HST-3000

Ethernet Testing

User's Guide

JDSU

HST-3000

Ethernet Testing

User's Guide

Communications Test and Measurement Solutions
One Milestone Center Court
Germantown, Maryland 20876-7100 USA
Toll Free 1-855-ASK-JDSU
Tel +1-240-404-2999
Fax +1-240-404-2195
www.jdsu.com

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

Trademarks JDS Uniphase, JDSU, HST-3000, and HST-3000C are trademarks or registered trademarks of JDS Uniphase Corporation in the United States and/or other countries.

Microsoft, Windows, Windows NT, Excel, HyperTerminal, and Internet Explorer are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

Ordering information This guide is a product of JDSU's Technical Information Development Department, issued as part of the HST-3000. The catalog number for a printed user's guide is ML-072301. The catalog number for a USB stick containing the manual in electronic form is ML-060301.

Terms and conditions

The provision of hardware, services and/or software are subject to JDSU's standard terms and conditions available at www.jdsu.com.

Federal Communications Commission (FCC) Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

– Reorient or relocate the receiving antenna.
– Increase the separation between the equipment and receiver.
– Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
– Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with the limits of a Class B digital device JDSU requires that quality interface cables be used when connecting to this equipment. Any changes or modifications not expressly approved by JDSU could void the user's authority to operate the equipment.

Industry Canada Requirements

This Class B digital apparatus complies with Canadian ICES-003.Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

WEEE and Battery Directive Compliance

JDSU has established processes in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive, 2002/96/EC, and the Battery Directive, 2006/66/EC.

This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from JDSU after 2005-08-13 can be returned for disposal at the end of its useful life. JDSU will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to JDSU for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to JDSU can be found in the Environmental section of JDSU's web site at www.jdsu.com. If you have questions concerning disposal of your equipment or batteries, contact JDSU's WEEE Program Management team at WEEE.EMEA@jdsu.com.

Contents

About This Guide

Topics discussed in this chapter include the following:

Purpose and scope

The purpose of this guide is to help you successfully use the features and capabilities of the HST-3000 with the Ethernet SIM. This guide includes task-based instructions that describe how to configure, use, and troubleshoot the Ethernet SIM during testing.

Assumptions

This guide is intended for novice, intermediate, and experienced users who want to use the HST-3000 with an Ethernet SIM efficiently and effectively. We assume that you have basic computer experience and are familiar with basic telecommunications safety, concepts, and terminology.

Terminology

The following terms have a specific meaning when they are used in this guide:

- **HST-3000** — The HST-3000 family of products or the combination of a base unit and a SIM.
- **SIM** — Service Interface Module. Referred to generically as the module.
- **10/100/1G** — Used on the GUI and throughout this guide to see 10BaseT, 100BaseTX, 1000Base TX (1 Gigabit) Ethernet electrical signals.
- **1G** — Also used on the GUI and throughout this guide to see 1 Gigabit Ethernet (1000BaseSX, 1000BaseLX, and 1000BaseZX) optical signals.
- **100M** — Used on the GUI and throughout this guide to see 100 Mbps (100BaseFX) Ethernet optical signals.

- **JDSU Ethernet test set** — A test set marketed by JDSU and designed to transmit an Acterna Test Packet (ATP) payload. These packets carry a time stamp used to calculate a variety of test results. The FST-2802 TestPad, the T-BERD/MTS 8000 Transport Module, the SmartClass Ethernet tester, the QT-600, and the HST with an Ethernet SIM can all be configured to transmit and analyze ATP payloads, and can be used in end-to-end and loopback configurations during testing.
- **IPoE —** Internet Protocol over Ethernet. IPOE is used on the GUI and throughout this guide to see the applications used to establish a standard layer 3 (IP) connection.
- **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.
- **IPv4 —** Internet Protocol Version 4. IPv4 is used on the GUI and throughout this guide to see the applications used to transmit and analyze traffic carrying version 4 IP packets.
- **IPv6 —** Internet Protocol Version 6. IPv6 is used on the GUI and throughout this guide to see the applications used to transmit and analyze traffic carrying version 6 IP packets.
- **Q-in-Q —** Also also known as VLAN stacking, Q-in-Q is used on the GUI and throughout this guide to see the frame encapsulation scheme that enables service providers to use a single VLAN to support customers with multiple VLANs. Q-in-Q VLANs can also be used to provide virtual access and connections to multiple services.
- **MPLS —** Multiple Path Label Switching. A frame encapsulation scheme that uses labels rather than routing tables to transmit layer 3 IP traffic over a layer 2 Ethernet network.

For definitions of other terms used in this guide, see “Glossary” on page 317.

HST-3000 Ethernet Testing User's Guide

This guide is an application-oriented user's guide containing information about using the HST-3000 with the Ethernet SIM to test and verify Ethernet and IP service. Also included is information about testing 1G optical Ethernet, 100M optical Ethernet, and multiple traffic streams using the features provided if you purchase the associated software options. For information about purchasing software options, contact your JDSU sales representative.

This guide also contains specifications and contact information for JDSU's Technical Assistance Center (TAC). This user's guide should be used in conjunction with the *HST-3000 Base Unit User's Guide*.

HST-3000 Base Unit User's Guide

The *HST-3000 Base Unit User's Guide* contains overall information relating to device and general functions such as using the unit with a keyboard, peripheral support, battery charging, saving and printing results, and managing files. This guide also contains technical specifications for the base unit and a description of JDSU's warranty, services, and repair information, including terms and conditions of the licensing agreement.

Safety and compliance information

Safety and compliance information are contained in a separate guide and are provided in printed format with the product.

Technical assistance

If you need assistance or have questions related to the use of this product, use the information in Table 1 to contact JDSU's Technical Assistance Center (TAC) for customer support.

Before you contact JDSU for technical assistance, please have the serial numbers for the service interface module (SIM) and the base unit handy (see "Locating the serial number" in the *HST-3000 Base Unit User's Guide*).

Table 1 Technical assistance centers

Region	Phone Number	
Americas	1-855-ASK-JDSU 240 404 2999 301-353-1550	tac@jdsu.com
Europe, Africa, and Mid-East	+49 (0) 7121 86 1345 (JDSU Germany)	hotline.europe@jdsu.com
Asia and the Pacific	+852 2892 0990 (Hong Kong) +8610 6833 7477 (Beijing-China)	

During off-hours, you can request assistance by doing one of the following: leave a voice message at the TAC for your region; email the North American TAC (tac@jdsu.com); submit your question using our online Technical Assistance request form at www.jdsu.com.

Conventions

When applicable, this guide uses the typographical conventions and symbols described in the following tables.

Table 2 Typographical conventions

Description	Example
User interface actions appear in this **typeface**.	On the Status bar, click **Start**.Use the Direction character tag for this convention.
Buttons or switches that you press on a unit appear in this **TYPEFACE**.	Press the **ON** switch.Use the Switch character tag for this convention.
Code and output messages appear in this `typeface`.	`All results okay`
Text you must type exactly as shown appears in this **`typeface`**.	Type: **`a:\set.exe`** in the dialog box. the CodeDirection character tag for this convention.
Variables appear in this ***typeface***.	Type the new ***hostname***.Use the Emphasis character tag for this convention.
Book references appear in this *typeface*.	see *Newton's Telecom Dictionary.*
A vertical bar | means "or": only one option can appear in a single command.	`platform [a|b|e]`
Square brackets [ ] indicate an optional argument.	`login [platform name]`
Slanted brackets < > group required arguments.	`<password>`

Table 3 Keyboard and menu conventions

Description	Example
A plus sign + indicates simultaneous keystrokes.	Press **Ctrl+s**
A comma indicates consecutive key strokes.	Press **Alt+f,s**

Table 3 Keyboard and menu conventions (Continued)

Description	Example
A slanted bracket (>) indicates choosing a submenu from menu.	On the menu bar, click **Start > Program Files**.

Table 4 Symbol conventions

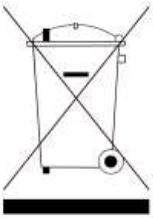
	This symbol represents a caution.
	This symbol represents a risk of electrical shock.
	This symbol represents a Note indicating related information or tip.
	This symbol, located on the equipment, battery, or packaging indicates that the equipment or battery must not be disposed of in a land-fill site or as municipal waste, and should be disposed of according to your national regulations.

Table 5 Safety definitions

DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Getting Started

1

This chapter provides basic information about testing using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

Overview

Using an HST-3000 with an Ethernet SIM, you can perform the test operations necessary to install, maintain, and trouble-shoot Ethernet and IP service. The unit allows you to test connectivity, verify throughput, measure delay, and transmit patterns to stress the jitter and noise characteristics of network elements and systems.

Before testing, you should familiarize yourself with basic Ethernet and IP concepts such as link initialization, flow control, frame and IP packet structures, and the various encapsulation schemes supported. Data sheets for this product, and white papers addressing basic Ethernet concepts are available at www.jdsu.com.

Features and capabilities

Features and capabilities of the HST-3000 with an Ethernet SIM include:

- Traffic generation—You can generate frames and configure traffic parameters such as bandwidth utilization, frame type (DIX or 802.3), and frame length. You can simulate different network traffic conditions and analyze the performance of a link by configuring traffic loads for constant, bursty, and ramped traffic.
- Dual port configuration—You can analyze Ethernet *or* IP traffic from two ports simultaneously.
- Multiple streams—You can transmit up to 8 streams simultaneously. Each stream depicts a particular type of traffic. Transmitting multiple streams allows you to verify how the network switching and routing equipment handles traffic based on the priority levels assigned to each stream.
- Filtered traffic—You can filter received traffic by specifying settings which define the characteristics of the traffic you want to monitor.

– Link status—Using the easy-to-interpret LEDs, you can obtain a quick summary of the state of the link or the traffic stream you are analyzing. This enables you to quickly verify circuit integrity, and to identify the source of a problem on the link.
– Verify end-to-end connectivity—You can ensure physical layer integrity and verify end-to-end connectivity of a circuit.
– Link utilization and throughput verification—You can generate traffic at a specific bandwidth to verify the error free throughput of a link. The HST allows you to loopback frames at the far end to qualify the link in both directions.
– BER testing—You can verify circuit performance by transmitting and analyzing BERT patterns.
– Identify problems with faulty interfaces—You can perform basic troubleshooting of links and verify the capability of network elements to support reliable communications by transmitting standard frames and packets over a circuit.
– Event log. A new event log now displays the date and time that significant events, errors, or alarms occurred during the course of your test.
– Optional color display. If your base unit has a color display, a green Summary results screen indicates that key test results were acceptable (and no errors were detected); a red screen indicates results are errored, and a yellow screen indicates that results occurred that require additional research. For additional details on the color display, see the *HST-3000 Base Unit User's Guide.*
– Q-in-Q support. You can configure, transmit, and analyze Q-in-Q encapsulated traffic.
– PPPoE support. You can configure your unit to emulate a PPPoE client and test over PPPoE links.
– IPv6 support. If you purchased the IPv6 Traffic option, you can transmit and analyze IPv6 traffic in terminate and monitor/through modes.

– Basic layer 4 support. If you purchased the TCP/UDP option, you can transmit and analyze IPv4 traffic with TCP or UDP headers in terminate mode. The IPv6 Traffic option is also required if you want the ability to transmit and analyze layer 4 IPv6 traffic.
– MPLS support. If you purchased the MPLS Traffic option, you can transmit MPLS encapsulated traffic when testing and qualifying core and metro networks.

What's new

This release of the Ethernet SIM supports the following new features:

– Loop Types. When you configure an instrument for a loop-back test, you can specify that you want to issue a Unicast loop-up command, or a Broadcast loop-up command. 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 network that responds.
– Mac-in-Mac testing.If you purchase the MiM testing option, you can transmit and analyze MAC-in-MAC Ethernet traffic over a PBB (Provider Backbone Bridged) network to verify end-to-end connectivity, and analyze link performance. For details, see "MAC-in-MAC testing" on page 105.
– Link and service layer OAM testing. OAM messages are supported, enabling you to identify trunk problems so you can initiate a switch to a protection path. When testing Ethernet First Mile OAM communications, you can loop-back an adjacent node or Ethernet demarcation device (EDD), and then exchange messages with the node or device to verify that auto-discovery and error notification are functioning properly. For details, see "OAM service and link layer testing" on page 94.
– Layer 2 transparency testing.You can transmit and analyze layer 2 traffic with headers (such as CDP, VTP, STP, and R/STP) to verify that a circuit can support a variety of control protocols irrespective of the transport

method. For details, see “Using J-Proof to verify layer 2 transparency” on page 71.

– JDSU Discovery. You can now automatically detect other JDSU test equipment on the network, and determine their services and capabilities.

– ATP payload definition. You can now specify a repeating static fill-byte pattern up to 64 bytes long to be inserted into Acterna Test Packets (ATPs).

– Throughput calculation. When your instrument is configured to transmit a constant load of traffic, it will now automatically estimate and display the ideal throughput utilized for each layer before you begin testing.

– Multiple stream testing enhancements. You can now configure your instrument to transmit a ramped load of traffic when running multiple streams applications. You can also transmit a fill-byte pattern in an ATP payload when transmitting layer 2, layer 3, or layer 4 streams.

– Multiple source addresses. When running layer 2 or layer 3 multiple streams applications with IPV4 traffic, you can now specify a different source MAC or IP address for each individual traffic stream.

– Link Stats result enhancements. You can now setup your instrument to report link throughput in Mbps or Kbps, or you can specify that the instrument should automatically determine the increment. You can also control the precision of certain measurements (up to four decimal points), and measure instantaneous packet jitter.

– Performance results. Additional performance and error results are now provided, such as counts of severely errored seconds, and unavailable seconds.

– RFC 2544 enhancements. You can now launch the automated RFC test when running standard Traffic applications. An asymmetric RFC 2544 test is also available, which allows you to run the test in an end-to-end configuration at different upstream and downstream line rates. The test is initiated by a master tester on the near end. The master tester then automatically configures the slave tester on the far end.

Software options

You can expand your testing capability by purchasing additional software options for the Ethernet SIM. The options available for purchase are as follows:

Table 6 Ethernet software options

Option	Description	Catalog Number
Optical Ethernet	Using this option, you can test 1G and 100M optical Ethernet network elements and services.	HST3000-OPTETH
Multiple Streams	Using this option, you can transmit up to 8 streams of traffic to verify how the network switching and routing equipment prioritizes traffic based on the priority levels (L2 and L3) assigned to each stream.	HST3000-MSTR
Layer 2 Transparency	Using this option, you can transmit and analyze layer 2 traffic with headers (such as CDP, VTP, STP, and R/STP) to verify that a circuit can support a variety of control protocols irrespective of the transport method.	HST3000 – L2TRANS
MAC-in-MAC	Using this option, you can transmit and analyze MAC-in-MAC Ethernet traffic over a PBB (Provider Backbone Bridged) network to verify end-to-end connectivity, and analyze link performance.	HST3000 – MIM
OAM	Using this option, you can test Ethernet First Mile OAM communications.	HST3000 – OAM
TCP/UDP	Using this option, you can transmit and analyze IPv4 layer 4 traffic with TCP or UDP headers in terminate mode. The IPv6 Traffic option is also required for layer 4 IPv6 testing.	HST3000-TCPUDP

Table 6 Ethernet software options (Continued)

Option	Description	Catalog Number
IPv6 Traffic	Using this option, you can transmit and analyze IPv6 traffic in terminate and monitor/through modes. The Layer 4 TCP/UDP option is also required for layer 4 IPv6 testing.	HST3000-IPV6
MPLS Traffic	Using this option, you can specify up to two MPLS labels for transmitted traffic when testing and qualifying core and metro networks.	HST3000-MPLS

Status LEDs

Six status LEDs are located on the front of the HST-3000, above the screen. Table 7 describes the status LEDs.

Table 7 Status LEDs

LED	Description
Sync	An LED that reports whether or not the link is active. – Solid green indicates the link is active. – If the Sync LED is not illuminated, the link is not currently active.
Data	An LED that reports the status of frame or packet detection. – Solid green indicates frames or packets have been detected in the traffic stream. – If the Data LED is not illuminated, frames are no longer being detected.
Error	An LED that reports error conditions. – Solid red indicates an error. To determine the type of error, observe the Summary result category. – If the Error LED is not illuminated, all Summary results are OK.

Table 7 Status LEDs (Continued)

LED	Description
Alarm	– The Alarm LED is not applicable when testing using the Ethernet SIM.
LpBk	This LED indicates the local loopback state of the HST unit. – Solid green indicates the HST has been placed in loopback mode either manually, or by a unit on the remote end. – If the LpBk LED is not illuminated, the local unit is not in loopback mode.
Batt	The Batt LED reports the battery status. **NOTE:** For information about charging the battery, changing batteries, and resetting the battery capacity indicator, see the *HST-3000 Base Unit User's Guide*.

In addition to the status LEDs, soft LEDs are provided in the LED result category. For descriptions of each of the soft LEDs, see "LED results" on page 304.

Connectors

The Ethernet SIM provides the physical interfaces needed to transmit and receive Ethernet and IP traffic. Two SFP connectors are provided on the top of the SIM for 1 Gigabit (1G) or

100M optical signals, and two RJ-45 connectors are provided on the left side of the SIM for 10/100/1G electrical signals (see Figure 1 on page 9).

NOTE:

When testing 1G or 100M optical signals, be certain to use a JDSU supported SFP. If you use a single-mode SFP, be certain to attenuate the signal.

For a list of currently supported SFPs, contact your JDSU TAC representative or your local JDSU sales office. You can also contact JDSU through the company web site, www.jdsu.com.

Table 8 on page 10 describes the connectors on the Ethernet SIM.

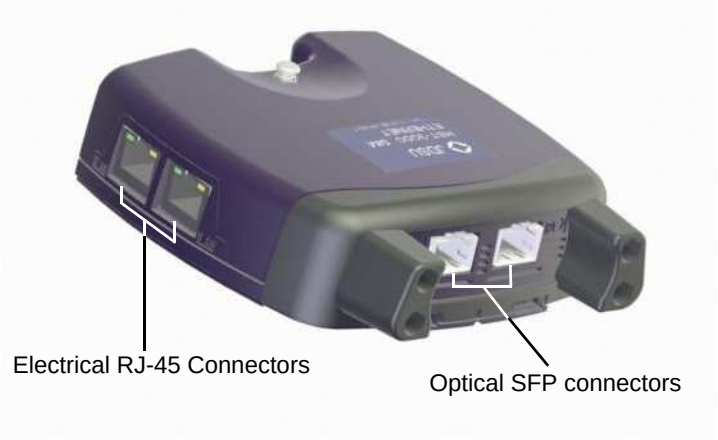


Figure 1 Ethernet interface connectors

Table 8 describes the connectors on the Ethernet SIM. For additional input and output specifications, see Appendix B.

Table 8 Ethernet connectors

Connector Label	Location	Type	Description
R/T 1 and R/T 2	Left side of SIM	RJ-45	Used for 10/100/1G electrical connections.
R/T 1 and R/T 2	Top of SIM	SFP	Used for 1G optical connections. The R/T 2 connector can also be used for 100M connections (100M testing is not supported on the R/T 1 connector).
ETHERNET	Top of Base Unit	RJ-45	Used for Ethernet TE, VoIP, and IP Video testing. *Do not use this connector when testing 10/100/1000 Mbps interfaces in monitor, thru, or terminate modes.* For details, see the *HST-3000 VoIP Testing User's Guide*.

Test applications

Terminate, monitor, and thru applications are provided when testing 10/100/1G electrical or 1G optical signals; terminate and monitor applications are available when testing 100M optical signals.

Terminate applications

When running a terminate application, the HST separates the transmit and receive paths. The received signal is terminated, and a completely independent signal is transmitted.

10/100/1G Electrical Ethernet terminate application

Figure 2 illustrates the signal path when running an electrical terminate application.

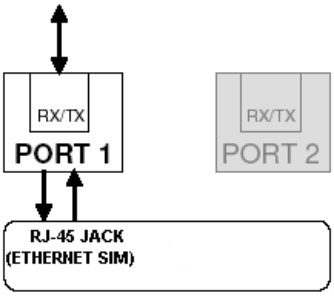


Figure 2 Terminate application: electrical signal path

1G Optical Ethernet terminate application

When running a terminate application for a 1G optical signal, events on the receiving SFP port (R/T 1) are analyzed, but a separate, independent signal is generated and transmitted by the HST. Analysis is restricted to the R/T 1 port.

Figure 3 illustrates the signal path when running a terminate application for a 1G optical signal.

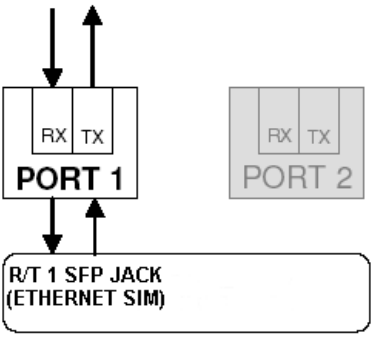


Figure 3 Terminate application: 1G optical signal path

100M Optical Ethernet terminate application

When running a terminate application for a 100M optical signal, events on the receiving SFP port (R/T 2) are analyzed, but they have no affect on the signal transmitted by the HST (the transmitted signal is generated independent of the received signal). Analysis is restricted to the R/T 2 port.

Figure 3 illustrates the signal path when running a terminate application for a 100M optical signal.

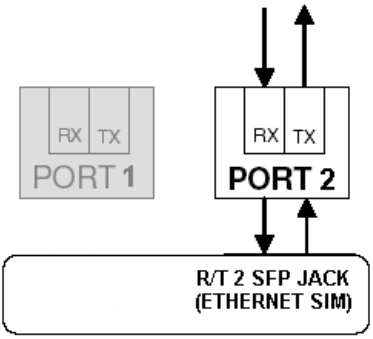


Figure 4 Terminate application: 100M optical signal path

Monitor applications

Before running a monitor application, in addition to selecting the Monitor/Thru application for the signal you are testing, you must specify **Monitor** as the test type (as opposed to the Thru type). The HST then analyzes the received signal.

10/100/1G Electrical Ethernet monitor application

When monitoring electrical signals, the HST analyzes the received signal on the R/T 1 RJ-45 port.

The HST does not pass the signal through to the transmitter, as it does in when running an electrical Thru application (see “10/100/1G Electrical Ethernet thru application” on page 15).

Figure 5 illustrates the signal path when monitoring electrical signals.

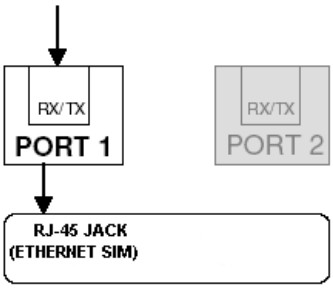


Figure 5 Monitor application: electrical signal path

1G Optical Ethernet monitor application

When monitoring 1G optical signals, the HST analyzes the received signal on the R/T 1 SFP port.

Figure 6 illustrates the signal path when monitoring 1G optical signals.

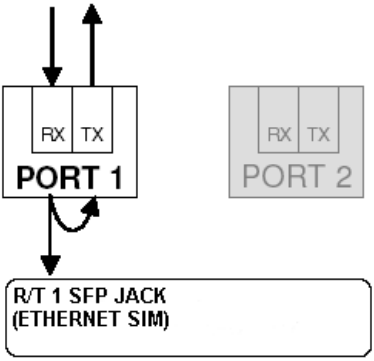


Figure 6 Monitor application: 1G optical signal path

100M Optical Ethernet monitor application

When monitoring 100M optical signals, the HST analyzes the received signal on the R/T 2 SFP port.

Figure 7 illustrates the signal path when monitoring 100M optical signals.

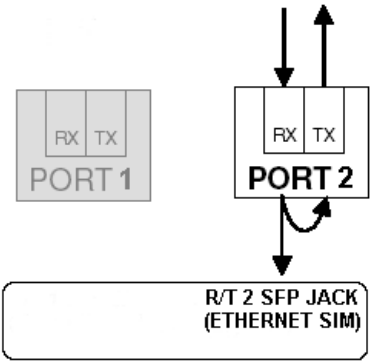


Figure 7 Monitor application: 100M optical signal path

Thru applications

Before running Thru applications, in addition to selecting the Monitor/Thru application for the signal you are testing, you must specify **Thru** as the test type (as opposed to the Monitor type). When configuring a Thru application, you can specify filter settings for each port, and test results can also be viewed for each port simultaneously.

When running Thru applications for 10/100/1G electrical and 1G optical signals, the HST monitors the signal on the receiving port, and then *passes it through to the opposite port's transmitter.*

10/100/1G Electrical Ethernet thru application

Figure 8 illustrates the signal path when running a Thru application for electrical signals.

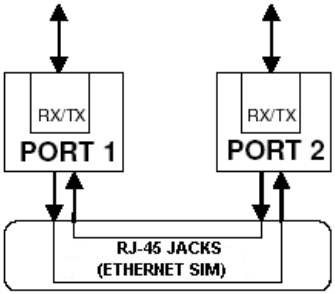


Figure 8 Thru application: electrical signal path

1G Optical Ethernet thru application

Figure 9 illustrates the signal path when running Thru applications for 1G optical signals.

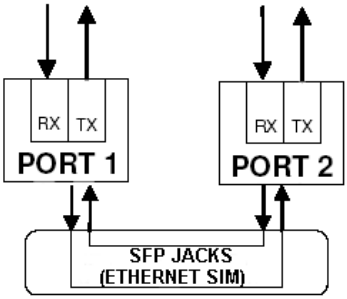


Figure 9 Thru application: 1G optical signal path

Test scenarios

The following scenarios describe the various tests you might perform using the HST. Your test requirements may vary; these scenarios are intended to provide an overview of typical test sessions. For step-by-step procedures for each of the key applications, see:

– Chapter 3 “Ethernet Testing” (for layer 2 applications)
– Chapter 4 “IP Testing” (for layer 3 applications)
– Chapter 5 “TCP/UDP Testing” (for layer 4 applications)

Before testing, we strongly recommend that you read “Configuring your test” on page 25 to become comfortable with the new interface. For detailed test result descriptions, see Appendix A.

Verifying connectivity and evaluating latency

In this scenario, you configure the HST to emulate service from customer equipment on the link, and then verify connectivity and evaluate latency on the circuit.

If you are testing on an unswitched network, you establish a hard loopback at the far end of the circuit, and then transmit and loop traffic back to the HST for analysis. See Figure 10.

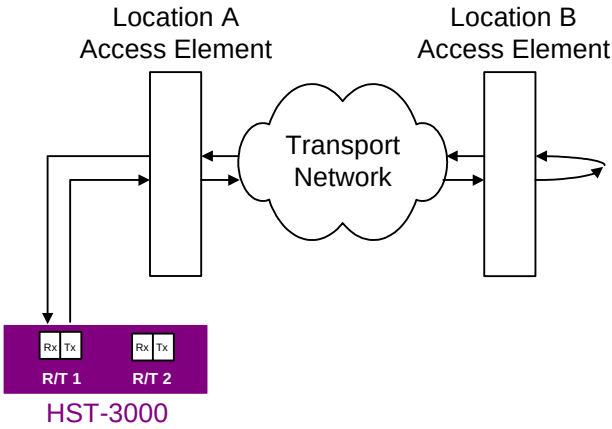


Figure 10 Hard loopback

If you are testing on a switched network, a second HST, or another JDSU Ethernet test set (such as the SmartClass Ethernet Tester, FST-2802, or MTS-8000 Transport Module) must be connected to the network at the far end, and a soft

loopback must be established by issuing a loop up command on the unit on the near end, or by initiating a local loopback (LLB) on the far end unit. See Figure 11.

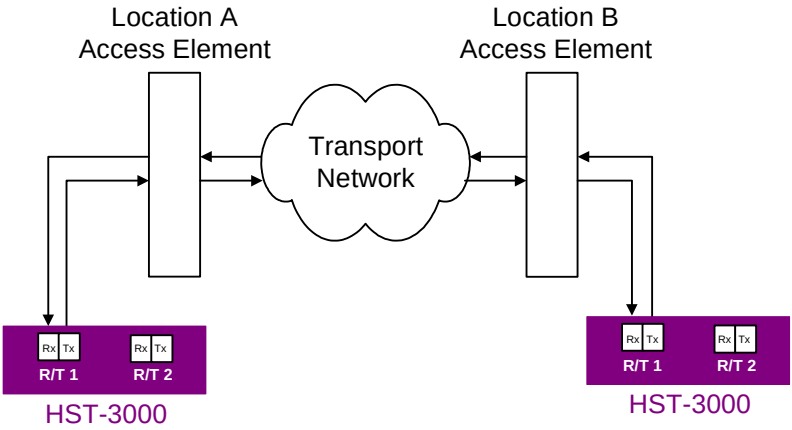


Figure 11 Soft Loopback at far end

Depending on the application you are running, the far end unit does the following for each received frame or packet:

– If you are running a layer 2 application, it swaps the source and destination MAC addresses.
– If you are running a layer 3 application, it swaps the source and destination MAC and IP addresses
– If you are running a layer 4 application, it swaps the source and destination MAC and IP addresses, and the source and destination port numbers.

After swapping the addresses (or port numbers), the unit then sends the frame or packet back to the near end unit for analysis.

Terminate tests are typically performed after the loopback is established to verify connectivity, measure frame and packet loss, measure round trip delay (latency), and insert and observe errors.

Verifying throughput and stressing the network

In this scenario, you configure the HST to transmit various loads of constant, ramped, and bursty traffic to stress the circuit and verify the quality of the link in both directions.

To emulate results in a live network with bi-directional traffic, a JDSU Ethernet test set must be connected to the network at the far end, and a soft loopback must be established by issuing a loop up command from the unit on the near end, or by initiating a local loopback (LLB) from the far end unit. See Figure 12 on page 19.

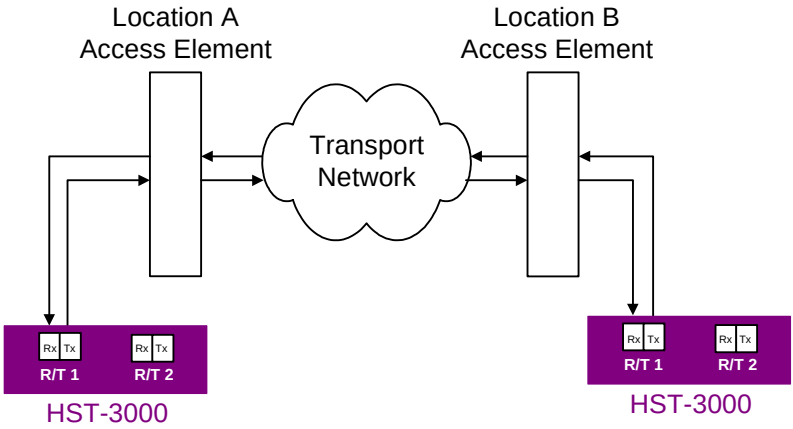


Figure 12 Soft Loopback at far end

After establishing the loopback, terminate tests configured for constant, ramped, and bursty loads of traffic are typically performed.

Monitoring statistics and troubleshooting traffic on a link

In this scenario, you configure the HST to monitor traffic or pass traffic through at key points in the network. When you configure the unit, you can specify settings that filter the received traffic for analysis. For example, you can configure the HST to display test results for all traffic carrying a specific BERT pattern in the payload, or for all traffic originating from a specific source address or VLAN.

To monitor traffic in a single direction when the network is in service, you must connect the HST to the circuit via a splitter or a mirror port on the switch. Figure 13 illustrates a splitter connection.

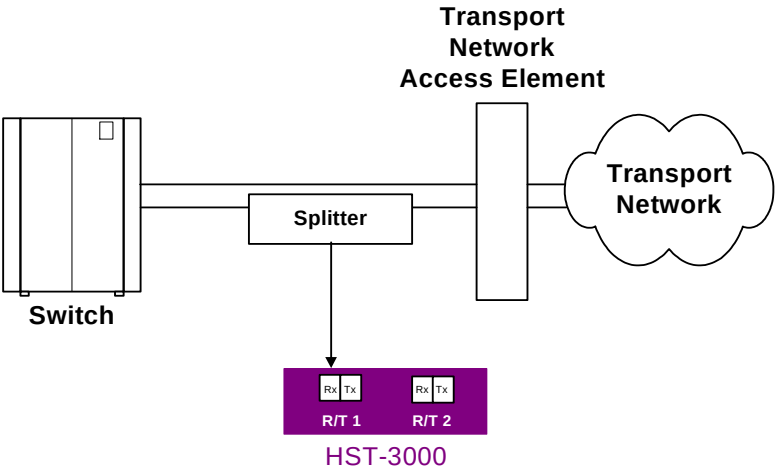


Figure 13 Monitoring traffic using a splitter

If you want to monitor full duplex 1 Gigabit Ethernet or electrical Ethernet traffic from both directions, you can use the two ports provided on the HST to pass traffic through your unit.

See Figure 14.

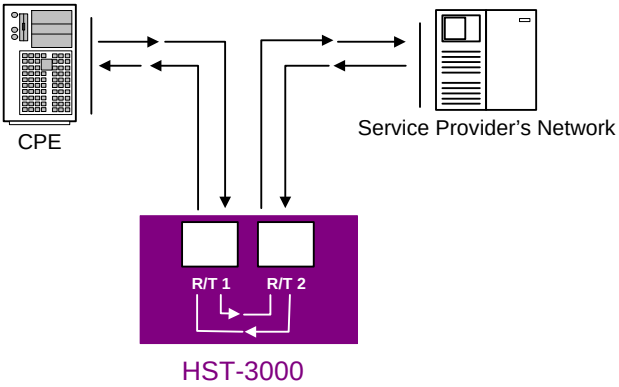


Figure 14 Monitoring traffic using a dual port THRU application

After connecting to the circuit, you monitor traffic by observing link statistics, counts, and errors for a specific MAC or IP address, or Port number, or for a particular VLAN ID, SVLAN ID, CVLAN ID, or MPLS label.

Using J-Connect to discover another JDSU test set

Before you begin testing, you can automatically detect other JDSU test instruments on the same subnet and determine their capabilities.You can then optionally configure key parameters for your test automatically based on a discovered instrument's settings.

Discoverable instruments

Discoverable test instruments include:

- The T-BERD/MTS 8000 Transport Module
- The T-BERD/MTS 6000A MSAM
- Other HST's with Ethernet SIMs

Prerequisites

To be discoverable, JDSU test instruments must:

- Run a software version that supports the JDSU Discovery feature.
- Be configured to be discoverable.
- Have a unique source IP address. JDSU test instruments of the same type (for example, HSTs) ship from the factory with the same default source IP address. If you want to discover the instrument on the subnet, be certain to specify a different source IP address.

If you want to use a discovered instrument's MAC and IP addresses to configure the settings on your instrument, verify the following:

- In the Ethernet Filter, verify that the Source Type is Unicast.
- In the Ethernet menu, verify that the Destination Type is also Unicast.
- In the IP Filter, verify that the filter is enabled, and that the Specify Source setting is Yes.
- Verify that you are not transmitting traffic.
- If you want to use the discovered MAC address as the destination address, turn ARP off.

Discovering an instrument

To discover another JDSU test instrument

1. Before testing, ensure that instruments on the subnet are discoverable by doing the following for each:

   a Launch a single-stream IPv4 terminate application (see “Launching an application” on page 28).

   J-Connect is not available when running MAC-in-MAC, multiple stream, or IPv6 applications.

   b Press the **Configure** navigation key, then use the right arrow key to display the Test Mode menu.

   c Verify that the Unit Discoverable setting is **Yes**.

   d Verify that a different source IP address is assigned to each instrument.

2. Connect your instrument to the circuit, and then do the following:

   a Launch a single-stream IPv4 terminate application.

   b Verify that the Sync and Data LEDs are illuminated, indicating that an active link is established.

   c On your instrument, press the **Action** soft key, and then select **Discover Units**.

   A message appears asking you to wait while the instrument discovers devices.

If the instrument discovered other test instruments, their unit identifiers appear on the Discovered Devices screen. A count of the number of discovered devices also appears.

If the instrument does not discover any other test instruments, a message appears stating that no devices were discovered.

NOTE:

You can also discover other instruments when you specify destination addresses for transmitted traffic, and source addresses carried in filtered traffic. For details, refer to "Configuring layer 2 Ethernet tests" on page 51, "Configuring layer 3 IP tests" on page 136, or "Configuring layer 4 traffic" on page 167.

About the Refresh soft key

The Refresh soft key appears whenever the Discovered Devices screen is displayed. Use the button to rediscover devices on the subnet (for example, if you suspect a discovered device is no longer connected to the circuit).

Sorting discovered instruments

By default, discovered instruments are listed by their unit identifiers. You can optionally sort them by serial number, application name, MAC, or IP address.

To sort discovered instruments

1. Discover the instruments.
2. On the Discovered Devices screen, press the **Display By ...**soft key.
3. Select the sort key.

The instruments are sorted using the new key.

Observing details for an instrument

After discovering the instruments, you can observe details for a particular instrument, and indicate whether or not you want to use the discovered instrument's MAC and IP address when you configure your instrument.

1 To observe details for a discovered instrument, highlight the instrument on the Discovered Devices screen, then press **OK**.

   The Device Details screen appears.

2 If you want to automatically apply the discovered instrument's MAC or IP address to your instrument's configuration, do the following:

   a To use the discovered instrument's MAC or IP address as the destination MAC or IP address for your transmitted traffic, highlight the checkbox under Tx, and then press **OK**.

   b To filter received traffic using the discovered instrument's destination MAC or IP address, highlight the checkbox under Rx, and then press **OK**.

3 Press the **Accept** soft key to save the settings, or the **Cancel** soft key to return to the previous screen without saving them.

Details were displayed, and your instrument is configured based on the settings you selected.

Configuring your test

Configuring your tests involves launching an application, selecting a test mode, and then specifying settings on the configuration menus. You can also optionally detect other JDSU test instruments on the same subnet (see "Using J-Connect to discover another JDSU test set" on page 21), and automatically configure various settings based on the discovered instruments capabilities.

Table 9 lists each of the available applications and test modes.

– You must select a Terminate application to run Ping, or Traceroute tests.

- You must select a Terminate or Multi-Stream Terminate to run Layer 4 tests.
- Certain softkeys, applications, and tests only appear if you purchased and loaded the associated software options.

