The current bandwidth utilized by the received traffic expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time. <p>Minimum</p> <ul style="list-style-type: none"> – The minimum bandwidth utilized by the received traffic since the last test restart expressed as a percentage of the line rate of available bandwidth. <p>Peak</p> <ul style="list-style-type: none"> – The peak bandwidth utilized by the received traffic since the last test restart expressed as a percentage of the line rate of available bandwidth.
Tx Mbps, Cur L1	The current bandwidth utilized by the transmitted traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Tx Mbps, Cur L2	The current data rate of transmitted frames calculated over the prior second of test time. Data rate is the frame bandwidth, excluding the preamble, start of frame delimiter, and minimum inter-frame gap.
VLAN ID	Displays the VLAN ID of the last received tagged frame.
VLAN User Priority	Displays the VLAN priority of the last received tagged frame.

L2 Link Counts results

[Table 18](#) describes the L2 Link Counts results, such as the number of received frames, number of transmitted frames, and number of unicast, multicast, or broadcast frames. The Received Frames result includes errored frames; all other results count valid frames only.

Table 18 L2 Link Counts results

Test Result	Description
Jumbo Frames	<p>Jumbo/Oversized frames are counted in this category. This includes count of received Ethernet frames with a length greater than:</p> <ul style="list-style-type: none"> 1518 bytes (non-tagged frames) 1522 bytes (VLAN tagged frames) 1526 bytes (Q-in-Q encapsulated frames)
1024 - < Jumbo Frames	A count of received Ethernet frames between 1024 bytes and less than Jumbo frames

Table 18 L2 Link Counts results (Continued)

Test Result	Description
128-255 Byte Frames	A count of received Ethernet frames with lengths between 128 and 255 bytes, inclusive.
256-511 Byte Frames	A count of received Ethernet frames with lengths between 256 and 511 bytes, inclusive.
512-1023 Byte Frames	A count of received Ethernet frames with lengths between 512 and 1023 bytes, inclusive.
64 Byte Frames	A count of received Ethernet frames with a length of 64 bytes.
65-127 Byte Frames	A count of received Ethernet frames with lengths between 65 and 127 bytes, inclusive.
Broadcast Frames	The number of Ethernet broadcast frames received since the last test restart.
Multicast Frames	The number of Ethernet multicast frames received since the last test restart.
Received Frames	A count of frames received since the last test restart, including errored frames.
Rx Acterna Frames	A count of received Acterna frames, including errored frames.
Rx Frame Bytes	A count of the total number of frame bytes received since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. <ul style="list-style-type: none"> – The count does not include the preamble or start of frame delimiter. – The count does include errored frames.
Rx Q-in-Q Frames	A count of received QinQ frames since the test was started, including errored frames.
Rx Stacked VLAN Frames	A count of received stacked VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
Span Tree Frames	A count of received 802.1d spanning tree frames since frame detection after the last test start or restart.
Transmitted Frames	A count of transmitted frames since the last test restart.
Tx Acterna Frames	A count of transmitted Acterna frames since the last test restart.
Tx Frame Bytes	A count of the total number of frame bytes transmitted since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. The count does not include the preamble.
Unicast Frames	The number of Ethernet unicast frames received since the last test restart.

L2 Filter Stats results

The L2 Filter Stat results provide a subset of the Link Stats Results to which the filters in the Filter tab under Settings have been applied.

L2 Filter Counts results

The L2 Filter Counts results provide a subset of the Link Count results to which the filters in the Filter tab under settings have been applied.

L3 Link Stats results

Table 19 describes the L3 Link Stats results, such as the average packet rate, peak packet rate, and the maximum, minimum, and average round trip delay measurements.

Table 19 L3 Link Stats results

Test Result	Description
Packet Rate	<p>Average</p> <ul style="list-style-type: none"> – The average rate of received packets, calculated over the time period elapsed since the last test restart. <p>Current</p> <ul style="list-style-type: none"> – The current rate of received packets. This measurement is an average taken over the prior second of test time. <p>Minimum</p> <ul style="list-style-type: none"> – The minimum rate of received packets over a one second period. <p>Peak</p> <ul style="list-style-type: none"> – The maximum rate of received packets over a one second period. <p>The packet rate is expressed in packets per second.</p>
Packet Size	<p>Average</p> <ul style="list-style-type: none"> – The average size of packets received since IP packet detection. <p>Minimum</p> <ul style="list-style-type: none"> – The minimum size of packets received since IP packet detection. <p>Maximum</p> <ul style="list-style-type: none"> – The maximum size of packets received since IP packet detection.
Rx Mbps, Cur L3	<p>The current bandwidth utilized by the received IP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.</p>