Table 9 Supported Applications, Test Modes, and Traffic

Soft key / Circuit	Application	Test/Traffic
ETH ELEC 10/100/1G electrical	Terminate	– Layer 2 Traffic – Layer 2 Transparency – Layer 3 IP Traffic – Layer 3 PING – Layer 3 Traceroute – Layer 4 Traffic
	Multi-Stream Terminate	– Layer 2 Streams – Layer 3 Streams – Layer 4 Streams
	Monitor / Thru	– Layer 2 Traffic – Layer 3 IP Traffic
	MAC-in-MAC Terminate	MAC-in-MAC (selected automatically)
	MAC-in-MAC Monitor / Thru	MAC-in-MAC (selected automatically)
	Cable Diagnostics	Cable Diagnostics (selected automatically)

Table 9 Supported Applications, Test Modes, and Traffic (Continued)

Soft key / Circuit	Application	Test/Traffic
ETH OPTIC 1G and 100M optical	Terminate	– Layer 2 Patterns[1] – Layer 2 Traffic – Layer 2 Transparency[1] – Layer 3 IP Traffic – Layer 3 PING – Layer 3 Traceroute – Layer 4 Traffic
	Multi-Stream Terminate	– Layer 2 Streams – Layer 3 Streams – Layer 4 Streams
	Monitor / Thru	– Layer 2 Traffic – Layer 3 IP Traffic
	MAC-in-MAC Terminate	MAC-in-MAC (selected automatically)
	MAC-in-MAC Monitor / Thru	MAC-in-MAC (selected automatically)
ETH TE	– Ethernet TE applications are documented in the *HST-3000 VoIP Testing User's Guide.* – IP Video applications are documented in the *HST-3000 IP Video Testing User's Guide.*	
IPv6 ELEC 10/100/1G electrical	– IPv6 Terminate	– Layer 3 IP Traffic – Layer 3 PING – Layer 3 Traceroute – Layer 4 Traffic
	– IPv6 Monitor / Thru	– Layer 3 IP Traffic

Table 9 Supported Applications, Test Modes, and Traffic (Continued)

Soft key / Circuit	Application	Test/Traffic
IPv6 OPTIC 1G and 100M optical	1G IPv6 Terminate	– Layer 3 IP Traffic – Layer 3 PING – Layer 3 Traceroute – Layer 4 Traffic
	1G IPv6 Monitor / Thru	– Layer 3 IP Traffic
	100M IPv6 Terminate	– Layer 3 IP Traffic – Layer 3 PING – Layer 3 Traceroute – Layer 4 Traffic
	100M IPv6 Monitor / Thru	– Layer 3 IP Traffic

1. Available for 1G Optical tests only.

Launching an application

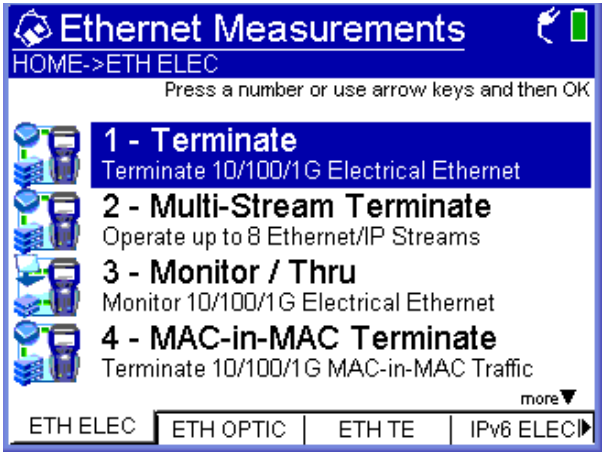
Before powering on your unit and launching an application, you must connect an Ethernet SIM to your base unit. For information about connecting a SIM and powering the HST, see the *HST-3000 Base Unit User's Guide*.

The following procedure describes how to launch an application.

To launch an application

1 Power on the HST-3000.

The Ethernet Measurements menu appears, listing the applications for testing 10/100/1G electrical circuits.



If necessary, use the soft keys to display additional Ethernet Measurements menus that allow you to select each of the applications listed in Table 9 on page 26.

2 Select an application for the circuit you are testing.

A "*Please Wait ... Launching Test Application*" message appears briefly, and an icon appears that indicates which port you should use to connect to the circuit you are testing.

The message disappears, the HST launches the application, and a menu listing each of the test modes for the application appears.

3 Select a test mode for the application. One of the following occurs:

   – If you are selecting the test mode the first time for an application, the HST immediately configures the test, and the Summary Results screen appears.

   – If you are selecting a different test mode for an application, a "*Please Wait ... Reconfiguring Test*" message appears briefly, the message disappears, the HST configures the test, and then the Summary Results screen appears.

4 To review or change the current test settings, press the **Configure** navigation key.

   The Summary Settings menu appears, listing each of the key settings required to run your test.

   – If the settings meet your test requirements, and if you do not need to change any of the settings on the other configuration menus, press **Home** to return to the Results display, and then press the **Restart** soft key to clear statistical and historical results and restart the test.

   – If you need to change the settings, proceed to "Specifying test mode and network visibility settings" on page 30 and "Specifying basic test settings" on page 35.

For information about purchasing options for the HST-3000, contact your JDSU representative or your local JDSU sales office. You can also contact JDSU through the company web site, www.jdsu.com.

Specifying test mode and network visibility settings

Before testing, you should select the test mode for your application, specify a unit identifier, and specify additional settings that impact the instrument and certain test features during

testing.Figure 15 shows the Test Mode menu,.

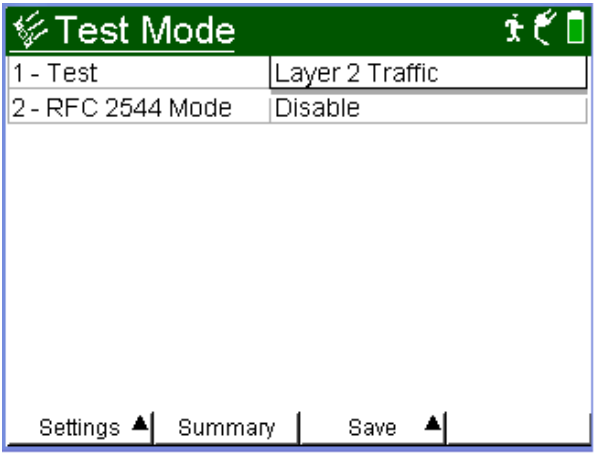


Figure 15 Test Mode Settings (Layer 3)

Figure 16 shows the Network Visibility settings.

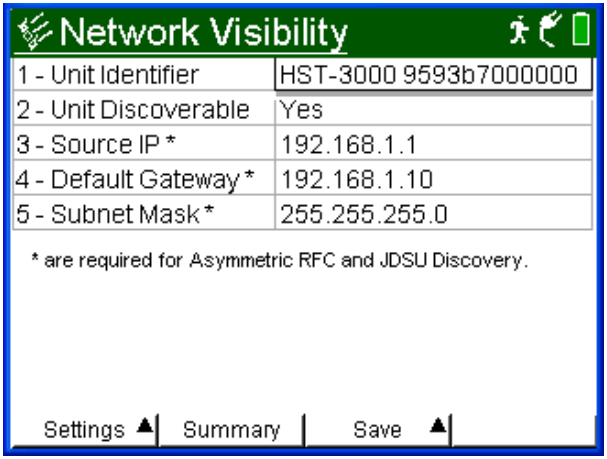


Figure 16 Network Visibility settings (Layer 2)

To specify test mode and network visibility settings

1 Launch an application (see "Launching an application" on page 28).

The HST launches the application, and the Summary Results screen appears.

2 Press the **Configure** navigation key, then use the right arrow key to display the Test Mode menu and specify the following:

Setting	Parameters
Test	Use this setting to select the test for the application that you launched.
Res. Precision	Select 3, or 4.
Result Unit	Select one of the following: – Mbps – Kbps – Auto. Select Auto to automatically determine the result unit. If the measurement is less than or equal to 1 Mbps, the result is presented in Kbps. If the result is higher than 1 Mbps, the result is presented in Mbps.

Setting	Parameters
RFC 2544 Mode	Select one of the following: – Disable. Select Disable if you do not intend to run RFC 2544 tests while running the current application. – Symmetric. Select Symmetric if you intend to run the standard symmetric test because the uplink and downlink speeds on the circuit you are testing are the same. – Asym Upstream. Select Asym Upstream if you intend to run the asymmetric test upstream only. – Asym Downstream. Select this if you intend to run the asymmetric test downstream only. – Asym Combined. Select this if you intend to run the asymmetrical test in both directions (upstream and downstream). For details, see Chapter 7 “Automated RFC 2544 Testing”.

3 Go to the Network Visibility menu, then specify the following:

Setting	Parameters
Unit Identifier	Use this setting to specify a unique ID for the instrument, which will be used during loop-back and multiple streams testing, and during the JDSU Discovery process. The factory-assigned ID appears by default.
Unit Discoverable	Select one of the following: – Yes. Allows other JDSU instruments on the same subnet with the JDSU Discovery feature to detect the instrument, and enables the discovery feature on your instrument. – No. Prevents other JDSU instruments from detecting the instrument, and disables the discovery feature on your instrument.
Source IP*[1] (Layer 2 Traffic only)	Enter the source IP address carried by all traffic generated by your unit.
Subnet Mask*[1] (Layer 2 Traffic only)	Enter the subnet mask.
Default Gateway*[1] (Layer 2 Traffic only)	Enter the default gateway address.

1. These settings only appear if you are running a Layer 2 Traffic test. They are required to run the Asymmetric RFC 2544 test, or to use the JDSU Discovery feature. If you are running layer 3 or layer 4 tests, the settings are specified on the IP Init configuration menu.

The settings are specified.

Specifying basic test settings

After you launch an application, you verify and specify test settings using the configuration menus. The following procedure describes how to access the test configuration menus and specify basic settings.

NOTE:

If you change settings while transmitting traffic, results will not reflect the true state of the circuit. Always stop traffic before changing settings.

To specify basic test settings

1 Launch an application and specify the test mode (see "Launching an application" on page 28).

The HST launches the application in the mode you specified, and the Summary Results screen appears.

2 Press the **Configure** navigation key.

The Summary Settings menu appears, listing the key settings for the application you launched. Figure 17 illustrates the settings for the Terminate 1G Optical Ethernet application when running a Layer 3 Traffic test.

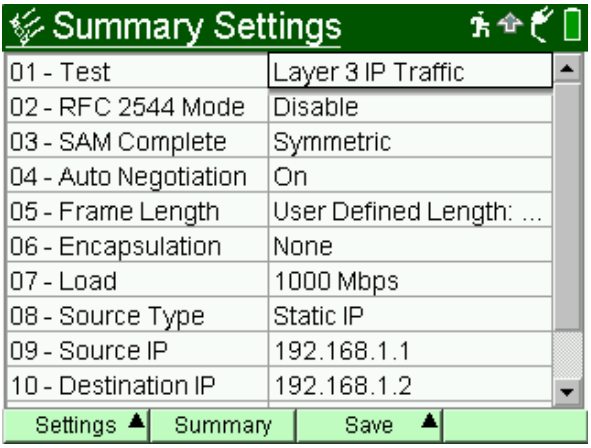


Figure 17 Summary Settings Menu

The settings and the values for the settings vary depending on the current application and test mode.

For example, if you launched a 10/100/1G Electrical application, and you are running the test in *Layer 2 Traffic* mode, the Error menu only allows you to specify whether you want to insert a single FCS error, or a burst of FCS errors into the traffic stream. If you are running the same test in *Layer 3 Traffic* mode, you can select FCS, IP Checksum, or Acterna Payload errors for insertion.

3 To change a setting, do the following:

a If the setting you need to change appears on the Summary Settings menu, proceed to step c.

b If the setting you need to change does not appear on the Summary Settings menu, use the left and right arrow keys on your keypad to scroll through the available configuration menus. For example, if you want to specify the quanta for pause frames, scroll to the Link Init configuration menu.

TIP:

If you know which menu the setting is on, you can also press the **Settings** soft key to select the menu.

c Press the number corresponding to the setting you want to change, and then select or type the value for the setting as appropriate.

If you type the value for a setting (such as a Destination IP address), **OK** stores the new value. **Cancel** returns you to the configuration menu without storing the new value.

Basic test settings are specified. For detailed instructions on configuring the remaining settings, see one of the following chapters:

– Chapter 2 “Running Cable Diagnostics”
– Chapter 3 “Ethernet Testing”
– Chapter 4 “IP Testing”

– Chapter 5 “TCP/UDP Testing”
– Chapter 6 “Multiple Streams Testing”

Saving test configurations

After you configure a test, you can save the configuration to use as a template for future tests.

To save a test configuration

1 Configure a test (see “Configuring your test” on page 25).

2 Press the **Save** soft key, and then do one of the following:

– To create a new configuration, select **Save Config**, type a name for the configuration using up to twenty characters, and then select **OK**. You do not need to enter a file extension.

– To overwrite an existing configuration, select **Overwrite Config**, use the arrow keys to highlight the configuration you want to overwrite, and then press **OK**.

The configuration is saved.

Deleting test configurations

You can delete test configuration at any time.

To delete a test configuration

1 Press the **Save** softkey, and then select **Delete Config**.

2 Use the arrow keys to highlight the configuration you want to delete, and then press **OK**.

The configuration is deleted.

Loading a configuration

You can load a saved configuration, and then use it as a template for your current test. After loading the configuration, you can change settings to meet your current requirements.

To load a configuration

1 Press the **Save** soft key, and then select **Load Config**.

A list of saved configurations appears.

2 Select the configuration you want to load, and then press **OK**.

The configuration is loaded.

Estimating throughput on the circuit

The instrument now automatically estimates the theoretical throughput for each layer when you configure a constant load of traffic for all single stream tests except Mac-in-Mac. This estimate represents the throughput that you would hope to attain given ideal circumstances on the circuit.

To estimate the ideal throughput on a circuit

1 If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):

- "Selecting a layer 2 test" on page 46
- "Selecting a layer 3 IP test" on page 120
- "Selecting a layer 4 TCP/UDP test" on page 165

2 Press the **Configure** navigation key.

A configuration menu appears.

3 Use the left and right arrow keys to go to the Traffic configuration menu.

4 Configure a constant load of traffic (see "Transmitting a constant load" on page 57).

The instrument calculates the ideal throughput, and displays it in a table under the settings.

Restarting tests

Pressing the **Restart** soft key (at the bottom of the Results display) clears statistical and historical results and restarts your test.

Viewing test results

After you start a test, the Summary category appears showing an overview of the test results. You can view other results by selecting a different test result category.

To view test results

1. Configure and run a test.
2. Press the **Display** soft key, and then do one of the following:
   - Use the arrow keys to highlight a result category, and then press **OK**.
   - Press the number corresponding to the category.

     If a leading zero appears in front of a number, you must also enter the leading zero. For example, if you want to display the third category listed on a menu with more than ten categories, press “0”, and then “3”. If you want to display the eleventh category on the menu, press “1” twice.

   The test results for the category appear.

For descriptions of test results, see “Test Results” on page 257.

Clearing history results

The following procedure describes how to clear history results in the LED and Summary categories.

To clear history results

1. Configure and run a test.
2. Press the **Home** button.
3. Press the **Results** soft key.
4. Select **Clear History**.

The HST-3000 clears any history results in the LED and Summary categories. Statistical results are not cleared and continue to accumulate.

Instrument settings and user preferences

For information about the following HST-3000 features, see the *HST-3000 Base Unit User's Guide*:

- Powering the HST-3000
- Changing instrument and preference settings, such as date and time format, port settings, sound, and screen settings
- International settings
- Updating your HST software
- Remote operation
- Web browser
- VT100 emulation
- Transferring files using FTP
- Managing files

Running Cable Diagnostics

2

This chapter provides information on running cable diagnostics using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

About cable diagnostics

Before testing 10/100/1000 electrical Ethernet, IP, or TCP/UDP, you can use the HST-3000 with an Ethernet SIM to examine the state of the cables used to transmit 10/100/1000 electrical signals. Typically this involves out-of-service testing to determine the link status, the pair status of each MDI or MDI-X pair, the pair assignments for 1000M links, the polarity for each MDI pair, and the pair skew. You can also use the HST to verify whether or not Power over Ethernet (PoE) service is available on the link (per IEEE 802.3af). Finally, if the link is inactive, you can use the HST to determine the nature of the fault.

You must use the R/T 1 port on the Ethernet SIM when running cable diagnostics.

Running cable diagnostics

Running cable diagnostics involves connecting to the link, selecting the Cable Diagnostics application, and then observing the measurements provided in the Cable Status results category.

To run cable diagnostics

1. Power on the HST-3000.

   The Ethernet Measurements menu appears, listing the applications for 10/100/1G electrical Ethernet testing.

2. Select the Cable Diagnostics application (see “Launching an application” on page 28).

   A “Please Wait” screen appears, indicating you should connect the HST to the link using the R/T 1 port on the left side of the Ethernet SIM, then the Cable Status results appear, indicating that the link is inactive and results are unavailable.

3 Connect the HST-3000 to the link.

4 Use the **Restart** soft key to start the diagnostics.

5 Observe the cable results and measurements.

Cable diagnostics are complete.

Viewing cable measurements

Cable measurements appear automatically on the Cable Status results display (see Figure 18).

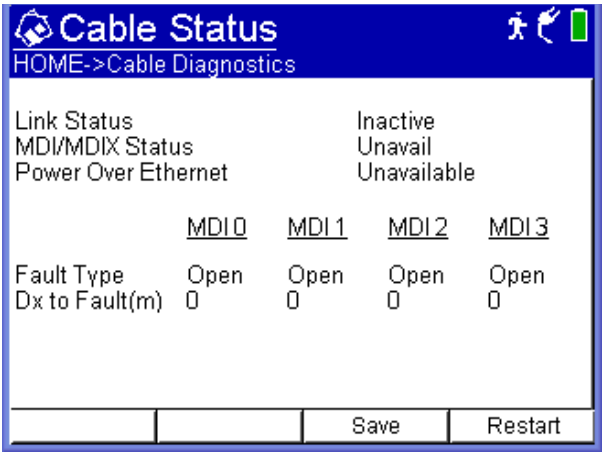


Figure 18 Cable Status results display

For detailed descriptions of each of the measurements, see “Cable Status results” on page 262.

Ethernet Testing

3

This chapter provides step-by-step instructions for testing Ethernet service using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

About Ethernet testing

Using the HST-3000 with an Ethernet SIM, you can turn up and troubleshoot Ethernet service on point-to-point unswitched and switched networks by verifying connectivity, measuring throughput, and verifying that quality of service statistics conform to those specified in a customer's Service Level Agreement.

Selecting a layer 2 test

When testing Ethernet service, you must select a layer 2 test for your application.

To select the test

1 Do one of the following:

- If you haven't already done so, launch the application for the circuit you are testing (see "Launching an application" on page 28), and then proceed to step 2.
- If you already launched your application and selected a test, but you want to change the test, go to the Test Mode menu, and then select the Test setting.

  A list of tests for the application appears.

2 Highlight and select one of the following:

- **Layer 2 Traffic**. Select this test to transmit or analyze standard layer 2 traffic.
- **Layer 2 Patterns.** (1G optical Ethernet applications only). Select this test if you want to stress the jitter and noise characteristics of Gigabit Ethernet components and systems by transmitting continuous random test

patterns (CRPAT), continuous jitter test patterns (CJPAT), or the compliant supply noise pattern (CSPAT).

– **J-Proof.** Also referred to as Layer 2 Transparency testing. Select this test if you want to verify that an Ethernet circuit can support a variety of control protocols (such as CDP, VTP, STP, and RSTP).

Discovering another JDSU test instrument

Before you begin testing, you can automatically detect other JDSU test instruments on the circuit and determine their capabilities.You can then optionally configure key parameters for your test automatically based on a discovered instrument's settings. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Initializing the link for Ethernet testing

Initializing an Ethernet link involves specifying the settings required to establish connectivity with another Ethernet device on a circuit (link), such as auto-negotiation, flow control, and speed and duplex settings (for 10/100 Ethernet traffic only). You can also enter the pause quanta for transmitted pause frames.

After specifying the link initialization settings, you are ready to connect the HST-3000 (or HST-3000s) to an access element on a circuit, and then turn the laser on (if you are testing 1G or 100M optical Ethernet).

– If you turned auto-negotiation ON, and another Ethernet device is on the circuit, the HST-3000 and the device automatically go through the auto-negotiation process. After auto-negotiation is complete, an Ethernet link is established, and idles are transmitted over the circuit.

– If you turned auto-negotiation OFF, the HST immediately transmits idles over the circuit.

To initialize an Ethernet link

1 If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):

– "Selecting a layer 2 test" on page 46

– "Selecting a layer 3 IP test" on page 120

– "Selecting a layer 4 TCP/UDP test" on page 165

– "Selecting a multiple streams test" on page 182

2 Press the **Configure** navigation key.

A configuration menu appears.

3 Use the left and right arrow keys to go to the Link Init configuration menu. Figure 19 illustrates the settings for 1G optical applications.

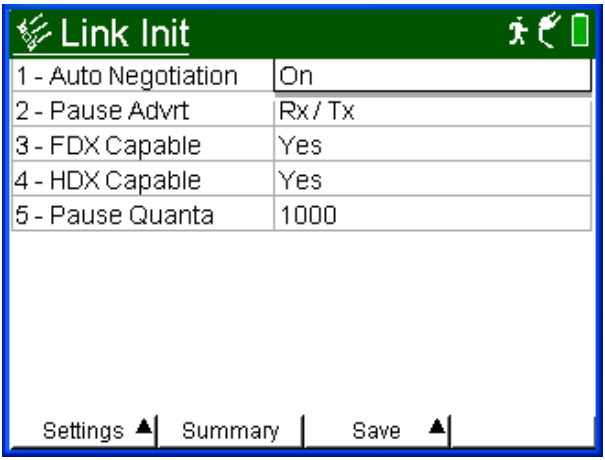


Figure 19 Link Init configuration menu

– If you selected 10/100/1G application, proceed to step 4.

– If you selected an optical 1G or 100M application, proceed to step 5.

4 If you selected 10/100/1G application, specify the following settings:

Setting	Parameters	Applicable
Auto Neg	– On – Off	Always **NOTE:** If you turn auto-negotiation on, flow control is also turned on automatically, and the Flow Control setting does not appear on the menu.
Flow Control	– On – Off	If Auto Neg value is Off
Speed (Mbps)	– 10 – 100 – 1000	– 10, 100 Always – 1000, If Auto Neg value is On
Duplex	– Half – Full	Always
Pause Quanta	– Enter a pause quanta ranging from 0 to 65535.	Always

5 If you selected an optical 1G or 100M application, specify values for the following settings:

Setting	Parameters	Applicable
Auto Neg	– On – Off	1G applications only
Flow Control	– On – Off	If Auto Neg is Off.
Pause Advrt	– No – Tx Only – Rx Only – Rx/Tx	1G applications, if Auto Neg is On
FDX Capable	– Yes – No	1G applications, if Auto Neg is On
HDX Capable	– Yes – No	1G applications, if Auto Neg is On
Pause Quanta	– Enter a pause quanta ranging from 0 to 65535.	Always

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button, and then do the following:

– If you are initializing a 1G or 100M optical Ethernet link, press the Action soft key, and then select **Laser On**.

– Verify that the Sync LED is green (indicating that the link is active).

– Display the Auto-Neg Stats results category to observe test results associated with link initialization.

Configuring layer 2 Ethernet tests

Before transmitting traffic over a link, you can specify settings that characterize the traffic and indicate the type of traffic load to transmit. You can also specify settings that filter received traffic for analysis.

Specifying frame characteristics

Before you transmit layer 2 traffic, you can specify the frame characteristics of the traffic, such as the frame type, payload (Acterna test frames or BERT patterns), frame length, and VLAN or Q-in-Q settings (if applicable).

You can also assign a user-defined MAC address to the unit. This allows the HST-3000 to emulate another device when transmitting traffic to verify that traffic with the device's MAC address passes through the network. The user-defined MAC address does not overwrite the unit's default, factory-assigned MAC address.

To specify frame characteristics for transmitted traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
   - "Selecting a multiple streams test" on page 182
2. Press the **Configure** navigation key.

   A configuration menu appears.

3 Use the left and right arrow keys to go to the Ethernet menu (see Figure 20).

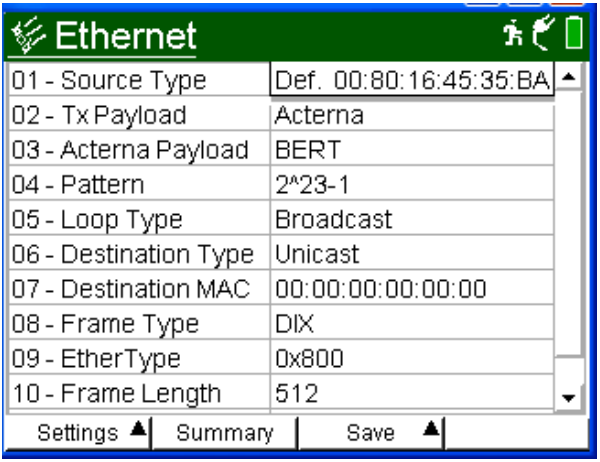


Figure 20 Ethernet configuration menu

4 Specify values for the following settings:

Setting	Parameters
Source Type	– Factory Default – User Defined Indicate whether you want traffic generated by the HST to carry the factory default MAC address, or a user defined address. If you specify User Defined, a Source MAC setting appears on the menu.
Source MAC	If you indicated that the Source Type was User Defined, specify the source MAC address for all traffic generated by the HST.
Tx Payload	– Acterna – BERT

Setting	Parameters
Acterna Payload	– BERT – Fill Pattern
Pattern (appears only if a BERT payload is selected in either the Tx Payload or Acterna Payload)	Select one of the following: – A predefined PRBS or fixed pattern. – User Defined, and then enter the pattern in hexadecimal format
Fill Pattern (appears only if a Fill Pattern payload is selected)	If you are transmitting a Fill Pattern in an ATP payload, specify the pattern in a hexadecimal format up to 64 bytes long.
Loop Type	– Unicast – Broadcast. Select Unicast to loop up a specific test instrument on the far end, or select Broadcast to loop up the first instrument on the network that responds. If you select Unicast, the Destination Type is also automatically set to Unicast.

Setting	Parameters
Destination Type	– Unicast - sends traffic to a single destination address and network device. – Multicast - sends traffic with a multicast address to a group of network devices. – Broadcast - sends traffic to all network devices on the link. **NOTE:** If you select Unicast, you can optionally use the Discover soft key to discover other instruments on the network, and then select the destination address for the device you want to transmit traffic to. For details, see "Using J-Connect to discover another JDSU test set" on page 21.
Destination MAC (appears only if you specified a Unicast or Multicast address type)	Type the address for Unicast or Multicast destinations. – If you specified Unicast as the address type, the left most byte in the address defaults to 00. – If you specified Multicast as the address type, the left most byte in the address defaults to 01.
Frame Type	– DIX – 802.3

Setting	Parameters
EtherType (DIX Frames only)	Type the protocol ID for the data in the frames using a 2 byte hexadecimal format. **NOTE:** When transmitting an Acterna payload, the EtherType is automatically set to x0800 and cannot be changed.
Frame Length	Select one of the following: – A predefined length. – Random, which sends frames with randomly generated, predefined RFC 2544 traffic lengths. – Undersized, and then specify the frame length. Undersized frames are not available when testing multiple streams. – User Defined, and then specify the frame length. – Jumbo Frame, and then specify the frame length.
Encapsulation	– None. – VLAN. If you select VLAN, be certain to specify the VLAN ID and Priority. – Q-in-Q. If you select Q-in-Q, be certain to specify the CVLAN (customer VLAN) and SVLAN (service provider VLAN) settings.

Setting	Parameters
VLAN (appears only if Encapsulation is VLAN)	– VLAN ID – User Priority
CVLAN (appears only if Encapsulation is Q-in-Q)	– CVLAN ID – User Priority
SVLAN (appears only if Encapsulation is Q-in-Q)	– SVLAN ID – User Priority – SVLAN TPID – SVLAN DEI Bit

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

The settings are specified for transmitted frames.

Configuring the traffic load

Before transmitting traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty, Ramp, or Flood) in 0.001% increments, beginning at 0.002%. The settings vary depending on the type of load.

NOTE:

If you configure the HST-3000 to transmit a constant, bursty, or ramped load of 100%, the unit is designed to transmit slightly less than 100% traffic (99.99% for 1G optical Ethernet and 10/100/1G electrical Ethernet) as a safeguard against overrunning network elements that can not support 100%. If you are certain the elements can support true 100% traffic, configure your unit to transmit a flood load (see “Transmitting a flooded load” on page 65).

Transmitting a constant load

With a **constant** load, the HST-3000 transmits frames continuously with a fixed bandwidth utilization. You can specify the load as a percent or a bit rate. See Figure 21.

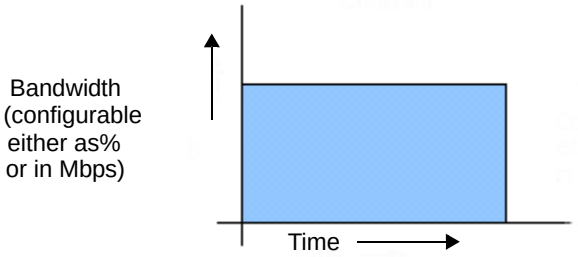


Figure 21 Constant traffic

When you setup a constant traffic load, you can specify the bandwidth as a percentage of the line rate or as a bit rate in Mbps.

To transmit a constant load of traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Use the left and right arrow keys to go to the Traffic configuration menu.

4 Specify values for the following:

Setting	Parameters
Load Type	Constant
Load Unit	– Bit Rate – Percent
Load (Mbps)	Enter the bandwidth to transmit in Mbps.
Load (%)	Enter the bandwidth as a percentage of the line rate.

The instrument estimates the theoretical throughput, and displays it in a table under the settings. The instrument will not estimate throughput if it is configured to transmit traffic with random frame sizes.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

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

Transmitting a bursty load

With a **bursty** load, the unit transmits frames at up to 100% bandwidth for a specific time interval, followed by no frame transmissions for a specific time interval. See Figure 22.

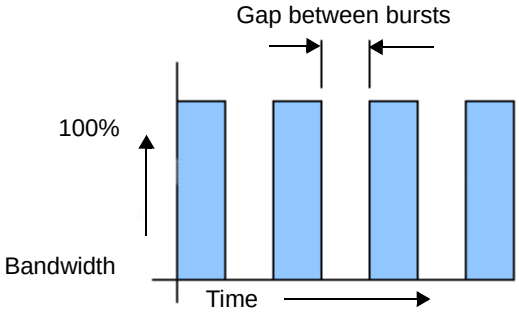


Figure 22 Bursty traffic

When you configure bursty traffic, you can specify the burst bandwidth as a percentage of the duty cycle, or by specifying the burst gap interval. If you specify the burst bandwidth as a percentage of the duty cycle, and then specify the number of frames per burst, the unit automatically calculates the burst gap for you.

To transmit a bursty load of traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Use the left and right arrow keys to go to the Traffic configuration menu.

4 Specify values for the following settings:

Setting	Parameters
Load Type	Burst
Burst Load Unit	– Interval – Percent
Duty Cycle (%) (if Burst Load Unit is Percent)	Enter the load to transmit during bursts as a percentage of the line rate.
Time Unit (if Burst Load Unit is Interval)	Select the unit of time for the burst and gap/idle times you will specify: – sec – msec – usec – nsec
Burst Time (if Burst Load Unit is Interval)	Enter the time to transmit each burst of traffic.
Gap/Idle Time (if Burst Load Unit is Interval)	Enter the time between each burst of traffic. The valid range for this setting adjusts depending on the Burst Time that you entered, to ensure that the duty cycle is at least 0.001%.

Setting	Parameters
Frames/Burst (if Burst Load Unit is Percent)	Select a predefined value, or select User Defined if you want to enter the number of frames using the keypad. Each burst of traffic will contain this many frames: – 16 – 64 – 256 – 1024 – User Defined
User Frms/Burst (if Frames/Burst is User Defined)	Enter the number of frames to transmit in each burst of traffic.
Burst Type	To transmit a continuous series of bursts, select: – Continuous To transmit a fixed number of burst, and then stop transmitting traffic, select: – Fixed
No. of Bursts (if Burst Type is Fixed)	Specify the number of bursts of traffic to transmit.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

The unit is configured to transmit a bursty load of traffic.

Transmitting a ramped load

With a **ramped** load, the HST-3000 automatically increases the load by the load step at the time intervals you specify as a load time. After the interval expires, the bandwidth is increased by the percentage specified and the process is

repeated. This allows you to easily verify the maximum throughput of a link. See Figure 23.

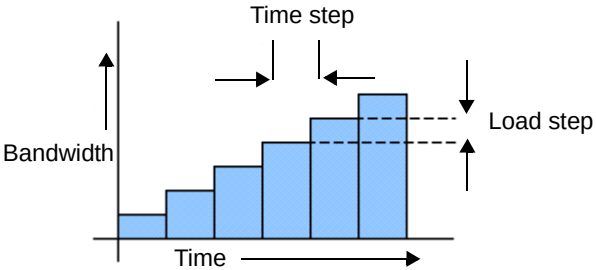


Figure 23 Ramped traffic

You can also specify criteria to tell the unit to stop incrementing the ramp if errored, dropped, or pause frames are detected in a load step.

If you want to stop incrementing a ramp when the unit detects dropped frames, be certain to configure your unit to transmit an Acterna payload, and loop the far-end device back to the traffic originating unit. Acterna frames carry a sequence number which the unit uses to determine whether frames were dropped.

NOTE:

When transmitting ramped traffic, **Restart** will not interrupt the ramp.

To transmit a ramped load of traffic

1 If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165

2 Press the **Configure** navigation key.

   A configuration menu appears.

3 Use the left and right arrow keys to go to the Traffic configuration menu.

4 Specify values for the following settings:

Setting	Parameters
Load Type	Ramp
Time Step(Sec)	Enter the time each step is transmitted in seconds.
Load Step(%)	Enter the percentage of the total bandwidth each step will be incremented.
Stop Load(Err'd)	If you want to stop the ramp from incrementing when errored frames are detected, select: – Yes If you do not want the ramp to stop incrementing, select: – No
# Errored Frames (if Stop Load(Err'd) is Yes)	Enter the number of errored frames that must be detected before the unit stops incrementing the ramp.

Setting	Parameters
Stop Load(Drop)	If you want to stop the ramp from incrementing when frames are dropped, select: – Yes If you do not want the ramp to stop incrementing, select: – No
# Drop Frames (If Stop Load(Drop) is Yes)	Enter the number of frames that must be dropped before the unit stops incrementing the ramp.
Stop Load(Pause)	If you want to stop the ramp from incrementing when pause frames are detected, select: – Yes If you do not want the ramp to stop incrementing, select: – No
# Pause Frames (If Stop Load(Pause) is Yes)	Enter the number of pause frames that must be detected before the unit stops incrementing the ramp.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

The unit is configured to transmit a ramped load of traffic.

Transmitting a flooded load

With a **flooded** load, the module transmits traffic at 100% of the interface rate.

> **NOTE:**
>
> True 100% traffic transmission may overrun certain network elements if the elements can not support it. If you are certain the elements can support 100% transmission, configure a flood load of traffic; otherwise, configure a constant load of traffic at 100% (see "Transmitting a constant load" on page 57).

To transmit a flooded load of traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Use the left and right arrow keys to go to the Traffic configuration menu, and then specify **Flood** as the Load Type.
4. If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

The unit is configured to transmit flooded traffic.

Filtering received traffic using layer 2 criteria

Before transmitting traffic, you can specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be analyzed and reported in the test result categories for layer 2 traffic.

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

TIPS:

- If you want to analyze all received traffic, verify that the Ethernet Filter settings are all **Don't Care**.
- If you want to use the JDSU Discovery feature to populate the filter, be certain to **Enable** the filter.

To filter received traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select your test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.

3 Use the left and right arrow keys to go to the Ethernet Filter configuration menu (see Figure 24).

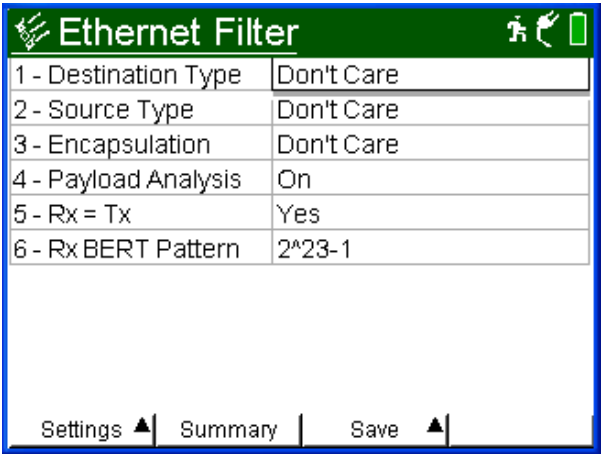


Figure 24 Ethernet Filter configuration menu

4 Specify the values for the following settings:

Setting	Parameters
Destination Type	To analyze frames for a specific type of destination address, select one of the following: – **Unicast** – **Multicast** – **Broadcast** If you do not want to filter frames based on the destination address type, select **Don't Care**.
Destination MAC (if Destination Type is Unicast or Multicast)	To analyze frames sent to a specific Unicast or Multicast address, enter the destination address.

Setting	Parameters
Source Type	– To analyze frames sent from a specific address, select **Unicast**. – If you do not want to filter frames sent from a specific address, select **Don't Care**.
Source MAC (if SourceType is Unicast)	To analyze frames sent from a specific address, enter the source address. **NOTE:** You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the source address for the device you want to filter traffic for. For details, see "Using J-Connect to discover another JDSU test set" on page 21.
Payload Analysis	– To analyze traffic with a BERT or Acterna payload, select **On**. – If you do not want to analyze traffic based on the type of payload (you want the unit to monitor live traffic), select **Off**.

Setting	Parameters
Rx BERT Pattern (if Payload Analysis is On)	To analyze frames with a specific BERT pattern, select one of the following: – **2^23-1** – **Inv 2^23-1** – **2^31-1** – **Inv 2^31-1** – **All Ones** – **All Zeros** – **User Defined**, and then enter the pattern.
Rx = Tx (if Tx Payload on Ethernet configuration menu is BERT)	– To analyze frames with the same payload specified for transmitted frames, select **Yes**. – If you want to analyze frames with a different payload, select **No**.
User Payload (if Rx BERT Pattern is User Defined)	Enter the pattern carried in the traffic you are analyzing.

Setting	Parameters
Encapsulation	– To analyze frames that are not tagged, select **None**. – To analyze VLAN tagged frames, select **VLAN**, and then specify the VLAN Tag and User Priority for the tagged frames. – To analyze Q-in-Q tagged frames, select **Q-in-Q**, and then specify the CVLAN Tag and User Priority, and the SVLAN settings for the tagged frames. – If you do not want to filter frames based on their tagged status, select **Don't Care**.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Summary Results screen.

The unit is configured to analyze received traffic satisfying the layer 2 filter criteria.

NOTE:

When running layer 3 IP tests, you can also specify layer 3 filter criteria (see "Filtering received traffic using layer 3 criteria" on page 142). When running layer 4 TCP/UDP tests, you can specify layer 2, layer 3, and layer 4 filter criteria (see "Filtering received traffic using layer 4 criteria" on page 175).

Transmitting layer 2 traffic

After you configure the layer 2 settings, you are ready to transmit traffic over the link.

To transmit traffic

1. If you haven't already done so, launch the terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Traffic test (see "Selecting a layer 2 test" on page 46).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Configure the HST for your test (see "Configuring layer 2 Ethernet tests" on page 51).
4. Press the **Home** button to return to the Summary Results screen.
5. Press the **Action** soft key again, and then select one of the following:
   - **Start Traffic** (if you configured a constant, bursty, or flooded load).
   - **Start Ramp** (if you configured a ramped traffic load).

The HST-3000 transmits traffic over the link.

Using J-Proof to verify layer 2 transparency

Using the J-Proof application, you can verify that an Ethernet circuit can support a variety of control protocols (such as CDP, VTP, STP, and RSTP), irrespective of the underlying transport method.

When you verify layer 2 transparency, the receiving test instrument loops back all test frames, including control frames and frames carrying a broadcast or multicast address. To do

so, you must then specify the settings for the outgoing loop-up frame. When the receiving instrument receives the loop-up frame, it is automatically placed into transparent loopback mode, and it returns all received test frames. You do not need to specify filter settings on the receiving instrument.

When initiating a loopback from the traffic originating instrument, you can send the loop-up frame to a specific test instrument (by specifying the appropriate unicast destination address), or you can send a broadcast loopup frame to loop-up the first test instrument that replies within the broadcast boundary.

When the test is completed, the far end instrument is automatically taken out of loop up mode.

To verify layer 2 transparency

1. If you haven't already done so, launch the terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the J-Proof test (see "Selecting a layer 2 test" on page 46).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Use the right arrow key to go to the Ethernet Loop Frame configuration menu, and then configure the outgoing loop frame by specifying the following:

Setting	Parameters
Source Type	– Factory Default – User Defined Indicate whether you want traffic generated by the HST to carry the factory default MAC address, or a user defined address. If you specify User Defined, a Source MAC setting appears on the menu.

Setting	Parameters
Source MAC (if Source Type is User Defined)	If you indicated that the Source Type was User Defined, specify the source MAC address for all traffic generated by the HST.
Loop Type	– Unicast – Broadcast. Select Unicast to loop up a specific test instrument on the far end, or select Broadcast to loop up the first instrument on the circuit that responds. If you select Unicast, the Destination Type is also automatically set to Unicast.
Frame Type	– DIX – 802.3
EtherType (DIX Frames only)	Type the protocol ID for the data in the frames using a 2 byte hexadecimal format.

Setting	Parameters
Encapsulation	– To transmit a loop frame that is not tagged, select **None**. – To transmit a VLAN tagged loop frame, select **VLAN**, and then specify the VLAN Tag and User Priority. – To transmit a Q-in-Q tagged loop frame, select **Q-in-Q**, and then specify the CVLAN Tag and User Priority, and the SVLAN settings for the tagged frames.

4 Use the right arrow key to go to the J-Proof Frame configuration menu, and then configure the outgoing transparency frames by specifying the following**:**

Setting	Parameters
Frame Number	Specify the number for the frame you are currently configuring. For example, if you are configuring the fifth transparency frame stored on your instrument, specify “5:. “Enabled” appears in parentheses to the right of the number if the frame is selected for transmission; “Disabled” appears if it is not selected. You can configure and transmit up to 20 types of transparency frames.

Setting	Parameters
Name	You can optionally specify a name for each transparency frame type using up to 20 characters.
Protocol	Select the control protocol carried in this type of transparency frame., or select User. If you select User, be certain to specify the frame type (DIX, 802.3-LLC, or 802.3-SNAP).
Type	The appropriate frame type for the protocol is set automatically. For example, if you set the protocol to STP; the type is automatically set to 802.3-LLC, and the DSAP, SSAP, and CTL values are set as appropriate. If you specified a User protocol, be certain to specify the frame type too.

Setting	Parameters
Encapsulation	– To transmit frames that are not tagged, select **None**. – To transmit VLAN tagged frames, select **VLAN**, and then specify the VLAN Tag and User Priority. – To transmit Q-in-Q tagged frames, select **Q-in-Q**, and then specify the CVLAN Tag and User Priority, and the SVLAN settings for the tagged frames.
Length	Specify the frame size.
Count	Specify the number of frames you want to trasnsmit.
Rate (fr/sec)	Enter the rate at which you want to transmit the frames.
Timeout (msec)	Enter the number of milliseconds the instrument will wait to receive the looped back frame before stopping transmission of frames.

Setting	Parameters
Destination Type	To transmit frames to a specific type of destination address, select one of the following: – **Unicast** – **Multicast** – **Broadcast** Most protocols only allow you to send traffic to a multicast address; however, if you specified a user-defined protocol, you can select a Unicast or Broadcast address type.
Destination MAC (if Destination Type is Unicast or Multicast)	To transmit frames to a specific Unicast or Multicast address, enter the destination address.
EtherType (DIX frames only)	Type the protocol ID for the data in the frames using a 2 byte hexadecimal format.
LLC (802.3 frames only)	Displays the DSAP, SSAP, and CTL values for the protocol that you specified.

5 Enable the transparency frames that you want to transmit by doing the following:

a Press the **Home** button to return to the Summary Results screen.

b Use the right arrow key to go to the J-Proof Frame List configuration menu.

c Scroll to and highlight the transparency frame that you want to enable using the up and down arrow keys.

d Press the pound key (#).

e Repeat step c and step d for any additional frames you want to enable.

6 After you configure the traffic originating instrument, verify that the Encapsulation setting for the Ethernet filter is set to Don't Care on the receiving instrument. This ensures that traffic will be looped back.

7 Press the **Home** button to return to the Summary Results screen.

8 Press the **Action** soft key again, and then select **Start Frame Sequence**.

The HST-3000 transmits traffic over the link.

Observing J-Proof (transparency) results

After transmitting and looping back test frames, you can observe results associated with transparency testing in the J-Proof results category.

To observe transparency results

– On the Summary Results screen, press the **Display** soft key, use the arrow keys to highlight the J-Proof result category, and then press **OK**.

Counts of transmitted and received frames, and the pass/fail status appears for each type of transparency frame transmitted.

Transparency results are displayed. For detailed result descriptions, refer to "J-Proof (transparency) results" on page 279.

NOTE:

When you run layer 2 transparency tests, Payload Analysis is automatically turned OFF. If you return to a layer 2 traffic test, Payload Analysis is turned back ON.

BER testing

If you are testing on an Ethernet network, when you perform an end-to-end test you can transmit BERT patterns in the frame payload to determine the ratio of erroneous bits to the total bits received.

To transmit a BERT pattern

1. If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Traffic test (see "Selecting a layer 2 test" on page 46).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Press the **Configure** navigation key.

   A configuration menu appears.
4. Use the left and right arrow keys to go to the Ethernet configuration menu.
5. In Tx Payload, select a BERT payload, and then select the pattern to transmit in the payload (see "Specifying frame characteristics" on page 51).
6. *Optional*. If you intend to insert Bit Errors into the traffic stream, go to the Error configuration menu, and then verify that the error type is set to Bit (see "Inserting errors" on page 81).
7. If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Main screen.
8. Press the **Action** soft key again, and then select **Start Traffic** (if you configured a constant, bursty, or flooded load), or **Start Ramp** (if you configured a ramped traffic load).

9 Verify that the Data LED is green, indicating that frames have been detected.

10 *Optional*. If you want to insert bit errors, press the **Action** soft key again, and then select the action for error insertion.

The HST-3000 transmits traffic with the BERT pattern in the payload over the link. Results associated with BER testing appear in the BERT results category (see "L2 BERT Stats results" on page 305).

Measuring service disruption time

You can use two HST-3000's in an end-to-end test to measure the service disruption time resulting from a switch in service to a protect line.

To measure service disruption time

1 If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Traffic test (see "Selecting a layer 2 test" on page 46).

2 Initialize the link (see "Initializing the link for Ethernet testing" on page 47).

3 On the near end HST, do the following:

   a Configure your test (see "Configuring layer 2 Ethernet tests" on page 51).

   b Press the Home button to view the test results display.

   c If the unit on the far end is in local loopback mode, press the **Action** soft key, and then select **Start Traffic**.

d Press the Action soft key again, and then clear the service disruption time by selecting **Reset Svc Disruption**.

4 Initiate the switch to the protect line.

The HST-3000 measures service disruption time, and displays the measurement as the `Service Disrupt` result in the Statistics category.

Inserting errors

You can use the HST-3000 to insert errors when you perform end-to-end and loopback tests.

To insert errors

1 If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below).

- "Selecting a layer 2 test" on page 46
- "Selecting a layer 3 IP test" on page 120
- "Selecting a layer 4 TCP/UDP test" on page 165
- "Selecting a multiple streams test" on page 182

2 Initialize the link (see "Initializing the link for Ethernet testing" on page 47).

3 If you are inserting pause frames into layer 3 or layer 4 traffic, establish an IPoE connection or a PPPoE session:

- If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
- If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.

4 Press the **Configure** navigation key.

A configuration menu appears.

5 Use the left and right arrow keys to go to the Error configuration menu.

6 Specify the error settings:

Error Type	Layer 2	Layer 3 IPv4	Layer 3 IPv6	Layer 4	Insertion Style
Bit[a]	Yes	N/A	N/A	N/A	– Single – Burst[b]
FCS	Yes	Yes	Yes	Yes	– Single – Burst[b]
Code Violations	Yes	Yes	Yes	Yes	– Single – Rate[c]
IP Checksum	N/A	Yes	No	Yes	– Single – Burst
TCP/UDP Checksum	N/A	N/A	N/A	Yes	– Single – Burst
Acterna Payload[d]	No	Yes	Yes	Yes	– Single – Burst

a. If you configured the unit to transmit a BERT payload, you can insert bit errors into the traffic stream.

b. If you specify Burst as the Insertion Style, a Burst Quantity setting appears, and you must specify the number of errors to insert in the burst.

c. If you specify Rate as the Insertion Style, an Insertion Rate setting appears, and you must specify the rate for error insertion.

d. If you configured the unit to transmit an Acterna payload, you can insert Acterna Payload errors into the traffic stream. Acterna Payload errors are Acterna frames that have an invalid or incorrect payload checksum.

7 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.

8 If you are inserting FCS, IP Checksum, Layer 4 Checksum, or Acterna Payload errors, press the Action soft key, then select one of the following:

   – **Start Traffic** (if you configured a constant, bursty, or flooded load).

   – **Start Ramp** (if you configured a ramped traffic load).

   You do not need to start traffic before inserting Code Violations.

9 To insert the errors, press the Action soft key, and then select the appropriate option for error insertion. For example, if you configured the unit to insert a burst of FCS errors, select **Insert Burst FCS Error**.

Errors are inserted into the traffic stream.

Inserting pause frames

You can use the HST-3000 to insert pause frames when you perform end-to-end and loopback tests. If you are testing 10/100/1G electrical Ethernet, your unit must be configured for full duplex (FDX) traffic.

To insert pause frames

1 If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):

   – "Selecting a layer 2 test" on page 46

   – "Selecting a layer 3 IP test" on page 120

   – "Selecting a layer 4 TCP/UDP test" on page 165

   – "Selecting a multiple streams test" on page 182

2 Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.

3 If you are inserting pause frames into layer 3 or layer 4 traffic, establish an IPoE connection or a PPPoE session:
   – If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   – If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.

4 Press the **Configure** navigation key.

   A configuration menu appears.

5 Use the left and right arrow keys to go to the Link Init menu, and then specify the quanta to be carried by the transmitted pause frames.

   To determine the pause duration, the receiving device performs the following calculation:
   – **10 Mbps electrical:** Quanta x 51.2 µs
   – **100 Mbps electrical:** Quanta x 5.12 µs
   – **1000 Mbps electrical and 1 GigE optical:** Quanta x 512 ns

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.

7 Press the **Action** soft key, and then select the option for pause frame insertion.

Pause frames are inserted into the traffic stream.

Configuring and viewing pause capabilities on Electrical Ethernet networks

When testing 10/100/1000 Electrical Ethernet networks, pause capabilities can be configured and those capabilities can be viewed. **NOTE:** These capabilities already exist in the Optical application, but have been added to the Electrical application.

Configuring pause capabilities

On the Link Init setup page, the **Pause Advrt** setting has been added. If Auto Negotiation is On, use Pause Advrt to configure the pause capabilities to be advertised during auto negotiation. Select **Neither** direction, **Tx Only**, **Rx Only**, or **Rx/Tx** (both).

Viewing pause capabilities

On the Auto-Neg Stats result menu, two results have been added: Pause Capable and Flow Control.

– **Pause Capable** indicates the advertised pauses capabilities of the Ethernet link partner.

Flow Control indicates the flow control (On/Off) on the near-end unit, based on the negotiated pause capabilities with the link partner.

Transmitting patterns

Using the HST-3000, you can stress the jitter and noise characteristics of Gigabit Ethernet components and systems by transmitting continuous random test patterns (CRPAT), continuous jitter test patterns (CJPAT), and the compliant supply noise pattern (CSPAT).

To transmit patterns

1. If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Patterns test (see "Selecting a layer 2 test" on page 46).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Press the **Configure** navigation key.

   A configuration menu appears.
4. Use the left and right arrow keys to go to the Patterns menu.
5. Select one of the following patterns:

Pattern	Emulates
CRPAT	A worst case scenario for deterministic jitter by transmitting frames with a broad spectral content.
CJPAT	Stress the timing margins in the received eye by exposing the data sampling circuits to large systematic phase jumps.
CSPAT	Emulate a worst case scenario for power supply noise within network transceivers.

6. If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.
7. To insert the pattern, press the **Action** soft key, and then select **Start Pattern**.

The pattern is transmitted.

Loopback testing

Loopback testing allows you to transmit Ethernet, IP, or TCP/UDP traffic from one HST-3000 (or another JDSU Ethernet test set), and then loop the traffic back through a second unit on the far end of a circuit.

When configuring a loopback test, you can now select a Unicast loopback type to loop up a specific test instrument on the far end, or a Broadcast loopback type to loop up the first instrument on the network that responds.

Using the Local Loopback feature

You can manually perform a local loopback by selecting the LLB action on the far end unit to loop frames back to the traffic originating HST.

The loopback unit always uses the labels specified for the transmitted traffic; therefore:

– If your near-end unit is in LLB mode and is configured to transmit traffic with a second MPLS label, but the unit's link partner is configured to transmit traffic with a single label, the out of sequence and lost frames counts reported by the module's link partner may increment if the incoming frame rate is too high.
– If your near-end module is in LLB mode, and is configured to transmit traffic with a single MPLS label, but the module's link partner is configured to transmit traffic with more than one label, the near-end module's receive bandwidth utilization will exceed its transmit bandwidth utilization.

NOTE:

You can not start an RFC script, or generate traffic when your instrument is in LLB mode. Your instrument simply loops received traffic back to the source test instrument.

To manually perform a local loopback

1. If you haven't already done so, launch the Terminate or Multi-Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
   - "Selecting a multiple streams test" on page 182
2. Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47).
3. If you are looping back layer 3 or layer 4 traffic, establish an IPoE connection or a PPPoE session:
   - If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   - If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124 (single stream tests only).
4. Configure the near end HST for your test. Depending on the test you selected, see:
   - "Configuring layer 2 Ethernet tests" on page 51.
   - "Configuring layer 3 IP tests" on page 136.
   - "Configuring layer 4 traffic" on page 167.
   - "Enabling streams and specifying the traffic load" on page 183 and "Configuring traffic streams" on page 187
5. Press the Home button to view the test results display.
6. On the far end HST:
   a. If you are running a single-stream test, verify that the applicable filter settings are either disabled or set to **Don't Care**, or that they match the settings for the traffic transmitted from the near end HST.

If you are running a multiple-stream test, the filters are automatically configured for you and can not be changed.

b Press the **Action** soft key, select **Loop,** and then select **LLB** to put the unit in loop back mode.

7 On the near end HST, press the **Action** soft key, then select one of the following:

– **Start Traffic** (if you configured a constant, bursty, or flooded load).

– **Start Ramp** (if you configured a ramped traffic load).

When the far end HST 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.

– Swaps the destination and source MAC or IP address, and if applicable, port number for every frame or packet it receives.

– Transmits the traffic back to the unit on the near end.

Traffic is looped back to the local unit.

To loop down the far end HST:

1 On the near end unit, press the **Action** soft key, then select **Stop Traffic** or **Stop Ramp**.

2 On the far end unit, select **LLB**.

The unit is looped down.

Using the automatic loopback feature

You can perform an automatic loopback by selecting the Loop Up action button on the traffic generating HST. A confirmation message from the HST on the far end appears on the display of the near end HST informing you that the far end HST is in loopback mode.

When using the automatic loopback feature, the HST must be configured as follows:

– If you are looping back layer 2 traffic, the near end HST 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 are looping back layer 3 traffic, you must specify the source IP address for the HST on the far end of the circuit as the *destination* IP address for traffic transmitted by the near end HST. *Be certain to specify the same destination address (link-local or global) for the filter on the receiving unit and the traffic looped back by the unit on the far end*.
– If you are looping back layer 3 MPLS traffic, received frames are looped through to the transmitter after swapping the Destination and Source MAC addresses. The MPLS labels are replaced with the labels defined for the loopback unit before the frames are looped through to the transmitter of the loopback unit.
– If you are looping back layer 4 traffic, the destination port number for the near end HST *must be configured* with the source port number for the HST on the far end. After you issue the Loop Up command, and the near end unit receives a response from the unit on the far end indicating that the loop up was successful, the near end unit's ATP Listen Port is automatically set to the destination port number carried in the looped back traffic and cannot be changed. The far end unit's ATP Listen Port will also automatically be set to the destination port carried in the traffic it receives from the near end unit.
– You can optionally specify unit identifiers for each HST (for example, "Joe_s HST" and "Sam_s HST"). When the HSTs send confirmation messages to each other indicating the status of the loopback, the message will identify each HST using the identifier. For details on specifying a unit identifier for your HST, see "Specifying test mode and network visibility settings" on page 30.

To perform an automatic loopback

1. If you haven't already done so, launch the Terminate or Multi-Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   - "Selecting a layer 2 test" on page 46
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
   - "Selecting a multiple streams test" on page 182
2. Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.
3. If you are looping back layer 3 or layer 4 traffic, establish an IPoE connection or a PPPoE session:
   - If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   - If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124 (single stream tests only).
4. Configure the near end HST as appropriate for your test. See:
   - "Configuring layer 2 Ethernet tests" on page 51.
   - "Configuring layer 3 IP tests" on page 136.
   - "Configuring layer 4 traffic" on page 167.
   - "Enabling streams and specifying the traffic load" on page 183 and "Configuring traffic streams" on page 187.
5. Press the Home button to view the test results display.
6. If you are looping back multiple streams of TCP/UDP traffic, on the far end HST, specify a listen port for each enabled stream that matches the destination port in the corresponding stream received from the near end HST. See "Configuring traffic streams" on page 187.

7 On the near end HST, do one of the following:
   – If you are looping back layer 2 traffic, proceed to step 8.
   – If you are looping back layer 3 or layer 4 traffic, specify the far end HST's source IP address as the destination IP address.

8 Press the **Action** soft key, select **Loop,** and then select **Loop Up** to put the far end unit in loop back mode. The following occurs:
   – A confirmation message appears on the display of the near end unit indicating that the loopback was successful.
   – If the layer 4 loopback confirmation message appeared, the ATP listen port (or ports for multiple streams) on the near end are automatically populated.
   – If the layer 4 loopback at the far end was successful, and you are looping back traffic using a single stream application, the ATP listen port on the far end is automatically populated.

9 Press the **Action** soft key a second time, then select one of the following:
   – **Start Traffic** (if you configured a constant, bursty, or flooded load).
   – **Start Ramp** (if you configured a ramped traffic load).

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

To loop down the far end HST:

1 On the near end unit, press the **Action** soft key, 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 on the near end unit indicating that the loop down was successful.

Monitoring Ethernet traffic

You can monitor and analyze 10/100/1G electrical or 1 G optical layer 2 traffic by selecting the MON / THRU application for the circuit you are testing.

To monitor Ethernet traffic

1. If you haven't already done so, launch the Mon / Thru application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Traffic test (see "Selecting a layer 2 test" on page 46).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Press the **Configure** navigation key.

   A configuration menu appears.
4. Use the left and right arrow keys to go to the Test Mode configuration menu.
5. Specify **Monitor** or **Thru** as the Type (for an explanation of Monitor and Thru types, see "Test applications" on page 10).
6. If you want to filter the traffic, use the right arrow key to go to the Ethernet Filter configuration menu, then specify the filter criteria (see "Filtering received traffic using layer 2 criteria" on page 65).
7. If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Main screen.

The HST monitors and analyzes received traffic. If you are testing in Thru mode, the HST passes received traffic through to the transmitter.

OAM service and link layer testing

You can position the instrument at various endpoints in a Maintenance Domain (MD) or Maintenance Association (MA) area to verify that no trunk problems occur per ITU-T Rec. Y.1731 and IEEE 802.1ag.

You can also use the HST to verify point-to-point link layer performance per IEEE 802.3ah.

When using your instrument for service layer OAM testing, you can do the following:

– Specify the Maintenance Domain (MD) level, Maintenance Entity Group (MEG) End Point IDs, and Maintenance Association (MA) IDs.
– Specify the Continuity Check Message (CCM) transmission rate.
– Specify the CCM and LBM address types (Unicast or Multicast) when running non-MAC-in-MAC applications.
– Specify thresholds for declaring a loss of continuity (LOC) if the number of consecutive missing CCM exceeds the number of messages expected within the calculated interval. This state may be used by Maintenance End Point devices to initiate a switch to a protect line.

When using your instrument for link layer OAM testing, you can also do the following:

– Discover an OAM peer, and automatically detect its capabilities.
– Indicate whether you want the instrument to serve in an active or passive role.
– Specify the Vendor OUI (Organizationally Unique Identifier) for the instrument.
– Indicate whether the instrument will advertise that it provides unidirectional support for failure detection, remote loopback, link events, and variable retrieval.
– Indicate whether you want the instrument to generate link faults, dying gasps, and critical events.

– Indicate whether you want the instrument to issue a remote loopback command to place its peer in loopback mode if the instrument is in active mode and its peer is capable of remote loopbacks.
– Retrieve MIB (Management Information Base) variables that provide management information about Ethernet variables from the instrument's OAM peer (if the peer is capable of providing MIB information).

When testing service and link OAM, you can observe results associated with your test in the OAM result category. For details, refer to "OAM results" on page 281.

Specifying OAM settings

Specifying OAM settings involves turning On the OAM tests that you want to perform (such as a service level continuity check, or a service layer LBM/LBR test), and, if you are testing the link layer, specifying defect and event parameters.

To specify OAM settings

1 If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 2 Traffic test (see "Selecting a layer 2 test" on page 46).

2 Initialize the link (see "Initializing the link for Ethernet testing" on page 47), and then specify the settings for the tests you intend to perform:

– For service layer CCM message settings, see step 3 on page 96.
– For service layer AIS settings, see step 4 on page 98.
– For service layer LBM/LBR settings, see step 5 on page 99.
– For service layer LTM/LTR settings, see step 6 on page 100.
– For link layer local configuration settings, see step 7 on page 101.
– For link layer defect settings, see step 8 on page 102.

3 Use the right arrow key to go to the S-OAM CCM configuration menu, and then specifying the following:

Setting	Parameters
Continuity Check	If you want to test continuity check messages, select **On**; otherwise, select **Off**, and proceed to step 4. **NOTE:** When you turn this On, CCMs will be transmitted continuously.
LOC Threshold	Specify the number of messages that must be received within the calculated interval.
CCM Rate	Specify the rate at which the instrument will transmit CCM messages. The instrument will transmit CCM messages at the rate specified; if it does not receive the number of messages back that you specify as the threshold within the calculated interval (CCM Rate times LOC Threshold (messages)), the instrument declares a loss of continuity (LOC). **NOTE:** 3.33 ms and 10 ms rates are not supported

Setting	Parameters
CCM Type (non MAC-in-MAC applications only)	Select one of the following: – **Unicast**. Select Unicast to send CCMs to its destination address. – **Multicast**. Select Multicast to send CCMs to a reserved multicast MAC address. This setting does not appear when running Mac-in-Mac applications.
MEG End ID	Specify the Maintenance Entity Group End Point ID for the instrument. The instrument encodes the ID that you specify in the CCMs that it sends to its peer.
Peer MEG End ID	Specify the Maintenance Entity Group End Point ID for the instrument's peer. The instrument uses the peer ID that you specify to indicate whether CCMs are detected with unexpected MEG End Point IDs.
MD Level	Specify the level for the Maintenance Domain (MD). The instrument uses the level that you specify to indicate whether CCMs for unexpected lower levels are detected in the traffic stream.

Setting	Parameters
Specify Domain	Select one of the following: – If you are testing per IEEE 802.1ag, select **Yes.** – If you are testing per ITU-T Rec. Y.1731, select **No**.
MD ID (Specify Domain must be yes)	If you indicated that you want to specify a domain ID, enter the ID using up to 22 characters. The instrument uses the ID that you specify to indicate whether CCMs are detected with different IDs.
MA ID	Specify the Maintenance Association ID, using up to 25 characters. The instrument uses the ID that you specify to indicate whether CCMs are detected with different IDs.

4 Go to the S-OAM AIS configuration menu, and then specifying the following:

Setting	Parameters
AIS State	If you want to test AIS, select **On**; otherwise, select **Off**, and proceed to step 5. **NOTE:** When you turn this On, AIS will be transmitted continuously.

Setting	Parameters
MD Level	Specify the level for the Maintenance Domain (MD). The instrument will indicate whether AIS for the specified level are detected in the traffic stream.
AIS Rate	Specify the rate at which the instrument will transmit AIS. **NOTE:** 3.33ms and 10ms rates are not supported
AIS Type (non MAC-in-MAC applications only)	Select one of the following: – **Unicast**. Select Unicast to send AIS to its destination address. – **Multicast**. Select Multicast to send AIS to a reserved multicast MAC address. This setting does not appear when running Mac-in-Mac applications.

5 Use the right arrow key to go to the S-OAM LBM/LBR configuration menu, and then specifying the following:

Setting	Parameters
LBM/LBR (ping)	If you want to test LBM or LBR, select **Enable**; otherwise, select **Disable**, and proceed to step 6. **NOTE:** When you enable this setting, a Send LBR action is available.

Setting	Parameters
MD Level	Specify the level for the Maintenance Domain (MD). The instrument will indicate whether AIS for the specified level are detected in the traffic stream.
LBM Type	Select one of the following: – **Unicast**. Select Unicast to send an LBM to its destination address. – **Multicast**. Select Multicast to send an LBM to a reserved multicast MAC address. This setting does not appear when running Mac-in-Mac applications.

6 Use the right arrow key to go to the S-OAM LTM/LTR configuration menu, and then specifying the following:

Setting	Parameters
LTM/LTR (ping)	If you want to test LTM or LTR, select **Enable**; otherwise, select **Disable**, and proceed to step 7. **NOTE:** When you enable this setting, a Send LTM action is available.

Setting	Parameters
MD Level	Specify the level for the Maintenance Domain (MD). The instrument will indicate whether AIS for the specified level are detected in the traffic stream.

7 Use the right arrow key to go to the L-OAM Local Config configuration menu, and then specifying the following:

Setting	Parameters
Link OAM State	If you want to enable link OAM, select **On**; otherwise, select **Off**, and proceed to step 8.
Mode	Select one of the following: – Active. Select Active if you want the instrument to automatically discover and monitor the peer on the link. – Passive. Select Passive if you want the peer to initiate the discovery process.
Vendor OUI	Specify the Vendor OUI (Organizationally Unique Identifier) for the instrument.

Setting	Parameters
Vendor Specific Info	Enter the value used to differentiate the vendor's product models or versions. Entry of a value is optional.
Max PDU Size	Specify the largest OAM PDU size.
Unidirectional	Select **Yes** to advertise that the instrument provides unidirectional support; otherwise, select **No**.
Link Events	Select **Yes** if the instrument supports Link Event interpretation; otherwise, select **No**.
Remote Loopback	Select **Yes** if the instrument supports OAM remote loopback mode; otherwise, select **No**.
Variable Retrieval	Select **Yes** if the instrument can send Variable Response OAM PDU; otherwise, select **No**.

8 Use the right arrow key to go to the L-OAM Defects configuration menu, and then specifying the following:

Setting	Parameters
Link Fault	If you want to indicate to the peer a fault has occurred, select **Yes**; otherwise, select **No**.

Setting	Parameters
Dying Gasp	If you want to indicate to the peer that an unrecoverable local failure condition has occurred, select **Yes**; otherwise, select **No**.
Critical Event	If you want to indicate to the peer that a critical event has occurred, select **Yes**; otherwise, select **No**.

9 Use the right arrow key to go to the L-OAM Events configuration menu, and then specifying the following:

Setting	Parameters
Sym Period Wndw	Specify the number of symbols that can be received in the period on the underlying physical layer.
Sym Period Thres	Specify the number of errored symbols in the window specified required for an error to be declared.
Frm Window	Specify the duration of the frame window in terms of the number of 100 ms period intervals. For example, 2 indicates that the window spans a 200 ms period interval.
Frm Threshold	Specify the number of detected errored frames required within the window specified for an error to be declared

Setting	Parameters
Frm Period Wndw	Specify the duration of the window in terms of frames.
Frm Period Thres	Specify the number of frame errors that must occur in the window to declare an error.
Frm Second Summary Wndw	Specify the duration of the period in terms of the 100 ms interval.
Frm Second Summary Thres	Specify the number of frame errors that must occur in the window to declare an error.

10 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Main screen.

11 If you are testing link layer OAM, loop up the instrument's peer (see "Using the automatic loopback feature" on page 89).

The OAM settings are specified.

Turning RDI or AIS analysis On

After you specify OAM settings, you can start traffic and monitor the circuit for RDI or AIS. If you turn RDI or AIS analysis On, you can also insert frames with RDI or AIS into the traffic stream.

To turn RDI or AIS analysis On

1. On the Main screen, press the Action soft key, then select one of the following:
   - **Start Traffic** (if you configured a constant, bursty, or flooded load).
   - **Start Ramp** (if you configured a ramped traffic load).
2. Press the Action soft key again, then select one of the following.
   - **RDI On**.
   - **AIS On**.
3. Repeat step 2 if you want to turn on the other item.

The instrument transmits traffic, and monitors the circuit for RDI or AIS. The instrument will continuously monitor the circuit for each, and generate AIS until you turn them Off.

Sending LBM or LTM messages

After you specify OAM settings, you can start traffic and send LBM or LTM messages.

To send LBM or LTM messages

1. On the Main screen, press the Action soft key, then select one of the following:
   - **Send LBM**
   - **Send LTM**
2. Repeat step 1 if you want to send the other message.

The instrument sends the message.

MAC-in-MAC testing

If you purchased the MAC-in-MAC option for your instrument, a series of MAC-in-MAC (MiM) applications are available which allow you to transmit and analyze unicast layer 2

Ethernet traffic carried on a PBB (Provider Backbone Bridged) trunk. When configuring the traffic, you specify a backbone destination address (B-DA), backbone source address (B-SA), and backbone tag (B-TAG) which designate the path for the backbone frame to the destination. You can also characterize the customer frame (carried in the backbone frame) by specifying the frame type, I-TAG settings, encapsulation settings, and frame size.

When analyzing MiM traffic, you can set up a filter on the receiving instrument to observe test results for traffic sharing the same B-TAG (tag settings for the backbone frame), I-TAG (tag settings for the customer frames), customer frame settings such as the frame type, encapsulation values, and the pattern carried in the customer frame payload.

Understanding MAC-in-MAC test results

When the instrument is configured for MiM testing, a subset of the standard layer 2 test results is provided for the backbone and customer frames. When observing results for the backbone frames, B-TAG and I-TAG information is also provided.

Understanding MAC-in-MAC LEDs

In addition to the standard LEDs provided for layer 2 Ethernet testing, a PBT Frame Detect LED is available which indicates whether the unit has detected MiM traffic on the circuit.

Configuring MAC-in-MAC tests

Before transmitting or analyzing traffic on a PBB trunk, you must select the appropriate MAC-in-MAC (MiM) test application, specify interface settings, specify frame and frame filter settings, and then configure the traffic load.

Instructions are provided in this section for the following:

– “Initializing the link for MiM testing” on page 107
– “Specifying frame characteristics” on page 107
– “Configuring the traffic load” on page 109

– "Filtering MiM traffic" on page 109
– "Specifying OAM settings" on page 95

Initializing the link for MiM testing

Before you transmit layer 2 MiM traffic, you can specify interface settings that provide the speed and duplex settings for 10/100/1000 Ethernet traffic, indicate how you want the unit to handle flow control, and provide the pause quanta for transmitted pause frames.

For detailed instructions on specifying these settings, refer to "Initializing the link for Ethernet testing" on page 47.

Specifying frame characteristics

Before you transmit layer 2 Ethernet traffic over a PBB trunk, you can specify the frame characteristics of the traffic, such as the backbone source address, destination address, tag settings, and payload (Acterna test frames or BER patterns).

To specify Ethernet customer and backbone frame settings

1 Use the right arrow to go to the Ethernet - Backbone Frame configuration menu, and then specify the following:

Setting	Parameters
B-DA	Enter the destination address using a 6 byte hexadecimal format.
B-SA Type	Select Default or User Defined.
B-SA (if B-SA Type is User Defined)	If you specified User Defined, enter the source MAC address using a 6 byte hexadecimal format.

Setting	Parameters
B-Tag VLAN	Enter the ID for the backbone VLAN used as the path to the destination, and the priority code point (PCP) ID representing the type of service the transmitted traffic is emulating.
B-Tag DEI Bit	Indicate whether the traffic is drop eligible by setting the DEI bit for the transmitted traffic.
I-Tag Priority	Enter the priority code point (PCP) ID representing the type of service the transmitted traffic is emulating.
I-Tag DEI Bit	Indicate whether the traffic is drop eligible by setting the DEI bit for the transmitted traffic.
I-Tag UCA Bit	Indicate whether you want to use the customer address by setting the bit.
I-Tag Service ID	Specify the backbone service instance ID for the traffic.

2 Go to the Customer Frame menu, and then specify settings that characterize the customer frame. For descriptions of each setting, refer to "Specifying frame characteristics" on page 51.

3 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Main screen.

The customer and backbone frame settings are specified.

Configuring the traffic load

Before transmitting layer 2 traffic over a MiM trunk, you can specify the type of traffic load the unit will transmit (Constant, Burst, Ramp or Flood). The settings vary depending on the type of load.

For an overview of the available traffic loads, see "Configuring the traffic load" on page 56.

Specifying OAM settings

You can position the instrument at various endpoints in a Maintenance Domain (MD) or Maintenance Association (MA) area to verify that no OAM trunk problems occur. You can also use the instrument to verify point-to-point link layer performance per ITU-T Rec. 802.3ah. For details, refer to "OAM service and link layer testing" on page 94.

Filtering MiM traffic

Before transmitting or monitoring layer 2 traffic on a MiM trunk, you can specify settings that indicate the expected received payload and determine which backbone 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.

If you want to observe results for the Customer Link (counts or statistics), ensure that the B-TAG and I-TAG filter settings, and the Customer filter settings match those carried in the analyzed traffic.

To filter MiM traffic

1. If you haven't already done so, launch the Mac-in-Mac application for the circuit you are testing (see "Launching an application" on page 28), and then proceed to step 2.
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).

3 Use the right arrow to go to the Filter - Backbone Frame configuration menu, and then specify the following:Use

Setting	Parameters
B-Tag VLAN ID	Enter the VLAN ID carried in the filtered traffic, or use the **Don't Care** button to analyze all received traffic irrespective of the VLAN ID.
B-Tag Priority	Enter the priority carried in the filtered traffic, or use the **Don't Care** button to analyze all traffic irrespective of the priority.
B-Tag DEI Bit	Indicate whether you want to analyze traffic that is Drop Eligible or Not Drop Eligible, or select **Don't Care** to analyze all traffic irrespective of the DEI Bit.
I-Tag Priority	Enter the priority ID carried in the filtered traffic, or use the **Don't Care** button to analyze all traffic irrespective of the priority.
I-Tag DEI Bit	Indicate whether you want to analyze traffic that is Drop Eligible or Not Drop Eligible, or select **Don't Care** to analyze all traffic irrespective of the DEI Bit.
I-Tag UCA Bit	Indicate whether you want to analyze traffic that uses a customer address, does not use a customer address, or select **Don't Care** to analyze all traffic irrespective of the UCA Bit.

Setting	Parameters
I-Tag Service ID	Enter the service ID carried in the filtered traffic, or use the **Don't Care** button to analyze all traffic irrespective of the ID.

the right arrow to go to the Filter - Customer Frame configuration menu, and then specify the following:

Setting	Parameters
Destination Type	To analyze frames for a specific type of destination address, select one of the following: – Unicast – Multicast – Broadcast If you do not want to filter frames based on the destination address type, select Don't Care.
Destination MAC	To analyze frames sent to a specific Unicast or Multicast address, enter the destination address.
Source Type	– To analyze frames sent from a specific address, select **Unicast**. – If you do not want to filter frames sent from a specific address, select **Don't Care**.
Source MAC (if Source Type is Unicast)	To analyze frames sent from a specific address, enter the source address.

Setting	Parameters
Encapsulation	– To analyze frames that are not tagged, select **None**. – To analyze VLAN tagged frames, select **VLAN**, and then specify the VLAN Tag and User Priority for the tagged frames. – To analyze Q-in-Q tagged frames, select **Q-in-Q**, and then specify the CVLAN Tag and User Priority, and the SVLAN settings for the tagged frames. – If you do not want to filter frames based on their tagged status, select **Don't Care**.
Payload Analysis	– To analyze traffic with a BERT or Acterna payload, select **On**. – If you do not want to analyze traffic based on the type of payload (you want the unit to monitor live traffic), select **Off**
Rx = Tx (if Payload on Ethernet -Customer Frame configuration menu is BERT)	– To analyze frames with the same payload specified for transmitted frames, select **Yes**. – If you want to analyze frames with a different payload, select **No.**

Setting	Parameters
Rx BERT Pattern (If Rx = Tx is No)	To analyze frames with a specific BERT pattern, select one of the following: – **2^23-1** – **Inv 2^23-1** – **2^31-1** – **Inv 2^31-1** – **All Ones** – **All Zeros** – **User Defined**, and then enter the pattern.
User Payload (if Rx BERT Pattern is User Defined)	Enter the pattern carried in the traffic you are analyzing.

4 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button to return to the Main screen.

The MiM filter settings are specified.