Table 19 L3 Link Stats results (Continued)

Test Result	Description
Total Util %	<p>Average</p> <ul style="list-style-type: none"> – The average bandwidth utilized by the received IP traffic. This measurement is an average taken over the prior second of test time. <p>Current</p> <ul style="list-style-type: none"> – The current bandwidth utilized by the received IP traffic. <p>Minimum</p> <ul style="list-style-type: none"> – The minimum bandwidth utilized by the received IP traffic since the last test restart. <p>Peak</p> <ul style="list-style-type: none"> – The peak bandwidth utilized by the received IP traffic since the last test restart. <p>Bandwidth utilization is expressed as a percentage of the line rate of available bandwidth.</p> <p>NOTE: The bandwidth utilization calculations are made on per-second boundaries and may happen in the middle of a large frame, causing the utilization to be reduced.</p>
Tx Mbps, Cur L3	The current bandwidth utilized by the transmitted IP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.

L3 Link Counts results

[Table 20](#) describes each of the L3 Link Counts results such as the number of received packets, number of transmitted packets, and number of unicast, multicast, or broadcast packets. The Received Packets result includes errored packets; all other results count valid packets only.

Table 20 L3 Link Counts results

Test Result	Description
Received Packets	A count of IP packets received since the last test restart, including errored packets.
Transmitted Packets	A count of IP packets transmitted since the last test restart. This result does not appear when testing in Monitor mode.
Unicast Packets	The number of Ethernet unicast IP packets received since the last test restart.
Multicast Packets	The number of multicast IP packets received since the last test restart.
Broadcast Packets	The number of Ethernet broadcast IP packets received since the last test restart.
L3 Filter Stats Results	A subset of the Link Stats results to which the filters in the Filter tab, under Settings, have been applied.

Table 20 L3 Link Counts results (Continued)

Test Result	Description
L3 Filter Count Results	A subset of the Link Count results to which the filters in the Filter tab, under Settings, have been applied.

L3/IP Config Status results

[Table 21](#) describes the L3 Config Status or IP Config Status results associated with the assignment of static IP addresses, or the assignment of IP addresses by a DHCP server.

Table 21 L3/IP Config Status results

Test Result	Description
Source IP Address	Displays the static Source IP setting.
IP Gateway	Displays the gateway address assigned for CPE (WAN) router.
IP Subnet Mask	Displays the Subnet mask assigned for the currently selected port.
Destination IP Address	Displays the destination IP address as defined for the currently selected port.
Destination MAC Address	Displays the hardware (MAC) address of either the gateway or the destination host as resolved by ARP for the currently selected port.

BERT Stats results

[Table 22](#) describes the L2 BERT Stats results typically associated with the transmission of BERT patterns on a Layer 2 (switched) network. In some instances, the instrument may detect BERT patterns while transmitting an Acterna payload (for example, if a device on the far end of the link is transmitting an all ones BERT pattern).

To view the L2 BERT Stats results while BER testing, transmit traffic with a BERT pattern in the payload over a Layer 2 network, and then set a result category to L2 BERT Stats.

Table 22 L2 BERT Stats results

Test Result	Description
Bit Error Rate	The ratio of pattern bit errors to received pattern bits since initially acquiring frame synchronization. NOTE: This ratio is determined using only the bits in the payload of the frame.
Bit Errored Seconds	The number of seconds during which one or more pattern bit errors occurred since initial frame synchronization.

Table 22 L2 BERT Stats results (Continued)

Test Result	Description
Bit Errors	A count of the number of received bits in a recognized pattern that do not match the expected value since initially acquiring frame synchronization.
Bit Error-Free Seconds	Number of error-free seconds during which error analysis has been performed since initial pattern synchronization.
Bit Error-Free Seconds,%	Number of error-free seconds divided by the number of seconds during which error analysis has been performed since initial pattern synchronization, expressed as a percentage.
Pattern Losses	Count of the number of times pattern synchronization was lost since initially acquiring pattern synchronization.
Pattern Loss Seconds	Count of the number of seconds during which pattern synchronization was lost since initially acquiring pattern synchronization.