Transmitting MiM traffic

Before you transmit layer 2 traffic over a MiM trunk, you must configure the traffic. For instructions, see:

– "Initializing the link for MiM testing" on page 107
– "Specifying frame characteristics" on page 107
– "Configuring the traffic load" on page 109
– "Filtering MiM traffic" on page 109
– "Specifying OAM settings" on page 95

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

To transmit MiM traffic

1. If you haven't already done so, launch the Mac-in-Mac terminate application for the circuit you are testing (see "Launching an application" on page 28).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. Configure the HST for your test (see "Configuring MAC-in-MAC tests" on page 106).
4. Press the **Home** button to return to the Summary Results screen.
5. Press the **Action** soft key again, and then select one of the following:
   - **Start Traffic** (if you configured a constant, bursty, or flooded load).
   - **Start Ramp** (if you configured a ramped traffic load).

The HST-3000 transmits traffic over the link.

Inserting errors or pause frames

Actions 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.

For detailed instructions, see "Inserting errors" on page 81 and "Inserting pause frames" on page 83.

Measuring round trip delay and packet jitter

You can measure round trip delay and packet jitter by transmitting traffic carrying an Acterna payload. Frames with an Acterna payload provide time stamps, enabling the unit to calculate the delay and jitter.

Measuring service disruption time

You can use two units in an end-to-end configuration to measure the service disruption time resulting from a switch in service to a protect line. The traffic originating unit must transmit a constant rate of traffic to obtain accurate measurements.

Monitoring layer 2 MiM traffic

Use the MiM Traffic Mon /Thru application whenever you want to analyze received traffic. When you configure your test, you can 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.

NOTE:

If you are testing from an optical interface, you must turn the laser on using the associated button to pass the signal through the unit's transmitter.

For detailed instructions, see "Monitoring Ethernet traffic" on page 93.

IP Testing

4

This chapter provides information on testing IP services using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

About IP testing

Using the HST-3000 with an Ethernet SIM, you can turn up and troubleshoot IP services on point-to-point unswitched and switched networks by verifying connectivity, measuring throughput, and verifying that quality of service statistics conform to those specified in a customer's Service Level Agreement.

If you purchased the IPv6 Traffic software option, applications are provided that allow you to transmit and analyze either IPv4 or IPv6 traffic. Table 10 lists the key differences between the applications:

Table 10 IPv4 and IPv6 applications

Feature	IPv4	IPv6
Source IP Configuration	– In IPoE mode, uses DHCP or manual configuration. For details, see "Establishing an IPoE connection for IPv4 traffic" on page 122. – In PPPoE mode, uses the client-server PPPoE login process. For details, see "Establishing a PPPoE session" on page 128.	Uses one of the following: – Stateful Auto-configuration (also known as DHCPV6) – Stateless Auto-configuration – Manual configuration For details, see "Establishing an IPoE connection for IPv6 traffic" on page 124.

Table 10 IPv4 and IPv6 applications (Continued)

Feature	IPv4	IPv6
Source IP Address	A single IP address is assigned to the interface transmitting IP traffic. For details, see "Establishing an IPoE connection for IPv4 traffic" on page 122.	Two IP addresses are assigned: – Link-local address. this source address is assigned locally, and must always go through duplicate address detection (DAD). – Global address. This second source address is not used locally; it is used to transmit traffic beyond the router. See "Establishing an IPoE connection for IPv6 traffic" on page 124.
Automatic MAC Address Resolution	Uses ARP	Uses Neighbor Solicitation
Traffic prioritization	Uses one of the following: – *Layer 2* VLAN or Q-in-Q encapsulation. – *Layer 3* MPLS encapsulation which uses labels and tunnel priorities.	Uses the following: – VLAN or Q-in-Q encapsulation. – Flow labels. The HST allows you to configure traffic with flow labels simply to determine whether routers on the circuit support the labels. See the explanation provided for the "Flow Label" setting on page 141. – MPLS encapsulation is not supported.
IP Header Checksums	Checksum error insertion supported. See the Error Type Table on page 82 for valid error types.	Does not use checksums. See the Error Type Table on page 82 for valid error types.

Table 10 IPv4 and IPv6 applications (Continued)

Feature	IPv4	IPv6
Error Messages	ICMPv4 messages appear in the Message result category.	ICMPv6 messages appear in the Message result category.

Selecting a layer 3 IP test

IPv4 and IPv6 applications are available for layer 3 IP testing. You *must* select an IPv4 test application if you intend to:

– Establish PPPoE sessions on electrical circuits.
– Transmit and analyze MPLS encapsulated traffic over electrical or optical circuits.

To select a layer 3 IP test

1 Do one of the following:

– If you haven't already done so, launch the application for the circuit you are testing (see "Launching an application" on page 28), and then proceed to step 2.

If you are testing a circuit carrying IPv4 traffic, be certain to launch the application using the ETH ELEC or ETH OPTIC softkey.

If you are testing a circuit carrying IPv6 traffic, be certain to launch the application using the IPv6 ELEC or IPv6 OPTIC softkey.

– If you already launched your application and selected a test, but you want to change the test, go to the Test Mode menu, and then select the Test setting.

A list of tests for the application appears.

2 Highlight and select one of the following:

– **Layer 3 IP Traffic**. Select this test to transmit or analyze standard layer 3 traffic.

If you select this test, you must also specify the Length Type (Packet Length or Frame Length). This indicates whether you want to specify the length for each packet as a frame length or as a packet length when you configure IP traffic.

If you are transmitting IPv4 traffic over an electrical circuit, you must also indicate whether you are testing in IPoE or PPPoE Data Mode.

– **Layer 3 PING**. Select this test to verify connectivity with another layer 3 or IP device.

– **Layer 3 Traceroute**. Select this test to trace a packet's route as it travels through a circuit to determine where problems in the network are occurring.

The test is selected.

Discovering another JDSU test instrument

Before you begin testing, you can automatically detect other JDSU test instruments on the circuit and determine their capabilities.You can then optionally configure key parameters for your test automatically based on a discovered instrument's settings. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Initializing the link for IPoE testing

Before you connect the HST-3000 (or HST-3000s) to an access element on a circuit, and turn the laser on (if you are testing 1G or 100M optical Ethernet), you must first specify the settings required to establish connectivity with another Ethernet device on the circuit (see "Initializing the link for Ethernet testing" on page 47).

After you specify the layer 2 Ethernet settings, the initialization process varies depending on the application you selected (IPv4 or IPv6) and, if you are testing an electrical circuit, the data mode (IPoE or PPPoE) that you selected. The following procedures provide instructions for establishing an IPoE connection:

– "Establishing an IPoE connection for IPv4 traffic" on page 122
– "Establishing an IPoE connection for IPv6 traffic" on page 124

If you need to establish a PPPoE session, see "Establishing a PPPoE session" on page 128.

Establishing an IPoE connection for IPv4 traffic

In addition to the settings required to establish an Ethernet link, when establishing an IPoE connection that will carry IPv4 traffic, you also specify settings that indicate whether you want to use ARP to determine the link partner's MAC address, and indicate whether the unit has a static or DHCP-assigned source IP, subnet, and gateway address.

To establish an IPoE connection that will carry IPv4 traffic

1 If you haven't already done so, launch your IPv4 application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   – "Selecting a layer 3 IP test" on page 120
   – "Selecting a layer 4 TCP/UDP test" on page 165
   – "Selecting a multiple streams test" on page 182

2 Press the **Configure** navigation key.

   A configuration menu appears.

3 Use the left and right arrow keys to go to the Link Init menu, and specify the settings required to initialize an Ethernet link (see "Initializing the link for Ethernet testing" on page 47).

4 Do the following:

a Use the left and right arrow keys to go to the IP Init menu (see Figure 25).

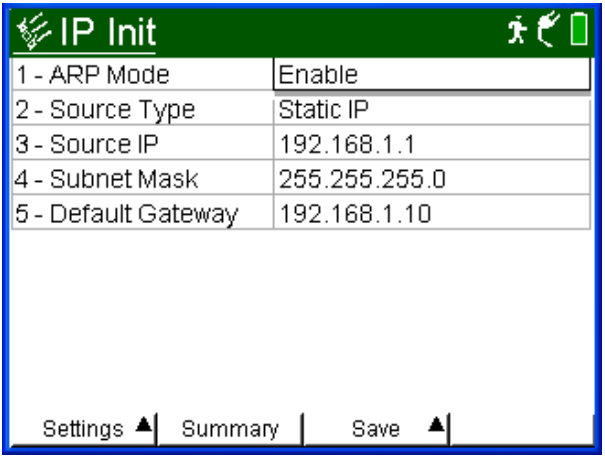


Figure 25 IP Init configuration menu

b Specify the following IP initialization settings:

Setting	Parameters
ARP Mode	– Enable - Enable ARP mode if you want the HST to issue an ARP request to automatically determine the MAC address of its link partner. In most instances ARP should be enabled. – Disable - If you disable ARP Mode, be certain to specify the Destination MAC address for the HST's link partner (on the Ethernet menu).

Setting	Parameters
Source Type	– DHCP - allows the unit to obtain an IP address from a DHCP server. – Static - allows you to manually specify the IP, subnet, and gateway addresses.
Source IP	If the Source Type is Static, enter the source IP address carried by all traffic generated by your unit.
Subnet Mask	If the source IP type is Static, enter the subnet mask.
Default Gateway	If the source IP type is Static, enter the default gateway address.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button, and then do the following:

– If you are initializing a 1G or 100M optical Ethernet link, press the Action soft key, and then select **Laser On**.

– Verify that the Sync LED is green (indicating that the link is active).

– Display the IP Config results category to observe test results associated with the IP connection.

The connection is established.

Establishing an IPoE connection for IPv6 traffic

In addition to the settings you specify to establish an Ethernet link, when establishing an IPoE connection that will carry IPv6 traffic, you also specify settings that indicate whether you want to:

– Manually specify the source addresses required to establish the connection.
– Use stateless auto-configuration to obtain the subnet prefix from a router, and then use the prefix in combination with the unit's MAC address to build the global address. It also obtains the subnet prefix length and default gateway address.
– Use a DHCPv6 server to obtain addresses (referred to as *stateful auto-configuration*).

Before establishing a connection, the unit performs Duplicate Address Detection (DAD) to verify that the locally assigned link-local address hasn't already been used.

TIP:

When specifying addresses manually, you can use two colons (::) to represent hexadecimal fields of consecutive zeros. For example:

2001:0db8:85a3:08d3:0000:0000:0370:7334

Can be represented by:

2001:0db8:85a3:08d3::0370:7334

To type colons in addresses, use the asterisk key (*). For details on using the HST keypad, see the *HST-3000 Base Unit User's Guide.*

To establish an IPoE connection that will carry IPv6 traffic

1 If you haven't already done so, launch your IPv6 application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   – "Selecting a layer 3 IP test" on page 120
   – "Selecting a layer 4 TCP/UDP test" on page 165

2 Press the **Configure** navigation key.

   A configuration menu appears.

3 Do the following:

a Use the left and right arrow keys to go to the IP Init menu (see Figure 26).

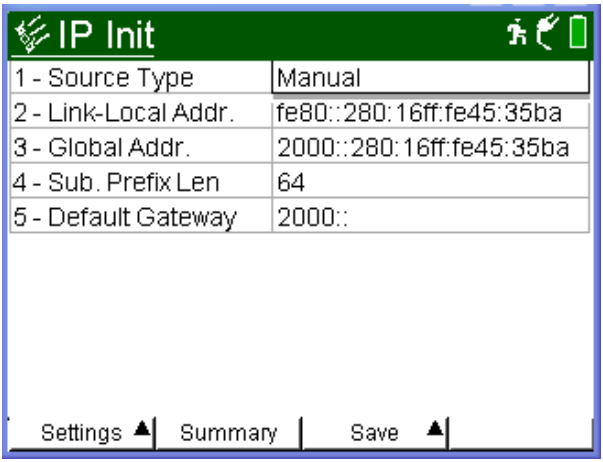


Figure 26 IP Init Menu

b Specify the settings required to initialize an Ethernet link (see "Initializing the link for Ethernet testing" on page 47).

4 Use the left and right arrows to go to the IP Init menu, and then specify the following IP settings for all IPv6 traffic generated by the HST:

Setting	Parameters
Source Type	– Stateful (DHCPv6) - 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 HST generates a tentative *link-local addres*s, and then performs Duplicate Address Detection to verify that the address isn't already used. If DAD is successful, the HST then obtains a subnet prefix from the router to build the required *global address*. – Manual - Select Manual if you want to specify the link-local address, global address, subnet prefix length, and default gateway.
Link-Local Addr (if Source Type is Manual)	Specify the link-local address.
Global Addr (if Source Type is Manual)	Specify the global address.
Sub. Prefix Len (if Source Type is Manual)	Specify the subnet prefix length. This length is used to determine whether the destination address resides on the same subnet as the source address.

Setting	Parameters
Default Gateway	Enter the default gateway address.
Preferred DNS (PING and Traceroute only)	Specify the address for the preferred DNS server.
Alternate DNS (PING and Traceroute only)	Specify the address for an alternate DNS server.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button, and then do the following:

- If you are initializing a 1G or 100M optical Ethernet link, press the Action soft key, and then select **Laser On**.
- Verify that the Sync LED is green (indicating that the link is active).
- Display the IP Config results category to observe test results associated with the IP connection.

The connection is established.

Establishing a PPPoE session

In addition to the settings you specify to establish an Ethernet link, when establishing a PPPoE session (available for IPv4 Terminate applications only), you also specify settings that allow you to log in to the PPPoE peer. The settings indicate whether you want your unit to emulate a PPPoE client or server, and provide the user name, password, and other information required to establish the session.

To establish a PPPoE session

1. If you haven't already done so, launch the electrical IPv4 terminate application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Do the following:

   a Use the left and right arrow keys to go to the Test Mode menu (see Figure 27).

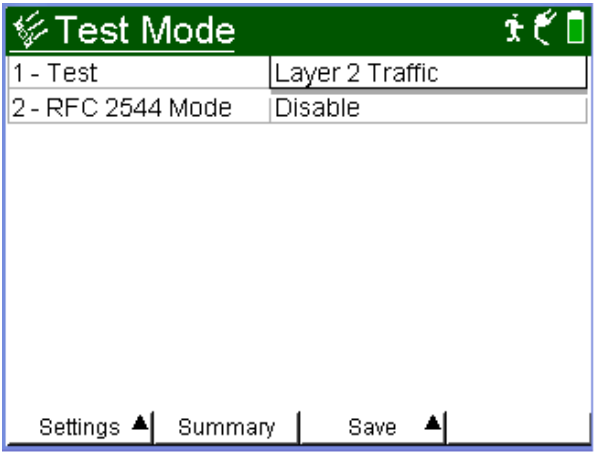


Figure 27 Test Mode configuration menu

   b Set the Data Mode to PPPoE.
4. Go to the Link Init menu, and specify the settings required to initialize an Ethernet link (see "Initializing the link for Ethernet testing" on page 47).

5 Do the following:

a Go to the PPP menu.

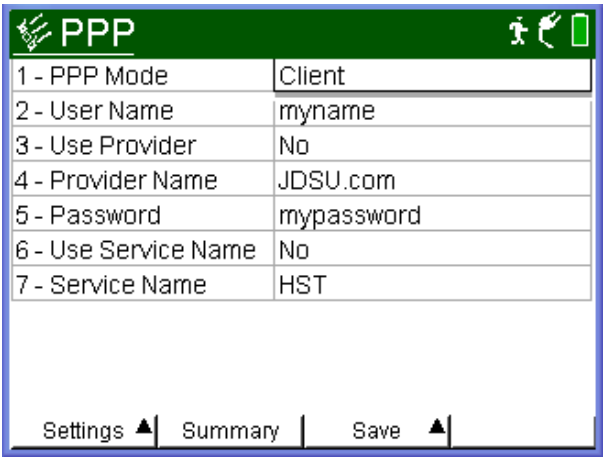


Figure 28 PPP configuration menu

b Specify the following settings. The Provider Name, Password, and Service Name you specify for the HST must match those of its PPPoE peer:

Settings	Parameters
PPP Mode	– Client. In most instances, the unit should emulate a PPPoE client. If you select Client mode, you do not need to specify the Local IP, Subnet Mask, or Remote IP settings on the IP Init menu because they will be provided by a PPPoE server. – Server. Select Server mode if the unit must operate as a PPPoE server. For example, if the unit is positioned before a BBRAR (Broadband Remote Access Router), it must function as a server. If you select Server mode, you must specify the settings (see step 6 on page 132).
User Name	Enter a valid user name for the ISP (Internet Service Provider).
Use Provider	– Yes. Select Yes if the ISP requires the provider's domain name be included with the User Name (for example, joe-smith@provider.net). – No. Select No if the ISP does not require the provider's domain name as part of the user name.
Provider Name	If you selected Yes as the Use Provider setting, specify the provider name. An at sign (@) and the provider name will automatically be appended to the User Name that you specified, and will be carried in the packet.

Settings	Parameters
Password	Enter the password for the user name that you specified. Remember passwords are often case-sensitive.
Use Service Name	– Yes. Select Yes if you want to specify a service name. If you specify a service name, your unit will only attempt to establish a PPPoE session with the service you specify. – No. Select No if you do not want to specify a service name.
Service Name	If you selected Yes as the Use Service Name setting, specify the name. The default service name is “HST”.

6 Do one of the following:

– If the HST is emulating a PPPoE client, proceed to step 7. The unit will use a static IP address.

– If the HST is emulating a PPPoE server, go to the IP Init menu, and then specify the following settings:

Settings	Parameters
Local IP	Enter the source IP address for traffic generated by your unit. This address is used as the remote IP address for the PPPoE client.
Subnet Mask	Enter the subnet mask.
Remote IP	Enter remote IP address for the HST server. This address is used as the local (source) IP address on the client side of the connection.

7 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** button, and then do the following:

a Press the Action soft key, and then select **Log-On**.

The unit discovers the MAC address of the PPPoE peer, and then uses the MAC address in combination with a session ID to uniquely identify the session.

b Observe the messages and events associated with the PPPoE login process in the Status Bar, the Message Log and the IP Config result category. For a list of potential messages, see “PPPoE messages” on page 134.

The PPPoE session is established. The HST will continuously send PPP echoes and replies to keep the session established.

PPPoE messages

The following messages may appear in the Status Bar and Message Log during the PPPoE login process.

Table 11 PPPoE messages

Message	Typically Indicates:	Resolution
PPP Authentication Failed	The user name, password, or provider name you specified were not accepted by the PPPoE server.	– It is possible that the user name and password you specified were not recognized by the PPPoE server. Verify that you specified the correct name and password. – If the PPPoE server requires a provider name, verify that the name you specified when you configured the PPP settings is correct. – It is possible that the PPPoE server does not require a provider name; if so, specifying one in the PPP settings results in a failed authentication. Set the Provider Name setting to **No**, and then try to establish the session again. – Try to establish a new session with the server.

Table 11 PPPoE messages (Continued)

Message	Typically Indicates:	Resolution
PPPoE Timeout	The HST is not physically connected to a PPPoE server, or it is configured to use a service that is not supported by the server.	– Verify that the HST is physically connected to the server. – Verify that the service name you specified is correct, or, if a service name is not required by the server, set the Service Name setting to **No**. – Try to establish a new session with the server.
Data Layer Stopped	The physical Ethernet link to the HST is lost.	Reconnect the physical Ethernet link. The HST will attempt to reconnect to the server.
PPP LCP Failed	There is a problem with the server.	Try to establish a new session with the server.
PPP IPCP Failed		
PPPoE Failed		
PPP Up Failed	The PPPoE server dropped a successful PPPoE session.	Try to establish a new session with the server.
Internal Error - Restart PPPoE	The HST experiences an internal error.	Try to establish a new session with the server.

Terminating a PPPoE session

After testing is complete, you must manually terminate the PPPoE session.

To terminate a PPPoE session

– Press the Action soft key, and then select **Log-Off**.

Configuring layer 3 IP tests

Before transmitting layer 3 traffic over a link, you can specify settings that characterize the IP traffic and indicate the type of traffic load to transmit. You can also specify settings that filter received traffic for analysis.

Specifying frame characteristics

Before you transmit layer 3 IP traffic, you can specify the frame characteristics of the traffic, such as the destination address type, frame type, and encapsulation settings (if applicable).

To specify frame characteristics for layer 3 traffic

1. If you haven't already done so, launch your IPv4 or IPv6 application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below:
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a multiple streams test" on page 182
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Use the left and right arrow keys to go to the Ethernet menu, and specify the frame characteristics (see "Specifying frame characteristics" on page 51).
4. If you launched an IPv4 application, and you want to transmit MPLS encapsulated traffic, specify the following settings:

Settings	Parameters
Encapsulation	Select **MPLS**.

Settings	Parameters
MPLS EtherType	– Select Unicast to send traffic to a single destination address and network device. – Select Multicast to send traffic with a multicast address to a group of network devices.
# MPLS Labels	Indicate whether MPLS traffic will carry one or two labels.
MPLS1 MPLS2 (if # MPLS Labels is 2)	Specify the ID (the label the network will use to route the traffic), priority, and TTL (time to live). Be certain to specify labels that have already been instantiated by routers on the network.

5 If you indicated that you want to specify a frame length when you configure your traffic (as opposed to a packet length), in Frame Length, select one of the pre-defined lengths, or specify a User Defined length in bytes.

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The frame settings are specified.

Specifying IP packet settings

If you selected the Layer 3 IP Traffic or Layer 4 Traffic test, before you transmit traffic you can specify the packet characteristics of the traffic, such as the destination IP address and packet payload.

– If you indicated that you want to specify a packet length for transmitted traffic, you also specify the length on the IP configuration menu.

– If you indicated that you want to specify a frame length for transmitted traffic, you must specify the length on the Ethernet configuration menu.

To specify packet characteristics for transmitted traffic

1 If you haven't already done so, launch your IPv4 or IPv6 application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):

– "Selecting a layer 3 IP test" on page 120

– "Selecting a layer 4 TCP/UDP test" on page 165

– "Selecting a multiple streams test" on page 182

2 Press the **Configure** navigation key.

A configuration menu appears.

3 Do the following:

a Use the left and right arrow keys to go to the IP menu (see Figure 29).

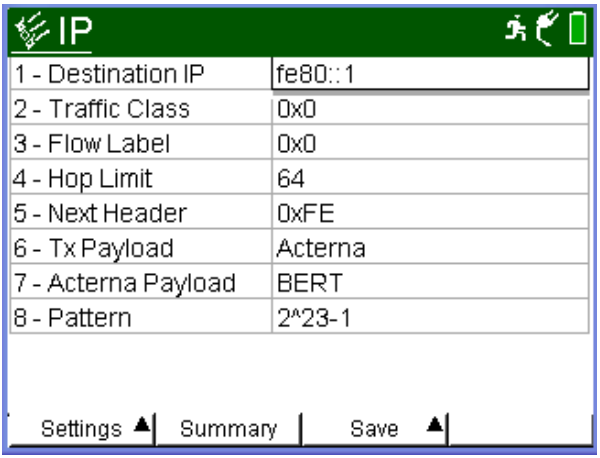


Figure 29 IP configuration menu (IPv4 settings)

b Specify values for the following settings:

IPv4	IPv6	Setting	Parameters
Yes	Yes	Destination IP	Enter the destination IP address for traffic generated by your unit. **NOTE:** You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the destination address for the device you want to transmit traffic to. For details, see "Using J-Connect to discover another JDSU test set" on page 21.
Yes	No	Time To Live	Specify the time after which a packet can be deleted by any device on a circuit as a number of hops. The default time to live setting is 64 hops.
Yes	No	TOS/DSCP	Enter a number representing the type of service in a binary format, or select a DSCP name.
No	Yes	Traffic Class	Enter a number representing the traffic class using a hexadecimal format ranging from 0x0 to 0xFF.
Yes	No	Protocol	Enter a number representing the protocol using a hexadecimal format ranging from 0x0 to 0xFF.
Yes	Yes	Tx Payload	Select one of the following: – Acterna – Fill Byte

IPv4	IPv6	Setting	Parameters
Yes	Yes	Acterna Payload	If you are transmitting an Acterna Tx Payload, select one of the following: – BERT – Fill Pattern
Yes	Yes	Pattern	If you are transmitting a BERT pattern in the ATP payload, select one of the following: – A predefined PRBS or fixed pattern. – User Defined, and then enter the pattern in hexadecimal format
Yes	Yes	Fill Byte	If you are transmitting a Fill Byte payload, enter the fill byte in hexadecimal format ranging from 0x0 to 0xFF.
Yes	Yes	Fill Pattern	If you are transmitting a Fill Pattern in an ATP payload, specify the pattern in a hexadecimal format up to 64 bytes long.
Yes	Yes	Packet Length (if Length Select setting on the Test Mode menu is Packet Length)	– A predefined length. – Random, which sends packets with randomly generated, predefined RFC 2544 traffic lengths. – User Defined, and then specify the packet length. – Jumbo, and then specify the packet length.

IPv4	IPv6	Setting	Parameters
No	Yes	Flow Label	If you are certain the routers on the circuit support flow labels for traffic prioritization, specify the flow label using a hexidecimal format ranging from 0x0 to 0xFFFFF; otherwise, use the default (0x0).
No	Yes	Hop Limit	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.
No	Yes	Next Header	Specify the code representing the type of data carried in the next header in the packet using a hexidecimal format ranging from 0x0 to 0xFF.

4 If you indicated that you want to specify a frame length for the traffic, use the left and right arrow keys to go to the Ethernet configuration menu, and then specify the length.

5 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The packet settings are specified for transmitted traffic.

Configuring the traffic load

Before transmitting IP traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty, Ramp, or Flood) in 0.001% increments, beginning at 0.002%. For details on configuring a traffic load, see “Configuring the traffic load” on page 56.

Filtering received traffic using layer 2 criteria

If you want to filter received traffic using layer 2 criteria, specify the criteria on the Ethernet Filter menu (see "Filtering received traffic using layer 2 criteria" on page 65).

Filtering received traffic using layer 3 criteria

You can specify settings that determine which packets will pass through the receive filter and be analyzed and reported in the test result categories for layer 3 IP traffic. Traffic that does not pass filter criteria is not reported in the test result categories.

TIPS:

- If you want to use the JDSU Discovery feature to populate the filter, be certain to **Enable** the filter.
- If you selected a Terminate application, and you want to analyze all received traffic, verify that the Ethernet Filter settings are all **Don't Care**, and that the IP Filter is **Disabled**.
- If you selected a Terminate application, and you want to analyze only layer 3 IP traffic, the IP Filter or IPv6 Filter must be **Enabled**.
- If you selected a Monitor / Thru application, and you want to monitor both IPv4 and IPv6 traffic, verify that the IP Version setting is **Don't Care**.
- If you selected a Monitor / Thru application, and you want to monitor only IPv4 or IPv6 traffic, verify that you specified the correct IP Version setting.
- If you selected a Monitor /Thru application, and you specified the Thru test type, you can specify filter criteria for Port 1 and Port 2.

Specifying IPv4 filter criteria

To specify IPv4 filter criteria

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Do the following:
   a. Use the left and right arrows to go to the IP Filter menu.

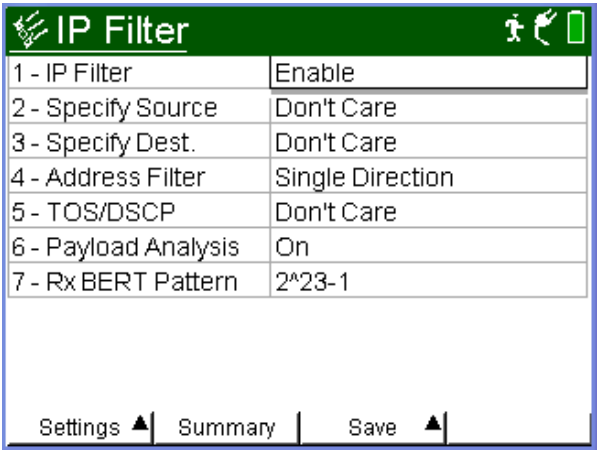


Figure 30 IP Filter menu (IPv4 settings)

b Specify values for the following settings:

Setting	Parameters
IP Filter	Select one of the following: – If you want to filter received traffic using layer 3 criteria, select **Enable**. You must enable the IP Filter if you want to analyze only layer 3 IP traffic. – If you do not want to filter received traffic using layer 3 criteria, select **Disable**.
Specify Source (if IP Filter is enabled)	Select one of the following: – To analyze received packets from any IP address, select **Don't Care**. – To analyze packets sent from a specific IP address, select **Yes**.
Source IP (if Source Address IP is Yes)	Enter the source address for filtered packets. **NOTE:** You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the source address for the device you want to filter traffic for. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Setting	Parameters
Source Subnet (if Specify Source is Yes)	Select one of the following: – To analyze received packets for a *specific source IP address*, select **None**. Packets with a source address that matches the address you specified as the Source IP filter setting will be analyzed. – To analyze packets that match specific prefix criteria, select **Prefix**, and then specify the length of the prefix that you want the filter to evaluate. Only packets that match the prefix portion of the source IP address (up to the length that you specified) will pass through the filter for analysis. – To analyze packets that match specific subnet address criteria, select **Mask**, and then specify the subnet address for the traffic that you want to evaluate. Only packets that carry the address will pass through the filter for analysis.
Specify Dest (if IP Filter is enabled)	Select one of the following: – To analyze received packets sent to any IP address, select **Don't Care**. – To analyze packets sent to a specific IP address, select **Yes**.

Setting	Parameters
Destination IP (if Specify Dest is Yes)	Enter the destination address for filtered packets.
Dest. Subnet	Select one of the following: – To analyze received packets sent to a *specific destination IP address*, select **None**. Packets with a destination address that matches the address you specified as the Destination IP filter setting will be analyzed. – To analyze packets sent to an address that matches specific prefix criteria, select **Prefix**, and then specify the length of the prefix that you want the filter to evaluate. Only packets with prefixes that match the prefix portion of the destination IP address (up to the length that you specified) will pass through the filter for analysis. – To analyze packets that have a destination subnet address that matches the address specified in the filter, select **Mask**, and then specify the subnet address for the traffic that you want to evaluate. Only packets sent to the address will pass through the filter for analysis.

Setting	Parameters
Address Filter	– To analyze traffic coming from a single direction on the circuit, select **Single Direction**. – To analyze traffic from either direction on the circuit, select **Either Direction**. Packets with *either a source address or destination address* that matches the address you specified as the Source IP filter will be analyzed.
TOS/DSCP (if IP Filter is enabled)	Select one of the following: – To analyze received packets for any type of service or DSCP, select **Don't Care**. – To analyze packets for a specific type of service, select **Type of Service**, and then specify the TOS using a binary format. – To analyze packets for a specific DSCP, select **DSCP**, and then select a name.

4 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The unit is configured to analyze received traffic satisfying the layer 3 IPv4 filter criteria.

Specifying IPv6 filter criteria

To specify IPv6 filter criteria

1. If you haven't already done so, launch your IPv6 application (see "Launching an application" on page 28), and then select a test (see the appropriate procedure below):
   - "Selecting a layer 3 IP test" on page 120
   - "Selecting a layer 4 TCP/UDP test" on page 165
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Do the following:
   a Use the left and right arrow keys to go to the IP Filter menu (see Figure 31).

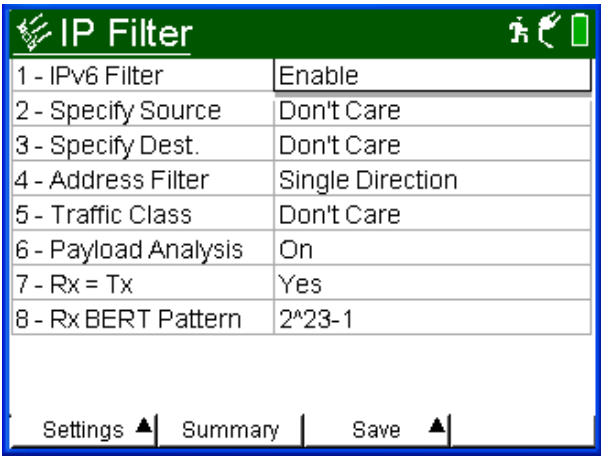


Figure 31 IP Filter configuration menu (IPv6 settings)

b Specify values for the following settings:

Setting	Parameters
IPv6 Filter	Select one of the following: – If you want to filter received traffic using layer 3 IPv6 criteria, select **Enable**. – If you do not want to filter received traffic using layer 3 IPv6 criteria, select **Disable**.
IP Version (if IPv6 Filter is enabled, and Monitor/Thru application was selected)	Select one of the following: – To monitor all received IP traffic (with IPv4 and IPv6 headers), select **Don't Care**. – If you want to monitor received IPv4 traffic, select **IPv4**. – If you want to monitor received IPv6 traffic, select **IPv6**.
Specify Source (if IPv6 Filter is enabled)	– To analyze received packets from any IP address, select **Don't Care**. – To analyze packets sent from a specific IP address, select **Yes**.

Setting	Parameters
Source IP (if Specify Source is Yes)	Enter the source address carried by filtered packets. **NOTE:** If you want to use this address to filter traffic *coming from* or *going to* this address, specify **Either Direction** as the Address Filter.
Source Prefix (if Specify Source is Yes)	– To analyze received packets for a *specific source IP address*, select **None**. Packets with a source address that matches the address you specified as the Source IP filter setting will be analyzed. – To analyze packets that match specific prefix criteria, select **Prefix**, and then specify the length of the prefix that you want the filter to evaluate. Only packets that match the prefix portion of the source IP address (up to the length that you specified) will pass through the filter for analysis.

Setting	Parameters
Specify Dest (if IPv6 Filter is enabled)	– To analyze received packets sent to any IP address, select **Don't Care**. – To analyze packets sent to a specific IP address, select **Yes**.
Destination IP	Enter the destination address carried by filtered packets.
Destination Prefix	Select one of the following: – To analyze received packets sent to a *specific destination IP address*, select **None**. Packets with a destination address that matches the address you specified as the Destination IP filter setting will be analyzed. – To analyze packets sent to an address that matches specific prefix criteria, select **Prefix**, and then specify the length of the prefix that you want the filter to evaluate. Only packets with prefixes that match the prefix portion of the destination IP address (up to the length that you specified) will pass through the filter for analysis.

Setting	Parameters
Address Filter	– To analyze traffic coming from a single direction on the circuit, select **Single Direction**. – To analyze traffic from either direction on the circuit, select **Either Direction**. Packets with *either a source address or destination address* that matches the address you specified as the Source IP filter will be analyzed.
Traffic Class Type	– To analyze received packets irrespective of their traffic class, select **Don't Care**. – To analyze packets for a specific traffic class, select **Traffic Class**, and then enter a number representing the class using a hexadecimal format ranging from 0x0 to 0xFF.

4 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The unit is configured to analyze received traffic satisfying the layer 3 IPv6 filter criteria.

Transmitting layer 3 IP traffic

After you configure the layer 3 IP settings, and your unit successfully determines the destination device's MAC address, you are ready to transmit traffic over the link. The HST automatically sends IPv4 ARP requests or IPv6 Neighbor Solicitation requests as appropriate during layer 3 IP testing.

To transmit layer 3 IP traffic

1. If you haven't already done so, launch your application (see "Launching an application" on page 28), and then select the Layer 3 IP Traffic test (see "Selecting a layer 3 IP test" on page 120).
2. Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.
3. Establish an IPoE connection or a PPPoE session:
   - If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   - If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.
4. Configure the HST for your test. See:
   - "Specifying frame characteristics" on page 51
   - "Configuring the traffic load" on page 56
   - "Filtering received traffic using layer 2 criteria" on page 65
   - "Specifying IP packet settings" on page 137
   - "Filtering received traffic using layer 3 criteria" on page 142
5. Press the Home button to view the Main screen.

6 Press the **Action** soft key again, and then select **Start Traffic** (if you configured a constant, bursty, or flooded load), or **Start Ramp** (if you configured a ramped traffic load).

The HST-3000 transmits traffic over the link.

Inserting errors

You can use the HST-3000 to insert errors into layer 3 IP traffic when you perform end-to-end and loopback tests. For details on error insertion, see “Inserting errors” on page 81 in Chapter 3 “Ethernet Testing”.

Inserting pause frames

You can use the HST-3000 to insert pause frames into layer 3 IP traffic when you perform end-to-end and loopback tests. If you are testing 10/100/1G electrical Ethernet, your unit must be configured for full duplex (FDX) traffic. For details on pause frame insertion, see “Inserting pause frames” on page 83 in Chapter 3 “Ethernet Testing”.

Loopback testing

Layer 3 IP loopback testing allows you to transmit IP traffic from one HST-3000, and then loop the traffic back through a second HST-3000 on the far end of a circuit. For details on loopback testing, see “Loopback testing” on page 87 of Chapter 3 “Ethernet Testing”

Ping testing

Using the HST-3000 with an Ethernet SIM, you can verify connectivity with another Layer 3 or IP device by sending ping request packets to the device. The device then responds to the ping request with a ping reply (if the device is responsive), or with another message indicating the reason no ping reply was sent.

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

To send ping packets to another Ethernet device

1. If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 3 PING test (see "Selecting a layer 3 IP test" on page 120).
2. Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.
3. Establish an IPoE connection or a PPPoE session:
   - If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   - If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.
4. Press the Configure key, and then use the left and right arrows to go to the **PING** menu.

5 Specify values for the following settings:

IPv4	IPv6	Setting	Parameters
Yes	Yes	Destination Type	Specify how you will identify the device you are verifying connectivity to: – IP Address - to type the address of the device. – Host Name - to type name of the device.
Yes	Yes	Destination IP (if Destination Type is IP Address)	Enter the destination IP address of the device you are pinging.
Yes	Yes	Destination Name (if Destination Type is Host Name)	Type the name for the destination host using up to 255 characters. For example, if the destination host's name is Yahoo, type "`www.yahoo.com`".
Yes	No	Time To Live	Specify the time after which a ping request or response can be deleted by any device on a circuit as a number of hops. The default time to live setting is 64 hops.
Yes	No	TOS/DSCP	Select one of the following: – Type of Service, then enter a number representing the type of service. – DSCP, then select a name.
No	Yes	Traffic Class	Enter a number representing the traffic class using a hexadecimal format ranging from 0x0 to 0xFF.

IPv4	IPv6	Setting	Parameters
No	Yes	Flow Label	If you are certain the routers on the circuit support flow labels for traffic prioritization, specify the flow label using a hexidecimal format ranging from 0x0 to 0xFFFFF; otherwise, use the default (0x0).
No	Yes	Hop Limit	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.
Yes	Yes	Ping Type	Specify how you want the HST to transmit pings: – Single - To send a single ping packet, select **Single**. – Multiple - To send a fixed number of ping packets, select **Multiple**, then specify the number of packets to send. – Continuous - To send a continuous stream of ping packets, select **Continuous**, and then specify the Interval between packets.
Yes	Yes	Ping Count (If Ping Type is Multiple)	Specify the number of ping packets to transmit. The minimum number of packets is 2; the maximum is 1024
Yes	Yes	Ping Interval (ms) (Multiple or Continuous Modes only)	Specify the interval between multiple or continuous ping packets. The interval can range between 1000 ms to 10000 ms.

IPv4	IPv6	Setting	Parameters
Yes	Yes	Packet Size	Specify one of the following: – IPv4 ping packets. Specify a length ranging from 46 to 1500 bytes. – IPv6 ping packets. Specify a length ranging from 48 to 1500 bytes.

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.

7 To insert a ping packet or packets, press the Action soft key, and then select **Start PING**.

The HST-3000 transmits the ping packet or packets. Results associated with Ping testing appear in the Ping results category (see "Ping results" on page 307).

Running Traceroute

You can run the traceroute test to determine where problems in the network are occurring. Before running traceroute, you specify settings such as the destination IP address, the maximum number of hops, and the response time.

To run traceroute

1 If you haven't already done so, launch the Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 3 Traceroute test (see "Selecting a layer 3 IP test" on page 120).

2 Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.

3 Establish an IPoE connection or a PPPoE session:

– If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.

– If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.

4 Press the Configure key, and then use the left and right arrows to go to the **Traceroute** menu (see Figure 32).

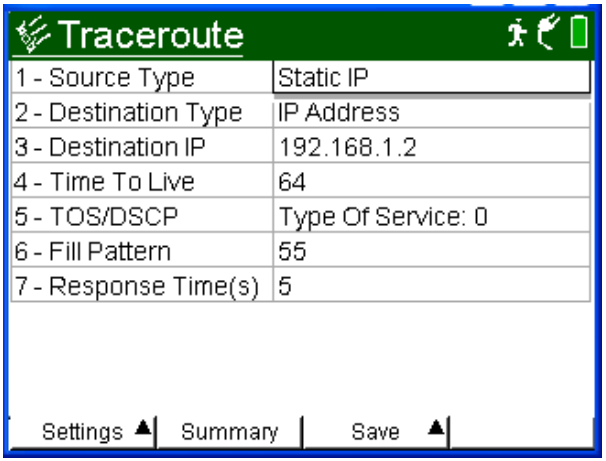


Figure 32 Traceroute configuration menu (IPv4 settings)

5 Specify values for the following settings:

IPv4	IPv6	Setting	Parameters
Yes	Yes	Destination Type	Specify how you will identify the far end device you are tracing the route to: – IP Address - to type the address of the device. – Host Name - to type name of the device.
Yes	Yes	Destination IP (if Destination Type is IP Address)	Enter the destination IP address of the device.

IPv4	IPv6	Setting	Parameters
Yes	Yes	Destination Name (if Destination Type is Host Name)	Type the name for the destination host using up to 255 characters. For example, if the destination host is Yahoo, type "www.yahoo.com".
Yes	No	Time To Live	Specify the time after which a ping request or response can be deleted by any device on a circuit as a number of hops. The default time to live setting is 64 hops.
Yes	No	TOS/DSCP	Select one of the following: – Type of Service, then enter a number representing the type of service in a binary format – DSCP, then select a name.
No	Yes	Traffic Class	Enter a number representing the traffic class using a hexadecimal format ranging from 0x0 to 0xFF.
No	Yes	Flow Label	If you are certain the routers on the circuit support flow labels for traffic prioritization, specify the flow label using a hexidecimal format ranging from 0x0 to 0xFFFFF; otherwise, use the default (0x0).
No	Yes	Hop Limit	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.
Yes	Yes	Response Time (s)	Enter the time (in seconds) the HST will wait to receive a response from a hop.

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.

7 To start tracing the route, press the Action soft key, and then select the **Start Trace**.

The HST-3000 traces the route. Results associated with traceroute testing appear in the Traceroute results category (see "Traceroute results" on page 308).

Monitoring IP traffic

You can monitor and analyze 10/100/1G electrical or 1 G optical layer 3 IP traffic by selecting the Monitor / Thru application for the circuit you are testing.

To monitor IP traffic

1 Launch the Monitor / Thru application for the rate you are testing (see "Launching an application" on page 28), and select the Layer 3 IP Traffic test (see "Selecting a layer 3 IP test" on page 120).

2 Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.

3 Press the **Configure** navigation key, and then use the left and right arrow keys to go to the Summary Settings or Test Mode menu.

4 Select the **Monitor** or **Thru** type (for an explanation of each application for the rate you are testing, see "Test applications" on page 10 through page 15).

If you select the Thru type, you can specify Ethernet and IP filter criteria for Port 1 and Port 2.

5 If you want to filter the traffic, specify the filter criteria on the Ethernet Filter menu (see "Filtering received traffic using layer 2 criteria" on page 142) and the IP Filter menu

(see “Filtering received traffic using layer 3 criteria” on page 142).

Configuration menus are provided that allow you to specify filter criteria for each port.

NOTE:
If you are running an IPv6 application, and you want to analyze all received layer 3 traffic (IPv4 and IPv6), be certain to set the IP Version setting to **Don’t Care**.

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate menu; otherwise, press the **Home** button to return to the Main screen.

The HST monitors and analyzes received traffic. If you are testing in Thru mode, received traffic is passed through to the transmitter of the opposite port.

TCP/UDP Testing

5

This chapter provides step-by-step instructions for testing TCP/UDP service using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

About TCP/UDP testing

If you purchased the TCP/UDP option, you can use the HST-3000 with an Ethernet SIM to:

– Transmit IPv4 traffic with a TCP or UDP header carrying a valid length, checksum, and destination port.
– Verify that routers are prioritizing traffic for various ports properly.
– Verify that the bandwidth allocated to a customer per their Service Level Agreement is available.

The IPv6 Traffic option is also required if you want the ability to transmit and analyze layer 4 IPv6 traffic.

Understanding the ATP Listen Port

Many applications (such as delay measurements, out of sequence counts, lost frames counts, and packet jitter measurements) and multiple-stream tests must be performed using traffic that carries an Acterna Test Packet (ATP) payload. Each of these packets has a time stamp and a unique sequence number which are used to calculate a variety of test results.

The HST uses the ATP Listen Port to determine whether received layer 4 traffic carries an ATP payload; therefore, it is essential that you specify the destination port carried in the

received traffic as the ATP Listen Port on the receiving unit. Figure 33 illustrates the settings required to loop back layer 4 traffic carrying an Acterna payload.

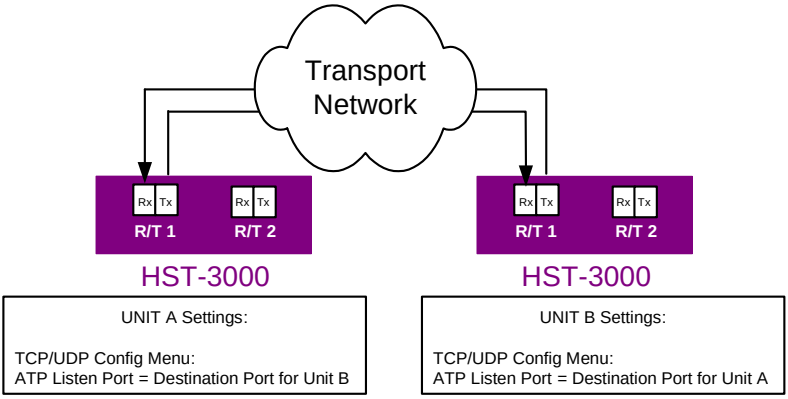


Figure 33 ATP Listen Port Loop back settings

For details on specifying the listen port, see "Filtering received traffic using layer 4 criteria" on page 175.

Selecting a layer 4 TCP/UDP test

IPv4 and IPv6 applications are available for layer 4 TCP/UDP testing.

To select a layer 4 TCP/UDP test

1 Do one of the following:

– If you haven't already done so, launch the application for the circuit you are testing (see "Launching an application" on page 28), and then proceed to step 2.

If you are testing a circuit carrying IPv4 traffic, be certain to launch the application using the ETH ELEC or ETH OPTIC softkey.

If you are testing a circuit carrying IPv6 traffic, be certain to launch the application using the IPv6 ELEC or IPv6 OPTIC softkey.

– If you already launched your application and selected a test, but you want to change the test, go to the Test Mode menu, and then select the Test setting.

  A list of tests for the application appears.

2 Select the **Layer 4 Traffic** test, and then specify the Length Type (Packet Length or Frame Length). This indicates whether you want to specify a packet or frame length when you configure layer 4 traffic. Frame lengths are specified on the Ethernet configuration menu; packet lengths are specified on the IP configuration menu.

3 If you are transmitting IPv4 traffic over an electrical circuit, you must also indicate whether you are testing in IPoE or PPPoE Data Mode.

The test is selected.

Discovering another JDSU test instrument

Before you begin testing, you can automatically detect other JDSU test instruments on the circuit and determine their capabilities.You can then optionally configure key parameters for your test automatically based on a discovered instrument's settings. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Specifying layer 2 and layer 3 settings

Before you transmit layer 4 traffic, you must first establish a layer 2 Ethernet link, and a layer 3 IPoE connection or PPPoE session. You must also specify the appropriate layer 2 and layer 3 settings for the traffic, such as the frame type, frame encapsulation, time to live, and type of service. After you

initialize the link, establish a connection or session, and specify the layer 2 and layer 3 settings, you then specify the required layer 4 settings before transmitting the traffic over the circuit.

For details on link initialization, see:

- "Initializing the link for Ethernet testing" on page 47
- "Establishing an IPoE connection for IPv4 traffic" on page 122
- "Establishing an IPoE connection for IPv6 traffic" on page 124
- "Establishing a PPPoE session" on page 128

For details on specifying layer 2 and layer 3 settings, see:

- "Configuring layer 2 Ethernet tests" on page 51
- "Configuring layer 3 IP tests" on page 136

Configuring layer 4 traffic

After initializing the link or establishing a PPPoE session and specifying layer 2 and layer 3 settings, you specify the layer 4 settings before transmitting traffic over the circuit.

Well known ports

A port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are pre-assigned to them by the IANA. These are known as well known ports (specified in RFC 1700). Port numbers range from 0 to 65536, but only ports numbers 0 through 1024 are reserved for privileged services and designated as *well-known ports*. This list of well-known port numbers specifies the port used by the server process as its contact port.

Table 12 on page 168 list some of the more commonly used well known ports.

Table 12 Well Known TCP/UDP Ports

Service Name	TCP Port	UDP Port
DHCP client	67	
DHCP server	68	
DHCP Manager	135	
DNS Administration	139	
DNS client to server lookup (varies)	53	53
IMAP	143	
IMAP (SSL)	993	
LDAP	389	
LDAP (SSL)	636	
POP3	110	
POP3 (SSL)	995	
SMTP	25	
FTP	21	
FTP-data	20	
HTTP	80	
HTTP-Secure Sockets Layer (SSL)	443	
L2TP		1701
NetMeeting Audio Call Control	1731	
NetMeeting H.323 call setup	1720	
NetMeeting H.323 streaming RTP over UDP		Dynamic
NetMeeting Internet Locator Server ILS	389	
NetMeeting RTP audio stream		Dynamic

Table 12 Well Known TCP/UDP Ports (Continued)

Service Name	TCP Port	UDP Port
NetMeeting T.120	1503	
NetMeeting User Location Service	522	
NetMeeting User Location Service ULS	522	
NNTP	119	
NNTP (SSL)	563	
Radius accounting (Routing and Remote Access)		1646 or 1813
Radius authentication (Routing and Remote Access)		1645 or 1812
Remote Install TFTP	69	
SNMP		161
SNMP Trap		162
Telnet	23	
WINS NetBios over TCP/IP name service		137
WINS Proxy		137
WINS Registration	137	
WINS Replication	42	

Specifying the traffic mode and ports

If you selected the Layer 4 Traffic test, before you transmit traffic you must indicate whether the traffic will carry a TCP or UDP header, and specify the source and destination port numbers for the generated traffic.

Port 0 (zero) is reserved by TCP/UDP for networking; therefore, it is not available when you configure your traffic.

The following port numbers are also reserved, and can not be used during loopback testing. They can be specified when testing end-to-end.

– 111
– 1022
– 1023

To specify packet characteristics for transmitted traffic

1 If you haven't already done so, launch the IPv4 or IPv6 Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 4 Traffic test (see "Selecting a layer 4 TCP/UDP test" on page 165).

2 Press the **Configure** navigation key.

A configuration menu appears.

3 Do the following:

a Use the left and right arrow keys to go to the TCP/UDP menu (see Figure 34).

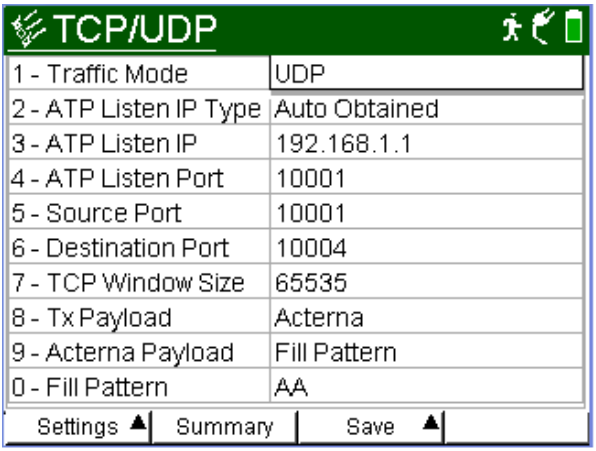


Figure 34 TCP/UDP configuration menu

b Specify values for the following settings:

Setting	Parameters
Traffic Mode	Indicate whether you want to transmit traffic with a **TCP** or **UDP** header.
ATP Listen IP Type	Select one of the following: – Auto Obtained – User Defined
ATP Listen IP (ATP Listen IP Type must be User Defined)	If you want to analyze traffic with an ATP payload, and you indicated that you want to specify a specify a user defined address, specify the IP address carried in the received ATP traffic. **NOTES:** – If your unit has been looped up by another HST, the ATP Listen IP will automatically be populated for you. – You can optionally use the Discover soft key to discover other instruments on the network, and then select the source address for the device you want to filter traffic for. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Setting	Parameters
ATP Listen Port	If you want to analyze traffic with an ATP payload, specify the port designated for ATP traffic. The default listen port is 10004. **NOTES:** – If your unit has been looped up by another HST, the ATP Listen Port will automatically be populated for you. – You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the source port for the device you want to filter traffic for. For details, see "Using J-Connect to discover another JDSU test set" on page 21.
Source Port[a]	Enter the source port number carried by all traffic generated by your unit.
Destination Port	Enter the destination port number carried by all traffic generated by your unit. **NOTE:** You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the destination port for the device you want to transmit traffic to. For details, see "Using J-Connect to discover another JDSU test set" on page 21.

Setting	Parameters
TCP Window Size	Enter a window size in bytes. The window size is used in combination with the average round trip delay measurement for your test to estimate the TCP throughput.
Acterna Payload	– BERT – Fill Pattern
Pattern (appears only if a BERT payload is selected)	Select one of the following: – A predefined PRBS or Fixed pattern. – User Defined, and then enter the pattern in hexa-decimal format
Fill Pattern (appears only if a Fill Pattern payload is selected)	If you are transmitting a Fill Pattern in an ATP payload, specify the pattern in a hexadecimal format up to 64 bytes long.

a. A summarized list of well known port numbers is provided in Table 12 on page 168.

4 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the Home key to return to the Summary Results screen.

The layer 4 header settings are specified for transmitted traffic.

Configuring the traffic load

Before transmitting TCP or UDP traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty, Ramp, or Flood) in 0.001% increments, beginning at 0.002%. For details on configuring a traffic load, see “Configuring the traffic load” on page 56.

Specifying the frame or packet length for transmitted traffic

Before transmitting TCP or UDP traffic, you must indicate the frame or packet length for each transmitted packet.

To specify the frame or packet length

1. If you haven't already done so, launch the IPv4 or IPv6 Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 4 Traffic test (see "Selecting a layer 4 TCP/UDP test" on page 165).
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Use the left and right arrow keys to do one of the following:
   - Go to the Ethernet menu, and then select or specify the frame length for transmitted traffic.
   - Go to the IP menu, and then select or specify the packet length for transmitted traffic.

The frame or packet length is specified.

Filtering received traffic using layer 2 criteria

If you want to filter received traffic using layer 2 criteria, specify the criteria on the Ethernet Filter menu (see "Filtering received traffic using layer 2 criteria" on page 65).

Filtering received traffic using layer 3 criteria

If you want to filter received traffic using layer 3 criteria, specify the criteria on the IP Filter menu (see "Filtering received traffic using layer 3 criteria" on page 142).

Filtering received traffic using layer 4 criteria

You can specify settings that determine which packets will pass through the layer 4 receive filter and be analyzed and reported in the test result categories. Traffic that does not pass filter criteria is not reported in the test result categories

TIPS:

- If you want to use the JDSU Discovery feature to populate the filter, be certain to **Enable** the filter.
- If you want to analyze all received traffic, verify that the Ethernet Filter settings are all **Don't Care**, and that the IP and L4 filters are both **Disabled**.
- If you want to analyze only layer 4 traffic, be certain to **Enable** the L4 filter.

To specify layer 4 filter criteria

1. If you haven't already done so, launch the IPv4 or IPv6 Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 4 Traffic test (see "Selecting a layer 4 TCP/UDP test" on page 165).
2. Press the **Configure** navigation key.

   A configuration menu appears.
3. Do the following:

a Use the left and right arrows to go to the TCP/UDP Filter menu (see Figure 35).

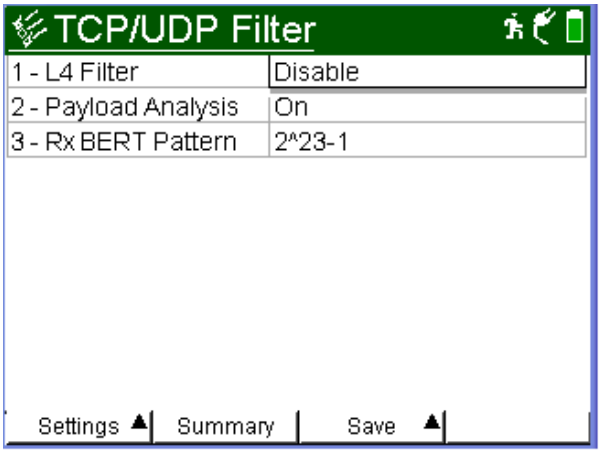


Figure 35 TCP/UDP Filter configuration menu

b Specify values for the following settings:

Setting	Parameters
L4 Filter	– If you want to filter received traffic using layer 4 criteria, select **Enable**. If you want to analyze only layer 4 traffic, you must enable the filter. – If you do not want to filter received traffic using layer 4 criteria, select **Disable**.
Traffic Mode (if L4 Filter is Enabled)	– To analyze traffic with TCP headers only, select **TCP**. – To analyze traffic with UDP headers only, select **UDP**. – To analyze all layer 4 traffic, select **Don't Care**.

Setting	Parameters
Source Port Filter (if L4 Filter is Enabled)	– To analyze traffic originating from a particular port, select **Yes**. – To analyze traffic originating from any port, select **Don't Care**.
Source Port (If Source Port Filter is Enabled)	Enter the source port number carried in the layer 4 header of filtered packets. **NOTE:** You can optionally use the Discover soft key to discover other instruments on the circuit, and then select the source port for the device you want to filter traffic for. For details, see "Using J-Connect to discover another JDSU test set" on page 21
Dest. Port Filter (if L4 Filter is Enabled)	– To analyze traffic sent to a particular port, select **Yes**. – To analyze traffic sent to any port, select **Don't Care**.
Destination Port (if Dest. Port Filter is Enabled)	Enter the destination port number carried in the layer 4 header of filtered packets.

4 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The unit is configured to analyze received traffic satisfying the layer 4 filter criteria.

Transmitting layer 4 traffic

After you configure the layer 4 settings, you are ready to transmit traffic over the circuit.

To transmit layer 4 traffic

1. If you haven't already done so, launch the IPv4 or IPv6 Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select the Layer 4 Traffic test (see "Selecting a layer 4 TCP/UDP test" on page 165).
2. Initialize the Ethernet link (see "Initializing the link for Ethernet testing" on page 47.
3. Establish an IPoE connection or PPPoE session:
   - If you are transmitting IPv4 traffic, see "Establishing an IPoE connection for IPv4 traffic" on page 122, or "Establishing a PPPoE session" on page 128.
   - If you are transmitting IPv6 traffic, see "Establishing an IPoE connection for IPv6 traffic" on page 124.
4. Configure the HST as appropriate for your test (see the appropriate procedures below):
   - "Specifying frame characteristics" on page 51
   - "Configuring the traffic load" on page 56
   - "Filtering received traffic using layer 2 criteria" on page 65
   - "Specifying IP packet settings" on page 137
   - "Filtering received traffic using layer 3 criteria" on page 142
   - "Specifying the traffic mode and ports" on page 169
   - "Filtering received traffic using layer 4 criteria" on page 175
5. Press the Home button to view the Main screen.

6 Press the **Action** soft key again, and then select **Start Traffic** (if you configured a constant, bursty, or flooded load), or **Start Ramp** (if you configured a ramped traffic load).

The HST-3000 transmits traffic over the circuit.

Inserting errors

You can use the HST-3000 to insert errors (such as TCP/UDP checksum errors) into layer 4 traffic when you perform end-to-end and loopback tests. For details on error insertion, see "Inserting errors" on page 81 of Chapter 3 "Ethernet Testing".

Inserting pause frames

You can insert pause frames into the traffic stream when transmitting layer 4 traffic. For details on pause frame insertion, see "Inserting pause frames" on page 83 of Chapter 3 "Ethernet Testing".

Loopback testing

Loopback testing allows you to transmit traffic from one HST-3000, and then loop the traffic back through a second HST-3000 on the far end of a circuit. For details on loopback testing, see "Loopback testing" on page 87 of Chapter 3 "Ethernet Testing".

Multiple Streams Testing

6

This chapter provides step-by-step instructions for transmitting and analyzing multiple streams of Ethernet, IP, or TCP/UDP traffic using the HST-3000 with an Ethernet SIM. Topics discussed in this chapter include the following:

About multiple streams testing

Using the HST-3000 with an Ethernet SIM, you can transmit up to eight streams of layer 2 Ethernet, layer 3 IP, or layer 4 TCP/UDP traffic carrying an Acterna Test Packet (ATP) payload. Before transmitting the streams, you can set up each stream to depict a particular type of traffic, and then verify that network routing and switching devices prioritize the traffic properly. You can also verify the bandwidth utilized and observe a count of transmitted, received, and lost frames or packets for each respective stream.

Selecting a multiple streams test

When testing multiple streams, you must select a layer 2, layer 3, or layer 4 streams test for your application.

To select the test

1. If you haven't already done so, launch the IPv4 Multiple Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28).
2. Select one of the following tests:
   - Layer 2 Streams.
   - Layer 3 Streams.
   - Layer 4 Streams.
3. If Press the **Configure** key, and then use the left and right arrow keys to go to the Test Mode configuration menu.
4. Do the following:
   a. Specify the result precision and unit of measure (see "Specifying test mode and network visibility settings" on page 30 of Chapter 1 "Getting Started".

b If you selected a layer 3 or layer 4 test, indicate whether you want to specify a packet or frame length when you configure IP or TCP/UDP traffic by selecting **Packet Length** or **Frame Length**.

c If you selected a layer 3 test, and you intend to transmit MPLS encapsulated traffic in every enabled stream, set MPLS Mode to **Enabled**; otherwise, select **Disabled**.

If you enable MPLS Mode, you can specify the MPLS EtherType and MPLS labels for each stream on the EthConfig per Stream configuration menu (see "Configuring traffic streams" on page 187).

The test is selected.

Enabling streams and specifying the traffic load

Before transmitting multiple traffic streams, you must specify the traffic characteristics that will apply to *all enabled streams*, enable each individual stream you intend to transmit, and configure the traffic load for the streams.

To enable traffic streams

1 If you haven't already done so, launch the IPv4 Multiple Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select your test (see "Selecting a multiple streams test" on page 182).

2 Press the **Configure** navigation key.

A configuration menu appears.

3 Press the **Settings** soft key, and then select the All Streams menu.

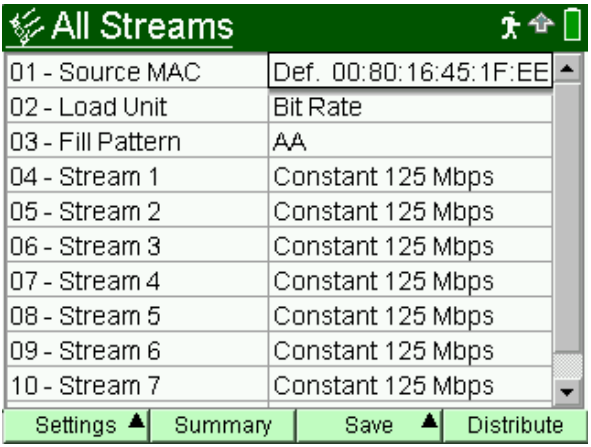


Figure 36 All Streams menu

4 Specify the following settings. These settings will apply to *every enabled stream*:

Settings	Parameters
Source MAC Mode (Layer 2 Streams only)	– If you want to assign a single source MAC address to be used by all enabled streams, select **Single**. – If you want to assign a different address for each stream, select **Per Stream**. **NOTE:** If you are running a layer 3 streams test, the Source Type is specified on the IP Init configuration menu.

Settings	Parameters
Source MAC (If Source MAC Mode is Single)	– If you want to use the factory assigned MAC address as the source address for transmitted streams, select **Factory Default**. – If you want to specify the source MAC address to be carried in transmitted streams, select **User Defined**, then type the address in the Source MAC fields. **NOTE:** If you indicated that you want to assign MAC addresses on a per stream basis, you must specify the addresses on the Eth Config per Stream configuration menu.
Load Unit	Indicate whether you intend to specify the bandwidth for each stream as a **Percent** of the line rate, or as a **Bit Rate** (in Mbps).
Fill Pattern	Specify the pattern that will populate the ATP payload for the transmitted streams.

5 If you are transmitting layer 3 or layer 4 streams, do the following:

a Use the left and right arrows to go to the IP Init configuration menu.

b If you are transmitting layer 3 streams, in Source Type, indicate whether you want to use **DHCP** to assign a source IP address to be used by all enabled streams, assign a **Static IP -Single** to be used by all enabled streams, or a **Static IP - Per Stream** to specify a different IP address for each stream.

If you are transmitting layer 4 streams, select **DHCP** or **Static IP - Single**. The same address will be used for all enabled streams.

c If you selected **Static IP - Single**, in Source IP, enter the address that will be used by all enabled streams.

If you selected **Static IP - Per Stream**, you will specify each stream's IP address on the IP Config per Stream configuration menu.

6 For each stream you want to enable, do the following:

a Use the up and down arrow keys to highlight the stream, and then press **OK**.

b Select **Constant** or **Ramped**.

c If you selected a constant load, specify the load as a percentage or a bit rate. If you indicate that you want to transmit a constant load for every enabled stream, you can optionally use the Distribute soft key to automatically distribute the load evenly across the streams.For a detailed discussion of constant traffic loads, refer to "Transmitting a constant load" on page 57.

If you selected a ramped load, specify the starting load (for example,.50 percent or 10 Mbps), and then specify the ramp step.For a detailed discussion of ramped traffic loads, refer to "Transmitting a ramped load" on page 61.

The traffic streams are enabled, and the traffic loads are specified. Proceed to "Configuring traffic streams".

Configuring traffic streams

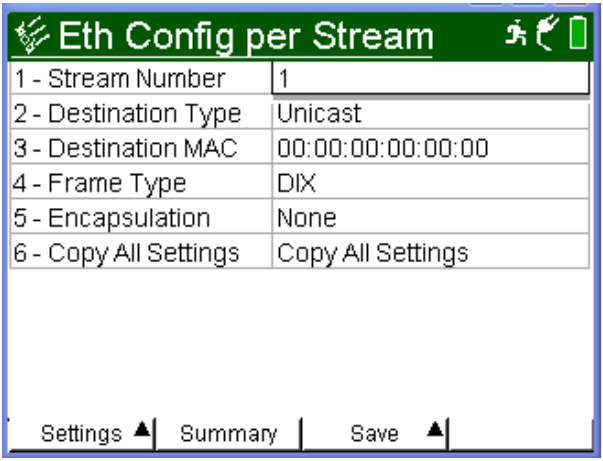
After you specify the traffic characteristics that apply to all streams, enable each of the traffic streams you want to transmit, and specify the traffic loads, you specify the layer 2, layer 3, and layer 4 characteristics for each stream (as appropriate). For example

- If you are transmitting layer 2 streams, you simply specify the layer 2 settings for each stream.
- If you are transmitting layer 3 streams, you specify layer 2 and layer 3 characteristics.
- If you are transmitting layer 4 streams, you specify layer 2, layer 3, and layer 4 characteristics.

To configure traffic streams

1. If you haven't already done so, launch the IPv4 Multiple Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select your test (see "Selecting a multiple streams test" on page 182).
2. Specify the settings that will apply to every enabled stream, enable the streams you want to transmit, and configure the traffic loads (see "Enabling streams and specifying the traffic load" on page 183).

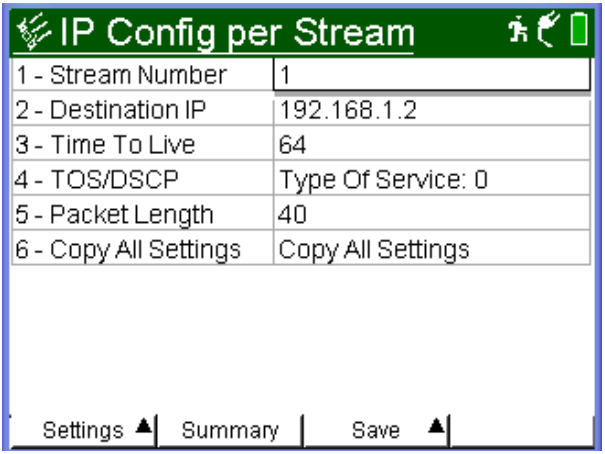
3 Use the right arrow key to go to the Eth Config per Stream menu, and then specify the layer 2 characteristics for the first stream.



To specify settings for additional streams, in Stream Number, specify the next stream number.

For an explanation of each of the settings, see step 4 on page 52 of “Specifying frame characteristics”.

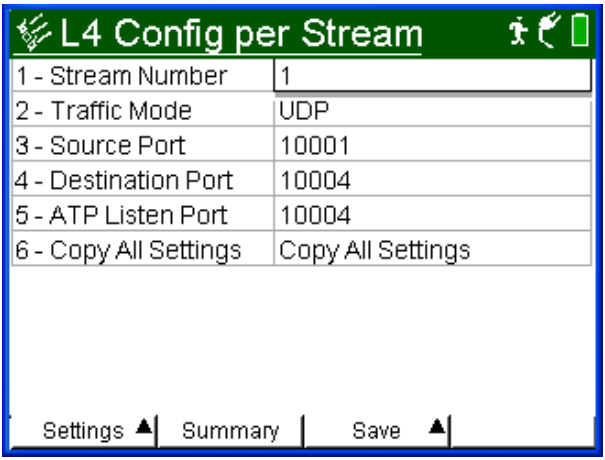
4 If you are transmitting layer 3 or layer 4 streams, use the right arrow key to go to the IP Config per Stream menu, and then specify the layer 3 characteristics for each stream.



If you are running a layer 3 test, and you indicated that you want to specify a different source IP address for each stream, be certain to enter the **Source IP** for each stream.

For an explanation of each of the settings, see step 3 on page 138 of “Specifying IP packet settings”.

5 If you are transmitting layer 4 streams, use the right arrow key to go to the L4 Config per Stream menu, and then specify the layer 4 characteristics for each stream.



For an explanation of each of the settings, see step 3 on page 170 of "Specifying the traffic mode and ports". For an explanation of the ATP Listen Port setting, see "Understanding the ATP Listen Port" on page 164.

6 If you need to specify other settings for the test, use the left and right arrow keys to go to the appropriate configuration menu; otherwise, press the **Home** key to return to the Summary Results screen.

The traffic streams are configured.

Copying a stream's settings to all streams

After you configure a traffic stream, you can optionally copy the stream's settings to the remaining streams.

To copy a traffic stream's settings

1. If you haven't already done so, launch the IPv4 Multiple Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select your test (see "Selecting a multiple streams test" on page 182).
2. Specify the settings that will apply to every enabled stream, enable the streams you want to transmit, and configure the traffic loads (see "Enabling streams and specifying the traffic load" on page 183).
3. Configure the first traffic stream (see "Configuring traffic streams" on page 187).
4. On the Eth Config per Stream, IP Config per Stream, or L4 Config per Stream configuration menu, select **Copy All Settings**.

   A message will appear asking if you want to copy the settings to every other enabled stream.
5. Select **OK**.

The HST copies the settings to every traffic stream.

Transmitting multiple streams

After you enable and configure traffic streams, you are ready to transmit the streams over the link.

1. If you haven't already done so, launch the IPv4 Multiple Stream Terminate application for the circuit you are testing (see "Launching an application" on page 28), and then select your test (see "Selecting a multiple streams test" on page 182).
2. Press the **Configure** navigation key.

   A configuration menu appears.

3 Use the left and right arrow keys to go to the Link Init menu, and then specify the settings required to initialize an Ethernet link (see "Initializing the link for Ethernet testing" on page 47).

4 If you are transmitting multiple streams of layer 3 or layer 4 traffic, go to the IP Init menu, and then specify the settings required to establish an IPoE connection (see "Establishing an IPoE connection for IPv4 traffic" on page 122).

5 Specify the settings that will apply to every enabled stream, enable the streams you want to transmit, and configure the traffic loads (see "Enabling streams and specifying the traffic load" on page 183).

6 Configure the streams (see "Configuring traffic streams" on page 187).

7 Press the **Home** key to return to the Summary Results screen.

8 Press the **Action** soft key again, and then select **Start Traffic**.

The HST-3000 transmits the traffic streams.

– If you are transmitting multiple layer 3 IP or layer 4 TCP/UDP streams, and you enabled ARP Mode, actions will not be available until all enabled streams ARP successfully.
– If you indicated that you wanted to use a DHCP server to obtain IP addresses for each stream, actions will not be available until an IP address is assigned to each stream.
– If your action buttons are not available, you can determine whether ARP or DHCP was successful by observing the IP Config test results (see "IP Config results" on page 294).

For details on ARP and DHCP settings, see "Establishing an IPoE connection for IPv4 traffic" on page 122.

Loopback testing

Loopback testing allows you to transmit multiple streams of Ethernet, IP, or TCP/UDP traffic from one HST-3000 (or another JDSU Ethernet test set), and then loop the streams back through a second unit on the far end of a circuit.

When looping back multiple streams of traffic, if an enabled stream does not successfully loop, the unit will not loop up the remaining streams. For example, if you are trying to loop up a series of four enabled streams, and stream one and stream two successfully loop, but stream three fails, the unit will not loop up stream three or stream four.

For step-by-step instructions, see "Loopback testing" on page 87 of Chapter 3 "Ethernet Testing".

Viewing test results for a stream

After you start a test, the Summary category appears showing an overview of the test results. You can view test results for an individual traffic stream by selecting the Streams category, and then specifying the stream number.

To view test results for a particular stream

1. Configure and run a multiple streams test.
2. Press the **Display** soft key, and then select the **Streams** category.

   A menu appears listing Stream 1 through Stream 8.
3. Select the stream you want to view results for.

The test results for the stream appear. For descriptions of the test results associated with multiple stream testing, see "Streams results" on page 289.

Automated RFC 2544 Testing

7

This chapter describes the automated RFC 2544 testing feature. Topics discussed in this chapter include the following:

About RFC 2544 testing

Using the HST-3000 with an Ethernet SIM, you can run RFC 2544 tests which automate the procedures recommended in RFC 2544 for Ethernet.

Classic RFC 2544 test—The classic RFC test prompts you to select key parameters for throughput, round trip time, frame loss rate, and back to back frame tests, runs the tests, and then automatically generates a text file of results for the tests. A PDF file is also generated which includes the test results in tabular and graphical formats. PDFs are not generated in every language; however, if a report is not generated in a particular language, an English PDF will be generated.

Expert RFC 2544 test—The expert RFC test allows you to configure and run the test just as you would any other test, using the standard configuration menus and actions. When you configure the test, you can indicate that you want to run a symmetrical, or an upstream, downstream, or combined asymmetrical test.

What's new

This release of the Ethernet SIM supports system recovery testing per RFC 2544. You can now use the HST to determine the amount of time it takes for a network element to recover from a state where it is dropping frames. For details, see "About the System Recovery test" on page 205.

Features and capabilities

The Ethernet SIM supports the following features when running the RFC 2544 tests:

- Q-in-Q support. You can transmit Q-in-Q encapsulated traffic when running the test.
- PPPoE support. You can configure your unit to emulate a PPP client, login to a PPP peer to establish a PPPoE session, and then transmit IPv4 packets over an electrical Ethernet circuit when running the test.

– IPv6 support. If you purchased the IPv6 Traffic option, you can transmit IPv6 traffic when running the test.
– Layer 4 support. If you purchased the TCP/UDP option, you can transmit layer 4 traffic when running the test.
– Graphical output of key results. When running the tests, frame loss, throughput, and latency (round trip delay) results are now 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.
– Expert RFC 2544 test. You can run symmetrical or asymmetrical Expert RFC 2544 tests. When running an asymmetrical test, you can run the test upstream, downstream, or in both directions.
– Asymmetric testing. You can run the Expert RFC 2544 test in asymmetric mode in an end-to-end configuration. This is useful for testing circuits carrying traffic at different upstream and downstream line rates. The test is initiated by a master tester (on the near end). The master tester then automatically configures the slave tester on the far end.
– JDSU Discovery. You can now discover other test instruments on the same subnet, and automatically configure your instrument to run the test using one of the discovered instruments as its test partner.

About symmetrical RFC 2544 tests

The Classic RFC 2544 test, or the Expert RFC 2544 test in symmetrical mode is useful if the uplink and downlink speeds on the circuit you are testing are the same. When running this test, the tester on the near-end loops up a tester on the far

end, then transmits traffic which is looped back to the near end. Before running this test, verify that the near end tester is not in LLB or loop back mode.

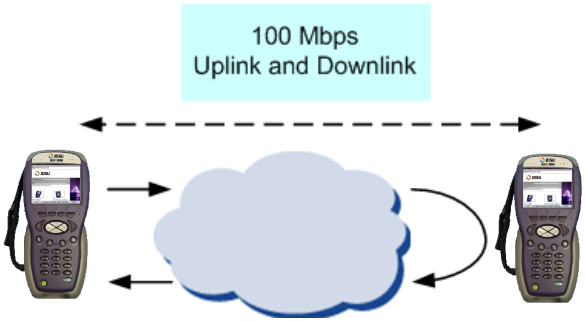


Figure 37 Symmetrical RFC test

About asymmetrical Expert RFC 2544 tests

The new RFC 2544 test is useful if the uplink and downlink speeds on the circuit are different (as illustrated in Figure 13 on page 67). The test can be run end-to-end; no loopback is required. When you configure the test, you indicate that you are testing Upstream, Downstream, or in both directions (Combined).