PCS Stats

[Table 23](#) lists and describes each of the test results available in the PCS Stats result category.

Table 23 PCS Error Stats

Test Result	Description
Alignment Marker Loss Seconds	Number of seconds during which Alignment Markers were not detected since initial frame synchronization.
Alignment Marker Lock Present	Alignment Marker Lock condition currently being detected.
Alignment Marker Lock History	Alignment Marker Lock condition detected and then lost at some time since initial frame synchronization.
Invalid Alignment Markers	A count of the number of Invalid Alignment Markers since initial frame synchronization.
Invalid Alignment Markers Rate	The ratio of the sum of Invalid Alignment Markers, across all lanes, to the sum of all Alignment Markers, across all lanes, since initial frame synchronization.
Invalid Alignment Marker Seconds	A count of the number of seconds containing at least one Invalid Alignment Marker, any lane, since initial frame synchronization.
Minimum Skew (bits)	The minimum skew (in bits) between lanes that was detected since Alignment Marker Lock.
Loss of Alignment (Deskew)	Loss of Alignment of the lanes due excessive interlane skew or invalid Alignment Marker data.
Maximum Virtual LaneSkew (ns)	The maximum skew (in ns) between lanes that was detected since Alignment Marker Lock.
Current Maximum Skew (bits)	The maximum inter-lane skew (in bits) that was detected during the period specified for error insertion.

Table 23 PCS Error Stats (Continued)

Test Result	Description
Current Maximum Skew (ns)	The maximum inter-lane skew (in ns) that was detected during the period specified for error insertion.
HI BER Seconds	A count of the number of seconds where High Bit Error Rate (HI BER) was detected in the Sync Bits since initial frame synchronization.
HI BER	A High Bit Error Rate (HI BER) was detected in the Sync Bits since initial frame synchronization.
HI BER History	A High Bit Error Rate (HI BER) was detected in the Sync Bits at some time in the past after initial frame synchronization.
PCS Block Errors	A count of the number of PCS Block Errors since initial frame synchronization.
PCS Block Error Rate	The ratio of the sum of block errors to the total number of blocks since initial frame synchronization.
PCS Block Error Seconds	A count of the number of seconds containing at least one PCS Block Error since initial frame synchronization.
PCS Invalid Blocks	The number of invalid Blocks detected since initial PCS synchronization.

Ethernet Per Lane results

Table 24 lists and describes each of the test results shown in the Ethernet Per Lane table when performing Ethernet testing.

Table 24 Ethernet Per Lane results

Test Result	Description
Max Skew VL ID	Shows Virtual Lane ID for virtual lane having the greatest skew.
Min Skew VL ID	Shows Virtual Lane ID for virtual lane having the least skew.
Max Skew (ns)	Shows skew value in nsecs for virtual lane having the greatest skew.
Max Skew (bits)	Shows skew value in bits for virtual lane having the greatest skew.
Virtual Lane ID	Shows Lane ID for each virtual lane.
Skew (bits)	Shows skew value in bits for each virtual lane.
Skew (ns)	Shows skew value in nsecs for each virtual lane.
Sync Acquired	Display of sync acquisition status for each virtual lane.
Marker Lock	Display of marker lock status for each virtual lane.

Error Stats results

To view the Layer 2 Error Stats results described in [Table 25](#) for Layer 2 Ethernet applications, set the result category to Error Stats.

Table 25 Error Stats results

Test Result	Description
Errored Frames	A summed count of FCS Errored Frames, Jabbers, and Undersized Frames.
FCS Errored Frames	A count of Ethernet frames containing Frame Check Sequence (FCS) errors. When receiving Ethernet jumbo frames containing FCS errors, the FCS error count does not increment. Instead, these frames are counted as Jabbers.
Frame Loss Ratio	The ratio of frames lost to the number of frames expected.
Jabbers	A count of received Ethernet frames that have a byte value greater than the maximum 1518 frame length (or 1522 bytes for VLAN tagged frames or 1526 bytes for Q-in-Q encapsulated frames) and an errored FCS.
Lost Frames	An estimated count of lost Acterna test frames in the received traffic. <ul style="list-style-type: none"> – If the instrument receives an Acterna test frame with a sequence number that is <i>greater</i> than the <i>next expected sequence number</i>, the lost frame count will be <i>incremented</i> by the <i>difference</i> between the sequence number in the received frame and next expected sequence number. The next expected sequence number is set to the received sequence number plus one. – If the instrument receives an Acterna test frame with a sequence number that is <i>less</i> than the <i>next expected sequence number</i>, the lost frame count will be <i>decremented by one</i> because the frame will be counted as an Out of Sequence (OoS) frame.
OoS Frames	An estimated count of out of sequence Acterna test frames in the received traffic. <ul style="list-style-type: none"> – If the instrument receives an Acterna test frame with a sequence number that is <i>less</i> than the <i>next expected sequence number</i>, the OoS frame count will be <i>incremented by one</i>. The next expected sequence number is unchanged.
Runts/Undersized	A count of Ethernet frames under the minimum 64 byte frame length.