Upstream - If you are testing Upstream, the master instrument configures a slave instrument to prepare it to receive traffic, sends traffic, then queries the slave for results concerning the upstream link.

Downstream - If you are testing Downstream, the slave generates traffic (as configured on the master instrument), and then transmits the traffic to the master. Results for the downstream link are then displayed on the master tester.

Uplink and downlink results can then be observed on the master tester.

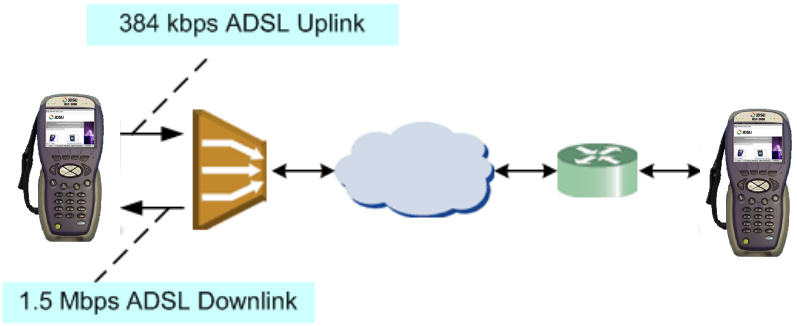


Figure 38 Asymmetrical RFC test

Combined - If you indicate that you want to run a combined test, an upstream test is performed, followed by a downstream test. Results can be observed on the master tester.

About the Throughput test

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

You now have the option to use the Standard RFC zeroing-in method for the throughput test (which is required when testing a half duplex link) or the new Enhanced JDSU zeroing-in method.

Standard RFC method

The Standard RFC zeroing-in method functions as follows:

Attempting Phase

For each frame length you select, beginning at the maximum test bandwidth you specified, the HST determines whether the number of transmitted frames carrying an Acterna payload is

equal to the number of frames carrying an Acterna payload received over a 5 second interval of time. If the maximum bandwidth shows no frame losses, it proceeds to the Verification phase. Otherwise, it proceeds to the Attempting Phase, Bandwidth Reducing Stage.

Attempting Phase, Bandwidth Reducing Stage

If frames were lost in the last attempt, the bandwidth is reduced by 50%, rounded to the nearest tenth, hundredth, or thousandth percent specified as the Bandwidth Measurement Accuracy. Traffic is then transmitted at the reduced bandwidth for another 5 seconds. If frames are lost, this stage is repeated. Otherwise, it proceeds to the Bandwidth Increasing Stage.

Attempting Phase, Bandwidth Increasing Stage

If no frames were lost, the bandwidth is increased by 50%, and traffic is transmitted. If no frames are lost, the Bandwidth Increasing Stage is repeated (bandwidth is increased again by 50%). Otherwise, it returns to the Bandwidth Reducing Stage.

The Attempting Phase continues until either no frames are lost, or the transmitted bandwidth reaches the lowest bandwidth limit (specified as the Bandwidth Measurement Accuracy). If the lowest bandwidth limit is reached without successfully receiving every transmitted frame, the test indicates that each of the test results is unavailable.

If Throughput results are unavailable, Latency and Packet Jitter results can not be derived; therefore, they will also be unavailable.

Verifying Phase

After the test determines the maximum bandwidth at which no frames are lost, it then transmits traffic at that bandwidth for the Throughput Trial Duration. If frames are lost, the test reduces the bandwidth by the Bandwidth Measurement Accuracy, and then retransmits traffic for the Throughput Trial Duration.

JDSU Enhanced method

The JDSU Enhanced 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%:
  - For 1Gig the test increases the load 3% over the L2 Avg. % Util measured above.
  - For 10 Mb we increase the load 30% over the L2 Avg. % Util measured above.
  - For 100 Mb we increase the load 3% over the L2 Avg. % Util measured above, or to 100%, if the above increase would exceed 100%.
- 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 you 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

Indicates whether or not pause frames were detected at the point where no frames were lost for a particular frame length.

These results are also reported when you run the Latency and Packet Jitter tests. See Figure 42 on page 223 for sample graphical results and result measurements.

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.

About the Latency (RTD) test

If you intend to run the Latency test as part of the test, you must also run the Throughput test. The Latency 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 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. Delay measured under 4 microseconds is averaged as 4 microseconds. Unavailable measurements are not included in the total trial average.

NOTE:

When running the Latency test in asymmetric mode, after looping up the instrument on the far end, the instrument performs a *symmetric* throughput test. Because the instrument loops up the far end instrument, the upstream and downstream latency measurements in asymmetric mode are actually the same measurement.

Latency test test results

See Figure 44 on page 225 for sample result measurements.

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.

About the Packet Jitter test

If you intend to run the Packet Jitter test as part of the test, you must also run the Throughput 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 otherworlds, 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. See Figure 43 on page 224 for sample result measurements.

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.

About the System Recovery test

If you intend to run the System Recovery test, the Expert RFC 2544 mode must be Symmetric, and you must also select and run the Throughput test. The HST uses the Throughput test to determine the maximum bandwidth at which no frames were lost, then the System Recovery test transmits traffic at 110% of the bandwidth (referred to as the “overload rate”) to force the receiving network element to drop

frames for each frame length you selected. The HST transmits the overload rate for at least 60 seconds, then reduces the transmission rate to 50 percent of the overload rate (referred to as the “recovery rate”). The HST then measures the time it takes for the network element to reach a state where it is no longer dropping frames.

If the Throughput test reaches the lowest bandwidth limit without ever successfully receiving all transmitted frames (in otherworlds, it lost frames), the System Recovery test will not run.

System Recovery test results

System Recovery results are presented statistically and graphically. See Figure 45 on page 226 for sample result measurements.

About the Frame Loss test

For each frame length you select, beginning at the maximum test bandwidth you specified, the HST transmits traffic for the amount of time you specified as the Frame Loss Trial Duration. If frames are lost during that time frame, the HST 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 HST 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 HST starts the entire process over again until two successive trials occur without losing frames.

Frame Loss test test results

Frame Loss results are presented in a tabular format, illustrating the frame loss rate versus the percent of the bandwidth. See Figure 45 on page 226 for sample graphs and result measurements.

About the Back to Back Frames test

Using the frame length and other settings such as the frame type and encapsulation, the HST 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 HST goes through the stages described for the Throughput test (see "About the Throughput test" on page 199) 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. See Figure 46 on page 227 for sample result measurements.

Optimizing the test time

When you configure a classic RFC 2544 test, or an Expert RFC 2544 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.

When running the Expert RFC 2544 test in asymmetric mode, the Latency test is run *after* the Throughput test, because it needs the symmetric Throughput measurement before it can measure latency.

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.

Running the Classic RFC 2544 test

Before running the Classic RFC 2544 test, it's important to understand which settings need to be specified outside of the automated test, and how to navigate through the screens and menus presented when you run the test.

Understanding the external settings

The test prompts you for most of the required settings; however, certain settings need to be specified outside of the automated test using the standard configuration menus listed in Table 13.

Table 13 RFC 2544 Configuration Menu Settings

Layer/Setting	To specify, see....
Layer 2 – Frame Type – Unit Identifier – Destination Type – Ether Type	"Specifying frame characteristics" on page 51
Layer 3 – TTL – TOS/DSCP – Protocol	"Specifying IP packet settings" on page 137
Layer 4 – ATP Listen Port	"Specifying the traffic mode and ports" on page 169

The test automatically prompts you for the remaining settings.

Navigating through the test

When navigating the screens and menus presented by the test, follow these guidelines:

– Use **OK** key to enable settings, or to proceed to the next screen.

- If **OK** is used to enable a setting, use the **Accept** soft key to proceed to the next screen.
- Use **Cancel** to return to the previous screen.
- If you change a setting for an existing test configuration, the unit will automatically prompt you to overwrite the existing configuration or create a new configuration (using the modified settings) by entering a new name.
- Use the **Summary** soft key to view the HST Setup screen and review key settings for the test.

Running the test

Before running the RFC 2544 test, verify that no other applications are running.

To run the Classic RFC 2544 test

1. Specify any settings that are not specified in the test. For details, see "Understanding the external settings" on page 209.
2. Press the **AutoTest** button.

   A test menu appears, with softkeys that allow you to display the ETH ELEC Scripts, ETH OPT Scripts, IPv6 ELEC Scripts, or IPv6 OPT Scripts menu. The IPv6 menus only appear if you purchased the IPv6 software option.
3. If necessary, use the left and right arrow key to display the appropriate menu for the rate you are testing, and then select the test.

   A screen appears briefly indicating that the test is launching, then the Choose Configuration menu appears. The menu lists any existing test configurations and provides options that allow you to create or delete configurations.

4 Do one of the following:

- If a configuration exists with the settings (or the majority of the settings) that you need to run the test, select the configuration from the menu. The Run or Edit Configuration As dialog box appears.
- To run the test without modifying the configuration settings, select **RUN**. Proceed to step 9 on page 213.
- To create a new configuration using the selected configuration as a template, type a name for the new configuration, and then select **OK**. The HST Setup dialog box appears, listing key parameters specified for the test. Proceed to step 5 on page 211.
- If you want to create a new configuration, select **New Configuration**. The New Configuration Name dialog box appears. Type a name for the new configuration, and then select **OK**. The HST Setup dialog box appears, listing key default parameters specified for the test. Proceed to step 5 on page 211.

5 Do one of the following:

- If the parameters on the HST Setup dialog box are acceptable, select **OK**, and then proceed to step 6 on page 212.
- If you need to change any of the parameters displayed on the HST Setup dialog box, select **Change**. The Choose Test Type menu appears. Select one of the following:

  Layer 2 Traffic - to run the script in layer 2 test mode.

  Layer 3 IP Traffic - to run the script in layer 3 test mode.

  Layer 4 Traffic - to run the script in layer 4 test mode.

  Proceed to step 6 on page 212.

6 A series of setup menus appear, listing options for configuring the test type you selected in step 5 on page 211.

- If the displayed parameters are acceptable, simply select **OK** or **Accept** to proceed to the next menu.
- If you want to change parameters for the test, use the up and down arrow keys to select a new value, or specify the new value, and then select **OK** or **Accept** to store the parameter and proceed to the next menu.
- If you want to return to a previous menu to change a setting, select **Cancel**.

After the test type parameters are all accepted or specified, the RFC 2544 Configurations dialog box appears, listing the configuration name, test name, the tests to run during the course of the test, and key parameters for each of the tests. Proceed to step 7 on page 212.

7 Do one of the following:

- If the current parameters for each of the tests on the RFC 2544 Configurations dialog box are acceptable, select **Run**, and proceed to step 9 on page 213.
- If you need to change the tests selected for the script, or change parameters for the tests, select **Change**, and then proceed to step 8 on page 212.

8 Use **OK** and **Accept** to navigate through a series of dialog boxes which prompt you to specify key parameters required for the test (for example, frame lengths, test options, and bandwidth criteria). Additional parameters for the test options you selected include:

When testing …	Specify…
Throughput	– the trial duration (in seconds) – the bandwidth measurement accuracy – pass/fail criteria
Latency (round trip delay)	– the number of trials – the trial duration (in seconds) – pass/fail criteria

When testing …	Specify…
Packet Jitter	– the number of trials – the trial duration (in seconds) – pass/fail criteria
Frame Loss	– the trial duration (in seconds) – the maximum bandwidth – the bandwidth granularity (as a percentage for the step)
Back to Back Frames	– the number of trials – the burst granularity – the maximum trial time

After you specify the final parameter, select **OK** to run the test. Proceed to step 9 on page 213.

9 A screen appears displaying the status of key events for the test, and a progress indicator appears that shows the estimated minimum amount of time required for the test to complete, It also provides a graphical illustration of the percent already completed.

– To scroll up or down through the events on the screen line by line, use the up or down arrow key.

– To scroll up or down a page at a time, press **Page Up** or **Page Down**.

The Classic RFC 2544 test is running.

NOTE:

You can stop the test script at any time using the **Stop** soft key.

Running the Expert RFC 2544 test

Running the Expert RFC 2544 test involves the following:

- Launching a single stream terminate application.
- Specifying the RFC 2544 Mode on the Test Mode configuration menu.
- Specifying the RFC 2544 settings, such as the load format (bit rate or percentage) and length type (frame or packet lengths).
- Enabling each of the tests that you want to run during the course of the RFC 2544 test.

Asymmetric testing for PPPoE and IPv6 traffic is not supported in this release.

When running the Expert RFC 2544 test, the Start Traffic action is turned off, because the test automatically transmits traffic when you start the test.

Running the test

Before running the Expert RFC 2544 test, verify that no other applications are running.

To run the Expert RFC 2544 test

1. If you haven't already done so, launch a single stream terminate application for the circuit you are testing (see "Launching an application" on page 28).
2. Initialize the link (see "Initializing the link for Ethernet testing" on page 47).
3. If you are using the JDSU Discovery feature to find your instrument's test partner (and configure key settings on your instrument), press the **Home** button to return to the Summary Results screen, press the **Action** soft key, then select **Discover Units**. For details on this feature, refer to "Discovering another JDSU test instrument" on page 166.

4 Use the right arrow key to display the Test Mode configuration menu, and then do the following:

a Specify the standard test mode settings (see "Specifying test mode and network visibility settings" on page 30).

b In RFC 2544 Mode, select **Symmetric**, **Asym Upstream**, **Asym Downstream**, or **Asym Combined**. If you intend to run the System Recovery test, you must select **Symmetric** mode.

5 Use the right arrow key to display the RFC 2544 Settings configuration menu, and then specify the following:

Setting	Parameter
Load Format	– Bit Rate – Percentage
AutoSave	– Enable – Disable
Customer	If you want the customer name to appear in report output, enter a name.
Technician	If you want the technician name to appear in report output, enter a name.
Location	If you want the location where you launched the test to appear in report output, enter it.
Comments	If you want to include comments in the report output, enter them.
NOTE: The following address settings are specified on the IP Init menu if you run the test using layer 3 or layer 4 traffic. They appear on the Network Visibility menu when you run the test using layer 2 traffic.	

Setting	Parameter
Remote IP	If you are running the test with layer 2 traffic, specify the remote IP address for the instrument on the far end.
Source IP	If you are running the test with layer 2 traffic, specify the source IP address for your instrument.
Default Gateway	If you are running the test with layer 2 traffic, specify default gateway.
Subnet Mask	If you are running the test with layer 2 traffic, specify subnet mask.

6 Specify the following settings as appropriate for your test:

a Layer 2 Settings (see "Configuring layer 2 Ethernet tests" on page 51).

b Layer 3 Settings (see "Configuring layer 3 IP tests" on page 136).

c Layer 4 Settings (See "Configuring layer 4 traffic" on page 167).

7 Use the left or right arrow key to go to the Test Selections, Test Selections (Upstrm) or Test Selections (Dnstrm) configuration menu, and then Enable the tests you want to run. You must enable the Throughput test to enable the Latency (RTD), System Recovery, and Packet Jitter tests.

If you are running the test in Asym (Combined) mode, Test Selection menus appear for both upstream and downstream tests.

8 Specify the maximum bandwidth to transmit during the course of each of the enabled tests.

NOTE: RFC 2544 tests always transmit a constant load of traffic.

9 Go to the Frame Length menu, then specify the length for Frame 1 through Frame 8. The instrument will transmit a series of frames with each length during the course of the Throughput test.

10 Go to the Throughput menu, then specify the accuracy, test duration, frame loss tolerance, and show pass/fail status settings.

NOTE: If you are transmitting jumbo frames, allow at least ten seconds after starting the test to reach the bandwidth specified.

11 If you enabled the Latency (RTD) test, go to the Latency menu, then specify the number of trials, trial duration, and show pass/fail status settings.

12 If you enabled the Packet Jitter test, go to the Jitter menu, then specify the number of trials, trial duration, and show pass/fail status settings.

13 If you enabled the System Recovery test, go to the System Recovery menu, then specify the number of trials and overload duration (at least 60 seconds).

14 If you enabled the Frame Loss test, go to the Frame Loss menu, then specify the test procedure (RFC 2544, top down, or bottom up), the trial duration, and the test granularity settings.

15 If you enabled the Back to Back Frames test, go to the Back to Back menu, then specify the number of trials, burst granularity, and maximum trial time

16 If you indicated that you want to run the Asymmetrical RFC in Combined mode, repeat step 7 on page 216 through step 15 on page 217 for the downstream tests.

17 If you haven't already done so, specify the remaining settings as appropriate for the traffic you are using for the test:

- IP Init (see "Establishing an IPoE connection for IPv4 traffic" on page 122).
- IP (see "Specifying IP packet settings" on page 137).
- TCP/UDP (see "Configuring layer 4 traffic" on page 167).

18 Press the **Home** button to return to the Summary Results screen.

19 Press the **Action** soft key, then select **Start RFC 2544**.

The RFC 2554 Log appears, which displays the status of key events during the course of the test.

- To scroll up or down through the events on the screen line by line, use the up or down arrow key.
- To scroll up or down a page at a time, press the blue up arrow key at the bottom, and the up or down arrow key at the top simultaneously.

The RFC 2544 test is running.

NOTE:

You can stop the test at any time by pressing the Action key, and then selecting **Stop RFC 2544**.

Viewing RFC 2544 test results

After running the test, the unit stores a text file and a PDF of the test results in the following directory:

```
/results/rfc2544
```

You can view the text file on your unit using the File Manager. To view the PDF file, you must first retrieve the file from your unit using `ftp`, and then view the file on a workstation with a PDF viewer. For details, see the *HST-3000 Base Unit User's Guide.*

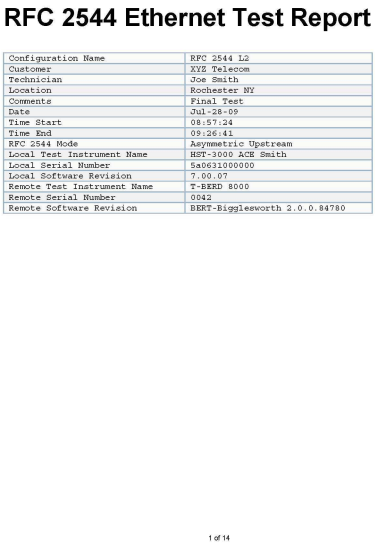
Sample RFC 2544 reports

Sample Expert RFC 2544 reports for tests run in Asymmetric mode are provided in Figure 39 on page 220 through Figure 46 on page 227. The samples provided were not generated using the same test.

The basic report structure consists of a report cover sheet, a summary of the overall test results, a summary of the setup parameters used to run the test, and then the results for each test that you ran.

System information is also provided such as the software version, test instrument name, and the HST's serial number. If you are running an asymmetric RFC 2544 test, this information is provided for the master and the slave HSTs.

Test results reported will vary depending on the circuit you are testing, the type of traffic (layer 2, layer 3, or layer 4), and the symmetric or asymmetric setting that you specified before running the test.

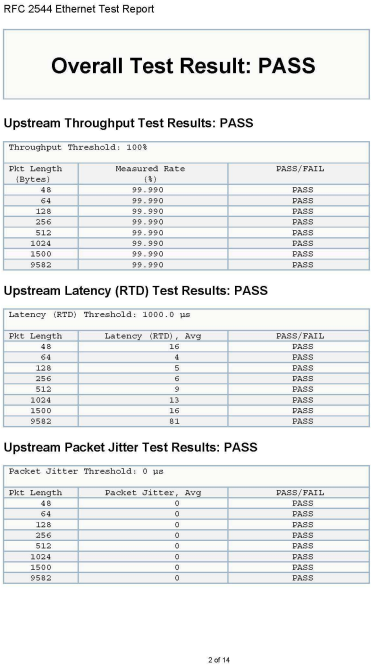


RFC 2544 Ethernet Test Report

Configuration Name	RFC 2544 L2
Customer	XYZ Telecom
Technician	Joe Smith
Location	Rochester NY
Comments	Final Test
Date	Jul-28-09
Time Start	08:57:24
Time End	09:26:41
RFC 2544 Mode	Asymmetric Upstream
Local Test Instrument Name	HST-3000 ACE Smith
Local Serial Number	5a0631000000
Local Software Revision	7.00.07
Remote Test Instrument Name	T-BERD 8000
Remote Serial Number	0042
Remote Software Revision	BERT-Bigglesworth 2.0.0.84780

1 of 14

Figure 39 Sample - Report Cover



RFC 2544 Ethernet Test Report

Overall Test Result: PASS

Upstream Throughput Test Results: PASS

Throughput Threshold: 100%

Pkt Length (Bytes)	Measured Rate (%)	PASS/FAIL
48	99.990	PASS
64	99.990	PASS
128	99.990	PASS
256	99.990	PASS
512	99.990	PASS
1024	99.990	PASS
1500	99.990	PASS
9582	99.990	PASS

Upstream Latency (RTD) Test Results: PASS

Latency (RTD) Threshold: 1000.0 µs

Pkt Length	Latency (RTD), Avg	PASS/FAIL
48	16	PASS
64	4	PASS
128	5	PASS
256	6	PASS
512	9	PASS
1024	13	PASS
1500	16	PASS
9582	81	PASS

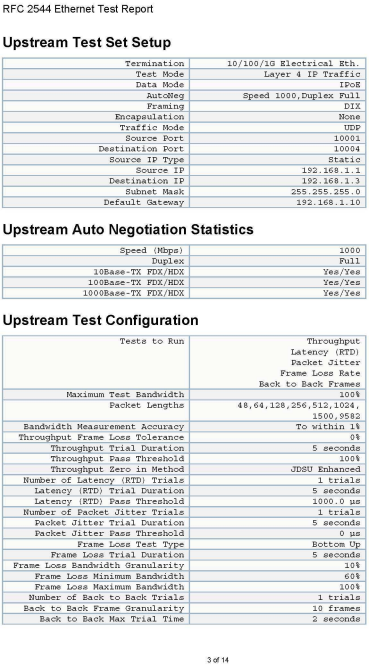
Upstream Packet Jitter Test Results: PASS

Packet Jitter Threshold: 0 µs

Pkt Length	Packet Jitter, Avg	PASS/FAIL
48	0	PASS
64	0	PASS
128	0	PASS
256	0	PASS
512	0	PASS
1024	0	PASS
1500	0	PASS
9582	0	PASS

2 of 14

Figure 40 Sample - Overall Results



RFC 2544 Ethernet Test Report

Upstream Test Set Setup

Termination	10/100/1G Electrical Eth.
Test Mode	Layer 4 IP Traffic
Data Mode	IPoE
AutoNeg	Speed 1000,Duplex Full
Framing	DIX
Encapsulation	None
Traffic Mode	UDP
Source Port	10001
Destination Port	10004
Source IP Type	Static
Source IP	192.168.1.1
Destination IP	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.10

Upstream Auto Negotiation Statistics

Speed (Mbps)	1000
Duplex	Full
10Base-TX FDX/HDX	Yes/Yes
100Base-TX FDX/HDX	Yes/Yes
1000Base-TX FDX/HDX	Yes/Yes

Upstream Test Configuration

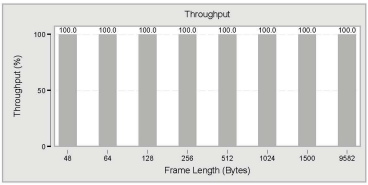
Tests to Run	Throughput Latency (RTD) Packet Jitter Frame Loss Rate Back to Back Frames
Maximum Test Bandwidth	100%
Packet Lengths	48,64,128,256,512,1024, 1500,9582
Bandwidth Measurement Accuracy	To within 1%
Throughput Frame Loss Tolerance	0%
Throughput Trial Duration	5 seconds
Throughput Pass Threshold	100%
Throughput Zero in Method	JDSU Enhanced
Number of Latency (RTD) Trials	1 trials
Latency (RTD) Trial Duration	5 seconds
Latency (RTD) Pass Threshold	1000.0 us
Number of Packet Jitter Trials	1 trials
Packet Jitter Trial Duration	5 seconds
Packet Jitter Pass Threshold	0 us
Frame Loss Test Type	Bottom Up
Frame Loss Trial Duration	5 seconds
Frame Loss Bandwidth Granularity	10%
Frame Loss Minimum Bandwidth	60%
Frame Loss Maximum Bandwidth	100%
Number of Back to Back Trials	1 trials
Back to Back Frame Granularity	10 frames
Back to Back Max Trial Time	2 seconds

3 of 14

Figure 41 Sample - RFC Configuration

RFC 2544 Ethernet Test Report

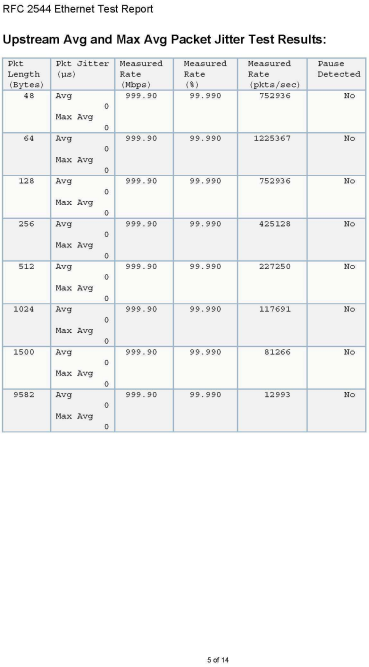
Upstream Throughput Test Results:



Pkt Length (Bytes)	Cfg Rate (Mbps)	Measured Rate (Mbps)	Measured Rate (%)	Measured Rate (pkts/sec)	Pause Detected
48	1000.000	999.899	99.990	752936	No
64	1000.000	999.899	99.990	1225367	No
128	1000.000	999.899	99.990	752936	No
256	1000.000	999.899	99.990	425128	No
512	1000.000	999.899	99.990	227250	No
1024	1000.000	999.898	99.990	117691	No
1500	1000.000	999.899	99.990	81266	No
9582	1000.000	999.903	99.990	12993	No

4 of 14

Figure 42 Sample - Throughput Results



RFC 2544 Ethernet Test Report

Upstream Avg and Max Avg Packet Jitter Test Results:

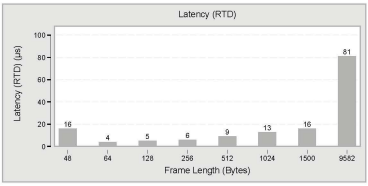
Pkt Length (Bytes)	Pkt Jitter (us)	Measured Rate (Mbps)	Measured Rate (%)	Measured Rate (pkts/sec)	Pause Detected
48	Avg 0 Max Avg 0	999.90	99.990	752936	No
64	Avg 0 Max Avg 0	999.90	99.990	1225367	No
128	Avg 0 Max Avg 0	999.90	99.990	752936	No
256	Avg 0 Max Avg 0	999.90	99.990	425128	No
512	Avg 0 Max Avg 0	999.90	99.990	227250	No
1024	Avg 0 Max Avg 0	999.90	99.990	117691	No
1500	Avg 0 Max Avg 0	999.90	99.990	81266	No
9582	Avg 0 Max Avg 0	999.90	99.990	12993	No

5 of 14

Figure 43 Sample - Packet Jitter Results

RFC 2544 Ethernet Test Report

Upstream Latency (RTD) Test Results:



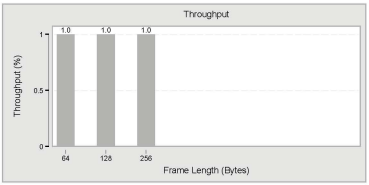
Pkt Length (Bytes)	Pkt Jitter (µs) Delay (µs)	Measured Rate (Mbps) Measured Rate (Mbps)	Measured Rate (%) Measured Rate (%)	Measured Rate (pkts/sec) Measured Rate (pkts/sec)	Pause Detected Pause Detected
48	16	999.90	99.990	752936	No
64	4	999.90	99.990	1225367	No
128	5	999.90	99.990	752936	No
256	6	999.90	99.990	425128	No
512	9	999.90	99.990	227250	No
1024	13	999.90	99.990	117691	No
1500	16	999.90	99.990	81266	No
9582	81	999.90	99.990	12993	No

8 of 14

Figure 44 Sample - Latency Results

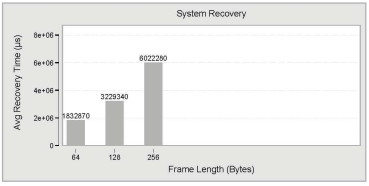
RFC 2544 Ethernet Test Report

Throughput Test Results:



Frame Length (Bytes)	Cfg Rate (Mbps)	Measured Rate (Mbps)	Measured Rate (%)	Measured Rate (frms/sec)	Pause Detected
64	Unavail	10.000	1.000	Unavail	No
128	Unavail	10.000	1.000	Unavail	No
256	Unavail	10.000	1.000	Unavail	No

System Recovery Test Results:



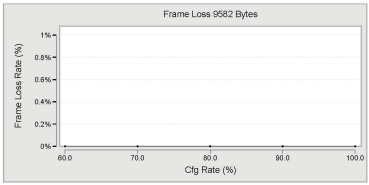
Frame Length (Bytes)	Overload Rate (%)	Recovery Rate (%)	Avg Recovery Time (us)	Pause Detected
64	1.100	0.550	1832870	No
128	1.100	0.550	3229340	No
256	1.100	0.550	6022280	No

4 of 4

Figure 45 Sample - System Recovery Results

RFC 2544 Ethernet Test Report

Frame Loss 9582 Bytes:



Cfg Rate (%)	Throughput Rate (%)	Pkt Loss Rate (%)	Pkts Lost	Pause Detected
60	60.01	0.00	0	No
70	70.00	0.00	0	No
80	80.00	0.00	0	No
90	90.00	0.00	0	No
100	99.99	0.00	0	No

Upstream Back to Back Test Results:

Pkt Length (Bytes)	Average Burst (pkts)	Average Burst (secs)	Pause Detected
48	158970	0.109	No
64	2278640	1.859	No
128	1376570	1.828	No
256	821670	1.933	No
512	441200	1.941	No
1024	207060	1.759	No
1500	160180	1.971	No
9582	25130	1.934	No

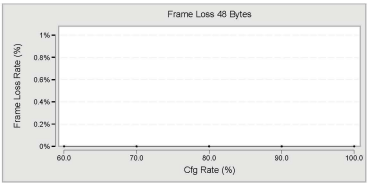
14 of 14

Figure 46 Sample - Back to Back Frame Results

RFC 2544 Ethernet Test Report

Upstream Frame Loss Test Results:

Frame Loss 48 Bytes:



Cfg Rate (%)	Throughput Rate (%)	Pkt Loss Rate (%)	Pkts Lost	Pause Detected
60	60.00	0.00	0	No
70	70.00	0.00	0	No
80	80.00	0.00	0	No
90	90.00	0.00	0	No
100	99.99	0.00	0	No

7 of 14

Figure 47 Sample - Frame Loss Results

SAMComplete Testing

8

This chapter provides information on using the SAMComplete sequence of tests. The following topics are discussed in this chapter:

About SAMComplete

SAMComplete functionality is standard on all units and all Ethernet line rates supported *except IPv6 applications*. Although all applications do not include SAMComplete functionality, if your instrument is appropriately configured for a capable application, you can use it to run the SAMComplete test.

This is a Ethernet Service Activation test Methodology (SAM) for multiple streams based on ITU-T Y.1564. It performs a two-phase test. First, the test verifies whether each service is properly configured by transmitting them individually. Second, multiple service instances are transmitted simultaneously, at its assigned Committed Information Rate (CIR) and performance is validated by ensuring all SLA parameters (FDV, FTD, RTD and Availability) are met.

The test involves the following steps:

– Enable SAMCompete
– Specify test, network and service settings
– Run the test
– Parse test data and provide graphical results

Enabling SAMComplete

Before specifying settings, you must enable the SAMComplete test.

To enable the SAMComplete test

1. If you haven't already done so, launch the Layer 2 or Layer 3 Traffic Terminate or Multiple Stream Terminate application for the circuit you are testing.
2. Press the **Configure** navigation key.

3 On the Summary Settings list, select **SAM Complete** and then select **Symmetric**.

Symmetric is used when only round-trip throughput and SLA parameters are defined because upstream and downstream transmission is identical as the test stream is being looped back to the source at the destination.

The SAMComplete test is enabled.

Specifying settings

After enabling the test, you must specify the settings used for the tests. The available SAMComplete settings vary depending on whether you are running a single-stream or multi-stream application.

Loading a saved configuration

If you have previously specified settings and saved them as a configuration profile, you can load the config profile. This allows consistent setups and quicker startup time.

To load a configuration

1 Press the **Save** soft key.

2 Select **Load Config**.

3 Choose a profile from the list, and then press OK.

Specifying test settings

To specify test settings

1 If you have not previously specified settings or wish to change settings, Press the **Configure** navigation key.

2 Press the **Settings** soft key, and then select **SAMComplete Settings**.

A list of settings appears.

3 From the SAMComplete Settings list, select **Global Settings** and then specify the following settings:

Setting	Description	Parameters
Configuration Test	Select whether to run the service configuration test.	On, Off
Config Test Steps	The number of steps below CIR.	1 - 10
Step Duration	The duration that traffic is generated for each step.	1 - 60 sec
Performance Test	Select whether to run the service performance test.	On, Off
Perf Test Duration	The duration that traffic is generated before the service performance test completes	1 - 1440 min
Stop on Failure	Select whether to stop the test when a failure occurs or continue through to completion.	Yes, No
Customer, Technician, Location, and Comments	If you want them to appear in the report output, enter the customer name, technician name, test location, and comments about the test.	Alphanumeric up to 25 characters

4 If running a multi-stream application, select **Service Select**, and then specify which services should be tested.

5 Select one of the following:

– If running a single-stream application, select **Service Settings**.

– If running a multi-stream application, select **All Services**.

Then specify the following:

Setting	Parameters
Loop Type (L2 applications only)	– Unicast - sends traffic to a single destination address and network device. – Broadcast - sends traffic to all network devices on the link. – **NOTE:** If you select Unicast, you can optionally use the Discover soft key to discover other instruments on the network, and then select the destination address for the device you want to transmit traffic to. For details, see "Using J-Connect to discover another JDSU test set" on page 21
Length Type (L3 applications only)	– Frame Length - Changing Service Properties > Service Type to "Voice, HDTV or SDTV" for any service forces Length Type to Frame Length. – Packet Length - Changes the Service Properties Service Type to "Data" for all services.
Source MAC (multi-stream application only)	– Factory default – User defined (and enter the MAC address)

Setting	Parameters
ARP Mode (L3 applications only)	– Enable - Enable ARP mode if you want the HST to issue an ARP request to automatically determine the MAC address of its link partner. In most instances ARP should be enabled. – Disable - If you disable ARP Mode, be certain to specify the Destination MAC address for the HST's link partner (on the Ethernet menu).
Source Type (L3 applications only)	– DHCP - allows the unit to obtain an IP address for each stream from a DHCP server. – Static - allows you to manually specify the IP, subnet, and gateway addresses. – Static IP-Per Stream allows you to manually specify the IP and other addresses for each stream.
Source IP (L3 applications only)	If the Source Type is Static, enter the source IP address carried by all traffic generated by your unit.
Subnet Mask (L3 applications only)	If the source IP type is Static, enter the subnet mask.
Default Gateway (L3 applications only)	If the source IP type is Static, enter the default gateway address.

6 Select **Service Properties**, and then specify the following settings:

Setting	Parameter
Service Name	Enter the name of the service, up to 21 characters.
Service Type	Select the service type: Data, Voice, HDTV, SDTV. **NOTE:** This setting affects the Length Type on the Service Settings. Voice, HDTV or SDTV forces the Length Type to Frame Type; and, reversely, changing the Length Type to Packet Length forces Service Type to Data.
Frame Type	Select the frame type: DIX, 802.3
Encapsulation	Select the encapsulation: None, VLAN, Q in Q
Codec (Voice Service Type)	Specify the Codec to use for voice calls.
Sampling Rate (Voice Service Type)	Select a sampling rate between 10 and 60 ms.
# Calls (Voice Service Type)	Specify the number of calls to place (max number depends on CIR for codec and interface rate)
# Channels (HDTV or SDTV Service Type)	Specify the number of calls to place (max number depends on CIR for codec and interface rate)
Compression (HDTV or SDTV Service Type)	Specify MPEG2 or MPEG4 compression.

7 Select one of the following:

– If running a single-stream application, select **Ethernet**.

– If running a multi-stream application, select **Network Settings Ethernet**.

Then specify the following settings:

Setting	Parameters
Service Number (multi-stream application only)	Select which service to configure: 1-8
Service Name	Enter the name of the service.
Source Type (L2 single stream applications only)	– Factory default – User defined (and enter the MAC address)
Tx Payload (single-stream application only)	Acterna or BERT (Always select Acterna for SAMComplete test)
Pattern (if Tx Payload is BERT)	Specify which BERT pattern to use for the test.
Acterna Payload (if Tx Payload is Acterna)	Specify whether the Acterna Payload is Fill pattern or BERT.
Fill Pattern (if Acterna Payload is Fill Pattern)	Specify the fill byte using hexadecimal format, up to 64 bytes.
Loop Type (L2 applications only)	– Unicast - sends traffic to a single destination address and network device. – Broadcast - sends traffic to all network devices on the link. – **NOTE:** If you select Unicast, you can optionally use the Discover soft key to discover other instruments on the network, and then select the destination address for the device you want to transmit traffic to. For details, see “Using J-Connect to discover another JDSU test set” on page 21

Setting	Parameters
Destination Type	– Unicast - sends traffic to a single destination address and network device. – Multicast - sends traffic with a multicast address to a group of network devices. – Broadcast - sends traffic to all network devices on the link. **NOTE:** If you select Unicast, you can optionally use the Discover soft key to discover other instruments on the network, and then select the destination address for the device you want to transmit traffic to. For details, see "Using J-Connect to discover another JDSU test set" on page 21.
Destination MAC (appears only if you specified a Unicast or Multicast address type)	Type the address for Unicast or Multicast destinations. – For the Unicast destination type, the left most byte in the address defaults to 00. – For the Multicast destination type, the left most byte in the address defaults to 01.
Frame Type	– DIX – 802.3
EtherType (single-stream application only)	Type the protocol ID for the data in the frames using a 2 byte hexadecimal format. **NOTE:** When transmitting an Acterna payload, the EtherType is automatically set to 0x800 and cannot be changed.

Setting	Parameters
Frame Length	Select one of the following: – A predefined length – Random – Undersized, and then specify the frame length – User Defined, and then specify the frame length – Jumbo Frame, and then specify the frame length
Encapsulation	– None. – VLAN. If you select VLAN, be certain to specify the VLAN ID and Priority. – Q-in-Q. If you select Q-in-Q, be certain to specify the CVLAN (customer VLAN) and SVLAN (service provider VLAN) settings.
Copy All Settings (multi-stream application only)	Specify whether these service settings should be copied and applied to all services.