RS-FEC results

Table 26 describes the RS-FEC Stats results.

Table 26 RS-FEC Stats results

Test Result	Description
LOAMPS Alarm	ON indicates that a LOAMPS alarm was detected at some point since the last restart of the test; OFF indicates that no LOAMP alarm has been detected.
LOAMPS Seconds	Count of the number of seconds during which a LOAMPS alarm was received.
LOA Alarm	ON indicates that a LOA alarm was detected at some point since the last restart of the test; OFF indicates that no LOA alarm has been detected.
LOA Seconds	Count of the number of seconds during which a LOA alarm was received.
HI SER Alarm	If a high symbol error rate (HI SER) alarm is declared and reported as an error (indicated with an ON status). If the rate is below the acceptable level, OFF appears as the status.
HI SER Seconds	Count of the number of seconds during which a HI SER alarm was received.
Excessive Corr. FEC BER	Status of alarm based on correctable FEC errors, configurable by the Correctable RS-FEC BER Threshold.
RS-FEC Correctable	Count of the number of correctable RS-FEC errors received since the last restart of the test. Available for A+B engines, A engine, B engine, for codewords (CW), Symbols, and Bits.
RS-FEC Correctable Rate	The ratio of correctable RS-FEC blocks to the total blocks received since the last restart of the test. Available for A+B engines, A engine, B engine, for codewords (CW), Symbols, and Bits.
RS-FEC Uncorrectable	Count of the number of uncorrectable RS-FEC errors received since the last restart of the test. Available for A+B engines, A engine, B engine, for codewords (CW), Symbols, and Bits.
RS-FEC Uncorrectable Rate	The ratio of uncorrectable RS-FEC blocks to the total blocks received since the last restart of the test. Available for A+B engines, A engine, B engine, for codewords (CW), Symbols, and Bits.

RS-FEC Per Lane results

The following information is available in tabular format for each of the 16 virtual lanes:

- Virtual Lane #
- Physical Name #
- Correctable A+B Symbol Errors (400GE only)

- Correctable A+B Bit Errors (400GE only)
- Correctable A+B Bit Error Rate (400GE only)

RS-FEC Error Distribution Results

The following information is available in tabular format and is organized based on the number of Symbol Errors per FEC block:

- Number of symbols
 - 1 to 15 for RS(544,514)
 - 1 to 7 for RS(527,514))
- Correctable A+B Codeword Errors (400GE only)
- Correctable A+B Codeword Error % (400GE only)
- Number of uncorrectable codeword errors

Graphical results

The Graphs result group provides test results such as Latency (RTD), Throughput, Instantaneous Packet Jitter, and Errors graphically. When viewing results graphically, a legend is provided under the graph with colors indicating what each color represents on the graph. For graphs that display time, absolute time is used.

To simplify the graph, select the legend and then choose the data that you want to observe, and hide the rest.

Graphs require significant system resources; therefore, you can optionally disable automatic graph generation if you intend to run other resource intense applications.

To disable graph generation

- 1 On the Main screen, select **Tools > Customize**
The Customize User Interface Look and Feel screen appears.
- 2 Clear the **Generate Graphs** setting, and then select **Close** to return to the Main screen.

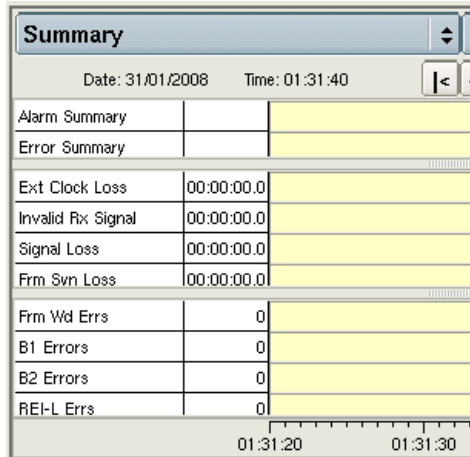
The unit will not automatically generate graphs. You can select the Generate Graphs setting at any time to resume automatic graph generation.

Histogram results

The Histogram result category provides a display of test results in a bar graph format. Histograms enable you to quickly identify spikes and patterns of errors over a specific interval of time (seconds, minutes, or hours).

A sample histogram is provided in [Figure 40](#).

Figure 40 Sample histogram



Results are updated once per second.

Event Log results

The event log result category provides a display listing any significant events, errors or alarms that occur during the course of your test. The log displays the value for each error or alarm, and provides the date and time that the error or alarm occurred.

Events are updated once per second.

Time test results

The Time category provides the current date, time, and the time elapsed since the last test start or restart. [Table 27](#) describes each of the Time results.

Table 27 Time results

Result	Description
Current Date	Current day and month.
Current Time	Current time of day in hours, minutes, and seconds (hh:mm:ss).
Test Elapsed Time	Amount of time in hours, minutes, and seconds (hh:mm:ss) since the last test restart.

Temperature

The temperature of the pluggable optics is available.



Glossary

Symbols/Numerics

802.3 — The IEEE specification for Ethernet. 802.3 also specifies a frame type that places the frame length in the Length/Type field of the Ethernet header, as opposed to the DIX Type II frame type which utilizes the Length/Type field to identify the payload Ethertype.

A

AC — Alternating Current. An AC power adapter is supplied with the instrument.

ARP — Address Resolution Protocol. Method for determining a host's hardware address if only the IP address is known. The instrument automatically sends ARP requests during layer 3 IP testing.

ATP — Acterna test packet. A test packet that contains a time stamp and sequence number for measuring round trip delay and counting out-of-sequence frames.

B

BER — Bit Error Rate.

BERT — Bit error rate test. A known pattern of bits is transmitted, and errors received are counted to figure the BER. The Bit Error Rate test is used to measure transmission quality.

C

CDP — Cisco Discovery Protocol.

CWDM4 — Coarse Wavelength Division Multiplexing 4 Lane. Optics supporting 100GigE circuits using CWDM technology and 4 lanes of 25 Gb/s traffic onto and demultiplexed from duplex singlemode fiber (SMF).

D

DA — Destination address.

DAD — IPv6 duplicate address detection. When going through the Multicast Listener Discovery process to obtain or verify a link local address, a device issues a neighbor solicitation using the tentative address to determine if the address is already used. This process is referred to as DAD.

DHCP — Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses dynamically as needed. Also supports static IP address assignment.

DIX — Digital, Intel, and Xerox. Ethernet Type II frame format.

DSCP — Differentiated Services Code Point. A method for specifying IP packets will be queued while waiting to be forwarded within a router.

E

Ethernet — A LAN protocol. Using the instrument, you can test and verify Ethernet network elements and services.

Ethernet link partner — The nearest Ethernet device on a link. The instrument auto-negotiates its capabilities with this device when you initialize a link.

F

FCS — Frame check sequence. A value calculated by an originating device and inserted into an Ethernet frame. The receiving device performs the same calculation, and compares its FCS value with the FCS value in the frame. If the values don't match (suggesting the frame is errored), an FCS error is declared. Switching devices will discard the frame.

FDV — Frame Delay Variation. Maximum frame jitter within SLA compliance.

FEC — Forward Error Correction. A method used to detect and reconstruct an erroneous transmitted message at the receiver, without requesting a retransmission.

FTD — Frame Transfer Delay. Maximum frame transfer time (source to destination) within SLA compliance.

FTP — File transfer protocol. Protocol used on LANs and the Internet to transfer files.

Frame Loss — Loss of frame synchronization.

G

GARP — Generic Attribute Registration Protocol.

GigE — Used to represent Gigabit Ethernet.

Global Addresses — Second IPv6 source address assigned to an interface. The global address is not used locally, and is broader in scope, typically to get past a router. If you use auto-configuration to establish a link, the global address is provided automatically.

GNSS — Global Navigation Satellite System.

GPS — Global Positioning System.

GUI — Graphical User Interface. Layout of commands in a user-friendly environment. *See also* UI (user interface).

GVRP — GARP VLAN Registration Protocol.