8 If running a L3 application, select **Network Settings IP**, and then specify the following settings:

Setting	Description
Service Number (multi-stream application only)	Select which service to configure: 1-8
Service Name (multi-stream application only)	Enter the name of the service.
Destination IP	Enter the destination IP address for traffic generated by your unit.

Setting	Description
Time To Live	Specify the time after which a packet can be deleted by any device on a circuit as a number of hops. The default time to live setting is 64 hops.
TOS/DSCP	Enter a number representing the type of service in a binary format, or select a DSCP name.
Copy All Settings (multi-stream application only)	Specify whether these service settings should be copied and applied to all services.
Protocol (single-stream application only)	(Read only field) The protocol ID for the data in the frames using a 2 byte hexadecimal format.
Tx Payload (single-stream application only)	Acterna or Fill Byte
Fill Byte (if Tx Payload is Fill Byte)	Specify the fill byte using hexadecimal format.
Acterna Payload (if Tx Payload is Acterna)	Specify whether the Acterna Payload is BERT pattern or Fill Pattern.
Fill Pattern (if Acterna Payload is Fill Pattern)	Specify the fill byte using hexadecimal format, up to 64 bytes.

9 Select **SLA Thresholds**, and then specify the following settings:

Setting	Description
Service Number (multi-stream application only)	Select which service to configure: 1-8
Service Name	Enter the name of the service.

Setting	Description
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.
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.
Policing	Selects whether policing test should be enabled. If enabled, each stream is transmitted at a pre-computed value >= (CIR+EIR) and test declared as success if received rate is below (CIR+EIR+M).
M Value	If Policing is On, specify the tolerance, or delta, in traffic rate which is allowed to be received above CIR+EIR before declaring a policing failure.
Frame Loss	The maximum frame loss rate (lost frames / total frames) allowed.
Frame Delay	The maximum allowed average delay/latency.
Delay Variation	The maximum allowed frame delay variation or jitter.

10 From the SAMComplete Settings list, select **Settings Overview**. A table appears that provides all settings for all services. Use the right and left arrows to view more of the table.

11 If desired, you can save the test settings by doing the following:

a Press the **Save** soft key.

b Select **Save Config**.

c Enter a name for the configuration, and then press OK.

Saving the configuration allows you to load the same settings later, enabling quicker startup time and consistent setups.

Running the test

After specifying settings, you are ready to run the test.

To run the test

1 Press the **Home** navigation key.

2 Press the **Display** soft key and then select **SAMComplete**.

The SamComplete Summary screen appears. Figure 48 shows a multi-stream test.

3 If testing on an optical interface, press the **Action** soft key and then select **Laser On**.

4 Press the **Action** soft key and then select **Start SAMComplete**.

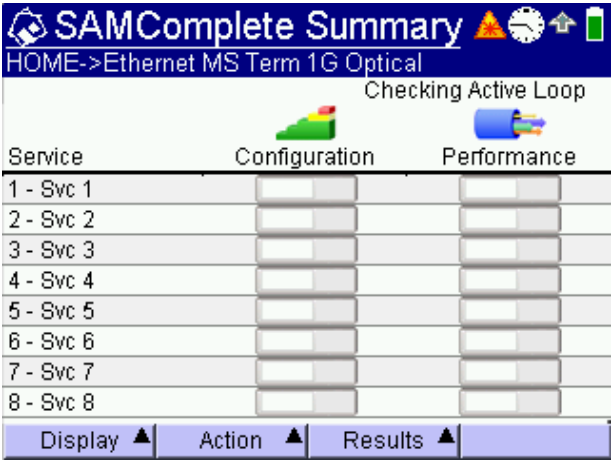


Figure 48 Multi-stream Summary screen

The test begins.

Managing test results

As each test runs, the results are updated on the screen. There are several categories of results available for viewing.

Viewing test results

The SAMComplete test has five categories of test results:

- Summary
- Config Status
- Config Step View
- Config Step Details
- Performance

To view test results

- Press the **Display** soft key, select **SAMComplete**, and then choose a result category.

Summary results

The Summary results provide a pass/fail indication for each service in sequential configuration test and the performance test where all services are tested in parallel. (Figure 48 on page 242 shows this screen at the beginning of the test.) The progress and status of each test is displayed in the progress bar under each test. The global test status is displayed in the upper right of the screen. After all tests finish, the global verdict appears in the upper left of the screen.

Config Status The Config Status results provide pass (green check mark) or fail (red x) verdicts for every step of the configuration test, for each service.Figure 49 provides an example of the Config Status results.

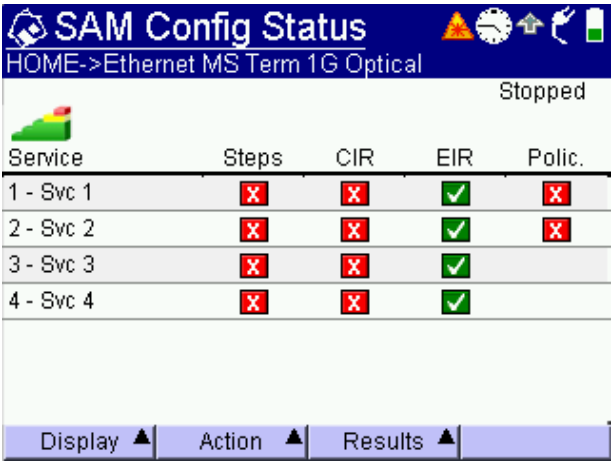


Figure 49 Multi-stream Config Status screen

Config Step View The Config Step View provides a graphic representation of the step test, for the selected service. The measured frame loss ratio, frame transfer delay, and frame delay variation for the highlighted step (scroll between steps using up/down arrow) are provided in the table above the graph. The CIR, EIR, and Policing Transmit rates are also included in the graph along with the configured SLA thresholds. Figure 50 provides an

example of the Config Step View results.

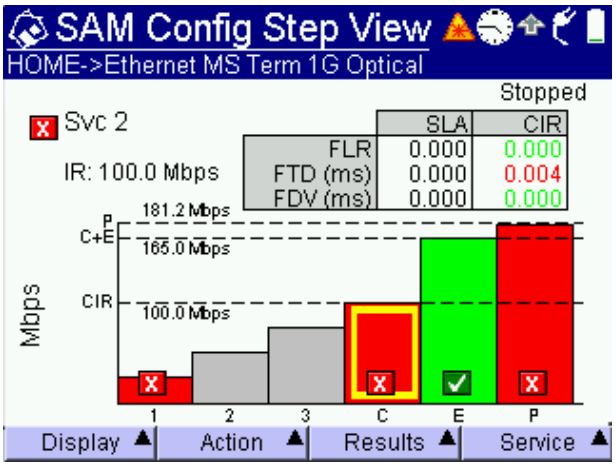


Figure 50 Multi-stream Config Step View

To see the results for a different service, press the **Service** soft key and select the desired service.

Config Step Details The Config Step Details screen collates all the steps of the graph view into a single tabular view.

Figure 51 provides an example of the Config Step Details results.

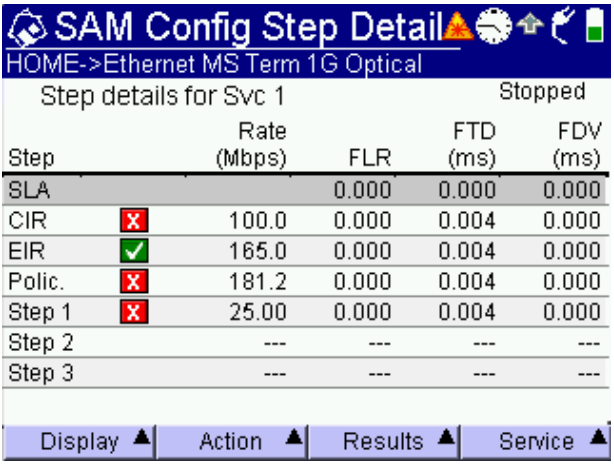


Figure 51 Multi-stream Config Step Detail

To see the results for a different service, press the **Service** soft key and select the desired service.

Performance The Performance results are available for several performance factors (SLAs):

– Status

  Provides an overview of the performance test result including the received information rate and average frame loss rate, delay and delay variation SLAs including pass/fail status for each SLA across all the services. Figure 52 on page 247 provides an example of the Performance *Status* results

– IR (information rate)

  Provides the current, min, max, and average information rate, as well as the CIR per service.

– Frame Loss

  Provides details for the frame loss results, including pass/fail, count of lost frames, the frame loss ratio (FLR), the SLA, and count of frames that were out of sequence (OOS) per service.

– Frame Delay

  Provides the current, min, max, and average frame delay, as well as the SLA per service.

– Delay Variation

  Provides the current, max, and average delay variation, as well as the SLA per service.

– Availability

  Provides statistics for the available seconds ratio, unavailable seconds, severely errored seconds, and aYes/No verdict regarding whether the service is available.

Figure 52 provides an example of the Performance *Status* results.

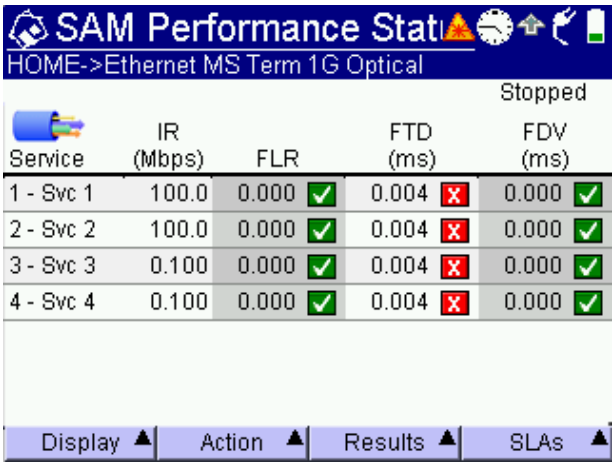


Figure 52 Multi-stream Performance Status

To see a different performance factor, press the **SLAs** soft key and select the desired SLA.

Managing test reports

After running tests, you can create a report for the test. Or, at any time, you can review a report.

Creating a report

You can save the results of a test in a report.

To create a report

1. After running a test, press the **Results** soft key, and then select Save SAMComplete Report.
2. Specify a name for the report, and then press the **OK** key.

   The report is created as both a PDF and TXT file are placed in the following directory:

   `/results/SAMComplete/`
   in the sub-directory for the type of test you were running.

   For example, if you were running an optical Ethernet Multi-Stream Terminate application, the report would be found in:
   `/results/SAMComplete/ethopic_mstr_term/`

Viewing a report

If you wish to review a report on the instrument, you can open the **`txt`** version using the file manager. You can export the PDF report for viewing on a PC or laptop.

Troubleshooting

9

This chapter describes how to identify and correct problems related to Ethernet testing with the HST-3000. Topics discussed in this chapter include the following:

Resolving problems

Table 14 describes situations that you may encounter when using the HST-3000.

Table 14 Problems and resolutions

Problem	Description	Resolution
Link is not active	After specifying link initialization settings and connecting the HST to the circuit, the Link Active status is No.	Verify the following: – The HST on the on the far end is connected to the circuit. – The HST and it's link partner are configured for the same rate of traffic. – The HST and it's link partner both have auto-negotiation turned ON, and share at least one common capability, or both have auto-negotiation turned OFF. If you are testing 10/100/1G electrical Ethernet: – Verify that the RJ-45 jacks on the left of the Ethernet SIM were used to connect to the circuit. The RJ-45 jack on the top of the base unit is only used for Ethernet TE, VoIP, and IP Video testing. If you are testing 1G or 100M optical Ethernet: – Verify that you turned the laser on using the **Laser On** action key.

Table 14 Problems and resolutions (Continued)

Problem	Description	Resolution
I suspect there is something wrong with my cable.	The cable may not be inserted properly, the wrong cable may be inserted, or a broken cable may be connected.	Use the HST cable diagnostics test to determine the nature of the problem. For details, see "Running cable diagnostics" on page 42.
Hard loopback at the far end is failing.	After establishing a hard loopback on a device at the far end of the network, traffic is not looped back to the HST on the near end.	– If you are testing on a switched Ethernet network, you must use two HSTs as end stations on a circuit. – If you are performing a layer 3 IP loopback test on an Ethernet network that doesn't support VLAN tagging, and you transmit VLAN tagged traffic, the loopback will fail. Reconfigure the HST to transmit untagged traffic. **NOTE:** If you are testing on an unswitched Ethernet network, you can use a hard loopback at the far end of the circuit.

Table 14 Problems and resolutions (Continued)

Problem	Description	Resolution
When trying to loop up an instrument on the far end using a loop up command, the loop up fails.	HSTs running older software releases so not support user-defined TPIDs. The latest HST software release allows you to specify a user-defined TPID. As a result, if you issue a loop up command from an HST with a user-defined TPID, the receiving HST (running an older version of software) will not respond to the loop up command. This will also occur when running Ping tests, or RFC 2544 tests with different SVLANs or TPIDs for the near and far end instruments.	– Verify that both HSTs are running the most recent software release. HST software releases are available at www.jdsu.com. – Verify that the specified SVLAN and TPID for traffic transmitted and received on both instruments match.

Table 14 Problems and resolutions (Continued)

Problem	Description	Resolution
While running a Ping test, throughput and performance test results do not seem to reflect the true state of the circuit.	After running a Ping test, bandwidth utilization, delay measurements, and other test results seem to indicate that the circuit is experiencing significant utilization and performance problems. This occurs for a variety of reasons: – Routers on the circuit and the target computer itself may impose a limit on how many ICMP echo packets to process per second. Echo packets that exceed the limits are discarded. – ICMP echo packets are often given a lower priority by devices on the circuit. As a result, round-trip time for Ping packets can be different than that experienced by true traffic which is given a higher priority. – Traffic shaping does not occur until enough packets flow through the circuit. Isolated packets, such as Ping packets, may not experience the same pace experienced by real application packets. Therefore, transmitting ping packets, even at a continuous rate, provides a poor indication of real IP throughput.	In most instances, you should configure and transmit a true load of traffic to measure throughput and verify performance. Run the Layer 2 Traffic, Layer 3 Traffic, or Layer 4 Traffic test as appropriate.

Table 14 Problems and resolutions (Continued)

Problem	Description	Resolution
My Ping test is failing, but I'm certain the device on the far end is capable of responding.	Determine whether there are ICMP Echo filters on the circuit, or if there are rate limiters restricting the number of ICMP packets.	Decrease the interval between transmitted ping packets.
I cannot establish an IP connection using stateful auto-configuration.	Stateful auto-configuration obtains an IPv6 address from a DHCPv6 server. The server is not available.	Use stateless auto-configuration to let the HST automatically generate an IPv6 address based on the MAC address and the subnet prefix returned by the router. The HST will verify that the address is not already used, then the connection will be established.
My unit is receiving layer 4 traffic, but delay measurements, out of sequence (OOS) counts, lost frame counts, and packet jitter measurements are not available.	Certain test results must be obtained using traffic that carries an Acterna Test Packet (ATP) payload. The HST uses the ATP Listen Port to determine whether received layer 4 traffic carries an ATP payload;	Verify that the ATP Listen Port on the receiving unit is set to the Destination Port specified for the traffic on the transmitting unit. See "Understanding the ATP Listen Port" on page 164 for an explanation and illustration of the required settings.

Table 14 Problems and resolutions (Continued)

Problem	Description	Resolution
My unit is receiving layer 4 TCP traffic, but it is falsely reporting checksum errors.	HSTs running older software releases interpret a zero (0) in the checksum of a TCP header as an error. The latest HST software release recognizes that a zero value does not constitute an error. As a result, if you transmit TCP traffic from an HST with a checksum value of zero, the receiving HST (running an older version of software) will falsely interpret the checksum as errored. This is more likely to occur when transmitting a heavy load or a sudden burst of traffic.It may also occur when running an RFC 2544 test with layer 4 TCP traffic.	Verify that both HSTs are running the most recent software release. HST software releases are available at www.jdsu.com.

Test Results

A

This appendix describes the test result categories and the results within each category that are available when running cable diagnostics or testing Ethernet, IP, or TCP/UDP service. Topics discussed in this appendix include the following:

About test results

After you start a test, if no errors or alarms have been detected, the Summary result category automatically displays a large “All Summary Results OK” message. If errors are detected, the results are displayed. To view test results in other categories, use the left and right arrow key to browse through the categories, or press the **Display** soft key, and then select a category.

The HST provides only filtered results (except for various error counts) when testing using the Ethernet SIM. If you want to observe results for un-filtered traffic, you must disable the IP filter and TCP/UDP filter (as appropriate), and set each of the individual Ethernet filters to Don’t Care when you configure your test.

An exception to this is MPLS encapsulated traffic. When you enable MPLS encapsulation on your unit, the Ethernet filter is automatically set to filter for MPLS encapsulated traffic by

default. Therefore frames (such as ARP requests and replies, VLAN frames, etc.) that are not MPLS encapsulated will not populate the results.

The following sections describe the test results for each of the categories. The test results for each category are listed alphabetically.

Summary results

The Summary category automatically displays error results that are non-zero, key results that are out-of-specification, or key informational results. This allows quick access to the results without having to search through each category.

If your HST has the optional color display, a green background indicates that all summary results are OK, and that no errors were detected on the circuit. A yellow background indicates that conditions occurred that do not necessarily constitute errors, but warrant additional investigation. For example, if the HST gained pattern synchronization, but then lost it, the Summary Result window will be yellow. A red background indicates that errors did occur on the circuit.

Table 15 describes the results that appear in the Summary category.

Table 15 Summary results

Result	Definition
Acterna Payload Errors	A count of received IP packets containing Acterna Payload checksum errors. **NOTE:** This result only appears if you receive an Acterna payload, and there are payload errors in the received data stream.

Table 15 Summary results (Continued)

Result	Definition
Bit Errors	A count of the number of received bits in a recognized pattern that do not match the expected value.
Errored Frames	A count of FCS errored frames, runts, and jabbers.
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. For Ethernet ping applications, the FCS Errored Frames result is the only result displayed in the Errors category. The other results in the Errors category are not applicable.
IP Checksum Errors	A count of received IP packets with a checksum error in the header.
IP Packet Length Errors	A count of received IP packets that exceed the available Ethernet payload.
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) and an errored FCS.
L2 Patt Sync	The data contained inside the frame payload is synchronized with a BERT pattern. This result is only applicable when the HST is configured for layer 2 testing.
L4 Checksum Errors	A count of received packets with a checksum error in the TCP/UDP header.
Link Active	Indicates whether the link is active.
Loss of Link	Indicates the link has become inactive since starting the test.

Table 15 Summary results (Continued)

Result	Definition
Loss of Signal	When testing 1G or 100M optical Ethernet, indicates the signal has been lost since starting the test.
Lost Frames	A count of lost Acterna test frames. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frames 4 and 5 were not detected), the lost frame count is incremented by two (frames 4 and 5 are lost). If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frames 11, 12, and 13 are missing), the lost frame count is incremented by three, resulting in a total count of five lost frames. **NOTE:** If the HST receives errored frames with errors in the sequence number field, the Lost Frames count will be incorrect.
OoS Frames	A count of each instance where the HST detects out of sequence Acterna test frames in the stream. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frame 6 is detected immediately following frame 3), the out of sequence count is incremented by one, resulting in a count of one instance of out of sequence frames. If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frame 14 is detected immediately following frame 10), the out of sequence number is incremented again by one, resulting in a total count of two instances of out of sequence frames.
Pause Frames	A count of PAUSE frames received from a remote Ethernet device since starting the test.
Runts	A count of Ethernet frames under the minimum 64 byte frame length containing Frame Check Sequence (FCS) errors.

Table 15 Summary results (Continued)

Result	Definition
SFP Valid	Indicates whether the SFP is recognized by the HST as MSA compliant.
Undersized	A count of frames under the minimum 64 byte frame length.

Cable Status results

The Cable Status category shows measurements associated with running cable diagnostics on a link (see Figure 53).

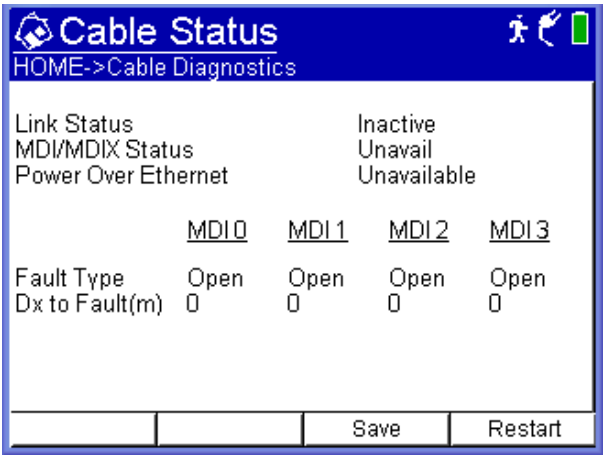


Figure 53 Cable Status results display

After running the electrical Ethernet Cable test, if the link is active, the type of cable your unit detected appears in the Cable Status result category.

Link Status result

After running the electrical Ethernet Cable test, the Link Status test result indicates one of the following:

– An active 10M or 100M link is established. If a 10M or 100M link is established, the MDI/MDIX status (see "MDI or MDIX Pair Status result" on page 263) is reported.
– An active 1G electrical link is established. If a 1G electrical link is established, the pair status, polarity, and pair skew for each MDI pair is reported. See "1G Pair Status result" on page 264, "Polarity result" on page 265 and "Pair Skew result" on page 265.
– The link is *inactive*. If the link is inactive, the unit indicates the type of fault and the fault's relative distance from the tester (see "Fault results" on page 265).

MDI or MDIX Pair Status result

The MDI/MDIX Status result indicates the resolved wiring (`MDI`, or `MDIX`) of the near end unit's RJ-45 jack. For example, if the far end can not auto-configure its interface, (in other words, the wiring is fixed), this result can help you determine whether a straight through or crossover cable is being used *or* the MDI/MDIX wiring of the far end port.

– You must know the *fixed MDI/MDIX status* of the far end port to determine the type of cable using the near end MDI/MDIX Status result. For example, if you know that the far end port is fixed at MDI, and the near end port detects MDIX, then you can conclude that a straight through cable is used.
– You must know the *cable type used* to determine the MDI/MDIX status of the far end port using the near end MDI/MDIX Status result. For example, if you know you are using a straight through cable, and the near end port detects MDIX, you can conclude that the wiring at the far end port is MDI.

Table 16 illustrates each of the possible resolutions.

Table 16 HST-3000 Ethernet MDI/MDIX Resolution

Far end port	Cable	Near end port
MDIX	straight through	MDI

Table 16 HST-3000 Ethernet MDI/MDIX Resolution

Far end port	Cable	Near end port
MDI	cross over	MDI
MDI	straight through	MDIX
MDIX	cross over	MDIX

1G Pair Status result

The Pair Status results for 1G electrical links provide the *current pair assignments for the link*. MDI pairs for 1G electrical links are assigned during the process of auto-negotiation; therefore, if for any reason the link becomes inactive, and then the link is re-established, the pair assignments could potentially change. For example, the first time you establish a link after auto-negotiation, the following pairs could be assigned:

Table 17 MDI pair assignments

MDI0	MDI1	MDI2	MDI3
1-2	3-6	4-5	7-8

If the link goes down (becomes inactive), and then is re-established, the following pairs could be assigned:

Table 18 MDIX pair assignments

MDI0	MDI1	MDI2	MDI3
3-6	1-2	7-8	4-5

Polarity result

The Polarity result indicates the polarity of each MDI pair on active 1G electrical links, indicating how each pair is physically wired to the unit's port.

- `Normal (+)` indicates a normal polarity for the pair.
- `Inverted (-)` indicates an inverted polarity for the pair.

Pair Skew result

The Pair Skew result is a measurement of timing differences between the MDI pairs on active 1G electrical links. Timing differences may occur for a variety of reasons. For example, if different insulating materials are used on the pairs, a variance in the signal velocity (skew) may occur. If the skew is significant, transmission of the signal may be impaired to such a degree that the received signal can not be synchronized.

Pair skew is reported in +/- 8ns increments.

Fault results

If a link is inactive, and a fault is detected, the unit indicates the type of fault detected (`Open`, `Short`, or `Unknown`) and the fault's relative distance from the tester within +/- 1 meter.

If you do not connect the cable to a far end device (completing the circuit), you can also use the Open detection feature to measure the length of a cable.

Fault types are defined as follows:

Open—Indicates there is a cut on the pair (or that the cable is not connected to a device at the far end of the circuit), and that the tester has detected an impedance exceeding 333 ohms. The distance from the near end tester to the end of the cable (or the cut) is also provided.

Short—Indicates a positive and negative line on the same pair are touching, and that the tester has detected an impedance less than 33 ohms.

Unknown—Indicates the tester has detected impedance outside of the ranges stated for Open and Short faults, or that the cable is properly terminated into another Ethernet port. *Unknown does not necessarily indicate that a fault was detected*.

NOTE:

If the far end of the cable is connected to a powered down IP phone, and the phone is an older model, there is a filter that connects between pairs 1-2 and 3-6 in the phone. Depending on the characteristics of the filter, your tester may report a fault for pairs 1-2 and 3-6.

Table 19 describes the results that appear in the Cable Status category.

Table 19 Cable Status test results

Result	Description
Cable Test Status	Indicates the status of cable diagnostics: – **N/A** indicates that the cable test (distance to fault) is not applicable. – **Complete** indicates that the cable test (distance to fault) is applicable, that the HST is finished running the diagnostics, and that the results and measurements displayed are valid.
Dx to Fault	For each fault detected, provides the distance from the HST to the fault. If no fault is detected, N/A appears.

Table 19 Cable Status test results (Continued)

Result	Description
Fault Type	For each fault detected, displays one of the following values: – **Normal** indicates the HST did not detect any faults on the link. – **Open** indicates the HST detected an incomplete path on the link for the pair. – **Short** indicates the HST detected a short for the pair. – **Unknown** indicates the HST detected a fault, but can not determine the nature of the fault. The distance detected faults (open or short) is provided as the Dx to Fault result.
Link Status	Indicates whether the link is active or inactive.
Power over Ethernet	Indicates whether or not PoE service is present on the link.

NOTE:

If the speed detected on the line is 1G electrical, the MDI/MDIX Status results are not applicable and therefore do not appear in the Cable Status category.

Signal

If you selected a 1G or 100M optical Ethernet application, the Signal category shows results associated with the SFP you are using to connect to the circuit, and the current signal level.

The Signal category is not applicable when testing 10/100/1G electrical Ethernet.

Table 20 Signal test results

Result	Description
SFP Valid	Indicates whether the SFP is recognized as a supported SFP (Yes, or No).
SFP Vendor Name	Displays the name of the SFP vendor (for example, JDS UNIPHASE).
SFP Id	Displays the SFP ID (for example, SX850).
Signal Level (dBm)	Displays the signal level in dBm.

Link Stats results

The Link Stats category lists link statistics such as the average frame or packet rate, maximum frame or packet rate, and the maximum, minimum, and average round trip delay measurements. Results in this category accumulate after you transmit layer 2 Ethernet, layer 3 IP, or layer 4 TCP/UDP traffic over the link. Table 21 describes the results that appear in the Statistics category.

Table 21 Link Stats test results

Result	Description
Delay, Avg (us)	The average round trip delay calculated in microseconds. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.

Table 21 Link Stats test results (Continued)

Result	Description
Delay, Max (us)	The maximum round trip delay calculated in microseconds. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.
Delay, Min (us)	The minimum round trip delay calculated in microseconds. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.
Frame Rate, Avg	The average rate of received frames, expressed in frames per second. The average is calculated over the time period that elapsed since the last test restart.
Frame Rate, Cur	The current rate of received frames, expressed in frames per second. This measurement is an average taken over the prior second of test time.
Frame Rate, Min	The minimum rate of received frames over a one second period, expressed in frames per second.
Frame Rate, Peak	The highest (peak) rate of received frames over a one second period, expressed in frames per second.
Frame Size, Avg	The average size of frames received since frame detection. The average is calculated over the time period that elapsed since the last test restart.
Frame Size, Max	The maximum size of frames received since frame detection.
Frame Size, Min	The minimum size of frames received since frame detection.

Table 21 Link Stats test results (Continued)

Result	Description
IPv6 Packet Size, Avg	The average size of IPv6 packets received since packet detection. The average is calculated over the time period that elapsed since the last test restart.
IPv6 Packet Size, Max	The maximum size of IPv6 packets received since packet detection.
IPv6 Packet Size, Min	The minimum size of IPv6 packets received since packet detection.
MPLS Label Depth, Max	Displays the maximum number of MPLS labels for all frames received since starting the test.
MPLS Label Depth, Min	Displays the minimum number of MPLS labels for all frames received since starting the test.
MPLS1 ID MPLS2 ID	Displays label 1 or label 2 for the last received MPLS encapsulated frame.
MPLS1 Priority MPLS2 Priority	Displays the label 1 or label 2 priority for the last received MPLS encapsulated frame.
MPLS1 TTL MPLS2 TTL	Displays the time to live (TTL) for label 1 or label 2 for the last received MPLS encapsulated frame.
Packet Jitter, Avg (us)	The smoothed average value of the packet delay variation since the last test restart (per RFC 1889), calculated in microseconds.
Packet Jitter, Max Avg (us)	The maximum Packet Jitter, Avg (us) measured since the last test restart, calculated in microseconds.
Packet Jitter, Peak (us)	The highest packet delay variation measured since the last test restart, calculated in microseconds.

Table 21 Link Stats test results (Continued)

Result	Description
Packet Size, Avg	The average size of IPv4 packets received since packet detection. The average is calculated over the time period that elapsed since the last test restart.
Packet Size, Max	The maximum size of IPv4 packets received since packet detection.
Packet Size, Min	The minimum size of IPv4 packets received since packet detection.
Rx Mbps, Cur L1	The current bandwidth utilized by received traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
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 and minimum inter-frame gap.
Rx Mbps, Cur L3	The current bandwidth utilized by received layer 3 IPv4 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur L3 (IPv6)	The current bandwidth utilized by the received layer 3 IPv6 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur L4	The current bandwidth utilized by received layer 4 IPv4 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.

Table 21 Link Stats test results (Continued)

Result	Description
Rx Mbps, Cur L4 (IPv6)	The current bandwidth utilized by the received layer 4 IPv6 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Est. TCP Thruput (Mbps)	Displays the estimated TCP throughput. The estimate is calculated by dividing the TCP Window Size that you specified on the TCP/UDP configuration menu (when you configured your test) by the average round trip delay measurement (Delay, Avg (us)) for the test. If a particular combination of TCP Window Size and round trip delay yields an estimated throughput that exceeds the line rate, the line rate will be displayed.
Svc Disruption (us)	The service disruption time (maximum inter-frame gap) when service switches to a protect line calculated in microseconds.
SVLAN Frame DEI	Displays the DEI of the last received Q-in-Q tagged frame.
SVLAN ID	Displays the SVLAN ID for the last received Q-in-Q tagged frame.
SVLAN Priority	Displays the SVLAN Priority for the last received Q-in-Q tagged frame.
Total Util %, Avg	The average bandwidth utilized by the received traffic, expressed as a percentage of the line rate of available bandwidth since the test started. The average is calculated over the time period elapsed since the test started.

Table 21 Link Stats test results (Continued)

Result	Description
Total Util %, Cur	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.
Total Util %, Min	The minimum bandwidth utilized by the received traffic since the test started expressed as a percentage of the line rate of available bandwidth.
Total Util %, Peak	The highest (peak) bandwidth utilized by the received traffic since the test started 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 and minimum inter-frame gap.
Tx Mbps, Cur L3	The current bandwidth utilized by the transmitted layer 3 IPv4 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Tx Mbps, Cur L3 (IPv6)	The current bandwidth utilized by the transmitted layer 3 IPv6 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.

Table 21 Link Stats test results (Continued)

Result	Description
Tx Mbps, Cur L4	The current bandwidth utilized by the transmitted layer 4 IPv4 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Tx Mbps, Cur L4 (IPv6)	The current bandwidth utilized by the transmitted layer 4 IPv6 traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
VLAN ID	Displays the VLAN ID for the last VLAN or Q-in-Q tagged frame received.
VLAN Priority	Displays the VLAN Priority for the last VLAN or Q-in-Q tagged frame received.

L2 Backbone results

When testing MiM encapsulated traffic, backbone link statistics and counts appear in the L2 Backbone Link Stats and L2 Backbone Link Counts categories. In addition to the standard link counts, counts of received PBB frames and frame bytes are provided. Additional statistics are provided for the B-Tag and I-Tag values carried in the analyzed traffic.

L2 Customer results

When testing MiM encapsulated traffic, customer link statistics and counts appear in the L2 Customer Link Stats and the L2 Customer Link Counts categories.

Link Counts results

The Link Counts category lists link counts such as the number of received frames or packets, number of transmitted frames or packets, and number of unicast, multicast, or broadcast frames. The Received Frames and Received Packets results include errored frames and packets; all other results count valid frames or packets only. Results in this category accumulate after you transmit layer 2 Ethernet, layer 3 IP, or layer 4 TCP/UDP traffic over the link. Table 22 describes the results that appear in the Link Counts category.

Table 22 Link Counts test results

Result	Description
1024-1518/1526	A count of received frames from: – 1024 to 1518 bytes (untagged) – 1024 to 1522 bytes (VLAN tagged) – 1024 to 1526 (Q-in-Q tagged) The count is inclusive since starting the test.
128-255 Byte Frames	A count of received Ethernet frames with lengths between 128 and 255 bytes, inclusive since starting the test.
256-511 Byte Frames	A count of received Ethernet frames with lengths between 256 and 511 bytes, inclusive since starting the test.
512-1023 Byte Frames	A count of received Ethernet frames with lengths between 512 and 1023 bytes, inclusive since starting the test.
64 Byte Frames	A count of received Ethernet frames with a length of 64 bytes since starting the test.
65-127 Byte Frames	A count of received Ethernet frames with lengths between 65 and 127 bytes, inclusive since starting the test.

Table 22 Link Counts test results (Continued)

Result	Description
Broadcast Frames	The number of Ethernet broadcast frames received since starting the test.
Broadcast Packets	The number of broadcast IP packets received since starting the test.
IPv4 Rx Packets	A count of all IPv4 packets received meeting filter criteria since starting the test. When monitoring traffic, IPv4 packets can be counted even if the HST is configured to filter for all IP traffic.
IPv6 Rx Packets	A count of all IPv6 packets received meeting filter criteria since starting the test.
IPv6 Tx Packets	A count of IPv6 packets transmitted since starting the test. This result does not appear when running the Monitor application.
Multicast Frames	The number of Ethernet multicast frames received since starting the test.
Multicast Packets	The number of multicast IP packets received since starting the test.
Pause Frames	A count of pause frames received from a remote Ethernet device since starting the test. Pause frames are utilized for flow control and alert the transmitting device that it must reduce the outgoing frame rate or risk a receiver overflow on the far end, resulting in dropped traffic.
Rx Acterna Frames	A count of received Acterna frames, excluding errored frames since starting the test.

Table 22 Link Counts test results (Continued)

Result	Description
Rx Collisions	A count of the number of times the HST has received a jam signal while it was not transmitting frames. Result only appears for half-duplex 10/100 Ethernet tests.
Rx Frame Bytes	A count of the total bytes received within an Ethernet frame from the Destination MAC Address to the FCS, inclusive.
Rx Frames	A count of all frames received meeting filter criteria since starting the test.
Rx Frames ALL	A count of frames received since starting the test, including errored frames. Frames do not need to satisfy filter criteria to be included in this count.
Rx IP Packets	A count of IP packets received since starting the test.
Rx L4 Destination Port	Displays the Destination Port number for the last layer 4 frame received.
Rx L4 Source Port	Displays the Source Port number for the last layer 4 frame received.
Rx QinQ Frames	A count of Q-in-Q encapsulated frames received since starting the test, excluding errored frames.
Rx Router Adv. Msg.	A count of received router advertisement messages when running an IPv6 application. This count is not reset when you restart a test; to reset the count you must bring down the link, reestablish the link, and then start the test again.
Rx TCP Packets	A count of TCP packets received since starting the test, excluding errored frames since starting the test.

Table 22 Link Counts test results (Continued)

Result	Description
Rx UDP Packets	A count of UDP packets received since starting the test, excluding errored frames since starting the test.
Rx VLAN Frames	A count of VLAN encapsulated frames received since starting the test, excluding errored frames.
Span Tree Frames	A count of received 802.1d spanning tree frames since frame detection.
Transmitted Frames	A count of frames transmitted since starting the test. This result does not appear when testing in Monitor application.
Tx Acterna Frames	A count of transmitted Acterna frames since starting the test. This result does not appear when testing using the Monitor application.
Tx Frame Bytes	A count of the total bytes transmitted within an Ethernet frame from the Destination MAC Address to the FCS, inclusive.
Tx IP Packets	A count of IP packets transmitted since starting the test. This result does not appear when testing in Monitor application.
Tx Late Collisions	A count of the number of times the HST has transmitted a frame, and then experiences a collision more than 64 byte times after the transmission begins. This result only appears for half-duplex 10/100/1G electrical Ethernet tests.

Table 22 Link Counts test results (Continued)

Result	Description
Tx Router Solicit Msg.	A count of transmitted router solicitation messages when running an IPv6 application. This count is not reset when you restart a test; to reset the count you must bring down the link, reestablish the link, and then start the test again.
Unicast Frames	The number of Ethernet unicast frames received since starting the test.
Unicast Packets	The number of IP unicast packets received since starting the test.

J-Proof (transparency) results

Table 23 lists the J-Proof results associated with the loopback of control frames for various protocols.

Table 23 J-Proof test results

Result	Description
Name	Displays the name specified when you configured the test frame.
Tx	A count of the number of test frames for a particular test frame type transmitted by the instrument since the last test start or restart.
Rx	A count of the number of test frames for a particular test frame type received by the instrument since the last test start or restart.

Table 23 J-Proof test results (Continued)

Result	Description
Status	Displays one of the following: – N/A. Indicates that a particular test frame is not configured to be transmitted. – IDLE. Indicates that a particular test frame is in the queue to be transmitted. – In Progress. Indicates that a particular test frame is currently being transmitted, and has not yet encountered an error. – Timeout. Indicates that for a particular test frame a timeout was reached while waiting for a transmitted frame to return; however, all frames were successfully looped back before the end of the test frame's transmission. – Payload Errors. Indicates that for a particular test frame all transmitted frames were successfully looped back, but a received frame contained a payload that was not the same as its transmitted payload. – Header Errors. Indicates that for a particular test frame, all transmitted frames were successfully looped back, but a received frame contained a header that was different from its transmitted header. – Count Mismatch. Indicates that the number of received frames for a particular test frame did not match the number of frames transmitted.

OAM results

Table 24 describes the Service Layer OAM CCM results, such as the number of RDI seconds, loss of continuity indicator, and the number of transmitted and received CCM frames. Continuity Check must be turned On to observe these results.

Table 24 S-OAM CCM test results

Result	Description
MD Level	Displays the maintenance domain level configured for the CCM frame received.
Maint ID	Displays the maintenance association ID configured for the CCM frame received.
Peer MEG End Point ID	Displays the maintenance entity group end point ID for the instrument's peer as configured.
Total Tx Frames	Count of the total number of CCM frames transmitted since the last OAM setting was specified or changed.
Total Rx Frames	Count of the number of CCM frames received since the last OAM setting was specified or changed.
RDI	Indicates whether or not remote defect indication is ON or OFF.
RDI Seconds	Count of the number of seconds during which an RDI was declared since starting or restarting the test.
Loss of Continuity	ON indicates that a loss of continuity has occurred.

Table 24 S-OAM CCM test results (Continued)

Result	Description
Unexpected MEG level	ON indicates that CCM frames have been received with a maintenance entity group level lower than that specified as the maintenance domain level when you configured the OAM settings for the transmitting instrument.
Mismerge	ON indicates that CCM frames have been received with the same maintenance domain level specified for transmitted frames, but the received CCM frames carry a different maintenance association ID (MAID).
Unexpected MEP	ON indicates that a CCM was received from a different maintenance end point than that specified as the instrument's peer MEG End Point.
Unexpected Period	ON indicates that a CCM was received with the correct maintenance domain level, maintenance association ID, and maintenance end point ID, but with a period value that was not the same as the instrument's CCM rate.

Table 25 describes the Service Layer OAM AIS results, such as a count of the number of AIS received and the number of AIS seconds.The AIS State must be turned On to observe these results.

Table 25 S-OAM AIS test results

Result	Description
AIS	Count of AIS alarms detected since initial frame synchronization.
AIS Seconds	Count of asynchronous test seconds in which AIS was present for any portion of the test second.

Table 25 S-OAM AIS test results (Continued)

Result	Description
Total Tx Frames	Count of the total number of AIS frames transmitted since the last OAM setting was specified or changed.
Total Rx Frames	Count of the number of AIS frames received since the last OAM setting was specified or changed.
Unexpected Period	ON indicates that an AIS was received with the correct maintenance domain level, maintenance association ID, and maintenance end point ID, but with a period value that was not the same as the instrument's AIS rate.

Table 26 describes the Service Layer OAM LBM results. LBM/LBR (Ping) must be Enabled to observe these results.

Table 26 S-OAM LBM test results

Result	Description
Total Tx LBM Frames	Count of the total number of LBM frames transmitted since the last OAM setting was specified or changed.
Total Rx LBR Frames	Count of the number of LBR frames received since the last OAM setting was specified or changed.
Total Rx LBM Frames	Count of the number of LBM frames received since the last OAM setting was specified or changed.
Total Tx LBR Frames	Count of the total number of LBR frames transmitted since the last OAM setting was specified or changed.

Table 27 describes the Service Layer OAM LTM results. LTM/LTR (Trace) must be Enabled to observe these results.

Table 27 S-OAM LTM test results

Result	Description
Total Tx LTM Frames	Count of the total number of LTM frames transmitted since the last OAM setting was specified or changed.
Total Rx LTR Frames	Count of the number of LTR frames received since the last OAM setting was specified or changed.
Total Rx LTM Frames	Count of the number of LTM frames received since the last OAM setting was specified or changed.
Total Tx LTR Frames	Count of the total number of LTR frames transmitted since the last OAM setting was specified or changed.

Table 28 describes the Link Layer OAM Local Op Mode results. The Link OAM State must be On to observe these results.

Table 28 L-OAM Local Op Mode test results

Result	Description
Mode	Displays the current mode (Active or Passive) for the instrument.
Parser Action	Indicates the local receiver is currently forwarding, looping back, or discarding non-OAM PDUs.
Muxer Action	Indicates the local transmitter is currently forwarding or discarding non-OAM PDUs.
Vendor OUI	Displays the Vendor OUI (Organizationally Unique Identifier) for the instrument.

Table 28 L-OAM Local Op Mode test results (Continued)

Result	Description
Max PDU Size	Displays the maximum PDU (Protocol Data Units) size supported by the local instrument.
Unidirectional	Indicates whether the local instrument advertises that it provides unidirectional support for failure detection.
Link Events	Indicates whether the local instrument is configured to monitor link events.
Local Loopback	Indicates whether the local instrument advertises that it provides loopback support.
Variable Retrieval	Indicates whether the local instrument supports sending Variable Response OAM PDUs.
Revision	Displays the current of the TLV (Type Length Value) revision for the local instrument.

Table 29 describes the Link Layer OAM Remote Op Mode results. The Link OAM State must be On to observe these results.

Table 29 L-OAM Remote Op Mode test results

Result	Description
Mode	Displays the current mode (Active or Passive) for the instrument's peer.
Parser Action	Indicates the remote receiver is currently forwarding, looping back, or discarding non-OAM PDUs.
Muxer Action	Indicates the remote transmitter is currently forwarding or discarding non-OAM PDUs.

Table 29 L-OAM Remote Op Mode test results

Result	Description
Vendor OUI	Displays the Vendor OUI (Organizationally Unique Identifier) for the instrument's peer.
Max PDU Size	Displays the maximum PDU (Protocol Data Units) size supported by the local instrument.
Unidirectional	Indicates whether the remote instrument advertises that it provides unidirectional support for failure detection.
Link Events	Indicates whether the remote instrument is configured to monitor link events.
Remote Loopback	Indicates whether the remote instrument is operating in remote loopback mode.
Variable Retrieval	Indicates whether the remote instrument supports sending Variable Response OAM PDUs.
Revision	Displays the current of the TLV (Type Length Value) revision for the remote instrument.

Table 30 describes the Link Layer OAM Counts results. Counts are provided for both transmitted and received frames The Link OAM State must be On to observe these results.

Table 30 L-OAM Counts test results

Tx and Rx Frame Results	Description
Information	A count of information frames transmitted or received since starting the test.

Table 30 L-OAM Counts test results (Continued)

Tx and Rx Frame Results	Description
Event Notification	A count of event notification frames transmitted or received since starting the test.
Variable Request	A count of variable request frames transmitted or received since starting the test.
Variable Response	A count of variable response frames transmitted or received since starting the test.
Loopback Control	A count of loopback control frames transmitted or received since starting the test.
Duplicate Event	A count of duplicate event frames transmitted or received since starting the test.
Unsupported	A count of unsupported frames transmitted or received since starting the test.
Organization Specific	A count of organization specific frames transmitted or received since starting the test.

Table 31 describes the Link Layer OAM States results. Results are provided for the OAM discovery process and for remote events. The Link OAM State must be On to observe these results.

Table 31 L-OAM States test results

State	Result	Description
Discovery	State	Displays one of the following: – FAULT – ACTIVE SEND LOCAL – PASSIVE WAIT – SEND LOCAL REMOTE
	Local	Displays one of the following: – 0 = Discovery can not complete – 1 = Discovery has not completed – 2 = Discovery has completed – 3 = Reserved
	Remote	Displays one of the following: – 0 = Discovery can not complete – 1 = Discovery has not completed – 2 = Discovery has completed – 3 = Reserve
Remote Event	Link Fault	Indicates whether a link fault occurred.
	Dying Gasp	Indicates whether an unrecoverable failure has occurred.
	Critical Event	Indicates whether a critical event has occurred.

Table 32 describes the Link Layer OAM History results. Results are provided for frame, frame period, and frame second events. The Link OAM State must be On to observe these results.

Table 32 L-OAM History test results

Events	Result	Description
Frame Event Frame Period Event Frame Sec Summary Event	Remote Time-stamp	Displays the time that the last event occurred.
	Remote Window	Indicates the duration of the period.
	Remote Threshold	Indicates the number of errors that must occur in the window to cause an event.
	Remote Errored Events	A count of the number of errors in the period.
	Remote Errored Totals	A count of errors since starting the test.
	Remote Event Total	A count of the number of events since starting the test.

Streams results

In addition to the standard test results accumulated and displayed for all analyzed traffic, the HST allows you to view results for a specific traffic stream in the Streams category. Table 33 describes the results that appear for a layer 2 or

layer 3 traffic stream.

Table 33 Streams test results

Result	Description
Delay, Avg (us)	The average round trip delay calculated in microseconds for the stream. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.
Delay, Cur (us)	The current round trip delay calculated in microseconds for the stream. This measurement is an average taken over the prior second of test time. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.
Delay, Max (us)	The maximum round trip delay calculated in microseconds for the stream. You must originate an Acterna payload to measure round trip delay. A unit in loopback mode will display invalid results because it is not originating the traffic.
Delay, Min (us)	The minimum round trip delay calculated in microseconds for the stream. Your near end HST must originate an Acterna payload and receive traffic from a far end JDSU Ethernet test set (in loopback mode) to measure delay accurately.
Frame Loss Ratio	The ratio of frames lost to the number of frames expected.

Table 33 Streams test results (Continued)

Result	Description
Lost Frames	A count of lost Acterna test frames for the stream. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frames 4 and 5 were not detected), the lost frame count is incremented by two (frames 4 and 5 are lost). If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frames 11, 12, and 13 are missing), the lost frame count is incremented by three, resulting in a total count of five lost frames. **NOTE:** If the HST receives errored frames containing errors in the sequence number field, the Lost Frames count will be incorrect.
OoS Frames	A count of each instance where the HST detects out of sequence Acterna test frames in the stream. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frame 6 is detected immediately following frame 3), the out of sequence count is incremented by one, resulting in a count of one instance of out of sequence frames. If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frame 14 is detected immediately following frame 10), the out of sequence number is incremented again by one, resulting in a total count of two instances of out of sequence frames.
Packet Jitter, Avg (us)	The smoothed average value of the packet delay variation for the stream since the last test restart (per RFC 1889), calculated in microseconds.
Packet Jitter, Max Avg (us)	The maximum Packet Jitter, Avg (us) measured for the stream since the last test restart, calculated in microseconds.

Table 33 Streams test results (Continued)

Result	Description
Packet Jitter, Peak (us)	The highest packet delay variation measured for the stream since the last test restart, calculated in microseconds.
Received Frames	A count of all frames received for the stream since starting the test, including errored frames.
Rx Acterna Frames	A count of all received frames for the stream with an Acterna payload meeting filter criteria since starting the test.
Rx L4 Destination Port	Displays the Destination Port number for the last layer 4 frame received in the stream.
Rx L4 Source Port	Displays the Source Port number for the last layer 4 frame received in the stream.
Rx Mbps, Cur L1	The current bandwidth utilized by the received layer 1 traffic in the stream expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur L2	The current bandwidth utilized by the received layer 2 traffic in the stream traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Q-in-Q Frames	A count of Q-in-Q encapsulated frames received for the stream meeting filter criteria since starting the test.
Rx VLAN Frames	A count of VLAN tagged frames received for the stream meeting filter criteria since starting the test.
SVLAN Frame DEI	Displays the DEI of the last received tagged frame in the stream.

Table 33 Streams test results (Continued)

Result	Description
SVLAN ID	Displays the SVLAN ID for the last received tagged frame in the stream.
SVLAN Priority	Displays the SVLAN Priority for the last received tagged frame in the stream.
Total Util%, Avg	The average bandwidth utilized by the received traffic in the stream, expressed as a percentage of the line rate of available bandwidth since the test started. The average is calculated over the time period elapsed since the test started.
Total Util%, Cur	The current bandwidth utilized by the received traffic in the stream expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time.
Total Util%, Min	The minimum bandwidth utilized by the received traffic in the stream since the test started expressed as a percentage of the line rate of available bandwidth.
Total Util %, Peak	The highest (peak) bandwidth utilized by the received traffic since the test started expressed as a percentage of the line rate of available bandwidth.
Tx Acterna Frames	A count of all transmitted frames for the stream carrying an Acterna payload since starting the test.
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.

Table 33 Streams test results (Continued)

Result	Description
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 and minimum inter-frame gap.
VLAN ID	Displays the VLAN ID of the last received tagged frame in the stream.
VLAN Priority	Displays the VLAN priority of the tagged frames in the stream.

IP Config results

The IP Config category lists results associated with the assignment of static IP addresses, the assignment of IP addresses by a DHCP server, or, if you are testing in PPPoE mode, results associated with the PPPoE log-on process. Results in this category accumulate after you transmit traffic over the link. Table 37 describes the results that appear in the IP Config category. When transmitting multiple streams, many results are available for each transmitted stream.

Table 34 IP Config test results

Result	Description
Data Mode	Indicates whether the HST is configured for a PPPoE session or an IPoE connection.
Dest. IP Addr.	Displays the Destination IP address as defined for the currently configured port.
Destination MAC Address	Displays the Destination MAC address obtained using ARP.

Table 34 IP Config test results (Continued)

Result	Description
DHCP Lease Time (s)	Displays the remaining lease time in seconds for the address issued by the DHCP server for IPv6 connections.
DNS Alternate Server	Displays the alternate server address assigned by the DHCP server or by static assignment for the currently configured port.
DNS Preferred Server	Displays the server address assigned by the DHCP server or by static assignment for the currently configured port.
Global Address	Displays the global address assigned to the HST manually, or during the auto-configuration process for IPv6 connections.
IP Gateway	Displays the Gateway address for the currently configured port.
IP Subnet Mask	Displays the Subnet mask.
Link Local Address	Displays the link local address of the HST if you are running an IPv6 application. DAD (duplicate address detection) must determine that there are no other devices with the link local address before the address appears.
Local IP Addr.	In PPPoE mode, displays the IP address for the currently configured port.
MAC Dest. Address	Displays the hardware (MAC) address of either the gateway or the destination host as resolved by ARP.

Table 34 IP Config test results (Continued)

Result	Description
PPPoE Status	Displays one of the following messages that indicate the current status of the PPPoE session: – INACTIVE – PPPOE ACTIVE – PPP ACTIVE – PPPOE UP – USER REQUESTED INACTIVE – PPPOE TIMEOUT – PPPOE FAILED – PPP LCP FAILED – PPP AUTHENTICATION FAILED – PPP IPCP FAILED – PPP UP FAILED – INVALID CONFIG
Preferred Life Time(s)	Displays the duration (in seconds) that addresses assigned via stateless auto-configuration using the prefix remain preferred.
Remote IP Addr.	Displays the IP address of the PPPoE partner. If your HST is operating as a server, the IP address of the client appears. If your HST is operating as the client, the IP address of the server appears.
Source IP Addr.	In IPoE mode, displays the IP address for the currently configured port.
Subnet Prefix Length	Displays the subnet prefix length used to generate the required IPv6 global address for the HST.
Valid Life Time(s)	Displays the duration (in seconds) that addresses generated from the prefix are considered valid when establishing a link.

Auto-Neg Stats results

The Auto-Neg Status category displays results associated with the auto-negotiation of capabilities between the HST and an Ethernet devices or two HSTs. Results in this category appear after you turn auto-negotiation ON on your HST(s), connect the HST(s) to the circuit, and then initialize the link.

Table 35 describes the results that appear in the Auto-Neg Status category when testing 10/100/1G electrical Ethernet service.

Table 35 Electrical Auto-Neg Stats test results

Result	Description
1000Base-T FDX	Indicates whether the Ethernet link partner is full duplex capable at 1000Base-TX (YES or NO).
1000Base-T HDX	Indicates whether the Ethernet link partner is half duplex capable at 1000Base-TX (YES or NO).
100Base-TX FDX	Indicates whether the Ethernet link partner is full duplex capable at 100Base-TX (YES or NO).
100Base-TX HDX	Indicates whether the Ethernet link partner is half duplex capable at 100Base-TX (YES or NO).
10Base-T FDX	Indicates whether the Ethernet link partner is full duplex capable at 10Base-TX (YES or NO).
10Base-T HDX	Indicates whether the Ethernet link partner is half duplex capable at 10Base-TX (YES or NO).
Duplex	Indicates the negotiated duplex setting for the link (half or full).
Flow Control	Indicates the negotiated flow control capabilities.

Table 35 Electrical Auto-Neg Stats test results

Result	Description
Link Advt. Status	Indicates that the HST has received a valid auto-negotiation capability advertisement from the Ethernet link partner and sent an acknowledgement.
Link Config ACK	Indicates that the Ethernet link partner has acknowledged the receipt of a valid auto-negotiation capability advertisement from the HST.
Remote Fault	If supported by the Ethernet link partner, indicates a reason for auto-negotiation failure. If auto-negotiation succeeded, the result will read “NO”.
Speed (Mbps)	Indicates the negotiated speed setting for the link (10, 100, or 1000 Mbps).

Table 36 describes the results that appear in the Auto-Neg Status category when testing 1G or 100M optical Ethernet service.

Table 36 Optical Auto-Neg Stats test results

Result	Description
Flow Control	Indicates the negotiated flow control capabilities.
Full-duplex	Indicates that the Ethernet link partner is full duplex capable.
Half-duplex	Indicates that the Ethernet link partner if half duplex capable.
Link Advt. Status	Indicates that the HST has received a valid auto-negotiation capability advertisement from the Ethernet link partner and sent an acknowledgement.

Table 36 Optical Auto-Neg Stats test results (Continued)

Result	Description
Link Config ACK	Indicates that the Ethernet link partner has acknowledged the receipt of a valid auto-negotiation capability advertisement from the HST. Applicable only when testing 1G optical Ethernet.
Pause Capable	Indicates the flow control capabilities of the Ethernet link partner. Those capabilities are: – TX Only: The Ethernet link partner will transmit PAUSE frames to alert the HST to reduce the transmitted bandwidth momentarily, however it will not reduce its transmitted bandwidth if it receives PAUSE frames. – RX Only: The Ethernet link partner will reduce its transmitted bandwidth momentarily if it receives PAUSE frames but it will not transmit PAUSE frames to alert the HST to reduce the transmitted bandwidth. – TX and RX: The Ethernet link partner will transmit PAUSE frames to alert the HST to reduce the transmitted bandwidth momentarily and it will reduce its transmitted bandwidth momentarily if it receives PAUSE frames – Neither TX and RX: The Ethernet link partner will not transmit PAUSE frames to alert the HST to reduce the transmitted bandwidth and it will not reduce its transmitted bandwidth if it receives PAUSE frames.

Table 36 Optical Auto-Neg Stats test results (Continued)

Result	Description
Remote Fault	If supported by the Ethernet link partner, indicates a reason for auto-negotiation failure. If auto-negotiation succeeded, the result will read “NO”.

Error Stats results

The Error Stats category lists error statistics such as the number of FCS errored frames, runts, and out of sequence (Oos) frames. Results in this category accumulate after you transmit traffic over the link. Table 37 describes the results that appear in the Error Stats category.

Table 37 Error Stats test results

Result	Description
Acterna Payload Errors	A count of received IP packets containing Acterna Payload checksum errors. **NOTE:** This result only appears if you receive an Acterna payload, and there are payload errors in the received data stream.
Code Violation Rate	The ratio of code violations to bits received since the last test restart.
Code Violation Seconds	A count of the number of seconds during which code violations occurred.
Code Violations	A count of invalid 10-bit code words in the bit stream.
Errored Frames	A count of FCS errored frames, runts, and jabbers.

Table 37 Error Stats test results (Continued)

Result	Description
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.
IP Checksum Errors	A count of received IP packets with a checksum error in the header.
IP Packet Length Errors	A count of received IP packets that exceed the available Ethernet payload.
Jabbers	A count of received frames that have a byte value greater than the maximum 1518 frame length (or 1522 bytes for VLAN tagged frames) and an errored FCS.
L4 Checksum Errors	A count of received layer 4 frames with a checksum error in the TCP/UDP header.
Lost Frames	A count of lost Acterna test frames. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frames 4 and 5 were not detected), the lost frame count is incremented by two (frames 4 and 5 are lost). If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frames 11, 12, and 13 are missing), the lost frame count is incremented by three, resulting in a total count of five lost frames. **NOTE:** If the HST receives errored frames containing errors in the sequence number field, the Lost Frames count will be incorrect.

Table 37 Error Stats test results (Continued)

Result	Description
OoS Frames	A count of each instance where the HST detects out of sequence Acterna test frames. For example, if the HST detects sequence numbers: 1, 2, 3, 6, 7, 8, (frame 6 is detected immediately following frame 3), the out of sequence count is incremented by one, resulting in a count of one instance of out of sequence frames. If the HST then detects sequence numbers 9, 10, 14, 15, 16 (frame 14 is detected immediately following frame 10), the out of sequence number is incremented again by one, resulting in a total count of two instances of out of sequence frames.
Runts	A count of frames under the minimum 64 byte frame length containing Frame Check Sequence (FCS) errors.
Rx Collisions	A count of the number of times the HST has received a jam signal while it was not transmitting frames. This result only appears for half-duplex 10/100 Ethernet tests.
Tx Collisions	A count of the number of times the HST has transmitted a frame, and then received a jam signal in the time slot for the frame. This result only appears for half-duplex 10/100/1G electrical Ethernet tests.
Tx Defers	A count of the number of times the transmitter prepared to send traffic, and then was forced to defer based on link activity. This result only appears for half-duplex 10/100/1G electrical Ethernet tests.
Undersized	A count of frames under the minimum 64 byte frame length.

Table 37 Error Stats test results (Continued)

Result	Description
IPv4/IPv6 Packet Length Errors	Count of IPv4 or IPv6 packets received with a value in the length field that exceeds the actual packet length.
ES	The number of available seconds during which one or more relevant errors were present.
SES	Seconds during which 30% or more of the frames were lost, contained FCS errors, or Loss of Link was detected. The following calculation is used to declare an SES: (FCS Error count + Lost Frame count) / (Frames Received count + Lost Frames) $\geq$ 0.3.
UAS	Unavailable time is defined as ten (10) consecutive severely errored seconds. These ten seconds are included in the UAS count. For example, if 12 consecutive SES occur, the UAS count will be 12. If only 3 consecutive SES occur, the UAS count will be zero.
ESR	The ratio of errored seconds to the number of available seconds.
SESR	The ratio of severely errored seconds to the number of available seconds.

LED results

The LED category shows the current and historical status for key events required when establishing a link (detecting a signal, establishing the link) and then detecting frames. Table 38 describes the results that appear in the LED cate-

gory.

Table 38 LED results

Result	Description
Acterna Detect	The HST has detected an Acterna Test Frame or Packet.
Frame Detect	The HST has detected frames.
L2 Patt Sync	The data contained inside the frame payload is synchronized with a BERT pattern. This result is only applicable when the HST is configured for layer 2 testing.
Link Active	The link is active.
Packet Detect	The HST has detected an IP packet. This result is only applicable when the HST is configured for layer 3 IP testing.
Pause Frame Detect	The HST has detected a pause frame.
Signal Present	A signal is present (optical tests only).
Sync Acquired	Synchronization has been acquired.
VLAN Frame Detect	The HST has detected VLAN Ethernet frames as defined in IEEE 802.p/q.
Q-in-Q Frame Detect	The HST has detected Q-in-Q encapsulated frames as defined in IEEE 802.p/q.

Stream LED results

If you are running a multiple streams test, the Stream LED category shows the current and historical status for key events required when establishing a link (detecting a signal, establishing the link) and then frame detection for each enabled stream. Table 39 describes the results that appear in

the Stream LED category.

Table 39 Stream LED results

Result	Description
Frame Detect	The HST has detected frames.
Packet Detect	The HST has detected an IP packet. This LED is only applicable when the HST is configured for layer 3 IP testing.
Pause Frame Detect	The HST has detected a pause frame.
Signal Present	A signal is present (optical tests only).
VLAN Frame Detect	The HST has detected VLAN Ethernet frames as defined in IEEE 802.1 p/q.
Q-in-Q Frame Detect	The HST has detected Q-in-Q encapsulated frames as defined in IEEE 802.1 p/q.
TCP Packet Detect	The HST has detected layer 4 packets with TCP headers.
UDP Packet Detect	The HST has detected layer 4 packets with UDP headers.

L2 BERT Stats results

The L2 BERT Stats category lists results associated with BER testing. Results in this category accumulate after you transmit traffic with a BERT pattern in the payload over the link.

Table 37 describes the results that appear in this category.

Table 40 L2 BERT Stats test results

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.
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.
Error-Free Seconds	A count of the number of error-free seconds during which error analysis has been performed since initial pattern synchronization.
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.
Total Bits	The total number of bits received since initial frame synchronization.

Pattern Stats results

The Pattern Stats category displays results associated with the transmission of layer 2 patterns over a circuit when testing optical Ethernet. Table 41 describes the results that appear in the Pattern Stats category.

Table 41 Pattern Stats test results

Result	Description
Rx Frames ALL	The number of valid and errored frames received since the link was established.
Tx Frames ALL	The number of frames transmitted since the link was established.

Ping results

The Ping category lists results associated with Ping testing. Results in this category accumulate after you transmit a ping packet over the link to verify connectivity. Table 42 describes the results that appear in the Ping category.

Table 42 Ping test results

Result	Description
Delay (ms)	The current round trip delay for all pings sent and successfully received by the HST since the last test restart. Calculated in milliseconds.
Delay, Avg (ms)	The round trip delay for all pings sent and successfully received by the HST since the last test restart. Calculated in milliseconds.
Delay, Max (ms)	The maximum round trip delay for the pings sent and successfully received by the HST. Calculated in milliseconds.

Table 42 Ping test results (Continued)

Result	Description
Delay, Min (ms)	The minimum round trip delay for the pings sent and successfully received by the HST. Calculated in milliseconds.
Lost Pings	Count of Ping requests sent by the HST for which replies were not received within 4 seconds.
Lost Pings %	Percent of the total transmitted Ping requests sent by the HST for which replies were not received within 4 seconds.
Ping Replies Rx	Count of the replies received in response to the ping requests sent by the HST.
Ping Replies Tx	Count of the replies sent in response to the ping requests received by the HST.
Ping Requests Rx	Count of the Ping requests received by the HST (in other words, requests sent to the HST's IP address) from another Layer 3 device on the network.
Ping Requests Tx	Count of the ping requests sent from the HST.

Traceroute results

The Traceroute category displays the hop number, average delay, and IP address to trace for each hop. After the trace is complete, the results display indicates that it is complete. For details on running the traceroute application, see "Running Traceroute" on page 158.

Message results

The Messages category displays messages associated with your tests. For example, during loopback testing, messages appear indicating that loop up or loop down of a unit on the far end was successful.

Event Table results

The Event Table category displays the date and time that significant events, errors, or alarms occurred during the course of your test. Events, errors and alarms listed in the log include but are not limited to:

- Signal Present
- Sync Acquired/Sync Lost
- Link Active
- PPPoE Login Status Messages
- FCS Errored Frames
- Runts
- Jabbers
- Undersized Frames
- Errored Frames
- Out of Sequence Frames
- Lost Frames (and Frame Loss Ratio)
- IP Checksum Errors
- L4 Checksum Errors
- Acterna Payload Errors
- IP Packet Length Errors
- IP Packet Errors
- Code Violations

A sample event table is provided in Figure 54.

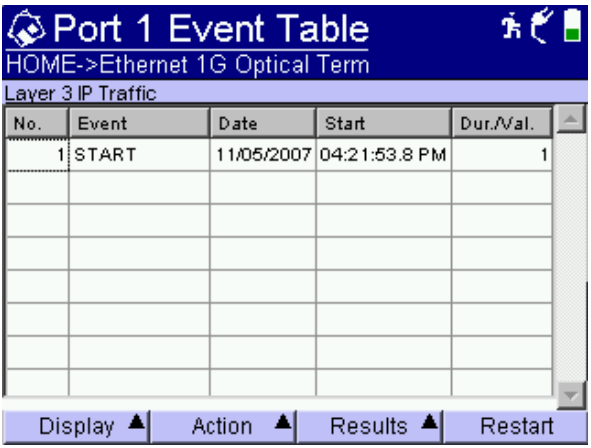


Figure 54 Sample Event Table

Event Histogram results

A histogram is a display or print output 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). For example, if you are running a Terminate application for layer 4 IPv6 traffic, you can observe patterns of layer 4 checksum errors and IPv6 packet length errors over a period of time. A sample histogram is provided

in Figure 55.

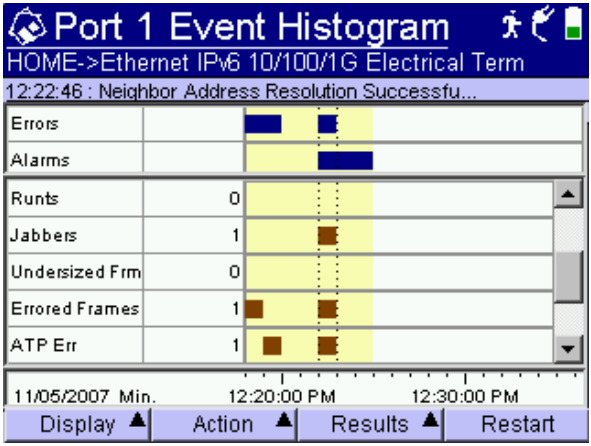


Figure 55 Sample Histogram (IPv6 application)

Use the up and down arrow keys to scroll through each of the events reported in the histogram.

NOTE:

When viewing a histogram, the left and right arrow keys can not be used to navigate through the other result categories. Use the Display softkey to select and then view another category.

Time results

The Time category provides the current date, time, and the time elapsed since the last test start or restart. Table 43 describes each of the Time results.

Table 43 Time results

Result	Description
Date	Current day and month.

Table 43 Time results (Continued)

Result	Description
Elapsed Time	Amount of time in hours, minutes, and seconds (hh:mm:ss) since the last test restart.
Time	Current time of day in hours, minutes, and seconds (hh:mm:ss).

Saving and printing results

For information about saving and printing test results, see the *HST-3000 Base Unit User's Guide*.

Specifications

B

This appendix contains specifications for the HST-3000 Ethernet SIM. Topics discussed in this appendix include the following:

Electrical specifications

The Ethernet SIMs 10/100/1000 Base-TX interface conforms to IEEE 802.3 electrical requirements. The electrical specifications for the 10 Mb/s interface are described in Table 44.

Table 44 10 Mb/s interface electrical specifications

Parameter	Specification
Cable	Cat-5 (or better) 100 Ohm STP cable, ≤100 meters.
Twisted pair differential	Output voltage 2.2 MIN Vpk, 2.5 TYP Vpk, 2.8 MAX Vpk
	Input voltage range 3.3V MAX
Output jitter	Per IEEE std 802.3 2005
Input jitter	Per IEEE std 802.3 2005

The electrical specifications for the 100 Mb/s interfaces are described in Table 45.

Table 45 100 Mb/s interface electrical specifications

Parameter	Specification
Cable	Cat-5 (or better) 100 Ohm STP cable, ≤100 meters.
Twisted pair differential	Output voltage 0.950 MIN Vpk, 1.000 TYP Vpk, 1.050 MAX Vpk
	Input voltage range 3.3V MAX
Output jitter	Per IEEE std 802.3 2005
Input jitter	Per IEEE std 802.3 2005

The electrical specifications for the 1G electrical interface are described in Table 46.

Table 46 1G electrical interface specifications

Parameter	Specification
Cable	Cat-5 (or better) 100 Ohm STP cable, £100 meters.
Twisted pair differential	Output voltage 0.67 MIN Vpk, 0.82 MAX Vpk
	Input voltage range 3.3V MAX
Output jitter	Per IEEE std 802.3 2005
Input jitter	Per IEEE std 802.3 2005

The electrical specifications for Power over Ethernet (PoE) testing appear in Table 47.

Table 47 Power over Ethernet specifications

Parameter	Specification
Interface	Complies with IEEE 802.3af
Class	Class 1 nominal load = 10.5 mA

SFP specifications

Each of the JDSU-recommended SFPs complies with the Small Form-factor (SFP) Transceiver MultiSource Agreement (MSA). Please see your SFP manufacturer's site for detailed specifications.

For a list of currently supported SFPs, contact your JDSU TAC representative or your local JDSU sales office. You can also contact JDSU through the company web site, www.jdsu.com.

Environmental specifications

The unit's operating temperature is 32° to 113° F (0° to 45° C).

Glossary

Numerics

100M — Used on HST user interface to represent 100 Mbps Ethernet.

1G — Used on HST user interface to represent both electrical and optical 1 Gigabit Ethernet rate.

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

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. To transmit Acterna test packets from an HST, you select an Acterna payload when you configure a test.

ARP — Address Resolution Protocol. Method for determining a host's hardware address if only the IP address is known. You can configure the HST to automatically send 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

Base Unit — The HST-3000 base unit houses the keypad, display screen, battery, and some connectors. Service interface modules (SIMs) connect to the base unit to provide testing functionality.

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

CJPAT — Continuous jitter test pattern.

CRC — Cyclic redundancy check. *See also* FCS.

CRPAT — Continuous random test pattern.

CSPAT — Compliant supply noise test pattern.

CVLAN — Customer VLAN. Used in Q-in-Q traffic to partition traffic for a particular customer (as opposed to the traffic for the service provider).

D

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.

E

EDD — Ethernet demarcation device.

EFM — Ethernet first mile.

Ethernet link partner — The nearest Ethernet device on a link. The HST 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.

FDX — Full duplex.

G

GigE — Used throughout this manual 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.

H

HDX — Half duplex.

I

Internet Protocol —

Commonly referred to as "IP". Protocol specifying the format and address scheme of packets transmitted over the Internet. Typically used with TCP.

IP — See Internet Protocol.

IPoE — Internet Protocol over Ethernet. Used on the HST GUI and through this guide to see the applications used to establish a standard layer 3 (IP) connection.

IPv4 — Internet Protocol Version 4.

IPv6 — Internet Protocol Version 6.

ITU — International Telecommunications Union based in Geneva, Switzerland.

J

Jabber — An Ethernet frame that exceeds the IEEE 802.3 maximum length of 1518 bytes (or 1522 bytes with a VLAN tag) and contains an errored FCS, or a Fibre Channel frame that exceeds the maximum length of 2140 bytes with an errored CRC.

J-Connect — Utility that allows you to detect other JDSU test instruments on a particular subnet, and use a detected instrument's addresses to automatically populate key traffic settings. Also known as JDSU Discovery.

JDSU Discovery — See J-Connect.

J-Proof — Application used to verify Layer 2 Transparency.

Jumbo frame — An Ethernet frame that exceeds the IEEE 802.3 maximum length of 1518 bytes (or 1522 bytes with a VLAN tag), or a Fibre Channel frame that exceeds 2140 bytes. You can transmit jumbo frames using the HST.

L

LED — Light emitting diode.

Link-Local Address — IPv6 address assigned to a device locally in an IP network when there is no other assignment method available, such as a DHCP server. These addresses must always go through duplicate address detection (DAD), even if you manually specify the address. *See also* DAD and Global Addresses.

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.

M

MAC Address — Media Access Control Address. Address assigned to every layer 2 (Ethernet) device to uniquely identify the device on a LAN. Also referred to as the "hardware" address or physical address.

MDI port — Medium Dependent Interface port. RJ-45 interface used by Ethernet NICs and routers that does not require use of a crossover cable (MDI ports do not cross the transmit and receive lines). An MDI port on one device connects to an MDI-X port on another device. MDI interfaces transmit using pins 1 and 2, and receive using pins 3 and 6. The HST-3000 supports cable diagnostics of MDI interfaces. *See also* MDI-X port.

MDI-X port — Medium Dependent Interface Crossover port. RJ-45 interface used by Ethernet NICs and routers that requires use of a cross-over cable (MDI-X ports cross transmit and receive lines. An MDI-X port on one device connects to an MDI port on another device. MDI-X interfaces transmit using pins 3 and 6, and receive using pins 1 and 2. The HST-3000 supports cable diagnostics of MDI-X interfaces.

MiM — MAC-in-MAC. MiM applications allow you to transmit and analyze unicast layer 2 Ethernet traffic carried on a PBB (Provider Backbone Bridged) trunk.

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.

O

OAM — Operations, Administration, and Maintenance. The HST allows you to run link and service layer OAM applications.

Overload rate — The maximum rate of transmitted traffic at which no frames are dropped (determined using the RFC 2544 Throughput test). The overload rate is used to force a receiving network element to drop frames when running the System Recovery test.

P

Packet — Bundle of data, configured for transmission. Consists of data to be transmitted and control information.

Passing rate — The maximum rate of transmitted traffic at which no frames are dropped (determined using the RFC 2544 Throughput test).

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.

Ping — Program which sends an ICMP echo request packet to an IP address and awaits a reply. Ping requests are typically used to test connectivity. You can transmit and respond to ping packets using the HST.

PoE — Power Over Ethernet.

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.

Q

Q-in-Q — Also referred to as VLAN stacking, a form of encapsulation that 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.

R

Recovery Rate — 50 percent of the overload rate used to force a network element to drop frames.

RFC 2544 — Document titled *Benchmarking Methodology for Network Interconnect Devices*, published by the Internet Engineering Task Force. RFC 2544 defines a series of tests that can be used to measure the performance characteristics of data networking devices. Using the HST, you can run automated tests configured using the key parameters required for each of the pre-defined tests.

RJ-45 — Jacks on the left side of the Ethernet SIM used for 10/100/1G electrical Ethernet testing. The RJ-45 jack on the top of the base unit is used for Ethernet TE, VoIP, and IP Video testing.

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.

S

Service disruption time — The time between Ethernet or Fibre Channel frames (maximum inter-frame gap) when service switches to a protect line. The Svc Disruption (ms) result in the L2 Link Stats category displays the service disruption time.

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 guide to represent pluggable optical transceivers (modules).**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).

T

TCP — Transmission Control Protocol. Layer 4 protocol that allows two devices to establish a connection and exchange streams of data. The HST can be configured to transmit and analyze layer 4 traffic carrying a TCP header.

TCP window size — The maximum number of bytes that a port can transmit over a TCP connection before being acknowledged by the receiving port.

Terminate — An application where the test set is terminating the circuit. In these applications, the test set sends and receives traffic.

Thru — An application where the test set is used in series with a network circuit to monitor the traffic on that circuit.

ToS — Type of service. When you configure the HST to transmit pings, you can optionally specify the type of service using the Advanced button on the PING tab.

TTL — Time to live. Time after which a fragmented ping request or response can be deleted by any device on a circuit. When you configure the HST to transmit pings, you can optionally specify the TTL value in seconds using the Advanced button on the PING tab.

Tx — Transmit.

U

UDP — User Datagram Protocol. Layer 4 protocol that offers a limited amount of service when messages are exchanged between devices in 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.

V

VLAN — Virtual LAN.

Index

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Communications Test and Measurement Regional Sales

North America
Toll Free: 1 855 ASK JDSU
Tel: +1 240 404 2999
Fax:+1 240 404 2195

Latin America
Tel: +55 11 5503 3800
Fax:+55 11 5505 1598

Asia Pacific
Tel: +852 2892 0990
Fax:+852 2892 0770

EMEA
Tel: +49 7121 86 2222
Fax:+49 7121 86 1222

www.jdsu.com

21109872-005
Revision 000, 06/2014
English

JDSU