H

Histogram — Print output of specific results in a bar graph format.

HI SER — High symbol error rate.

Hz — Hertz (cycles per second).

I

ISI — Inter-symbol Interference. ISI is often a symptom of dispersion on multi-mode fiber.

ITU — International Telecommunications Union based in Geneva, Switzerland.

J

J-Proof — Application used to verify Layer 2 Transparency.

L

LAN — Local Area Network.

LCD — Liquid Crystal Display.

LED — Light emitting diode.

LLB — Line loopback.

LLC — Logical link control. Three bytes carried in 802.3 frames which specify the memory buffer the data frame is placed in.

LLDP — Link Layer Discovery Protocol.

M

MMF — Multi-mode Fiber.

Msg — Message.

MPLS — Multiprotocol Label Switching. A form of frame encapsulation that uses labels rather than routing tables to transmit layer 3 traffic over a layer 2 Ethernet network.

MPTS — Multiple program transport stream.

MSTP — Multiple Spanning Tree Protocol.

MTIE — The maximum time interval error (peak-to-peak value) in the clock signal being measured that occurs within a specified observation interval in seconds. *See also TDEV and TIE.*

Multipat — Multiple patterns. An automated sequence of 5 BERT patterns for three minutes each. The Multipat sequence consists of ALL ONES, 1:7, 2 in 8, 3 in 24, and QRSS.

N

NE — Near-end. Used by ITU performance measurements to indicate which end of the network is being tested.

NetFlow — NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information.

NID — Network Interface Device. Device located on the customer premises used by carriers to properly demark and manage their network.

NIU — Network Interface Unit. Electronic device at the point of interconnection between the service provider communications facilities and terminal equipment at a subscriber's premises.

NOC — Network Operations Center.

NSA — Non-service affecting.

O

OAM — Operations, Administration, and Maintenance. The instrument allows you to run link and service layer OAM applications.

OOF — Out of framing.

OOM — Out of multi framing.

OOS — Out of sequence.

OPU — Optical channel payload unit.

OTN — Optical Transport Network. Network protocol that facilitates the transmission of different types of client signals, such as SONET, SDH, and Ethernet over a single optical network through the use of an OTN wrapper, which provides the overhead required for proper network management.

OWD — One-Way Delay.

P

Packet — Bundle of data, configured for transmission. Consists of data to be transmitted and control information.

Packet Delay Variation — The difference in one-way-delay as experienced by a series of packets.

PAT — Program Association Table.

Pattern sync — The condition occurring when the data received matches the data that is expected for a period of time defined by the pattern selected.

PCAP — File format used for packet captures on the instrument.

PCR — Program Clock Reference.

PCS — Physical Coding Sublayer.

PDV — Packet Delay Variation. The difference in one-way delay for pairs of packets in a flow.

PE — Provider edge.

Peak IFG time — The time between Ethernet (maximum inter-frame gap) when service switches to a protect line. The Svc Disruption (us) result in the Link Stats category displays the service-disruption time based on the peak IFG.

PID — Program ID.

PM — Path monitoring.

PPPoE — Point to Point Protocol over Ethernet. PPPoE is used on the GUI and throughout this guide to see the applications used to establish a connection to a PPPoE peer via a login process. The HST can emulate a PPPoE client or server.

PPS — Pulse per second.

PTP — Precision time protocol

Q

Q-in-Q — Also known as VLAN stacking, enables service providers to use a single VLAN to support customers who have multiple VLANs. Q-in-Q VLANs can also be used to provide virtual access and connections to multiple services available over the ISPs, ASPs, and storage services.

QoS — Quality of Service.

R

RDI — Remote Defect Indication. A terminal will transmit an RDI when it loses its incoming signal.

REI — Remote Error Indicator.

RFI — Remote Failure Indicator.

RRH — Remote Radio Head.

RSTP — Rapid Spanning Tree Protocol.

RS-232 — Set of standards specifying electrical, functional and mechanical interfaces used for communicating between computers, terminals and modems.

RS-FEC — Reed Solomon Forward Error Correction.

RTD — Round-Trip Delay. Maximum frame transfer delay when measured at source after signal is looped back from far end.

RTP — Real-time Transport Protocol. Standardized packet format for delivering audio and video over the Internet. MPEG video streams are often encapsulated in RTP packets.

Runt — An Ethernet frame that is shorter than the IEEE 802.3 minimum frame length of 64 bytes and contains an errored FCS, or a Fibre Channel frame that is shorter than the minimum 28 byte frame length containing an errored CRC.

Rx — Receive or receiver or input.

S

SA — 1. Source address. 2. Service affecting.

SD — Signal Degradation.

Secs — Seconds.

SER — Symbol Error Rate.

Service disruption time — For Ethernet measurements, this function largely supersedes the Peak IFG function in that it provides service-disruption-time measurements by using selectable triggers that include an inter-frame gap trigger based on either any frame type or frames specifically with Acterna (ATP) as payload.

SF — Signal Fail.

SFD — Start of frame delimiter. Part of an Ethernet frame preamble that indicates that the destination address frame is about to begin.

SFP — Small form-factor pluggable module. Used throughout this manual to represent pluggable optical transceivers (modules).

Skew — A timing variation between lanes.

SLA — Service Level Agreement.

SMF — Single-mode Fiber.

SNAP — Subnetwork Access Protocol. Protocol used in 802.3 frames which specifies a vendor code and an Ethertype. When you transmit pings using the 400G Module, you can transmit 802.3 frames with logical link control (LLC) and SNAP.

SPTS — Single Program Transport Stream.

STP — Spanning Tree Protocol.

SVLAN — Stacked VLAN. Used in Q-in-Q traffic to provide a second encapsulation tag, expanding the number of VLANs available. Often considered the VLAN assigned to the service provider (as opposed to the customer).

Sync — Synchronization.

T

TCP — Transmission Control Protocol. Layer 4 protocol that allows two devices to establish a connection and exchange streams of data.

TCP Window Size — The maximum number of bytes that a port can transmit over a TCP connection before being acknowledged by the receiving port.

TDEV — Time Deviation. A measure of the phase error variation versus the integration time. It is calculated based on the TIE. *See also TIE and MTIE.*

TEM — Timing Expansion Module.

Term — See Terminate.

Terminate — An application where the instrument is terminating the circuit. In these applications, the instrument sends and receives traffic.

Through — An application where the instrument is used in series with a network circuit to monitor the traffic on that circuit.

TIE — Time Interval Error. Represents the time deviation of the signal under test relative to a reference source. Used to calculate MTIE and TDEV. *See also MTIE and TDEV.*

ToD — Time of Day. Signal provided by GNSS receivers and antenna for the purpose of synchronizing the time in instruments used to perform precise measurements, such as one way delay.

TOH — Transport Overhead.

TU — Tributary unit.

Tx — Transmit or transmitter or output.

U

UAS — Unavailable seconds.

UDP — User Datagram Protocol. Layer 4 protocol that offers a limited amount of service when messages are exchanged between devices on an IP network. UDP uses IP to transmit data from one device to another device; however, unlike TCP, UDP does not divide a message into packets, and then reassemble the packets at the far end.

UI — Unit Interval. One bit period at the data rate being measured.

us — Microseconds (also expressed as μs).

USB — Universal Serial Bus. A bus designed to handle a broad range of devices, such as keyboards, mice, printers, modems, and hubs.

V

VDC — Volts Direct Current.

VIAVI Ethernet test set — A test set marketed by VIAVI and designed to transmit an Acterna Test Packet (ATP) payload with a time stamp that is used to calculate a variety of test results. T-BERD / MTS 5800, MSAM, CSAM, Transport Module, OneAdvisor 800 400G module, and OneAdvisor 1000 400G Module can all be configured to transmit and analyze ATP payloads, and can be used in end-to-end and loopback configurations during testing.

VLAN — Virtual LAN.

VNC — Virtual Network Computing. A thin client system that enables you to run applications on a VNC server from any other computer connected to the Internet. Using VNC, you can run the instrument from a remote workstation.

VPLS — Virtual Private LAN Service. An MPLS application which provides multi-point to multi-point layer 2 VPN services, allowing geographically dispersed sites to share an Ethernet broadcast domain by connecting each site to an MPLS-based network.

W

WAN — Wide area network.

X

XFP — 10 Gigabit Small Form Factor Pluggable Module.



22142947
R013, December 2023
English

Viavi Solutions

North America:	1.844.GO VIAVI / 1.844.468.4284
Latin America	+52 55 5543 6644
EMEA	+49 7121 862273
APAC	+1 512 201 6534
All Other Regions:	viavisolutions.com/contacts
email	TAC@viavisolutions.com